UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

NETWORK-1 TECHNOLOGIES, INC., *Plaintiff*, v. SAMSUNG ELECTRONICS CO., LTD. and SAMSUNG ELECTRONICS AMERICA, INC., *Defendants*.	Civil Action No. 2:25-cv-00667-JRG-RSP JURY TRIAL DEMANDED

DEFENDANTS' PATENT LOCAL RULE 3-3
DISCLOSURE OF INVALIDITY CONTENTIONS

I. Introduction 1

II. Reservations 2

III. U.S. Patent No. 11,233,780 ("the '780 Patent") 6

A. Identification of Prior Art 6

1. Prior Art Patents 7

2. Prior Art Non-Patent Publications 8

3. Prior Art Systems 8

B. Primary References 9

C. Secondary References 10

D. Obvious Combinations 10

1. Exemplary Combinations 11

2. Motivations to Combine 13

IV. U.S. Patent No. 11,606,204 ("the '204 Patent") 43

A. Identification of Prior Art 43

1. Prior Art Patents 43

2. Prior Art Non-Patent Publications 44

3. Prior Art Systems 45

B. Primary References 45

C. Secondary References 46

D. Obvious Combinations 47

1. Exemplary Combinations 48

2. Motivations to Combine 50

V. U.S. Patent No. 11,916,893 ("the '893 Patent") 105

A. Identification of Prior Art 105

1. Prior Art Patents 105

2. Prior Art Non-Patent Publications 106
3. Prior Art Systems 107
B. Primary References 108
C. Secondary References 108
D. Obvious Combinations 109
1. Exemplary Combinations 110
2. Motivations to Combine 111
VI. U.S. Patent No. 11,973,864 ("the '864 Patent") 140
A. Identification of Prior Art 140
1. Prior Art Patents 140
2. Prior Art Non-Patent Publications 141
3. Prior Art Systems 142
B. Primary References 143
C. Secondary References 144
D. Obvious Combinations 144
1. Exemplary Combinations 145
2. Motivations to Combine 147
VII. U.S. Patent No. 12,166,869 ("the '869 Patent") 202
A. Identification of Prior Art 202
1. Prior Art Patents 202
2. Prior Art Non-Patent Publications 203
3. Prior Art Systems 204
B. Primary References 204
C. Secondary References 205
D. Obvious Combinations 206

1. Exemplary Combinations 206

2. Motivations to Combine 209

VIII. U.S. Patent No. 12,207,094 ("the '094 Patent") 248

A. Identification of Prior Art 248

1. Prior Art Patents 249

2. Prior Art Non-Patent Publications 250

3. Prior Art Systems 250

B. Primary References 251

C. Secondary References 252

D. Obvious Combinations 252

1. Exemplary Combinations 253

2. Motivations to Combine 255

IX. Invalidity Contentions Under 35 U.S.C. § 112 283

A. Indefiniteness Under 35 U.S.C. § 112, ¶ 2 284

1. '780 Patent 284

2. '204 Patent 284

3. '893 Patent 285

4. '864 Patent 285

5. '869 Patent 285

6. '094 Patent 285

B. Lack of Enablement/Lack of Written Description Under 35 U.S.C. § 112, ¶ 1 285

1. '780 Patent 287

2. '204 Patent 287

3. '893 Patent 287

4. '864 Patent 288

5. ’869 Patent 288

6. ’094 Patent 288

X. Document Production 289

I. Introduction

Pursuant to Patent Local Rule 3-3 and the Court's September 9 Order Granting Plaintiff's Motion for Extension of Deadlines (Dkt. 20), Defendants Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc., (collectively, "Defendants" or "Samsung") make the following Disclosure of Invalidity Contentions to Plaintiff Network-1 Technologies, Inc. ("Plaintiff" or "Network-1") for Case No. 2:25-cv-00667-JRG-RSP.

Plaintiff has asserted U.S. Patent Nos. 11,233,780 ("the '780 Patent"), 11,606,204 ("the '204 Patent"), 11,916,893 ("the '893 Patent"), 11,973,864 ("the '864 Patent"), 12,166,869 ("the '869 Patent"), and 12,207,094 ("the '094 Patent") (collectively, "the Asserted Patents" or "the Patents-in-Suit") against Defendants. Complaint (E.D. Tex. 2:25-cv-00667, Dkt. 1). In Plaintiff's Patent Local Rule 3-1 and 3-2 Disclosures ("Infringement Contentions"), served on September 30, 2025, Plaintiff has asserted the following claims against Defendants:

- Claims 1, 2, 5-10, 13-14, and 17-19 of the '780 Patent;
- Claims 1, 3-6, 9-11, and 18-20 of the '204 Patent;
- Claims 1, 2, 4-10, and 12-17 of the '893 Patent;
- Claims 1, 3-6, 9-11, 16, and 18-20 of the '864 Patent;
- Claims 1-20 of the '869 Patent; and
- Claims 1, 2, 5-10, 13-15 and 19-21 of the '094 Patent

Defendants' Invalidity Contentions address only those claims asserted in Plaintiff's Infringement Contentions. Defendants submit these Invalidity Contentions without waiving any argument about the sufficiency or substance of Plaintiff's Infringement Contentions.

Based on its investigation to date, Defendants hereby: (a) identify each item of prior art that anticipates each asserted claim or renders it obvious; (b) specify whether each such item of

prior art anticipates each asserted claim and/or renders it obvious and, if a combination of items of prior art makes a claim obvious, identify each such combination and the motivation to combine such items; (c) submit a chart identifying where specifically in each item of prior art each element of each asserted claim is found, including for each element that is governed by 35 U.S.C. § 112 ¶ 6, the identity of the structure(s), act(s), or material(s) in each item of prior art that performs the claimed function; and (d) identify any grounds of invalidity of the asserted claims based on indefiniteness under 35 U.S.C. § 112 ¶ 2 or enablement or written description under 35 U.S.C. § 112 ¶ 1.

In addition, pursuant to Patent Local Rule 3-4, and based on its investigation to date, Defendants have produced or are producing documents concurrently with these Invalidity Contentions.

II. Reservations

Defendants reserve the right to amend these Invalidity Contentions. The information and documents that Defendants produce are based on information available to date and are subject to further revision.

The information and documents that Defendants produce are based on Defendants' present understanding of Plaintiff's infringement theories as advanced by Plaintiff in its Infringement Contentions. Plaintiff's Infringement Contentions are deficient in numerous respects. For example, Plaintiff has failed to identify specifically where each element of each asserted claim is found within each accused instrumentality. Defendants provided notice to Plaintiff of the deficiencies in its Infringement Contentions, including in a letter to Plaintiff sent October 24, 2025. Plaintiff has failed to cure the deficiencies and has not put Defendants on notice of its theories of infringement. If Plaintiff attempts or is permitted to cure such deficiencies, amends its contentions, or provides additional information regarding its

infringement theories, doing so may lead to further grounds for invalidity, and thus Defendants specifically reserve the right to amend or supplement its Invalidity Contentions.

Further, because discovery (including third party discovery) is at an early stage, Defendants reserve the right to amend or supplement these Invalidity Contentions. For example, as explained in the sections below, on information and belief, multiple third parties have knowledge, documentation, and/or corroborating evidence relating to invalidity and/or prior art. It is therefore likely that Defendants will discover additional prior art or additional information relating to known prior art, and Defendants reserve the right to supplement these contentions after becoming aware of additional prior art or information. Defendants further reserve the right to introduce and use such supplemental materials at trial.

Defendants' claim charts in Exhibits A-F cite particular teachings and disclosures of the prior art as applied to limitations of the asserted claims. However, persons having ordinary skill in the art may view an item of prior art generally in the context of other publications, literature, products, and understanding. Accordingly, the cited portions are only exemplary, and Defendants reserve the right to rely on uncited portions of the prior art references and on other publications and expert testimony as aids in understanding and interpreting the cited portions, as providing context thereto, and as additional evidence that a claim limitation is known or disclosed. Defendants reserve the right to establish what was known to a person having ordinary skill in the art through other publications, products, and/or testimony. Defendants also reserve the right to rely on uncited portions of the prior art references, other publications, and testimony to establish that a person of skill in the art would have been motivated to combine certain of the cited references so as to render the claims obvious. Citations to figures are inclusive of all discussion of those figures.

Defendants further reserve the right to argue that the asserted claims are invalid under 35 U.S.C. § 102(a), if discovery reveals that the named inventor of the Asserted Patents did not invent the subject matter recited in the asserted claims. If applicable, Defendants will provide the name of the person(s) from whom, and the circumstances under which, the invention or any part of it was derived. Defendants further reserve the right to argue that the asserted claims are unenforceable due to inequitable conduct if discovery reveals such grounds.

Defendants further intend to rely on inventor admissions concerning the scope of the asserted claims or of the prior art relevant to the asserted claims found in, *inter alia*, the patent prosecution history and/or reexamination history for the Asserted Patents and related patents and/or patent applications; any deposition testimony of a named inventor of the Asserted Patents; and the papers filed and any evidence submitted by Plaintiff in conjunction with this litigation. Defendants reserve the right to contend that the asserted claims are invalid for failure to name the correct inventor(s), and/or to contend that Plaintiff lacks standing to bring this litigation with respect to such patents.

Furthermore, nothing stated herein shall be treated as an admission or suggestion that Defendants agree with Plaintiff regarding the scope of any asserted claim or the claim constructions in its Infringement Contentions. To the extent that Defendants' Invalidity Contentions reflect claim constructions consistent with or suggested by Plaintiff's Infringement Contentions, no inference is intended nor should any be drawn that Defendants agree with Plaintiff's claim constructions. By applying any of Plaintiff's apparent claim constructions and interpretations, Defendants do not concede in any way that those constructions and interpretations are correct, but rather assert the fundamental principle that whatever infringes a

claim if later in time anticipates if earlier in time. Defendants expressly reserve the right to propose alternative constructions to those that have been or may be advocated by Plaintiff.

Nor shall anything in these Invalidity Contentions be treated as an admission that Defendants' accused products meet any limitation of any asserted claim. Defendants deny that it infringes any claim of the Asserted Patents. To the extent that any prior art contains a claim element that is the same as or similar to an accused product, inclusion of that prior art in Defendants' Invalidity Contentions shall not be deemed a waiver by Defendants of any claim construction or non-infringement position. Defendants expressly reserve the right to contest any claim construction asserted by Plaintiff and expressly reserve all non-infringement arguments.

In its Infringement Contentions, Plaintiff contends that the Asserted Patents are entitled to the following priority dates:[1]

- The '780, '893, and '094 Patents claim priority to U.S. App. No. 14/099,329, and Plaintiff contends that each is therefore entitled to a priority date of at least December 6, 2013
- The '869 Patent claims priority to U.S. App. No. 14/084,141, and Plaintiff contends that it is entitled to a priority date of at least November 19, 2013.
- The '204 and '864 Patents claim priority to U.S. App. No. 14/055,606, and Plaintiff contends that each is therefore entitled to a priority date of at least October 16, 2013.

[1] Plaintiff hinges its P.R. 3-1(e) disclosure "on the present state of ***Atlas's*** knowledge" and "***Atlas's*** investigation." *See* September 20 Infringement Contentions at 8. Defendants assume that this is an inadvertent error, and considers such references to "Atlas" as intending to refer to "Network-1" or "Network-1 Technologies, Inc."

Defendants dispute that the ’780, ’893, and ’094 Patents are entitled to a priority date of December 6, 2013, at least because U.S. App. No. 14/099,329 fails to provide written description support for the claims of those patents.[2] Accordingly, the ’780 Patent is entitled to a priority date no earlier than its filing date, and the ’893 and ’094 Patents are entitled to filing dates no earlier than the filing date of ’893 Patent. Certain prior art references Defendants rely upon, namely, SGP.22, SCP11, and Nix ’175, are prior art to the extent the ’780, ’893, and ’094 Patents are not entitled to their earliest priority claim

Regarding all Asserted Patents, to the extent Plaintiff later argues, or it is determined that, any different priority date applies, Defendants reserve the right to amend these contentions accordingly. Defendants further reserve the right to seek discovery regarding conception and reduction to practice, as appropriate, and to demonstrate earlier invention by other parties, public use and/or the on-sale bar under 35 U.S.C. § 102(a)(1), and/or applicants’ failure to comply with 35 U.S.C. § 112.

III. U.S. Patent No. 11,233,780 (“the ’780 Patent”)

A. Identification of Prior Art

Defendants incorporate by reference, as if set forth fully herein, all filings and exhibits from *Inter Partes* Review IPR2026-00114, filed November 26, 2025 with the U.S. Patent Trial and Appeal Board (“PTAB”), including any subsequent and future filings in that case.

In addition to the prior art cited on the face of the ’780 Patent and related patents, the admitted prior art in the specifications of the ’780 Patent and related patents, the prior art cited in any file histories, reexaminations, *inter partes* review proceedings, reissue proceedings, or

[2] For example, U.S. App. No. 14/099,329, to which the ’780, ’893, and ’094 Patents claim priority, fails to disclose (1) receiving the symmetric key from the subscription manager (claim 1 of ’780, ’094, and ’083 Patents); and (2) both a first and a second private / public UICC key pair (claim 1 of ’780 and ’094 Patents).

other examination or post-grant proceedings of the ’780 Patent and related patents, and the prior art cited in any invalidity contentions or expert reports submitted in any action or proceedings involving the ’780 Patent or related patents, Defendants identify the following prior art that anticipates each asserted claim or renders it obvious.

1. Prior Art Patents

The following patents and patent publications are prior art to the asserted claims under at least 35 U.S.C. §§ 102(a)(1) and/or (a)(2), and/or 35 U.S.C. § 103. The identification of any patent or patent publication shall be deemed to include any counterpart patent or application filed, published, or issued anywhere in the world.

Patent or Publication Number	Country of Origin	Filing Date	Date of Issue or Publication
U.S. Pat. App. Pub. No. 2013/0301828 (“Gouget”)	United States	September 24, 2010 (EP) March 23, 2013 (PCT)	November 14, 2013
U.S. Pat. App. Pub. No. 2013/0227646 (“Haggerty”)	United States	February 14, 2013	August 29, 2013
U.S. Pat. App. Pub. No. 2010/0267383 (“Konstantinou”)	United States	April 15, 2009	October 21, 2010
U.S. Pat. App. Pub. No. 2016/0127132 (“Lee”)	United States	May 30, 2013 (KR) November 30, 2015 (PCT)	May 5, 2016
U.S. Patent No. 9,100,175 (“Nix”)	United States	December 6, 2013	August 4, 2015
U.S. Patent No. 8,761,390 (“Peirce”)	United States	June 30, 2008	June 24, 2014
U.S. Pat. App. Pub. No. 2015/0350881 (“Weiss”)	United States	December 21, 2012 (EP) June 19, 2015 (PCT)	December 3, 2015

2. Prior Art Non-Patent Publications

The following non-patent publications are prior art to the asserted claims under at least 35 U.S.C. §§ 102(a)(1) and/or (a)(2), and/or 35 U.S.C. § 103.

Title	Author/Publisher	Date of Publication
A Fast and Secure Elliptic Curve Based Authenticated Key Agreement Protocol For Low Power Mobile Communications ("Abi-Char")	Pierre E. Abi-Char, et al., IEEE	2007
Ansi X9.63 Overview Key Agreement and Key Transport Using Elliptic Curve Cryptography ("ANSI X9.63 Overview")	Simon Blake-Wilson, Certicom	2000
Protocols for Authentication and Key Establishment ("Boyd-Mathuria")	Colin Boyd & Anish Mathuria, Springer	2003
GlobalPlatform Card Specification Version 2.2.1 Public Release ("GlobalPlatform")	GlobalPlatform, Inc.	January 2011
SGP.22 - RSP Technical Specification Version 2.0 ("SGP.22")	GSM Association	October 14, 2016
Secure Profile Provisioning Architecture for Embedded UICC ("Park (IEEE)")	Jaemin Park, et al., IEEE	November 7, 2013
GlobalPlatform Card Secure Channel Protocol '11' Card Specification v.2.2 – Amendment F Version 1.0 Public Release ("SCP11")	GlobalPlatform, Inc.	May 2015

3. Prior Art Systems

Defendants' investigation into publicly available prior art systems that teach and/or render obvious each element of any asserted claims is ongoing. Fact discovery is at an early

stage, and Defendants may require discovery from third parties regarding publicly available prior art systems. On information and belief, prior art systems from the following companies teach and/or render obvious each element of the asserted claims of the ’780 Patent: Cinterion (now Telit); Gemalto (now Thales); Giesecke+Devrient; GlobalPlatform; NXP Semiconductors N.V.; Oberthur Technologies (now IDEMIA); and Sierra Wireless. Defendants reserve the right to amend its identification of prior art systems as Defendants become aware of the existence, functionality, and/or characteristics of prior art systems as a result of its investigation and forthcoming discovery. In addition to the prior art products, components, systems, and methods that may be identified as a result of discovery, Defendants also reserve the right to rely on the documents and publications identified in the corresponding claim charts as prior art publications.

B. Primary References

Defendants contend that the primary prior art references identified below and described in the charts attached as Exhibits A-01 to A-08, by themselves, anticipate the asserted claims of the ’780 Patent. To the extent that a primary reference is deemed not to anticipate a claim for failing to teach one or more limitations of that claim, Defendants contend that the claim would nonetheless have been obvious to a person of ordinary skill in the art at the time of the invention in view of the prior art reference itself, as described in the attached charts. Defendants’ prior art charts (attached as Exhibits A-01 thru A-08) set forth the particular claims that are anticipated under 35 U.S.C. § 102 and/or rendered obvious under 35 U.S.C. § 103 by each item of prior art and identify where specifically in each item of prior art, each element of each asserted claim is found.

Exhibit	Primary References
A-01	*Protocols for Authentication and Key Establishment* (“Boyd-Mathuria”)

A-02	*GlobalPlatform Card Specification Version 2.2.1 Public Release* ("GlobalPlatform")
A-03	U.S. Pat. App. Pub. No. 2013/0301828 ("Gouget")
A-04	U.S. Pat. App. Pub. No. 2013/0227646 ("Haggerty")
A-05	U.S. Patent No. 9,100,175 ("Nix")
A-06	*Secure Profile Provisioning Architecture for Embedded UICC* ("Park (IEEE)")
A-07	*SGP.22 - RSP Technical Specification Version 2.0* ("SGP.22")
A-08	U.S. Pat. App. Pub. No. 2015/0350881 ("Weiss")

C. Secondary References

Exhibit A-A lists secondary prior art references and identifies, on a limitation-by-limitation basis, where specifically each secondary reference teaches the limitations of the asserted claims. To the extent that a primary reference is deemed, by itself, not to anticipate or render obvious a claim for failing to teach one or more limitations, the claim would nonetheless have been obvious to a person of ordinary skill in the art at the time of the invention by the combination of the primary reference with one or more of the other primary references listed above and/or the references listed as disclosing those alleged missing limitations in Exhibit A-A.

D. Obvious Combinations

To the extent that a primary reference is deemed, by itself, not to anticipate or render obvious a claim for failing to teach one or more limitations, the claim would nonetheless have been obvious to a person of ordinary skill in the art at the time of the invention by the combination of the primary reference with one or more other primary references and/or the knowledge of someone skilled in the art. For example, a person of ordinary skill in the art would have been motivated to combine any reference in Exhibits A-01 to A-08 with any other reference(s) in

Exhibit A-01 to A-08. Such combinations would be achieved, for example, by merely combining the disclosures described in the respective claim charts for each reference.

Defendants also contend that any of the primary references (or combination of primary references) could be combined with any of the secondary references (or combination of secondary references) in Exhibit A-A to render obvious the asserted claims. Such combinations would be achieved by merely combining the disclosures described in the respective claim charts for each reference.

The obviousness combinations are provided in the alternative to Defendants' anticipation contentions and are not to be construed to suggest that any reference included in the combinations is not itself anticipatory.

1. Exemplary Combinations

Below are examples of prior art references that would have been combined by one of ordinary skill in the art at the time of the alleged invention. These combinations are merely examples. The asserted claims of the '780 Patent are rendered obvious by:

- Park (IEEE) in combination with GlobalPlatform and Abi-Char.
- Park (IEEE) in combination with GlobalPlatform and ANSI X9.63 Overview.
- Park (IEEE) in combination with GlobalPlatform, Abi-Char, and Weiss.
- Park (IEEE) in combination with GlobalPlatform, ANSI X9.63 Overview, and Weiss.
- Nix in combination with Park (IEEE) and GlobalPlatform.
- Boyd-Mathuria alone or in combination with one or more of Abi-Char, ANSI X9.63 Overview, GlobalPlatform, Gouget, Haggerty, Konstantinou, Lee, Nix, Park (IEEE), Peirce, SCP11, SGP.22, and/or Weiss.

- GlobalPlatform alone or in combination with one or more of Abi-Char, ANSI X9.63 Overview, Boyd-Mathuria, Gouget, Haggerty, Konstantinou, Lee, Nix, Park (IEEE), Peirce, SCP11, SGP.22, and/or Weiss.
- Gouget alone or in combination with one or more of Abi-Char, ANSI X9.63 Overview, Boyd-Mathuria, GlobalPlatform, Haggerty, Konstantinou, Lee, Nix, Park (IEEE), Peirce, SCP11, SGP.22, and/or Weiss.
- Haggerty alone or in combination with one or more of Abi-Char, ANSI X9.63 Overview, Boyd-Mathuria, GlobalPlatform, Gouget, Konstantinou, Lee, Nix, Park (IEEE), Peirce, SCP11, SGP.22, and/or Weiss.
- Nix alone or in combination with one or more of Abi-Char, ANSI X9.63 Overview, Boyd-Mathuria, GlobalPlatform, Gouget, Haggerty, Konstantinou, Lee, Park (IEEE), Peirce, SCP11, SGP.22, and/or Weiss.
- Park (IEEE) alone or in combination with one or more of Abi-Char, ANSI X9.63 Overview, Boyd-Mathuria, GlobalPlatform, Gouget, Haggerty, Konstantinou, Lee, Nix, Peirce, SCP11, SGP.22, and/or Weiss.
- SGP.22 alone or in combination with one or more of Abi-Char, ANSI X9.63 Overview, Boyd-Mathuria, GlobalPlatform, Gouget, Haggerty, Konstantinou, Lee, Nix, Park (IEEE), Peirce, SCP11, and/or Weiss.
- Weiss alone or in combination with one or more of Abi-Char, ANSI X9.63 Overview, Boyd-Mathuria, GlobalPlatform, Gouget, Haggerty, Konstantinou, Lee, Nix, Park (IEEE), Peirce, SCP11, and/or SGP.22.

2. Motivations to Combine

To the extent a finder of fact finds that a primary prior art reference does not disclose one or more limitations of an asserted claim, the asserted claim is nevertheless obvious because the alleged missing limitations contain nothing beyond ordinary improvements. In other words, the asserted claim combines known elements to achieve predictable results or chooses between clear alternatives known to those of skill in the art, particularly in view of the state of the art as reflected in the relevant prior art.

Moreover, as explained above, it would have been obvious to a person of skill in the art at the time of the alleged invention of the asserted claims to combine any primary reference with any combination of other primary references or secondary references so as to practice the asserted claims. To the extent that Plaintiff argues that any concept claimed in the asserted claims is not disclosed in a primary reference, it would, at a minimum, have been obvious to adapt the primary reference to include the concept or combine it with other primary references or secondary references that disclose the concept. Each concept described and claimed in the Asserted Patents was known to those of skill in the art as available design choices for the technologies at issue.[3]

The Supreme Court has held that "[t]he combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 416 (2007). "When a work is available in one field of endeavor, design incentives and other market forces can prompt variations of it, either in the same field or a different one." *Id.* at 417. As the Supreme Court made clear, "[f]or the same reason, if a technique has been used to improve one device, and a person of ordinary skill in the

[3] Each concept described and claimed in the '780 Patent was known to those of skill in the art as available design choices for data encryption technology and/or using such technology to provision and/or authenticate mobile devices for use with a wireless network in a wide range of applications for different scenarios and circumstances.

art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill." *Id*.

To determine whether there is an apparent reason to combine the known elements in the fashion claimed by the patent at issue, a court can "look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art." *Id*. at 418. For example, obviousness can be demonstrated by showing "there existed at the time of invention a known problem for which there was an obvious solution encompassed by the patent's claims." *Id*. at 420. "[A]ny need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed." *Id*. Common sense also teaches that "familiar items may have obvious uses beyond their primary purposes, and in many cases a person of ordinary skill will be able to fit the teachings of multiple patents together like pieces of a puzzle." *Id*.

However, the Supreme Court in *KSR* held that a claimed invention can be obvious even if there is no explicit teaching, suggestion, or motivation for combining the prior art to produce that invention. In summary, *KSR* holds that patents that are based on new combinations of elements or components already known in a technical field may be found to be obvious. *See, generally*, *KSR*, 550 U.S. 398. Specifically, the Court in *KSR* rejected a rigid application of the "teaching, suggestion, or motivation [to combine]" test. *Id*. at 418. "In determining whether the subject matter of a patent claim is obvious, neither the particular motivation nor the avowed purpose of the patentee controls. What matters is the objective reach of the claim." *Id*. at 419. "Under the correct analysis, any need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the

manner claimed." *Id*. at 420. A key inquiry is whether the "improvement is more than the predictable use of prior art elements according to their established functions." *Id*. at 417.

The rationale to combine or modify prior art references is significantly stronger when, as here, the references seek to solve the same problem, come from the same field, and correspond well to each other. *In re Inland Steel Co*., 265 F.3d 1354, 1362 (Fed. Cir. 2001). The Federal Circuit has held that two references may be combined as invalidating art under similar circumstances, namely "[the prior art] focus[es] on the same problem that the … patent addresses: enhancing the magnetic properties of … steel. Moreover, both [prior art references] come from the same field …. Finally, the solutions to the identified problems found in the two references correspond well." *Id*. at 1364 (concerning patents and prior art relating to improving the magnetic and electrical properties of steel).

In view of the Supreme Court's *KSR* decision, the PTO issued a set of Examination Guidelines. Examination Guidelines for Determining Obviousness Under 35 U.S.C. §103 in view of the Supreme Court Decision in *KSR International Co. v. Teleflex, Inc*., 72 Fed. Reg. 57526 (October 10, 2007). Those Guidelines summarized the *KSR* decision and identified various rationales for finding a claim obvious, including those based on other precedents. Those rationales include:

> (A) Combining prior art elements according to known methods to yield predictable results;
> (B) Simple substitution of one known element for another to obtain predictable results;
> (C) Use of known technique to improve similar devices (methods, or products) in the same way;
> (D) Applying a known technique to a known device (method, or product) ready for improvement to yield predictable results;
> (E) "Obvious to try" – choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success;

> (F) Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations would have been predictable to one of ordinary skill in the art;
>
> (G) Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention.

Id. at 57529. The above rationales likewise apply in rendering obvious the asserted claims of the Asserted Patents.

The references disclosed herein, alone or in combination, contain an explicit and/or implicit teaching or motivation to combine them due to the following: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference addresses similar problems; and (5) the knowledge of those skilled in the art that the disclosed elements had been or could be used together.

As an example of those reasons and motivations to combine the references, Abi-Char, ANSI X9.63 Overview, Boyd-Mathuria, GlobalPlatform, Gouget, Haggerty, Konstantinou, Lee, Nix, Park (IEEE), Peirce, SCP11, SGP.22 and/or Weiss generally relate to encryption technology, and/or using such technology to provision or authenticate a mobile device for use with a wireless network. *See* Exs. A-01 to A-08 and A-A. The references disclose similar components and techniques for data encryption, and/or using encryption to provision or authenticate mobile devices. *Id.* The attached charts in Exhibits A-01 to A-08 and A-A provide additional reasons and motivations to combine the charted references.

Additionally, the primary and secondary references listed above are analogous art. They are all directed to encryption technology, and in particular, to provisioning and/or authenticating a mobile device for use with a wireless network. *See, e.g.*, Abi-Char at Abstract ("To provide

secure communication for mobile devices, authenticated key agreement protocol is an important primitive for establishing session key …. In this paper we present a fast and Secure Authenticated Key Agreement (EC-SAKA) protocol based on Elliptic Curve Cryptography."), ANSI X9.63 Overview at 3 ("Specifies key agreement and key transport schemes using elliptic curve cryptography"), Boyd-Mathuria at VII ("We believe that this book is the first comprehensive treatment of protocols for authentication and key establishment."), GlobalPlatform at 2-3 ("Its goal is to reduce barriers hindering the growth of cross-industry, multiple Application smart cards …. Although this specification defines card components, command interfaces, transaction sequences, and interfaces that can be common across many different industries, it does not detail the implementation of the lower layers security, which may vary from one industry to the other. This specification is also intended for a more general audience as it describes the generic security concepts and the various actors involved in a multi-Application Card Management System."), Gouget at [0010] ("The purpose of the invention is to provide a method for establishing a secure channel between a client C and a remote server S when the client C and the server S exchange data through an intermediate entity G."), Haggerty at Abstract ("Methods and apparatus for large scale distribution of electronic access control clients. In one aspect, a tiered security software protocol is disclosed. In one exemplary embodiment, a server electronic Universal Integrated Circuit Card (eUICC) and client eUICC software comprise a so-called 'stack' of software layers …. The tiered security software protocol is configured for large scale distribution of electronic Subscriber Identity Modules (eSIMs)."), Konstantinou at Abstract ("algorithm disclosed here is a method for a mobile station device to select a network for wireless communications"), Lee at Abstract ("The present invention relates to a method and apparatus for installing a profile, and more specifically, to a method for managing mobile communication subscriber information

(profile), such as for remotely installing and uninstalling a profile onto a security module (Universal Integrated Circuit Card (UICC)) that is embedded inside a terminal and that is not attachable or detachable, thereby replacing UICC."), Nix at 1:18-22 ("methods and systems [that] support the authentication of a user associated with the eUICC"), Park (IEEE) at Abstract ("In this paper, a novel secure profile provisioning architecture for eUICCs is proposed."), Peirce at Abstract ("A system and method for producing cryptographic keys for use by an embedded processing device within a manufactured product. A pseudo random number generator is seeded with entropy data gathered by the embedded device, and the result is used to generate a public-private key pair."), SCP11 at 7 ("This document specifies a new secure channel protocol, named Secure Channel Protocol '11' (SCP11), based on Elliptic Curve Cryptography (ECC) for mutual authentication and secure channel initiation and on AES for secure messaging."), SGP.22 at 7 ("This specification provides a technical description of: The eUICC Architecture; The interfaces used within the Remote SIM Provisioning Architecture; and The security functions used within the Remote SIM Provisioning Architecture."), Weiss at Abstract ("A method of providing a secure element of a mobile terminal with a subscription profile…").

A person of ordinary skill in the art would look to the primary and secondary references to improve or tailor the disclosure thereof to tailor to particular settings or particular factors. A person of ordinary skill in the art would have understood the general trend and motivation to optimize the security, effectiveness, and efficiency of profile provisioning, authentication, and data encryption procedures. A POSITA would have understood that doing so could increase system performance, including in terms of, for example, security and/or efficiency. *See, e.g.*, Abi-Char at Abstract ("To provide secure communication for mobile devices, authenticated key agreement protocol is an important primitive for establishing session key …. In this paper we

present a fast and Secure Authenticated Key Agreement (EC-SAKA) protocol based on Elliptic Curve Cryptography …. The new protocol achieves many of the required security and performance properties. It can resist dictionary attacks mounted by either passive or active network intruders. It can resist Man-In-The Middle attack. It also offers perfect forward secrecy which protects past sessions and passwords against future compromise. In addition, it can resist known-key and resilience to server attack …. Our proposed protocol offers significantly improved performance in computational and communication load over comparably many authenticated key agreement protocols…"), ANSI X9.63 Overview at 3 ("Specifies key agreement and key transport schemes using elliptic curve cryptography … Specifies a variety of schemes to meet the diverse security needs of communications protocols"), Boyd-Mathuria at VII ("Authentication and key establishment are fundamental building blocks for securing electronic communications. Cryptographic algorithms for encryption and integrity cannot perform their function unless secure keys have been established and the users know which parties share such keys. It is essential that protocols for providing authentication and key establishment are fit for their purpose."), GlobalPlatform at 2 ("For smart cards to reach their true potential, consumers need to be able to use them for a wide variety of functions. For example, the cards can be used with mobile phones to make purchases over the Internet as well as to securely access a PC. Smart cards should also be cost effective and easily multifunctional …. GlobalPlatform defines a flexible and powerful specification for Card Issuers to create single- and multi-Application chip card systems to meet the evolution of their business needs."), Gouget at [0020]-[0022] ("The invention solves the problem of man-in-the-middle attack in case of the exposure of a permanent secret key used to establish a secure channel. There is neither need for an additional device nor an additional mutual authentication. Thanks to the invention, a secure

channel is established between the server S and the client C such that the gateway G cannot access to the plaintext data transmitted into the secure channel, even if the permanent secret key skc has been revealed.”), Haggerty at [0013]-[0014] (“Accordingly, new solutions and infrastructure are needed to leverage the enhanced flexibility provided by electronic access clients (e.g., eSIMs), and to support secure and ubiquitous distribution thereof. The present disclosure provides, inter alia, for large scale distribution of electronic access control clients.”), Konstantinou at Abstract (“exemplary algorithm provides the flexibility to select between 3GPP2 (1×RTT and EVDO) technologies and 3GPP (LTE/GSM/UMTS) technologies as well as specific operators' networks for domestic and international roaming”), Lee at [0010]-[0011] (“Unlike the conventional UICC which is manufactured and distributed for specific mobile communication operators, the newly introduced embedded security module is capable of allowing for the user who has purchased the terminal to install and maintain the authentication information of various mobile communication operators securely and flexibly in such a way of subscribing and unsubscribing to a specific mobile communication operator or switching the subscription between operators. Thus, the present invention aims to provide a method for installing UICC information of various mobile communication operators in an embedded security module (instead of the conventional detachable UICC) remotely through a network.”), Nix at 3:10-16 (“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.”), Park (IEEE) at Abstract (“Embedded UICC (eUICC) is a new form of UICC … [T]he profiles necessary for its operations should be provisioned remotely into the eUICC by new entity. For the remote provisioning, SM (Subscription Manager) is newly

introduced by the standardization organization. However, this new ecosystem around eUICCs can cause tremendous security issues unless thorough consideration of security is accompanied during standardization because the profiles usually include the security-sensitive information. In this paper, a novel secure profile provisioning architecture for eUICCs is proposed. Our architecture mainly defines the overall architecture of the secure profile provisioning for eUICCs.”), Peirce at 1:50-2:2 (“As applied to embedded processing devices, the generation of the cryptographic keys can be problematic because they typically do not have entropy hardware or software engines of the type found in personal computers. Instead pseudo random number generators (PRNG) are typically used. These PRNGs are generally implemented in software and require a seed value that is used to generate a pseudo-random number. This generated number is then used to produce the cryptographic keys. The generation of strong keys using PRNGs generally necessitates the use of a seed value that cannot later be discovered. For an embedded processing device having restricted computing capabilities, obtaining such a seed value can be problematic …. According to one aspect of the invention, there is provided a method of producing cryptographic keys for use in communicating with a manufactured product”), SCP11 at 11 (“[T]his protocol allows authentication and secure channel initiation based on certificates instead of pre-shared keys. This provides greater flexibility in cases where the two entities setting up the secure channel are not deployed in strict pairs.”), SGP.22 at 7 (“The adoption of this technical solution will provide the basis for global interoperability between different Operator deployment scenarios, for example network equipment (e.g. Subscription Manager Data Preparation (SM-DP+)) and various eUICC platforms.”), Weiss at [0005] (“[T]he problem addressed by the present invention is to provide for methods and devices that allow providing the secure element of a mobile terminal over-the-air with a subscription profile.”).

One of skill in the art would also have been motivated to combine the different publications and patents that were authored by employees of a given company or assigned to the same assignee and/or related to the same subject matter. The common architect of the references demonstrate that they relate to continued work in a common field of effort and continued related developments in that field. Additionally, based on the teachings of the references and/or the knowledge of one of ordinary skill, one of skill in the art would have been motivated to combine different references from the same company. For example, a POSITA would have been motivated to combine at least GlobalPlatform and SCP11, both of which were published by the same company: GlobalPlatform, Inc. And, one of skill in the art would have been motivated to combine prior art systems or products with any related or applicable documentation or literature for that system, including for the reason that these materials are related.

In addition, below are additional motivations to combine prior art for particular claim limitations. The following discussion of specific claim limitations are merely examples and are not limiting.

For example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach a secure profile provisioning architecture (*e.g.*, limitations 1[PRE], 1[C], 1[D], 1[E], 1[F], 1[G], 1[H], 1[I], 1[J], 1[K], 7, 10, 17, 18), it would have been obvious to a person of ordinary skill in the art at the time of the invention to combine the primary reference with any of the prior art that discloses a secure profile provisioning architecture (*e.g.*, limitations 1[PRE], 1[C], 1[D], 1[E], 1[F], 1[G], 1[H], 1[I], 1[J], 1[K], 7, 10, 17, 18) in Exhibits A-01 to A-08 or Exhibit A-A. For example, several prior art references, including at least Abi-Char, ANSI X9.63 Overview, Boyd-Mathuria, GlobalPlatform, Gouget, Haggerty, Konstantinou, Lee, Nix, Park (IEEE), Peirce, SCP11, SGP.22, and/or Weiss explicitly describe or disclose a secure profile

provisioning architecture. *See, e.g.*, Abi-Char at 1, 2, 3, 4; ANSI X9.63 Overview at 3, 7, 12; Boyd-Mathuria at 49, 81, 125, 136, 140, 141; GlobalPlatform at 156, 174, 194, 198, 202-203, 216, 234, 246-247, 251-253, 255-256, 258, 260, 264, 266-268, 275-276; Gouget at Abstract; Haggerty at Abstract, [0005], [0008], [0015], [0045]-[0046], [0048], [0084], [0100], [0114], [0121], [0131]-[0133]; Konstantinou at [0031], [0158], [0163], [0166]; Lee at Abstract, [0011], [0062]; Nix at 41:40-44, 42:37-42, 43:6-19, 47:52-55, 48:65-49:6, 49:7-19; Park (IEEE) at 297, 300, 301, 303; Peirce at Abstract, 1:6-9, 2:66-3:54, 8:18-51; SCP11 at 12, 13, 20, 30; SGP.22 at 9, 11, 12, 22, 23, 26-28, 51-54, 62-67, 93-94, 131-132; Weiss at [0002], [0012], [0014], [0015], [0020], [0059]-[0062], [0063].

A person skilled in the art would have understood the benefits of a secure profile provisioning architecture, would have recognized that configuring a system to comprise a secure profile provisioning architecture would provide benefits to the system, and would have been motivated to incorporate these features into a system accordingly. For example, a POSITA would have understood that configuring a system to comprise a secure profile provisioning architecture would yield a complete, secure, and efficient architecture for eUICC profile provisioning. *See, e.g.*, Abi-Char at Abstract ("To provide secure communication for mobile devices, authenticated key agreement protocol is an important primitive for establishing session key …. In this paper we present a fast and Secure Authenticated Key Agreement (EC-SAKA) protocol based on Elliptic Curve Cryptography …. The new protocol achieves many of the required security and performance properties. It can resist dictionary attacks mounted by either passive or active network intruders. It can resist Man-In-The Middle attack. It also offers perfect forward secrecy which protects past sessions and passwords against future compromise. In addition, it can resist known-key and resilience to server attack …. Our proposed protocol offers significantly

improved performance in computational and communication load over comparably many authenticated key agreement protocols…"), ANSI X9.63 Overview at 4 ("Specify schemes capable of meeting common security needs"), Boyd-Mathuria at VII ("We believe that this book is the first comprehensive treatment of protocols for authentication and key establishment …. Authentication and key establishment are fundamental building blocks for securing electronic communications. Cryptographic algorithms for encryption and integrity cannot perform their function unless secure keys have been established and the users know which parties share such keys. It is essential that protocols for providing authentication and key establishment are fit for their purpose."), GlobalPlatform at 18-19 ("The GlobalPlatform architecture is designed to provide Card Issuers with the system management architecture for managing these smart cards …. The GlobalPlatform card architecture is comprised of a number of components that ensure hardware and vendor-neutral interfaces to Applications and off-card management systems."), Gouget at [0020]-[0022] ("The invention solves the problem of man-in-the-middle attack in case of the exposure of a permanent secret key used to establish a secure channel. There is neither need for an additional device nor an additional mutual authentication. Thanks to the invention, a secure channel is established between the server S and the client C such that the gateway G cannot access to the plaintext data transmitted into the secure channel, even if the permanent secret key skc has been revealed."), Haggerty at [0009]-[0014] ("Prior SIM card based approaches suffer from a number of disabilities. For instance, traditional UICCs support only a single USIM (or more generally 'SIM') access control client. If a user wants to authenticate to a cellular network using a different SIM, the user must physically exchange the SIM card in the device with a different SIM card …. The present disclosure provides, inter alia, for large scale distribution of electronic access control clients."), Konstantinou at Abstract ("The exemplary

algorithm provides the flexibility to select between 3GPP2 (1×RTT and EVDO) technologies and 3GPP (LTE/GSM/UMTS) technologies as well as specific operators' networks for domestic and international roaming."), Lee at Abstract ("The present invention relates to a method and apparatus for installing a profile, and more specifically, to a method for managing mobile communication subscriber information (profile), such as for remotely installing and uninstalling a profile onto a security module (Universal Integrated Circuit Card (UICC)) that is embedded inside a terminal and that is not attachable or detachable, thereby replacing UICC."), Nix at 4:48-51 ("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."), Park (IEEE) at Abstract ("Embedded UICC (eUICC) is a new form of UICC … [T]he profiles necessary for its operations should be provisioned remotely into the eUICC by new entity. For the remote provisioning, SM (Subscription Manager) is newly introduced by the standardization organization. However, this new ecosystem around eUICCs can cause tremendous security issues unless thorough consideration of security is accompanied during standardization because the profiles usually include the security-sensitive information. In this paper, a novel secure profile provisioning architecture for eUICCs is proposed. Our architecture mainly defines the overall architecture of the secure profile provisioning for eUICCs."), Peirce at 1:6-9 ("The present invention relates generally to techniques for generating cryptographic keys used in secure data communications and, in particular, to such techniques used for manufactured products having embedded processing devices."), SCP11 at 11 ("[T]his protocol allows authentication and secure channel initiation based on certificates instead of pre-shared keys. This provides greater flexibility in cases where the two entities setting up the secure channel are not deployed in strict pairs."), SGP.22 at 19 ("This section describes the internal high-level architecture of the eUICC

…. Operator Profiles are stored inside security domains within the eUICC and are implemented using GlobalPlatform standards. These ensure that it is impossible for any Profile to access the applications or data of any other Profile stored on the eUICC. The same mechanism is currently in use within SIM cards to ensure payment applications are kept secure."), Weiss at [0003] ("It is foreseeable that at least for some of these devices it will not be possible or at least very difficult to provide the secure element beforehand with the necessary subscription credentials, including for instance an IMSI. This is because in a lot of M2M devices the secure element will most likely be implemented in the form of a surface mounted chip or chip module without the possibility of providing the secure element with the necessary subscription credentials beforehand. Consequently, once in the field, these M2M devices and their non-personalized secure elements require the provision of subscription credentials over-the-air."). Thus, a person of ordinary skill in the art would have been motivated to modify any of the primary references to include this feature. A person of ordinary skill in the art would also have had a reasonable expectation of success. A person of ordinary skill in the art would have understood that these references disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach procedures for mutual authentication and/or sensitive data encryption (*e.g.*, limitations 1[C], 1[D], 1[E], 1[F], 1[G], 1[H], 1[I], 1[J], 1[K], 6, 8, 9, 10, 17, 18, 19), it would have been obvious to a person of ordinary skill in the art at the time of the invention to combine the primary reference with any of the prior art that discloses procedures for mutual authentication and/or sensitive data encryption (*e.g.*, limitations 1[C], 1[D], 1[E], 1[F], 1[G], 1[H], 1[I], 1[J], 1[K], 6, 8, 9, 10, 17, 18, 19) in Exhibits A-01 to A-08 or Exhibit A-A. For

example, several prior art references, including at least Abi-Char, ANSI X9.63 Overview, Boyd-Mathuria, GlobalPlatform, Gouget, Haggerty, Lee, Nix, Park (IEEE), Peirce, SCP11, SGP.22, and/or Weiss explicitly describe or disclose procedures for mutual authentication and/or sensitive data encryption. *See, e.g.*, Abi-Char at 1, 2, 3, 4; ANSI X9.63 Overview at 3, 7, 12; Boyd-Mathuria at 49, 81, 125, 136, 140, 141; GlobalPlatform at 156, 174, 194, 198, 202-203, 216, 234, 246-247, 251-253, 255-256, 258, 260, 264, 266-268, 275-276; Gouget at Abstract; Haggerty at Abstract, [0008], [0015], [0045]-[0046], [0048], [0084], [0100], [0114], [0121], [0131]-[0133]; Lee at Abstract, [0011], [0062]; Nix at 33:60-63, Figure 2a, Claim 1; Park (IEEE) at 297, 300, 301, 303; Peirce at Abstract, 1:6-9, 2:66-3:54, 8:18-51; SCP11 at 12, 13, 20, 30; SGP.22 at 9, 11, 12, 17, 22, 23, 24, 26-28, 51-54, 62-67, 75, 81, 93-94, 131-132, 202, 210; Weiss at [0012], [0014], [0015], [0038], [0042], [0063].

A person skilled in the art would have understood the benefits of procedures for mutual authentication and/or sensitive data encryption, would have recognized that configuring a system to comprise procedures for mutual authentication and/or sensitive data encryption would provide benefits to the system, and would have been motivated to incorporate these features into a system accordingly. For example, a POSITA would have understood that configuring a system to comprise procedures for mutual authentication and/or sensitive data encryption would yield a complete, secure, and efficient architecture for eUICC profile provisioning. Indeed, a POSITA would have recognized that applying procedures for mutual authentication and/or sensitive data encryption would provide an additional layer of protection for the most sensitive data within the profile, ensuring that even if some aspects were compromised, the critical key materials could remain protected. *See, e.g.*, Abi-Char at Abstract ("To provide secure communication for mobile devices, authenticated key agreement protocol is an important primitive for establishing session

key …. In this paper we present a fast and Secure Authenticated Key Agreement (EC-SAKA) protocol based on Elliptic Curve Cryptography …. The new protocol achieves many of the required security and performance properties. It can resist dictionary attacks mounted by either passive or active network intruders. It can resist Man-In-The Middle attack. It also offers perfect forward secrecy which protects past sessions and passwords against future compromise. In addition, it can resist known-key and resilience to server attack …. Our proposed protocol offers significantly improved performance in computational and communication load over comparably many authenticated key agreement protocols…"), ANSI X9.63 Overview at 4 ("Specify schemes capable of meeting common security needs"), Boyd-Mathuria at VII ("We believe that this book is the first comprehensive treatment of protocols for authentication and key establishment …. Authentication and key establishment are fundamental building blocks for securing electronic communications. Cryptographic algorithms for encryption and integrity cannot perform their function unless secure keys have been established and the users know which parties share such keys. It is essential that protocols for providing authentication and key establishment are fit for their purpose."), GlobalPlatform at 23 ("The primary goal of the GlobalPlatform is to ensure the security and integrity of the card's components for the life of the card …. To ensure card security and integrity, the GlobalPlatform is designed to support a range of secure mechanisms for: Data integrity; Resource availability; Confidentiality; Authentication."), Gouget at [0020]-[0022] ("The invention solves the problem of man-in-the-middle attack in case of the exposure of a permanent secret key used to establish a secure channel. There is neither need for an additional device nor an additional mutual authentication. Thanks to the invention, a secure channel is established between the server S and the client C such that the gateway G cannot access to the plaintext data transmitted into the secure channel, even if the permanent secret key skc has been

revealed."), Haggerty at [0009]-[0014] ("Prior SIM card based approaches suffer from a number of disabilities. For instance, traditional UICCs support only a single USIM (or more generally 'SIM') access control client. If a user wants to authenticate to a cellular network using a different SIM, the user must physically exchange the SIM card in the device with a different SIM card …. The present disclosure provides, inter alia, for large scale distribution of electronic access control clients."), Lee at [0005]-[0011] ("The conventional UICC is manufactured on demand as a dedicated card for a specific mobile communication operator. Accordingly, the authentication information (e.g. USIM application, IMSI, and K value) for connection to the corresponding operator network is stored in the UICC in the manufacturing stage. The mobile communication operator provides the subscriber with the manufactured UICC," and "[t]he subscriber may insert the UICC into a mobile communication terminal to use the corresponding mobile communication operator' s network and application services and, if necessary, may detach the UICC from the terminal and attach to another terminal so as to use the authentication information, contacts, and phonebooks stored in the corresponding UICC with the new terminal as they were …. Unlike the conventional UICC which is manufactured and distributed for specific mobile communication operators, the newly introduced embedded security module is capable of allowing for the user who has purchased the terminal to install and maintain the authentication information of various mobile communication operators securely and flexibly in such a way of subscribing and unsubscribing to a specific mobile communication operator or switching the subscription between operators. Thus, the present invention aims to provide a method for installing UICC information of various mobile communication operators in an embedded security module (instead of the conventional detachable UICC) remotely through a network."), Nix at 3:32-36 ("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.”), Park (IEEE) at Abstract (“[T]his new ecosystem around eUICCs can cause tremendous security issues unless thorough consideration of security is accompanied during standardization because the profiles usually include the security-sensitive information.”), Peirce at 1:21- 25 (“In some cases, it is desirable to establish authenticated, secure data communications in which the exchanged data is encrypted. Although various approaches can be used, cryptographic keys are perhaps most commonly used for this purpose”), SCP11 at 11 (“[T]his protocol allows authentication and secure channel initiation based on certificates instead of pre-shared keys. This provides greater flexibility in cases where the two entities setting up the secure channel are not deployed in strict pairs.”), SGP.22 at 33 (“The RSP ecosystem relies on remote secure communication to achieve function execution requests and data exchanges. Any of the remote secure communication defined for RSP SHALL follow the hereunder rules … Mutual authentication[,] Data privacy[,] Communication protection[,] Authorisation[.]”), Weiss at [0014] (“Preferably, the first server decrypts the encrypted version of the identification element IDse, the encrypted version of the session key Kses and the encrypted version of the hardware configuration HWconf of the secure element and/or the mobile terminal using the configuration key Kconf provided by the second server so that the first server can verify the validity of the configuration key Kconf provided by the second server by verifying that the identification element IDse sent in the clear is identical to the identification element IDse resulting from the decryption of the encrypted version of the identification element IDse using the configuration key Kconf.”). Thus, a person of ordinary skill in the art would have been motivated to modify any of the primary references to include this feature. A person of ordinary skill in the art would

also have had a reasonable expectation of success. A person of ordinary skill in the art would have understood that these references disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach key exchange and/or agreement protocols or mechanisms (*e.g.*, limitations 1[C], 1[D], 1[E], 1[F], 1[G], 1[H], 1[I], 1[J], 1[K], 2, 5, 7, 17, 18), it would have been obvious to a person of ordinary skill in the art at the time of the invention to combine the primary reference with any of the prior art that discloses key exchange and/or agreement protocols or mechanisms (*e.g.*, limitations 1[C], 1[D], 1[E], 1[F], 1[G], 1[H], 1[I], 1[J], 1[K], 2, 5, 7, 17, 18) in Exhibits A-01 to A-08 or Exhibit A-A. For example, several prior art references, including at least Abi-Char, ANSI X9.63 Overview, Boyd-Mathuria, GlobalPlatform, Gouget, Haggerty, Lee, Nix, Park (IEEE), Peirce, SCP11, SGP.22, and/or Weiss explicitly describe or disclose key exchange and/or agreement protocols or mechanisms. *See, e.g.*, Abi-Char at 1, 3; ANSI X9.63 Overview at 3, 7, 12; Boyd-Mathuria at 49, 81, 125, 136, 140, 141; GlobalPlatform at 156, 174, 194, 198, 202-203, 216, 234, 246-247, 251-253, 255-256, 258, 260, 264, 266-268, 275-276; Gouget at Abstract; Haggerty at Abstract, [0008], [0015], [0045]-[0046], [0048], [0084], [0100], [0114], [0121], [0131]-[0133]; Lee at Abstract, [0011], [0062]; Nix at 51:65–52:23; Park (IEEE) at 297, 300, 301, 303; Peirce at Abstract, 1:6-9, 2:66-3:54, 8:18-51; SCP11 at 12, 13, 20, 30; SGP.22 at 15, 27-28, 34, 51-53, 62-65, 93-94, 131-132, 140, 210; Weiss at [0002], [0010]-[0011], [0012], [0014], [0015], [0020], [0046], [0063].

A person skilled in the art would have understood the benefits of key exchange and/or agreement protocols or mechanisms, would have recognized that configuring a system to

comprise key exchange and/or agreement protocols or mechanisms would provide benefits to the system, and would have been motivated to incorporate these features into a system accordingly. For example, a POSITA would have understood that configuring a system to comprise key exchange and/or agreement protocols or mechanisms would yield a complete, secure, and efficient architecture for eUICC profile provisioning. Indeed, a POSITA would have recognized that configuring a system to comprise key exchange and/or agreement protocols or mechanisms would provide an additional layer of protection for the most sensitive data within the profile. Key exchange and/or agreement protocols or mechanisms were well-established and known to provide confidentiality, integrity, and mutual authentication. *See, e.g.*, Abi-Char at Abstract ("To provide secure communication for mobile devices, authenticated key agreement protocol is an important primitive for establishing session key …. In this paper we present a fast and Secure Authenticated Key Agreement (EC-SAKA) protocol based on Elliptic Curve Cryptography …. The new protocol achieves many of the required security and performance properties. It can resist dictionary attacks mounted by either passive or active network intruders. It can resist Man-In-The Middle attack. It also offers perfect forward secrecy which protects past sessions and passwords against future compromise. In addition, it can resist known-key and resilience to server attack …. Our proposed protocol offers significantly improved performance in computational and communication load over comparably many authenticated key agreement protocols…"), ANSI X9.63 Overview at 3 ("Specifies key agreement and key transport schemes using elliptic curve cryptography … Specifies a variety of schemes to meet the diverse security needs of communications protocols"), Boyd-Mathuria at VII ("We believe that this book is the first comprehensive treatment of protocols for authentication and key establishment …. Authentication and key establishment are fundamental building blocks for securing electronic

communications. Cryptographic algorithms for encryption and integrity cannot perform their function unless secure keys have been established and the users know which parties share such keys. It is essential that protocols for providing authentication and key establishment are fit for their purpose."), GlobalPlatform at 23 ("The primary goal of the GlobalPlatform is to ensure the security and integrity of the card's components for the life of the card …. Because the cards are only part of a larger card system involving multiple parties and off-card components, the GlobalPlatform also relies upon non-cryptographic, procedural means of protection, such as code testing and verification, physical security, and secure key handling."), Gouget at [0020]-[0022] ("The invention solves the problem of man-in-the-middle attack in case of the exposure of a permanent secret key used to establish a secure channel. There is neither need for an additional device nor an additional mutual authentication. Thanks to the invention, a secure channel is established between the server S and the client C such that the gateway G cannot access to the plaintext data transmitted into the secure channel, even if the permanent secret key skc has been revealed."), Haggerty at [0009]-[0014] ("Prior SIM card based approaches suffer from a number of disabilities. For instance, traditional UICCs support only a single USIM (or more generally 'SIM') access control client. If a user wants to authenticate to a cellular network using a different SIM, the user must physically exchange the SIM card in the device with a different SIM card …. The present disclosure provides, inter alia, for large scale distribution of electronic access control clients."), Lee at [0016] ("According to an embodiment of the present invention, a profile management server for managing the embedded security module of a terminal and a profile provision server for generating a UICC profile in association with a specific mobile communication operator are separated such that the terminal encodes a session key and authenticate the profile with a digital certificate provided by the profile provision server and thus

can transfer the encoded profile to the embedded security module of the terminal without exposing the content of the profile to the profile management server positioned between the profile provision server and the terminal."), Nix at 3:28-32 ("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."), Park (IEEE) at 301 ("KAM is software running inside the eUICC to perform the key agreement protocol …. For the security, the SM-DP Credentials should not be revealed to any party, even SM-SR, except for eUICC. To accomplish this, KAM is designed and applied to SPA."), Peirce at 1:50-2:2 ("As applied to embedded processing devices, the generation of the cryptographic keys can be problematic because they typically do not have entropy hardware or software engines of the type found in personal computers. Instead pseudo random number generators (PRNG) are typically used. These PRNGs are generally implemented in software and require a seed value that is used to generate a pseudo-random number. This generated number is then used to produce the cryptographic keys. The generation of strong keys using PRNGs generally necessitates the use of a seed value that cannot later be discovered. For an embedded processing device having restricted computing capabilities, obtaining such a seed value can be problematic …. According to one aspect of the invention, there is provided a method of producing cryptographic keys for use in communicating with a manufactured product"), SCP11 at 11 ("[T]his protocol allows authentication and secure channel initiation based on certificates instead of pre-shared keys. This provides greater flexibility in cases where the two entities setting up the secure channel are not deployed in strict pairs."), SGP.22 at 93-94 ("Public key of the eUICC used to verify an eUICC signature …. Private key of the SM-DS used to provide signatures for authentication to the eUICC …. Public key of the EUM used to verify

EUICC Certificates …. One-time public key of the EUICC used for key agreement …. One-time private key of the EUICC used for key agreement."), Weiss at [0002]-[0005] ("[T]he SIM contains subscription credentials for authenticating and identifying the user of the mobile terminal, including in particular an International Mobile Subscriber Identity (IMSI) and an authentication key Ki. These subscription credentials are generally stored on the SIM by the SIM manufacturer/vendor or the MNO during a SIM personalization process prior to providing the user of the mobile terminal with his SIM …. [T]he problem addressed by the present invention is to provide for methods and devices that allow providing the secure element of a mobile terminal over-the-air with a subscription profile."). Thus, a person of ordinary skill in the art would have been motivated to modify any of the primary references to include this feature. A person of ordinary skill in the art would also have had a reasonable expectation of success. A person of ordinary skill in the art would have understood that these references disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach random number generation protocols (*e.g.*, limitations 1[C], 1[E]), it would have been obvious to a person of ordinary skill in the art at the time of the invention to combine the primary reference with any of the prior art that discloses random number generation protocols (*e.g.*, limitations 1[C], 1[E]) in Exhibits A-01 to A-08 or Exhibit A-A. For example, several prior art references, including at least Abi-Char, ANSI X9.63 Overview, Boyd-Mathuria, GlobalPlatform, Gouget, Haggerty, Nix, Park (IEEE), Peirce, SGP.22, and/or Weiss explicitly describe or disclose random number generation protocols. *See, e.g.*, Abi-Char at 3; ANSI X9.63 Overview at 6, 10; Boyd-Mathuria at 9, 136, 140, 141; GlobalPlatform at 194; Gouget at

Abstract, [0011]-[0012], [0036], [0040]-[0041]; Haggerty at [0121]; Nix at 22:32-43, 41:63-64, 42:11-30; Park (IEEE) at 300, 301; Peirce at Abstract, 8:18-51; SGP.22 at 27-28, 35, 62, 63, 94; Weiss at [0046].

A person skilled in the art would have understood the benefits of random number generation protocols, would have recognized that configuring a system to comprise random number generation protocols would provide benefits to the system, and would have been motivated to incorporate these features into a system accordingly. For example, a POSITA would have understood that configuring a system to comprise random number generation protocols would improve the security of the system by helping to ensure that the keys used in the exchanges were derived from sufficiently random and unpredictable sources that were readily available to the eUICC-storing devices in these systems. *See, e.g.*, Abi-Char at 2 ("Because round trips and large blocks are critical factors in terms of communication load and because exponentiations and random numbers are to be critical factors in terms of computation load, such properties are listed below: Computational efficiency[,] Communication efficiency[,] Nature of security guarantees[,] Storage of secrets."), ANSI X9.63 Overview at 6 ("A number of primitives (mathematical building blocks) must be specified in order to build schemes …. Curves selected in any manner. Verifiably random selection option"), Boyd-Mathuria at 9 ("There are various mechanisms that may be employed to allow users to check that session keys have not been replayed …. In this method, A will generate a new random value NA commonly known as a nonce (a number used only once). Definition 1.1. A nonce is a random value generated by one party and returned to that party to show that a message is newly generated."), GlobalPlatform at 194 ("The Secure Channel is always initiated … by the off-card entity by passing a 'host' challenge (random data unique to this Secure Channel Session) to the card. The card, on receipt of this challenge,

generates its own 'card' challenge (again random data unique to this Secure Channel Session). The card, using the host challenge, the card challenge and its internal static keys, creates new secret Secure Channel session keys and generates a first cryptographic value (card cryptogram) using one of its newly created Secure Channel session keys …. This card cryptogram along with the card challenge, the Secure Channel Protocol identifier, and other data is transmitted back to the off-card entity. As the off-card entity should now have all the same information that the card used to generate the card cryptogram, it should be able to generate the same Secure Channel session keys and the same card cryptogram and by performing a comparison, it is able to authenticate the card."), Gouget at [0020]-[0022] ("The invention solves the problem of man-in-the-middle attack in case of the exposure of a permanent secret key used to establish a secure channel. There is neither need for an additional device nor an additional mutual authentication. Thanks to the invention, a secure channel is established between the server S and the client C such that the gateway G cannot access to the plaintext data transmitted into the secure channel, even if the permanent secret key skc has been revealed."), Haggerty at [0121] ("When the user exports an eSIM, the AP retrieves a list of installed profiles from eUICC; for each profile, eUICC also returns the associated principal and a nonce generated for anti-replay. When the user chooses to export a profile, the AP uses information contained in the principal to obtain a single sign-on (SSO) token from the service provider, where the user would be prompted to enter username and password for the purpose. The SSO token is passed together with principal and nonce to the server broker in export request. The server broker can process the authentication with the service provider, using the SSO token supplied by the device. Once authentication passes, the flow mirrors eSIM delivery to the device, except that the client and server roles are reversed. At a high level, the server broker initiates a session with the eUICC, creates a request

BLOB for the export. In the request, it includes the nonce that the eUICC generated, to indicate that the operation has passed L3 authentication. The eUICC verifies the request BLOB, encrypts the eSIM with the server agent's public key, creates a batch descriptor and L3 owner information for the eSIM. The eSIM together with L3 and L2 information can be sent to the server."), Nix at 22:32-43 ("The creation of random numbers with a high degree of entropy may be important the use of cryptographic algorithms 141."), Park (IEEE) at 301 ("KAM is software running inside the eUICC to perform the key agreement protocol …. For the security, the SM-DP Credentials should not be revealed to any party, even SM-SR, except for eUICC. To accomplish this, KAM is designed and applied to SPA."), Peirce at 1:50-2:2 ("As applied to embedded processing devices, the generation of the cryptographic keys can be problematic because they typically do not have entropy hardware or software engines of the type found in personal computers. Instead pseudo random number generators (PRNG) are typically used. These PRNGs are generally implemented in software and require a seed value that is used to generate a pseudo-random number. This generated number is then used to produce the cryptographic keys. The generation of strong keys using PRNGs generally necessitates the use of a seed value that cannot later be discovered. For an embedded processing device having restricted computing capabilities, obtaining such a seed value can be problematic …. According to one aspect of the invention, there is provided a method of producing cryptographic keys for use in communicating with a manufactured product"), SGP.22 at 28 ("Profile protection can optionally be performed using … random keys per Profile…"), Weiss at [0046] ("Preferably, the session key Kses is a nonce, i.e. an arbitrary number used only once. This ensures that for every subscription profile update session, such as the subscription profile update session shown in FIG. 2, a different session key Kses is used. As is well known to the person skilled in the art, such a nonce can be created, for

instance, by using a pseudorandom number generator, preferably a cryptographically secure pseudorandom number generator."). Thus, a person of ordinary skill in the art would have been motivated to modify any of the primary references to include this feature. A person of ordinary skill in the art would also have had a reasonable expectation of success. A person of ordinary skill in the art would have understood that these references disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach specific types or aspects of connected or networked devices (*e.g.*, limitations 1[A], 1[B], 2, 10, 13, 14, 19), it would have been obvious to a person of ordinary skill in the art at the time of the invention to combine the primary reference with any of the prior art that discloses specific types or aspects of connected or networked devices (*e.g.*, limitations 1[A], 1[B], 2, 10, 13, 14, 19) in Exhibits A-01 to A-08 or Exhibit A-A. For example, several prior art references, including at least Abi-Char, ANSI X9.63 Overview, Boyd-Mathuria, GlobalPlatform, Gouget, Haggerty, Konstantinou, Lee, Nix, Park (IEEE), Peirce, SGP.22, and/or Weiss explicitly describe or disclose specific types or aspects of connected or networked devices. *See, e.g.*, Abi-Char at Abstract; ANSI X9.63 Overview at 3, 7, 12, 22; Boyd-Mathuria at 23, 24, 126-131, 175, 177, 190-193; GlobalPlatform at 2; Gouget at [0051]; Haggerty at [0017], [0042], [0131]; Konstantinou at Abstract; Lee at Abstract, [0001], [0107]; Nix at 1:27-33, 4:20-27, 9:42-53, 20:42-49; Park (IEEE) at Abstract, 297, 298; Peirce at Abstract, 3:8-23, 3:64-4:42, 4:43-54, 6:29-65, 7:16-33; SGP.22 at 7, 9, 11, 17, 200; Weiss at [0020], [0031], [0033].

A person skilled in the art would have understood the benefits of applying teachings to specific types or aspects of connected or networked devices, would have recognized that

configuring a system to comprise specific types or aspects of connected or networked devices would provide benefits to the system, and would have been motivated to incorporate these features into a system accordingly. For example, a POSITA would have understood that applying teachings to specific types or aspects of connected or networked devices would broaden the applicability of the disclosed systems. Incorporating specific types or aspects of connected or networked devices would have amounted to a straightforward substitution of one known secure element implementation for another, yielding predictable results. *See, e.g.*, Abi-Char at Abstract ("The increased progress in wireless mobile communication has attracted an important amount of attention on the security issue."), ANSI X9.63 Overview at 3 ("Primarily designed to meet the needs of the financial services industry, but also generally applicable"), Boyd-Mathuria at 193 ("Despite the inexorable increase in the availability of computing resources there has been considerable interest in protocols that can be implemented on devices with limited computational power. Typical examples of such devices are mobile terminals and embedded hardware. Very often the low-power device is a client required to establish a key with a computationally powerful server and so an acceptable solution may have unbalanced computational requirements: the server end can bear an increased computational load in order to ease the burden on the client side. Another technique that is effective is to allow the client side to pre-compute values which can be used during the protocol execution; mobile terminals typically have the opportunity to make off-line computations during the idle time between awaiting calls."), GlobalPlatform at 2 ("For smart cards to reach their true potential, consumers need to be able to use them for a wide variety of functions. For example, the cards can be used with mobile phones to make purchases over the Internet as well as to securely access a PC. Smart cards should also be cost effective and easily multifunctional."), Gouget at [0051] ("It will be well understood that a smartcard with a middle-

ware installed on a smartcard host is not a limited example. The invention can be advantageously applied to any web service deployment with a client-middleware installed in the dubious environment of a smartcard host such as a user's PC.”), Haggerty at [0007] (“Access control is required for secure communication in most prior art wireless radio communication systems.”), Konstantinou at [0001] (“The present subject matter relates to techniques and equipment to select a network for wireless communications … with sufficient flexibility to select between 3GPP2 (1×RTT and EVDO) technologies and 3GPP (LTE/GSM/UMTS) technologies as well as specific operators’ networks for domestic and international roaming so as to allow the operator to optimize roaming agreements in different markets and maximize revenue from roaming.”), Lee at [0011] (“Thus, the present invention aims to provide a method for installing UICC information of various mobile communication operators in an embedded security module (instead of the conventional detachable UICC) remotely through a network.”), Nix at 3:22-27 (“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.”), Park (IEEE) at 297 (“The eUICC was initially considered to be utilized as the same roles of UICC [to] be adopted into the small device … These days, the fields of its usages are being considered to be extended to the CEDs (Consumer Electronic Devices) for the smaller form factor to save the physical space of the device.”), Peirce at 1:13-30 (“As computer electronics continue to reduce in cost and size, the applications for embedded processing devices are continuing to increase, and there now exists many types of manufactured products that contain some type of embedded processing device, whether microprocessor based or otherwise. Some embedded devices are designed to undergo data communication with one or

more external, possibly remote devices. In some cases, it is desirable to establish authenticated, secure data communications in which the exchanged data is encrypted.”), SGP.22 at 7 (“This document defines a technical solution for the remote provisioning and management of the Embedded UICC (eUICC) in consumer Devices as defined in RSP Architecture …. The adoption of this technical solution will provide the basis for global interoperability between different Operator deployment scenarios, for example network equipment (e.g. Subscription Manager Data Preparation (SM-DP+)) and various eUICC platforms.”), Weiss at [0003] (“One particular field of application of secure elements, such as SIMs, eUICCs, UICCs and the like, which is expected to grow rapidly in the near future is M2M (machine-to-machine) communication, i.e. the communication between machines over a cellular communications network without human intervention, also called the Internet of things …. It is foreseeable that at least for some of these devices it will not be possible or at least very difficult to provide the secure element beforehand with the necessary subscription credentials, including for instance an IMSI. This is because in a lot of M2M devices the secure element will most likely be implemented in the form of a surface mounted chip or chip module without the possibility of providing the secure element with the necessary subscription credentials beforehand. Consequently, once in the field, these M2M devices and their non-personalized secure elements require the provision of subscription credentials over-the-air.”). Thus, a person of ordinary skill in the art would have been motivated to modify any of the primary references to include this feature. A person of ordinary skill in the art would also have had a reasonable expectation of success. A person of ordinary skill in the art would have understood that these references disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

IV. U.S. Patent No. 11,606,204 ("the '204 Patent")

A. Identification of Prior Art

Defendants incorporate by reference, as if set forth fully herein, all filings and exhibits from *Inter Partes* Review IPR2026-00115, filed November 7, 2025 with the PTAB, including any subsequent and future filings in that case.

In addition to the prior art cited on the face of the '204 Patent and related patents, the admitted prior art in the specifications of the '204 Patent and related patents, the prior art cited in any file histories, reexaminations, *inter partes* review proceedings, reissue proceedings, or other examination or post-grant proceedings of the '204 Patent and related patents, and the prior art cited in any invalidity contentions or expert reports submitted in any action or proceedings involving the '204 Patent or related patents, Defendants identify the following prior art that anticipates each asserted claim or renders it obvious.

1. Prior Art Patents

The following patents and patent publications are prior art to the asserted claims under at least 35 U.S.C. §§ 102(a)(1) and/or (a)(2), and/or 35 U.S.C. § 103. The identification of any patent or patent publication shall be deemed to include any counterpart patent or application filed, published, or issued anywhere in the world.

Patent or Publication Number	Country of Origin	Filing Date	Date of Issue or Publication
U.S. Pat. App. Pub. No. 2012/0300934 ("Ala-Laurila '934")	United States	August 9, 2012	November 29, 2012
U.S. Pat. App. Pub. No. 2010/0135491 ("Bhuyan '491")	United States	January 22, 2008	June 3, 2010
U.S. Pat. App. Pub. No. 2014/0024343	United States	December 2, 2011	October 10, 2013

Patent or Publication Number	Country of Origin	Filing Date	Date of Issue or Publication
("Bradley '343")			
U.S. Pat. App. Pub. No. 2007/0083766A1 ("Farnham '766")	United States	October 19, 2006	April 12, 2007
U.S. Pat. App. Pub. No. 2013/0301828 ("Gouget '828")	United States	September 6, 2011	November 14, 2013
U.S. Pat. App. Pub. No. 2004/0221163A1 ("Jorgensen '163")	United States	January 16, 2004	November 4, 2004
U.S. Pat. App. Pub. No. 2009/0323967A1 ("Peirce '967")	United States	June 30, 2008	December 31, 2009
U.S. Pat. App. Pub. No. 2009/0068985 ("Nguyen '985")	United States	September 12, 2007	March 12, 2009
U.S. Pat. No. 8,391,841 ("Semple '841")	United States	May 23, 2011	March 5, 2013
PCT Pat. App. Pub. No. WO2008/005162 ("Wang '162")	World Intellectual Property Organization (Patent Cooperation Treaty)	June 14, 2007	January 10, 2007

2. Prior Art Non-Patent Publications

The following non-patent publications are prior art to the asserted claims under at least 35 U.S.C. §§ 102(a)(1) and/or (a)(2), and/or 35 U.S.C. § 103.

Title	Author/Publisher	Date of Publication
A Design of Safe AKA Module for Adapted Mobile Payment System on Openness Smartphone Environment ("Jeong (2010)")	Jeong et al., Journal of Korea Multimedia Society Vol. 13, No. 11	November 2010

Title	Author/Publisher	Date of Publication
ANSI X9.63 Overview: *Key Agreement and Key Transport Using Elliptic Curve Cryptography* ("ANSI X9.63 Overview")	Blake-Wilson, Certicom Corp.	2000
Protocols for Authentication and Key Establishment ("Boyd-Mathuria")	Colin Boyd & Anish Mathuria, Springer	2003
Certicom Research, Standards for Efficient Cryptography, SEC 1: Elliptic Curve Cryptography ("SEC-1")	Brown, Certicom Corp.	May 2009

3. Prior Art Systems

Defendants' investigation into publicly available prior art systems that teach and/or render obvious each element of any asserted claims is ongoing. Fact discovery is at an early stage, and Defendants may require discovery from third parties regarding publicly available prior art systems. On information and belief, prior art systems from the following companies teach and/or render obvious each element of the asserted claims of the '204 Patent: Cinterion (now Telit); Gemalto (now Thales); Giesecke+Devrient; GlobalPlatform; NXP Semiconductors N.V.; Oberthur Technologies (now IDEMIA); and Sierra Wireless. Defendants reserve the right to amend its identification of prior art systems as Defendants become aware of the existence, functionality, and/or characteristics of prior art systems as a result of its investigation and forthcoming discovery. In addition to the prior art products, components, systems, and methods that may be identified as a result of discovery, Defendants also reserve the right to rely on the documents and publications identified in the corresponding claim charts as prior art publications.

B. Primary References

Defendants contend that the primary prior art references identified below and described in the charts attached as Exhibits B-01 to B-09, by themselves, anticipate the asserted claims of

the ’204 Patent. To the extent that a primary reference is deemed not to anticipate a claim for failing to teach one or more limitations of that claim, Defendants contend that the claim would nonetheless have been obvious to a person of ordinary skill in the art at the time of the invention in view of the prior art reference itself, as described in the attached charts. Defendants’ prior art charts (attached as Exhibits B-01 to B-09) set forth the particular claims that are anticipated under 35 U.S.C. § 102 and/or rendered obvious under 35 U.S.C. § 103 by each item of prior art and identify where specifically in each item of prior art, each element of each asserted claim is found.

Exhibit	Primary References
B-01	U.S. Pat. App. Pub. No. 2012/0300934 (“Ala-Laurila ’934”)
B-02	U.S. Pat. App. Pub. No. 2010/0135491 (“Bhuyan ’491”)
B-03	Boyd and Mathuria, *Protocols for Authentication and Key Establishment* (“Boyd-Mathuria”)
B-04	U.S. Pat. App. Pub. No. 2007/0083766A1 (“Farnham ’766”)
B-05	Jeong et al., *A Design of Safe AKA Module for Adapted Mobile Payment System on Openness Smartphone Environment* (“Jeong (2010)”)[4]
B-06	U.S. Pat. App. Pub. No. 2009/0323967A1 (“Peirce ’967”)
B-07	U.S. Pat. App. Pub. No. 2009/0068985 (“Nguyen ’985”)
B-08	U.S. Pat. No. 8,391,841 (“Semple ’841”)
B-09	PCT Pat. App. Pub. No. WO2008/005162 (“Wang ’162”)

C. Secondary References

Exhibit B-A lists secondary prior art references and identifies, on a limitation-by-limitation basis, where specifically each secondary reference teaches the limitations of the asserted claims. To the extent that a primary reference is deemed, by itself, not to anticipate or

[4] Jeong was originally published in Korean. References to Jeong in these contentions are to a certified translation of the original Korean paper. Both the original and the certified translation of Jeong are included in the accompanying document production.

render obvious a claim for failing to teach one or more limitations, the claim would nonetheless have been obvious to a person of ordinary skill in the art at the time of the invention by the combination of the primary reference with one or more of the other primary references listed above and/or the references listed as disclosing those alleged missing limitations in Exhibit B-A.

D. Obvious Combinations

To the extent that a primary reference is deemed, by itself, not to anticipate or render obvious a claim for failing to teach one or more limitations, the claim would nonetheless have been obvious to a person of ordinary skill in the art at the time of the invention by the combination of the primary reference with one or more other primary references and/or the knowledge of someone skilled in the art. For example, a person of ordinary skill in the art would have been motivated to combine any reference in Exhibits B-01 to B-09 with any other reference(s) in Exhibits B-01 to B-09. Such combinations would be achieved, for example, by merely combining the disclosures described in the respective claim charts for each reference.

Defendants also contend that any of the primary references (or combination of primary references) could be combined with any of the secondary references (or combination of secondary references) in Exhibit B-A to render obvious the asserted claims. Such combinations would be achieved by merely combining the disclosures described in the respective claim charts for each reference.

The obviousness combinations are provided in the alternative to Defendants' anticipation contentions and are not to be construed to suggest that any reference included in the combinations is not itself anticipatory.

1. Exemplary Combinations

Below are examples of prior art references that would have been combined by one of ordinary skill in the art at the time of the alleged invention. These combinations are merely examples. The asserted claims of the ’204 Patent are rendered obvious by:

- Semple ’841 in combination with Wang ’162.
- Semple ’841 in combination with Bhuyan ’491 and/or Wang ’162.
- Semple ’841 in combination with Peirce ’967 and/or Wang ’162.
- Semple ’841 in combination with Jorgensen ’163 and/or Wang ’162.
- Semple ’841 in combination with SEC-1 and/or Wang ’162.
- Semple ’841 in combination with Bhuyan ’491, SEC-1, and/or Wang ’162.
- Semple ’841 in combination with Peirce ’967, SEC-1, and/or Wang ’162.
- Semple ’841 in combination with Jorgensen ’163, SEC-1, and/or Wang ’162.
- Ala-Laurila ’934 alone or in combination with one or more of Bhuyan ’491, Boyd-Mathuria, Farnham ’766, Jeong (2010), Nguyen ’985, Peirce ’967, Semple ’841, Wang ’162, Bradley ’343, Gouget ’828, Jorgensen ’163, SEC-1, and/or ANSI X9.63 Overview.
- Bhuyan ’491 alone or in combination with one or more of Ala-Laurila ’934, Boyd-Mathuria, Farnham ’766, Jeong (2010), Nguyen ’985, Peirce ’967, Semple ’841, Wang ’162, Bradley ’343, Gouget ’828, Jorgensen ’163, SEC-1, and/or ANSI X9.63 Overview.
- Boyd-Mathuria alone or in combination with one or more of Ala-Laurila ’934, Bhuyan ’491, Farnham ’766, Jeong (2010), Nguyen ’985, Peirce ’967, Semple

’841, Wang ’162, Bradley ’343, Gouget ’828, Jorgensen ’163, SEC-1, and/or ANSI X9.63 Overview.

- Farnham ’766 alone or in combination with one or more of Ala-Laurila ’934, Bhuyan ’491, Boyd-Mathuria, Jeong (2010), Nguyen ’985, Peirce ’967, Semple ’841, Wang ’162, Bradley ’343, Gouget ’828, Jorgensen ’163, SEC-1, and/or ANSI X9.63 Overview.
- Jeong (2010) alone or in combination with one or more of Ala-Laurila ’934, Bhuyan ’491, Boyd-Mathuria, Farnham ’766, Nguyen ’985, Peirce ’967, Semple ’841, Wang ’162, Bradley ’343, Gouget ’828, Jorgensen ’163, SEC-1, and/or ANSI X9.63 Overview.
- Nguyen ’985 alone or in combination with one or more of Ala-Laurila ’934, Bhuyan ’491, Boyd-Mathuria, Farnham ’766, Jeong (2010), Peirce ’967, Semple ’841, Wang ’162, Bradley ’343, Gouget ’828, Jorgensen ’163, SEC-1, and/or ANSI X9.63 Overview.
- Peirce ’967 alone or in combination with one or more of Ala-Laurila ’934, Bhuyan ’491, Boyd-Mathuria, Farnham ’766, Jeong (2010), Nguyen ’985, Semple ’841, Wang ’162, Bradley ’343, Gouget ’828, Jorgensen ’163, SEC-1, and/or ANSI X9.63 Overview.
- Semple ’841 alone or in combination with one or more of Ala-Laurila ’934, Bhuyan ’491, Boyd-Mathuria, Farnham ’766, Jeong (2010), Nguyen ’985, Peirce ’967, Wang ’162, Bradley ’343, Gouget ’828, Jorgensen ’163, SEC-1, and/or ANSI X9.63 Overview.

- Wang ’162 alone or in combination with one or more of Ala-Laurila ’934, Bhuyan ’491, Boyd-Mathuria, Farnham ’766, Jeong (2010), Nguyen ’985, Peirce ’967, Semple ’841, Bradley ’343, Gouget ’828, Jorgensen ’163, SEC-1, and/or ANSI X9.63 Overview.

2. Motivations to Combine

To the extent a finder of fact finds that a primary prior art reference does not disclose one or more limitations of an asserted claim, the asserted claim is nevertheless obvious because the allege missing limitations contain nothing beyond ordinary improvements. In other words, the asserted claim combines known elements to achieve predictable results or chooses between clear alternatives known to those of skill in the art, particularly in view of the state of the art as reflected in the relevant prior art.

Moreover, as explained above, it would have been obvious to a person of skill in the art at the time of the alleged invention of the asserted claims to combine any primary reference with any combination of other primary references or secondary references so as to practice the asserted claims. To the extent that Plaintiff argues that any concept claimed in the asserted claims is not disclosed in a primary reference, it would, at a minimum, have been obvious to adapt the primary reference to include the concept or combine it with other primary references or secondary references that disclose the concept. Each concept described and claimed in the Asserted Patents was known to those of skill in the art as available design choices for the technologies at issue.[5]

[5] Each concept described and claimed in the ’204 Patent was known to those of skill in the art as available design choices for data encryption technology and/or using such technology to provision and/or authenticate mobile devices for use with a wireless network in a wide range of applications for different scenarios and circumstances.

The Supreme Court has held that "[t]he combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 416 (2007). "When a work is available in one field of endeavor, design incentives and other market forces can prompt variations of it, either in the same field or a different one." *Id*. at 417. As the Supreme Court made clear, "[f]or the same reason, if a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill." *Id*.

To determine whether there is an apparent reason to combine the known elements in the fashion claimed by the patent at issue, a court can "look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art." *Id*. at 418. For example, obviousness can be demonstrated by showing "there existed at the time of invention a known problem for which there was an obvious solution encompassed by the patent's claims." *Id*. at 420. "[A]ny need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed." *Id*. Common sense also teaches that "familiar items may have obvious uses beyond their primary purposes, and in many cases a person of ordinary skill will be able to fit the teachings of multiple patents together like pieces of a puzzle." *Id*.

However, the Supreme Court in *KSR* held that a claimed invention can be obvious even if there is no explicit teaching, suggestion, or motivation for combining the prior art to produce that invention. In summary, *KSR* holds that patents that are based on new combinations of elements or components already known in a technical field may be found to be obvious. *See,*

generally, *KSR*, 550 U.S. 398. Specifically, the Court in *KSR* rejected a rigid application of the "teaching, suggestion, or motivation [to combine]" test. *Id*. at 418. "In determining whether the subject matter of a patent claim is obvious, neither the particular motivation nor the avowed purpose of the patentee controls. What matters is the objective reach of the claim." *Id*. at 419. "Under the correct analysis, any need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed." *Id*. at 420. A key inquiry is whether the "improvement is more than the predictable use of prior art elements according to their established functions." *Id*. at 417.

The rationale to combine or modify prior art references is significantly stronger when, as here, the references seek to solve the same problem, come from the same field, and correspond well to each other. *In re Inland Steel Co*., 265 F.3d 1354, 1362 (Fed. Cir. 2001). The Federal Circuit has held that two references may be combined as invalidating art under similar circumstances, namely "[the prior art] focus[es] on the same problem that the … patent addresses: enhancing the magnetic properties of … steel. Moreover, both [prior art references] come from the same field …. Finally, the solutions to the identified problems found in the two references correspond well." *Id*. at 1364 (concerning patents and prior art relating to improving the magnetic and electrical properties of steel).

In view of the Supreme Court's *KSR* decision, the PTO issued a set of Examination Guidelines. Examination Guidelines for Determining Obviousness Under 35 U.S.C. §103 in view of the Supreme Court Decision in *KSR International Co. v. Teleflex, Inc*., 72 Fed. Reg. 57526 (October 10, 2007). Those Guidelines summarized the *KSR* decision and identified various rationales for finding a claim obvious, including those based on other precedents. Those rationales include:

> (A) Combining prior art elements according to known methods to yield predictable results;
> (B) Simple substitution of one known element for another to obtain predictable results;
> (C) Use of known technique to improve similar devices (methods, or products) in the same way;
> (D) Applying a known technique to a known device (method, or product) ready for improvement to yield predictable results;
> (E) "Obvious to try" – choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success;
> (F) Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations would have been predictable to one of ordinary skill in the art;
> (G) Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention.

Id. at 57529. The above rationales likewise apply in rendering obvious the asserted claims of the Asserted Patents.

The references disclosed herein, alone or in combination, contain an explicit and/or implicit teaching or motivation to combine them due to the following: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference addresses similar problems; and (5) the knowledge of those skilled in the art that the disclosed elements had been or could be used together.

As an example of those reasons and motivations to combine the references, Ala-Laurila '934, Bhuyan '491, Boyd-Mathuria, Farnham '766, Jeong (2010), Nguyen '985, Peirce '967, Semple '841, Wang '162, and the specified secondary references generally relate to encryption technology, and/or using such technology to provision or authenticate a mobile device for use with a wireless network. *See* Exs. B-01 to B-09 and B-A. The references disclose similar

components and techniques for data encryption, and/or using encryption to provision or authenticate mobile devices. *See id.* The attached charts in Exhibits B-01 to B-09 and B-A provide additional reasons and motivations to combine the charted references.

Additionally, the primary and secondary references listed above are analogous art. They are all directed to encryption technology, and in particular, to provisioning and/or authenticating a mobile device for use with a wireless network. *See, e.g.*, Ala-Laurila '934 at Abstract ("Arranging data ciphering in a telecommunication system comprising at least one wireless terminal, a wireless local area network and a public land mobile network. At least one first ciphering key according to the mobile network is calculated in the mobile network and in the terminal for a terminal identifier using a specific secret key for the identifier. Data transmission between the mobile network and the terminal is carried out through the wireless local area network. A second ciphering key is calculated in the terminal and in the mobile network using said at least one first ciphering key. The second ciphering key is sent from the mobile network to the wireless local area network. The data between the terminal and the network is ciphered using said second ciphering key."), [0002] ("The disclosure relates to arranging data ciphering in wireless telecommunication systems and particularly in Wireless Local Area Networks WLAN."); Bhuyan '491 at Abstract ("A method of providing authentication of a mobile device in a telecommunications network comprising the steps of: providing a user defined first password to an authentication server in the communications network; generating a set of security parameters by an authentication server and provisioning the security parameters to a mobile device, wherein the security parameters are stored at the mobile device and wherein the security parameters comprises an encryption key; authenticating the mobile device by challenging the integrity of the encryption key stored at the mobile device and verifying a first response generated

by the mobile device in response to the challenge, wherein verifying comprises comparing by the network whether the first response matches a second response, wherein the first response is based on the encryption key stored at the mobile device and a second password input by the user, and the second response is generated by the network and is based on the encryption key generated by the authentication server and the user defined first password."), [0001] ("The present invention relates to a method of authentication in a telecommunications network, in particular a method of authenticating a mobile device using a network provisioned security module and subsequent secure communications between the mobile device and the network."); Boyd-Mathuria at Chapter 1.2.1 ("The reader is probably already aware of the obvious problem with our first attempt. Nevertheless it is our purpose here to be explicit about our assumptions. The problem is that the session key KAB must be transported to A and B but to no other entities. It is an assumption that the adversary, against whose attacks we are implementing our security, can eavesdrop on all messages that are sent or received. This is a realistic assumption in typical communications systems such as the Internet and corporate networks. Indeed, if this possibility can be discounted then there is probably no need to apply security at all."), Chapter 1.4 ("In this section we highlight the importance of distinguishing the possible different properties that may be provided by cryptographic algorithms. A good understanding of the algorithms and methods of cryptography is highly beneficial in assessing cryptographic protocols…."); Farnham '766 at Abstract ("This invention generally relates to secure communications links for data transmission and more particularly relates to data communications links in which asymmetric cryptographic techniques are used to establish a secure link using symmetric cryptography. A method of establishing a secure communications link between a terminal and a server, the method comprising, assembling a message comprising a secret number and a digital signature for the

secret number, the digital signature being generated using a private key for the server, encrypting the message at the server end of the communications link using a public key for the terminal, sending said encrypted message from the server to the terminal, decrypting said encrypted message at the terminal using a private key for the terminal, validating the message by checking the digital signature using a public key for the server; and establishing said secure communications link using said secret number, wherein the public and private keys for the terminal and server are public and private keys of an asymmetric cryptographic technique. Corresponding software is also provided. The method facilitates fast and if desired, anonymous, download of software to a mobile communications system terminal."); Jeong (2010) at Abstract ("The USIM-based AKA authentication process is essential to a mobile payment system on smart phone environment. In this paper a payment protocol and an AKA module are designed for mobile payment system which is suitable for openness smart phone environment. The payment protocol designs the cross authentication among components of the mobile payment system to improve the reliability of the components. The AKA module of mobile payment system based on 3GPP-AKA protocol prevents the exposure of IMSI by creating the SSK (Shared safe Key) through advance registration and solves the SQN (SeQuence Number) synchronization problem by using timestamp. Also, by using the SSK instead of authentication vector between SN and authentication center, the existing bandwidth (688×N)×R bit between them is reduced to 320×R bit or 368×R bit. It creates CK and IK which are message encryption keys by using OT-SSK (One-Time SSK) between MS and SN. In addition, creating the new OT-SSK whenever MS is connected to SN, it prevents the data replay attack."); Nguyen '985 at Abstract ("A system that incorporates teachings of the present disclosure may include, for example, a server having a controller to implement an Elliptic Curve Diffie-Hellman (ECDH) cryptosystem and manage a

key exchange, authentication, and certificate exchange with a communication device also implementing the ECDH cryptosystem, wherein the server communicates over a network that provides an encrypted communication link for the communication device. Other embodiments are disclosed.”), [0001] (“The present disclosure relates generally to communication systems and more specifically to a method and apparatus for end-to-end mobile user security in a network.”); Peirce ’967 at Abstract (“A system and method for producing cryptographic keys for use by an embedded processing device within a manufactured product. A pseudo random number generator is seeded with entropy data gathered by the embedded device, and the result is used to generate a public-private key pair. The process can be carried out during manufacturing so that the public key of each manufactured product can be stored in a database along with a unique identifier for the embedded device associated with the key. In one particular example, a vehicle having an installed telematics unit uses the key generating process to self-generate keys using entropy data available to the vehicle.”), [0001] (“The present invention relates generally to techniques for generating cryptographic keys used in secure data communications and, in particular, to such techniques used for manufactured products having embedded processing devices.”); Semple ’841 at Abstract (“A mutual authentication method is provided for securely agreeing application-security keys with mobile terminals supporting legacy Subscriber Identity Modules (e.g., GSM SIM and CDMA2000 R-UIM, which do not support 3G AKA mechanisms). A challenge-response key exchange is implemented between a bootstrapping server function (BSF) and mobile terminal (MT). The BSF generates an authentication challenge and sends it to the MT under a server-authenticated public key mechanism. The MT receives the challenge and determines whether it originates from the BSF based on a bootstrapping server certificate. The MT formulates a response to the authentication challenge based on keys derived from the

authentication challenge and a pre-shared secret key. The BSF receives the authentication response and verifies whether it originates from the MT. Once verified, the BSF and MT independently calculate an application security key that the BSF sends to a requesting network application function to establish secure communications with the MT."), 1:23–29 ("The present invention generally relates to systems and methods for securing wireless communications. More specifically, one feature of the invention provides a novel authentication and key agreement scheme for devices supporting legacy network authentication mechanisms, in order to provide application security keys by taking advantage of legacy wireless authentication and key agreement mechanisms."); Wang '162 at Abstract ("A wireless transmit/receive unit (WTRU) includes a control plane (C-plane) packet data convergence protocol (C-PDCP) layer which performs ciphering of a signaling message. The C-PDCP layer is activated upon power up of the WTRU and initial security parameters are loaded to the C-PDCP layer. An initial connection signaling message and a user identity are ciphered using the initial security parameters even before the WTRU is authenticated. The initial security parameters including a ciphering key (CK) may be generated from system information broadcast from the network. The CK may be a public key for asymmetric encryption, and may be selected from a public key set broadcast by or derived from the network system information. An index of the selected public key may be separately encoded. Alternatively, the index may be communicated by using a Diffie-Hellman key exchange method."), [0003] ("More particularly, the present invention is related to a method and apparatus for security protection of an original user identity (ID) in an initial access signaling message in a wireless communication system including third generation (3G) long term evolution (LTE).").

In addition, below are additional motivations to combine prior art for particular claim limitations. The following discussion of specific claim limitations are merely examples and are not limiting.

For example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach using secure methods of authenticating a mobile device with a wireless network employing encryption techniques (in regards to Limitations 1[pre], 1[a], 1[b], 1[g], and 1[h])[6], it would have been obvious to a person of ordinary skill in the art at the time of the invention to combine the primary reference with any of the prior art that disclose Limitations 1[pre], 1[a], 1[b], 1[g], and 1[h] in Exhibits B-01 to B-09 or B-A. For example, several prior art references, including Ala-Laurila '934, Bhuyan '491, Boyd-Mathuria, Farnham '766, Jeong (2010), Nguyen '985, Peirce '967, Semple '841, Wang '162, and Secondary References explicitly describe or using secure methods of authenticating a mobile device with a wireless network. *See, e.g.*, Ala-Laurila '934 at Abstract, [0002]–[0009], [0018]–[0025], Figs. 1–3; Bhuyan '491 at Abstract, [0001]–[0007], [0045]–[0046], [0059], [0062], [0092], Figs 2–3, 5–6; Boyd-Mathuria at Chapters 1.2.2, 1.4.2, 1.6.1, 2.2.2, 3.2, 4.2, 4.3.6, 5.7.1, 6.3.1, A; Farnham '766 at Abstract, [0001]–[0003], [0007]–[0009], [0021], [0032], [0046]–[0051], [0069]–[0071], Figs 1–3; Jeong (2010) at Abstract, Sections 1, 2.2, 5, Figs 1–6; Nguyen '985 at Abstract, [0001]–

[6] Specifically, Limitation 1[pre]: "A mobile device comprising;" Limitation 1[a]: "at least one processor;" Limitation 1[b]: "at least one computer-readable medium operatively connected to the at least one processor and having stored thereon instructions that, when executed by the at least one processor, cause the mobile device to perform a method of authentication with a wireless network, the method comprising;" Limitation 1[g]: "(5) sending a message to a server for the wireless network, the message comprising the module encrypted data and the module public key, wherein the server mutually derives the symmetric ciphering key using at least the module public key, and wherein the wireless network selects the pre-shared secret key for the mobile device using the module identity;" and Limitation 1[h]: "(6) authenticating the mobile device with the wireless network using a message digest with the pre-shared secret key."

[0004], [0024]–[0029], [0036]–[0046], Figs 1–2, 4–6; Peirce ’967 at Abstract, [0001]–[0004], [0019]–[0020], [0037]–[0039], Figs 1–3; Semple ’841 at Abstract, 1:23–2:43, 5:17–62, 7:4–47, 8:4–9:3, Figs. 1, 4–7; Wang ’162 at [0003], [0007]–[0015], [0026]–[0034], Figs. 1–4.

A person skilled in the art would have understood the benefits of using secure methods of authenticating a mobile device with a wireless network (in regards to Limitations 1[pre], 1[a], 1[b], 1[g], and 1[h]), given the well-known and complementary weaknesses in that process, and therefore would have been motivated and had a reasonable expectation of success to incorporate this feature into the device or method for a mobile device application according. *See, e.g.*, Ala-Laurila ’934 at Abstract (“Arranging data ciphering in a telecommunication system comprising at least one wireless terminal, a wireless local area network and a public land mobile network. At least one first ciphering key according to the mobile network is calculated in the mobile network and in the terminal for a terminal identifier using a specific secret key for the identifier. Data transmission between the mobile network and the terminal is carried out through the wireless local area network. A second ciphering key is calculated in the terminal and in the mobile network using said at least one first ciphering key. The second ciphering key is sent from the mobile network to the wireless local area network. The data between the terminal and the network is ciphered using said second ciphering key.”), [0002] (“The disclosure relates to arranging data ciphering in wireless telecommunication systems and particularly in Wireless Local Area Networks WLAN.”), [0025] (“FIG. 2 shows the essential functions according to a preferred embodiment of the invention for authenticating the terminal MT and for calculating a ciphering key. The terminal MT is offered an identifier IMSI and a secret key Ki by the subscriber identity application SIM included therein. The authentication process of the terminal MT is typically triggered when the MT starts setting up a connection 201 (Connection setup) with the

WLAN network WLAN. Then the MT is provided with an IP address through a DHCP server (Dynamic Host Configuration Protocol). Before the terminal MT is allowed to establish a connection with other networks than the network WLAN, the authentication must be performed in an acceptable manner."); Bhuyan '491 at [0003] ("The present invention relates to a method of authentication in a telecommunications network, in particular a method of authenticating a mobile device using a network provisioned security module and subsequent secure communications between the mobile device and the network."), [0003] ("Security provisions, including authentication, under GSM are based upon a key sharing principle, where a secure smart card, a SIM (subscriber identity module), is used to store a secret key that is been preloaded onto the card when the card is made. The secret key is thus shared a priori between the mobile phone and the network operator before any communication is initiated. This shared secret key forms the basis for all subsequent key generation used for authentication and ciphering of communications to and from the mobile phone."), [0059] ("In step 308, the provisioning server 204 makes a request to the authentication server 206 for security module parameters. The authentication server 206 receives the request and generates in response to the request a unique identifier for the mobile device 210 in step 310 as well as a secret key Ki. In this example, the identifier is referred to as the IMSI (international mobile subscriber identity). However, the identity is not restricted to having the limitations and format of a GSM IMSI. The term IMSI is used here to provide a simple reference to the unique identity, which is also associated with the subscriber or user."), [0062] ("In step 318, the provisioning server 204 encrypts and sends a file containing the security parameters IMSI and Ki to the mobile device 210 specified by the mobile number given in step 304. The file is encrypted using the password provided by the user in step 304. Also sent with the encrypted file is the software-based security module. The security module

is an application that is run by the mobile device 210 that executes the various methods used for authentication and ciphering which will be described in more detail below. The security module uses security parameters during its operation and also includes operator specific cryptographic functions such as F1 and F2 described below."); Boyd-Mathuria at Chapter 1.6.1 ("Eavesdropping is perhaps the most basic attack on a protocol. Nearly all protocols address eavesdropping by using encryption. It is obvious that encryption must be used to protect confidential information such as session keys. In certain protocols there may be other information that also needs to be protected. An interesting example is that protocols for key establishment in mobile communications usually demand that the identity of the mobile station remain confidential. Eavesdropping is sometimes distinguished as being a passive attack since it does not require the adversary to disturb the communications of legitimate principals. The other attacks we consider all require the adversary to be active. It should be remembered that many sophisticated attacks include eavesdropping of protocol runs as an essential part."), Chapter 4.3.6 ("MSR Protocol … In the following, the notation SCB is a structure known as the secret certificate of the mobile station, B, which is issued by a trusted central authority. This certificate can be checked by anyone using the public key of the central authority in order to verify the mobile's identity. Unlike a usual public key certificate, this certificate must be kept secret from all other mobile users and eavesdroppers, because it is all that is required to masquerade as B. Protocol 4.26 shows the basic MSR protocol [36]…. 1. A à B : A, KA … 2. B à A: EA(KAB), {B, SCB}KAB … Protocol 4.26: Basic MSR protocol of Beller, Chang and Yacobi. … Upon receiving the base A's public key KA, the mobile uses it to encrypt the session key KAB, and sends the encrypted message to A. The mobile also sends its identity and secret certificate encrypted under KAB to authenticate KAB to the base. The symmetric encryption with KAB in

message 2 is of negligible computational effort compared to the public key encryption in the same message; therefore the computational effort at the mobile is effectively limited to that of modulo squaring of the session key."), Chapter 5.7.1 ("[The] proposed a protocol for use in a wireless environment that is based on the Yacobi-Shmuely protocol, but with a small and significant difference. In Protocol 5.34 the server or base station, A, carries out the exponentiation using U A on behalf of the mobile station, B, with the aim of reducing the computational load on B. Apart from this change in where the computation takes place, the protocol (including the shared secret) is the same as Protocol 5.33."); Farnham '766 at Abstract ("This invention generally relates to secure communications links for data transmission and more particularly relates to data communications links in which asymmetric cryptographic techniques are used to establish a secure link using symmetric cryptography. A method of establishing a secure communications link between a terminal and a server, the method comprising, assembling a message comprising a secret number and a digital signature for the secret number, the digital signature being generated using a private key for the server, encrypting the message at the server end of the communications link using a public key for the terminal, sending said encrypted message from the server to the terminal, decrypting said encrypted message at the terminal using a private key for the terminal, validating the message by checking the digital signature using a public key for the server; and establishing said secure communications link using said secret number, wherein the public and private keys for the terminal and server are public and private keys of an asymmetric cryptographic technique. Corresponding software is also provided. The method facilitates fast and if desired, anonymous, download of software to a mobile communications system terminal."), [0003] ("Secure data transmission is important for m-commerce but, in addition to this, the secure download and installation of software onto mobile

terminals will also be important for multimedia entertainment, telle-medicine, upgrades for programmable mobile terminals, upgrades to different wireless standards, and the like. Reconfigurable mobile terminals are able to provide increased flexibility for end users who can customize the terminals for their personal needs by downloading and installing the desired applications, for example to support different types of radio systems and to allow the integration of different systems. However techniques are needed to protect mobile terminals against hackers maliciously substituting their software for software available from a handset manufacturer, network operator or trusted third party source."), [0046] ("The main objective of both these approaches is to protect terminals against malicious downloaded software. They do not protect against attacks that involve physical modifications of the terminal, such as the replacement of program memory, nor are they are intended to limit the distribution and use of software or to protect a software module against reverse-engineering. The security of the symmetric approach, however, requires that the terminal maintain the secrecy of the cryptographic key that it shares with the ticket server, whereas the asymmetric approach relies on a public-key, i.e. the level of secrecy required to protect the symmetric key is necessary for protecting the public key."); Jeong (2010) at Section 2.2 ("Figure 2 illustrates 3GPP-AKA, the USIM authentication process in the wireless Internet environment. When the USIM/MS identifies itself by sending IMSI (International Mobile Subscriber Identity) or TMSI (Temporary Mobile Subscriber Identity) information to the SN (Serving Network), the SN transmits an authentication data request message and the IMSI/TMSI received from the terminal to the AuC (Authentication Center) of the HN (Home Network), which is the authentication center. The HN generates an authentication vector AV (Authentication Vector) for the received IMSI and transmits it to the SN in response to the authentication data request."), Section 5 ("The user authentication of the mobile payment

protocol proposed in this paper eliminates the possibility of USIM exposure by encrypting and transmitting the USIM from the store to the certifier with each shared secret key, and generates a new session key using the USIM, a random value, the user's master key, the store's master key, and the payment center's master key every time the identity of the user, store, and payment center is verified, so that malicious users cannot attempt to make mobile payments due to the exposure of the previous session key."); Nguyen '985 at Abstract ("A system that incorporates teachings of the present disclosure may include, for example, a server having a controller to implement an Elliptic Curve Diffie-Hellman (ECDH) cryptosystem and manage a key exchange, authentication, and certificate exchange with a communication device also implementing the ECDH cryptosystem, wherein the server communicates over a network that provides an encrypted communication link for the communication device. Other embodiments are disclosed."), [0001] ("The present disclosure relates generally to communication systems and more specifically to a method and apparatus for end-to-end mobile user security in a network."), [0003] ("Although GSM differs significantly from its predecessor technologies with regard to signaling and speech channels, GSM is still vulnerable to basic forms of passive security attack, such as eavesdropping. This is mainly due to a signaling link within the fixed infrastructure part of the GSM signaling network which can expose users' unencrypted phone calls and data to an attacker if the attacker can manage to gain direct access to the signaling network."); Peirce '967 at [0001] ("The present invention relates generally to techniques for generating cryptographic keys used in secure data communications and, in particular, to such techniques used for manufactured products having embedded processing devices."), [0002] ("As computer electronics continue to reduce in cost and size, the applications for embedded processing devices are continuing to increase, and there now exists many types of manufactured products that

contain some type of embedded processing device, whether microprocessor based or otherwise. Some embedded devices are designed to undergo data communication with one or more external, possibly remote devices. In some cases, it is desirable to establish authenticated, secure data communications in which the exchanged data is encrypted. Although various approaches can be used, cryptographic keys are perhaps most commonly used for this purpose. In public key cryptography, a public-private key pair is created with the public key then being available for use by anyone desiring encrypted communication with the holder of the private key. Digital certificates issued by a trusted third party (certificate authority) can also be used to authenticate the public key to a particular entity."), [0039] ("For public-private key pairs, once the keys are generated, the private key is stored in the manufactured product, such as in memory included within the embedded device. This is shown at step 108. Then, the public key is transmitted electronically (for example, wirelessly) from the manufactured product and stored in an external database, step 110. A unique ID of the manufactured product or its embedded device can also be stored in the database and associated with the public key so that subsequent communications can be targeted individually to that particular product. For example, a serial number or MAC address for the embedded device can be used. At this point, the generation of the keys is complete and the manufactured product can be distributed by, for example, transferring possession of the product to another entity."); Semple '841 at 1:23–29 ("The present invention generally relates to systems and methods for securing wireless communications. More specifically, one feature of the invention provides a novel authentication and key agreement scheme for devices supporting legacy network authentication mechanisms, in order to provide application security keys by taking advantage of legacy wireless authentication and key agreement mechanisms."), 8:4–9:3 ("FIG. 5 illustrates a method of authenticating a mobile terminal using a bootstrapping server

function and authentication of the server function according to one embodiment of the invention. This method may be implemented when a network application function wishes to agree on keys with a mobile terminal (MT) prior to initiating a network application transaction. For example, GSM Authentication and Key Agreement (AKA) are based on a challenge-response protocol. A secret key Ki as well as two algorithms A3 and A8 are stored in a Subscriber Identity Module (SIM) inside the MT as well as the network home location register (HLR)/Authentication Center (AuC). The SIM is designed to be tamper-proof and contains secret data and algorithms that cannot be easily read out by a user. A request for a key is generated and sent from the MT, which has a legacy SIM inside, to a bootstrapping server function (BSF) 502. The BSF obtains authentication information for the MT from a network HLR or AuC 504…. The MT verifies whether the authentication challenge originates from the expected BSF based on a bootstrapping server certificate 508…. The authentication response is sent from the MT to the BSF 512. The BSF then verifies the origin of the authentication response based on an independently obtained secret key 514…. In an alternative implementation, the MT may calculate a third key using the one or more secret keys (SRES and Kc obtained from the SIM) and other parameters (obtained from the authentication challenge or response or from the SIM). This third key is then used to formulate the authentication response (e.g., compute the message authentication code). The BSF may also calculate the same key since it knows the same keys and/or parameters as the MT. Thus, the BSF can verify whether the authentication response originated from the MT.”); Wang ’162 at [0013] (“Therefore, it would be desirable to provide a method and system for protecting initial control signaling messages and especially the WTRU identity, (i.e., IMSI), during the initial connection for attachment and authentication procedure.”), [0015] (“The present invention is related to a method and apparatus for security protection of an original user identity in an initial

access signaling message in a wireless communication system including third generation (3G) LTE. A WTRU includes a control plane (C-plane) packet data convergence protocol (C-PDCP) layer which performs ciphering and integrity protection of a signaling message. The C-PDCP layer is activated upon power up of the WTRU and initial security parameters are loaded to the C-PDCP layer. An initial connection signaling message for network attachment, and a user ID, (e.g., an IMSI), are ciphered using the initial security parameters even before the WTRU is authenticated. The initial security parameters are loaded from a universal subscriber identity module (USIM) and generated from system information broadcast from the network. The system information includes a public key set with at least one public key for asymmetric encryption of the IMSI or information from which the public key(s) can be derived. The initial security parameters for ciphering include a CK. The CK may be a public key or may be selected from the public key set broadcast by or derived from the network system information. An index of the selected public key may be separately encoded. Alternatively, the index may be communicated by using a Diffie-Helhnan key exchange method."), [0031] ("The NAS layer 211 triggers an RRC connection by sending an attach message along with an IMSI to the RRC layer 212 (step 308). The RRC layer 212 sends an LTE RRC connection request to the C-PDCP layer 213 including the attach message and MAC-I and preferably a public land mobile network (PLMN) identity (ID) (step 310). The C-PDCP layer 213 then performs ciphering on the attach message and the IMSI with the initial CK (from USIM or system information broadcast), and sends an LTE RRC connection request message including ciphered attach message and IMSI along with the MAC-I from the RRC layer 212 (steps 312, 314). Unlike the conventional attachment procedure, the attach message and the IMSI are protected with initial CK and IK."). Thus, a person of ordinary skill in the art would have been motivated to modify any of the primary

references to include this feature. A person of ordinary skill in the art would also have had a reasonable expectation of success. A person of ordinary skill in the art would have understood that these references disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach using encryption techniques and a symmetric key to encrypt and decrypt module identity for a mobile device for submission to a server or a mobile network (in regards to Limitations 1[pre], 1[a], 1[b], 1[e], 1[f], and 1[g])[7], it would have been obvious to a person of ordinary skill in the art at the time of the invention to combine the primary reference with any of the prior art that disclose Limitations 1[pre], 1[a], 1[b], 1[e], 1[f], and 1[g] in Exhibits B-01 to B-09 or B-A. For example, several prior art references, including Ala-Laurila '934, Bhuyan '491, Boyd-Mathuria, Farnham '766, Jeong (2010), Nguyen '985, Peirce '967, Semple '841, Wang '162, and Secondary References explicitly describe or disclose using encryption techniques and a symmetric key to encrypt and decrypt the subscriber identity for a mobile device for submission to the mobile network. *See, e.g.*, Ala-Laurila '934 at Abstract, [0002]–[0007],

[7] Specifically, Limitation 1[pre]: "A mobile device comprising;" Limitation 1[a]: "at least one processor;" Limitation 1[b]: "at least one computer-readable medium operatively connected to the at least one processor and having stored thereon instructions that, when executed by the at least one processor, cause the mobile device to perform a method of authentication with a wireless network, the method comprising;" Limitation 1[e]: "(3) deriving a symmetric ciphering key using (i) an elliptic curve integrated encryption scheme with the server public key and the module private key and (ii) an American National Standards Institute standard X-9.63 key derivation function;" Limitation 1[f]: "(4) generating a module encrypted data using the symmetric ciphering key and the symmetric ciphering algorithm, wherein the module encrypted data includes the module identity;" and Limitation 1[g]: "(5) sending a message to a server for the wireless network, the message comprising the module encrypted data and the module public key, wherein the server mutually derives the symmetric ciphering key using at least the module public key, and wherein the wireless network selects the pre-shared secret key for the mobile device using the module identity."

[0022]–[0028], Figs.1–3; Bhuyan ’491 at Abstract, [0001]–[0006], [0045]–[0051], Figs. 2–3, 5–6; Boyd-Mathuria at Chapters 1.4, 1.6.1, 2.3, 3.4, 4.3.6, A; Farnham ’766 at Abstract, [0001]–[0009], [0021], [0027]–[0032], [0046]–[0051], [0069]–[0071], Figs. 1–3; Jeong (2010) at Abstract, Sections 2.2, 3.1.2, 3.2, 4.1.2, 5, Figs. 4–6; Nguyen ’985 at Abstract, [0001]–[0004], [0012]–[0024], [0036]–[0046], Figs. 1–2, 4–6; Peirce ’967 at Abstract, [0001]–[0004], [0034]–[0041] Figs. 1–3; Semple ’841 at Abstract, 1:23–2:43, 9:19-10:43, 10:44-11:35, Figs. 1–3, 6–7; Wang ’162 at [0003], [0012]–[0015], [0031]–[0042], Figs. 1–4.

A person skilled in the art would have understood the benefits of using encryption techniques and a symmetric key to encrypt and decrypt the subscriber identity for a mobile device for submission to a server or a mobile network (in regards to Limitations 1[pre], 1[a], 1[b], 1[e], 1[f], and 1[g]), given the well-known and complementary confidentiality and security considerations in that process, and therefore would have been motivated and had a reasonable expectation of success to incorporate this feature into the device or method for a mobile device application according. *See, e.g.*, Ala-Laurila ’934 at [0004] (“However, a problem in some wireless telecommunication networks, such as IEEE802.11 WLAN networks, is that the ciphering keys used for ciphering traffic must be stored in advance in the terminal and access point. If the network does not have the same key as the terminal, then the data between the network and the terminal cannot be ciphered. To add different ciphering keys is difficult, and a safe data transmission cannot always be offered for terminals moving in different networks.”), [0025]–[0026] (“FIG. 2 shows the essential functions according to a preferred embodiment of the invention for authenticating the terminal MT and for calculating a ciphering key. The terminal MT is offered an identifier IMSI and a secret key Ki by the subscriber identity application SIM included therein. The authentication process of the terminal MT is typically triggered when the

MT starts setting up a connection 201 (Connection setup) with the WLAN network WLAN. Then the MT is provided with an IP address through a DHCP server (Dynamic Host Configuration Protocol). Before the terminal MT is allowed to establish a connection with other networks than the network WLAN, the authentication must be performed in an acceptable manner. The MT requests 202 (IMSI request) the identity module SIM for the IMSI identifier and the SIM returns 203 the IMSI identifier. The MT sends 204 the authentication starting request (MT_PAC_AUTHSTART_REQ) which preferably comprises a Network Access Identifier NAI. The NAI comprises the IMSI identifier obtained from the identity module SIM. The NAI may be presented, for example, in the form 12345@GSM.org, where 12345 is the IMSI identifier and GSM.org is the domain name of the mobile network, which has conveyed the identity module SIM. The request 204 is preferably sent in ciphered form to the PAC using the Diffie-Hellman algorithm, for example. The MT preferably also sends a specific protection code MT_RAND in the request 204, said code typically being a challenge code. Using the protection code MT_RAND the MT may later be ensured that the party conveying the GSM triplets actually has access to the secret key Ki, which is to be maintained in the GSM home network of the subscriber. However, the use of the protection code is not obligatory.”); Bhuyan ’491 at [0001]–[0006] (“The present invention relates to a method of authentication in a telecommunications network, in particular a method of authenticating a mobile device using a network provisioned security module and subsequent secure communications between the mobile device and the network. Security in communication systems has always been important and mobile cellular communication systems have been no different. In early ‘first generation’ analogue mobile phone systems, a third party could eavesdrop on the communications between a mobile terminal and the mobile network relatively easily over the radio interface. These problems were partly

mitigated when 'second generation' digital systems, such as GSM (Global System for Mobile communications), were adopted by mobile operators. Security provisions, including authentication, under GSM are based upon a key sharing principle, where a secure smart card, a SIM (subscriber identity module), is used to store a secret key that is been preloaded onto the card when the card is made. The secret key is thus shared a priori between the mobile phone and the network operator before any communication is initiated. This shared secret key forms the basis for all subsequent key generation used for authentication and ciphering of communications to and from the mobile phone. The SIM also holds other data as well as the shared secret key, commonly referred to as Ki, such as SIM applications, encryption algorithms, and user identifiers such as the IMSI (International mobile subscriber identity). SIM cards have been proven to be reasonably secure and tamper-proof and have been commonly used in both GSM and 3G mobile telecommunications networks for some time. However, SIM cards suffer from a number of drawbacks. In particular, provisioning of SIM cards is a complex process brought about by having to manufacture the tamper resistant modules, initialising the cards with the requisite data (IMSI, Ki and operator secrets) and then distributing and handling of the physical cards to the subscriber. Furthermore, most mobile devices these days also only have the capacity to use a single SIM card, and thus access to networks is limited to those allowed by the single SIM. The few devices that can handle multiple SIM cards are rare and are usually more complex and costly to manufacture as well as being more difficult to use."); Boyd-Mathuria at Chapter 1.4 ("Confidentiality ensures that data is only available to those authorised to obtain it. This is usually achieved through encryption of the data so that only those with the correct decryption key can recover it. In cryptographic protocols confidentiality is essential to ensure that keys and other data are available only as intended."), Chapter 4.3.6 ("MSR Protocol…In the following, the

notation *SCB* is a structure known as the *secret certificate* of the mobile station, *B,* which is issued by a trusted central authority. This certificate can be checked by anyone using the public key of the central authority in order to verify the mobile's identity. Unlike a usual public key certificate, this certificate must be kept secret from all other mobile users and eavesdroppers, because it is all that is required to masquerade as *B.* Protocol 4.26 shows the basic MSR protocol [36]…. 1. $A \rightarrow B : A, K_A$ … 2. $B \rightarrow A: E_A(K_{AB}), \{B, SC_B\}K_{AB}$ … Protocol 4.26: Basic MSR protocol of Beller, Chang and Yacobi. … Upon receiving the base *A's* public key K_A, the mobile uses it to encrypt the session key K_{AB}, and sends the encrypted message to *A.* The mobile also sends its identity and secret certificate encrypted under K_{AB} to authenticate K_{AB} to the base. The symmetric encryption with K_{AB} in message 2 is of negligible computational effort compared to the public key encryption in the same message; therefore the computational effort at the mobile is effectively limited to that of modulo squaring of the session key."); Farnham '766 at Abstract ("This invention generally relates to secure communications links for data transmission and more particularly relates to data communications links in which asymmetric cryptographic techniques are used to establish a secure link using symmetric cryptography. A method of establishing a secure communications link between a terminal and a server, the method comprising, assembling a message comprising a secret number and a digital signature for the secret number, the digital signature being generated using a private key for the server, encrypting the message at the server end of the communications link using a public key for the terminal, sending said encrypted message from the server to the terminal, decrypting said encrypted message at the terminal using a private key for the terminal, validating the message by checking the digital signature using a public key for the server; and establishing said secure communications link using said secret number, wherein the public and private keys for the terminal and server are public and private

keys of an asymmetric cryptographic technique. Corresponding software is also provided. The method facilitates fast and if desired, anonymous, download of software to a mobile communications system terminal.”), [0001] (“This invention generally relates to secure communications links for data transmission and more particularly relates to data communications links in which asymmetric cryptographic techniques are used to establish a secure link using symmetric cryptography.”), [0007] (“A Public Key Infrastructure normally includes provision for digital identity Certificates. To prevent an individual posing as somebody else an individual may prove his identity to a certification authority which then issues a certificate signed using the authority’s private key and including the public key of the individual. The Certification Authority’s public key is widely known and therefore trusted and since the certificate could only have been encrypted using the authority's private key, the public key of the individual is verified by the certificate. Within the context of a mobile phone network a user or the network operator can authenticate their identity by signing a message with their private key; likewise a public key can be used to verify an identity. Further details of PKI for wireless applications can be found in WPKI, WAP-217-WPKI, version 24—April 2001 available at www.wapforum.org and in the X.509 specifications (PKIX) which can be found at www.ietf.org, all hereby incorporated by reference.”); Jeong (2010) at Section 3.2 (“(1) In the existing AKA, we need to solve the privacy problem and the synchronization problem of SQN by transmitting the IMSI plaintext of the terminal. Therefore, the IMSI, T_{MS}(timestamp), and SN_{ID} located near the terminal are concatenated to generate the authentication value of the MS using the function $f^1_K()$. Also, E-$IMSI_{MS}$, MAC_{MS}, HN_{ID}, and T_{MS}, which are values encrypted with $SSK_{MS\text{-}HN}$, a shared secret key between HN and MS, are transmitted to the SN located near the MS. … $MAC_{MS} = f^1 SSK_{MS\text{-}HN}$ ($IMSI_{MS}$ || T_{MS} || SN_{ID}) … E- $IMSI_{MS}$ = E($SSK_{MS\text{-}HN}$, $IMSI_{MS}$) … (2) The SN forwards the

received E-IMSI$_{MS}$, MAC$_{MS}$, T$_{MS}$ to the corresponding certificate authority (HN)."), Section 5 ("With the rapid development of communication and the widespread use of the Internet, many people are frequently accessing remote servers in a distributed computing environment, but data transmission over insecure channels without an authenticated protection system is exposed to many problems such as replay attacks, offline password attacks, and impersonation attacks. In this paper, we design a safe Authentication Key Agreement (AKA) module for mobile payment system suitable for openness smartphone environment that can solve these problems. The AKA module proposed in this paper prevents IMSI exposure by generating a shared secret key between the MS and the HN for user authentication and encrypting and transmitting the IMSI value of the USIM, and prevents data replay attack by generating a new OT-SSK for each connection by generating message encryption keys, CK and IK, using a one-time shared secret key, OT-SSK, between the MS and SN."); Nguyen '985 at Abstract ("A system that incorporates teachings of the present disclosure may include, for example, a server having a controller to implement an Elliptic Curve Diffie-Hellman (ECDH) cryptosystem and manage a key exchange, authentication, and certificate exchange with a communication device also implementing the ECDH cryptosystem, wherein the server communicates over a network that provides an encrypted communication link for the communication device. Other embodiments are disclosed."), [0001] ("The present disclosure relates generally to communication systems and more specifically to a method and apparatus for end-to-end mobile user security in a network."), [0016] ("The MS 116 can include an identification module 118, such as a secure identification or identity module (e.g., a SIM card), containing subscription information, account data, personal information, and private/public key information. The identification module 118 can have an associated memory (not shown) for storing data associated with a private key. The private key

can be used to generate a public key which can be used to securely encrypt data. The private key is kept secret, while the public key may be widely distributed. The keys are related mathematically, but the private key cannot be practically derived from the public key. Data encrypted with the public key can be decrypted only with the corresponding private key. This can be used to ensure confidentiality. Data signed with the sender's private key can be verified by anyone who has access to the sender's public key, thereby proving that the sender signed it and that the message has not been tampered with. This can be used to ensure authenticity.”), [0020] (“ECC is an approach to public-key cryptography based on an algebraic structure of elliptic curves over finite fields. An elliptic curve is a plane curve defined by an equation of the form $y^2=x^3+ax+b$. The set of points on such a curve can be shown to form a commutative group G, such that a*b=b*a for all a and b in G. Elliptic Curve Diffie-Hellman (ECDH) is a key agreement protocol that allows the two MSs to establish a shared secret key over an insecure channel. The secret key can then be used to encrypt subsequent communications using a symmetric key cipher.”); Peirce ’967 at Abstract (“A system and method for producing cryptographic keys for use by an embedded processing device within a manufactured product. A pseudo random number generator is seeded with entropy data gathered by the embedded device, and the result is used to generate a public-private key pair. The process can be carried out during manufacturing so that the public key of each manufactured product can be stored in a database along with a unique identifier for the embedded device associated with the key. In one particular example, a vehicle having an installed telematics unit uses the key generating process to self-generate keys using entropy data available to the vehicle.”), [0001] (“The present invention relates generally to techniques for generating cryptographic keys used in secure data communications and, in particular, to such techniques used for manufactured products having

embedded processing devices.”), [0039] (“For public-private key pairs, once the keys are generated, the private key is stored in the manufactured product, such as in memory included within the embedded device. This is shown at step 108. Then, the public key is transmitted electronically (for example, wirelessly) from the manufactured product and stored in an external database, step 110. A unique ID of the manufactured product or its embedded device can also be stored in the database and associated with the public key so that subsequent communications can be targeted individually to that particular product. For example, a serial number or MAC address for the embedded device can be used. At this point, the generation of the keys is complete and the manufactured product can be distributed by, for example, transferring possession of the product to another entity.”); Semple ’841 at 1:23–29 (“The present invention generally relates to systems and methods for securing wireless communications. More specifically, one feature of the invention provides a novel authentication and key agreement scheme for devices supporting legacy network authentication mechanisms, in order to provide application security keys by taking advantage of legacy wireless authentication and key agreement mechanisms.”), 9:35–59 (“In one embodiment, a request for authentication keys may be initiated by MT 606 retrieving its associated International Mobile Subscriber Identity (IMSI) 600 from its SIM 608 and sending it to a bootstrapping server function (BSF) 604. The BSF 604 sends the IMSI 600 to the HLR 602 where it may verify whether the IMSI 600 belongs to a MT that subscribes to the network. The HLR 602 may be operated by the service provider for the subscriber whose SIM is contained in MT 606. The HLR 602 selects, for example, a 128-bit random challenge RAND and together with pre-shared secret key Ki, uses them as inputs for two algorithms A3 and A8 to yield 32-bit output signed response SRES and 64-bit output secret confidentiality key Kc, respectively. The HLR 602 then provides the triplets (RAND, SRES, Kc) to the BSF 604, corresponding to the

identity IMSI 600 of SIM 608. The BSF 604 generates a random secret exponent x and computes a Diffie-Hellman public key P^x, where P is a generator of a cyclic group previously provisioned to both the BSF 604 and MT 606, such as the multiplicative group of a finite field or the additive group of an elliptic curve. The BSF 602 then sends a triplet (RAND, P^x, SIG) 610 to the MT 606, where SIG is a digital signature computed using the BSF 604 RSA private key. The message 610 may be further enhanced to include other server-authenticated parameters such as a transaction identifier."); Wang '162 at [0003] ("More particularly, the present invention is related to a method and apparatus for security protection of an original user identity (ID) in an initial access signaling message in a wireless communication system including third generation (3G) long term evolution (LTE)."), [0012]–[0013] ("For the process illustrated in Figure 1, the RRC connection request message with the IMSI, the RRC setup request message, the RRC setup complete message, the initial direct transfer message with an optional IMSI, the authentication request message and the authentication response message are not protected, but transmitted in an open environment unprotected. The fact that the important WTRU identity, (i.e., IMSI), is sent over the air unprotected provokes an 'IMSI catching threat.' The caught IMSI could be used by a malignant denial of service (DoS) attack or other possible attacks to the network and users. Therefore, it would be desirable to provide a method and system for protecting initial control signaling messages and especially the WTRU identity, (i.e., IMSI), during the initial connection for attachment and authentication procedure."). Thus, a person of ordinary skill in the art would have been motivated to modify any of the primary references to include this feature. A person of ordinary skill in the art would also have had a reasonable expectation of success. A person of ordinary skill in the art would have understood that these references disclose interrelated

teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach using a message digest for device authentication in a mobile/tele-communications context (in regards to Limitations 1[pre], 1[a], 1[b], and 1[h])[8], it would have been obvious to a person of ordinary skill in the art at the time of the invention to combine the primary reference with any of the prior art that disclose Limitations 1[pre], 1[a], 1[b], and 1[h] in Exhibits B-01 to B-09 or B-A. For example, several prior art references, including Ala-Laurila '934, Bhuyan '491, Boyd-Mathuria, Farnham '766, Jeong (2010), Nguyen '985, Peirce '967, Semple '841, Wang '162, and Secondary References explicitly describe or disclose using a message digest for device authentication with the mobile network. *See, e.g.*, Ala-Laurila '934 at Abstract, [0002]–[0009], [0016]–[0018], [0022]–[0031], [0039]–[0047] Figs 1–5; Bhuyan '491 at Abstract, [0001]–[0006], [0045]–[0052], [0074]–[0091], Figs. 1, 3–4, 6; Boyd-Mathuria at Chapters 1.4, 1.4.2, 1.4.4, 1.6.1, 1.6.2, 2.3, 2.3.1, 2.6.4, 3.3.2, 3.3.3, 3.3.4, 4.3.5, 3.4, 4.3.6, 5.4.8, A; Farnham '766 at Abstract, [0001]–[0009], [0012]–[0018], [0041]–[0045], [0051]–[0052], [0069]–[0075], [0083]–[0087], Figs. 1–3; Jeong (2010) at Abstract, Sections 1, 2, 2.1, 2.2, 3.1.2, 3.2, 4.1.1, 5, Figs. 2, 4–6; Nguyen '985 at Abstract, [0001]–[0004], [0012]–[0024], [0036]–[0046], Figs. 1–2, 4–6; Peirce '967 at Abstract, [0001]–[0014], [0034]–[0042], Figs. 1–3; Semple

[8] Specifically, Limitation 1[pre]: "A mobile device comprising;" Limitation 1[a]: "at least one processor;" Limitation 1[b]: "at least one computer-readable medium operatively connected to the at least one processor and having stored thereon instructions that, when executed by the at least one processor, cause the mobile device to perform a method of authentication with a wireless network;" and Limitation 1[h]: "(6) authenticating with the wireless network using a message digest with the pre-shared secret key."

’841 at Abstract, 1:23–2:43, 7:4–58, 8:30–9:18, 9:60–10:24, Figs. 3–6; Wang ’162 at [0003]–[0015], [0027]–[0036], [0045]–[0051], [0064]–[0066], Figs. 1–7.

A person skilled in the art would have understood the benefits of using a message digest for device authentication in a mobile/tele-communications context (in regards to Limitations 1[pre], 1[a], 1[b], and 1[h]), given the well-known and complementary confidentiality and security considerations in that process, and therefore would have been motivated and had a reasonable expectation of success to incorporate this feature into the device or method for a mobile device application according. *See, e.g.*, Ala-Laurila ’934 at [0002] (“The disclosure relates to arranging data ciphering in wireless telecommunication systems and particularly in Wireless Local Area Networks WLAN.”), [0008] (“According to a preferred embodiment of the invention at least one authentication response according to the mobile network is calculated in the terminal and in the mobile network on the basis of at least one challenge code and a ciphering key. A check response is calculated in the terminal on the basis of at least one authentication response and the first ciphering key. The check response is sent to the mobile network. The check response is calculated in the mobile network on the basis of at least one authentication response and at least one first ciphering key. The check response sent by the terminal is compared with the check response calculated by the mobile network. The second ciphering key is sent from the mobile network to the wireless local area network, if the check response sent by the terminal and calculated by the mobile network correspond with one another. This embodiment provides the advantage that a subscriber (identity module) can be reliably authenticated in the mobile network. Consequently a data transmission connection and data ciphering can be allowed only for the authenticated terminals in the wireless local area networks.”), [0031]–[0032] (“The GAGW sends 210 the PAC an acknowledgment message of the authentication request

GAGW_PAC_AUTHSTART_RESP comprising one or more challenge codes RAND for the terminal MT and preferably also a check sum SIGNrand. This message may also include data associated with billing. The message can also be ciphered using the protection code MT-RAND. The PAC sends 211 the terminal MT an acknowledgment message of the authentication request PAC MT_AUTHSTART_RESP comprising at least one challenge code RAND and preferably the check sum SIGNrand. The terminal MT feeds 212 the challenge code/s RAND into the identity module SIM. The SIM calculates 213 (Calculate Kc(s)) at least one first ciphering key Kc according to the mobile network GSMNW and an authentication response (responses) SRES in a manner that corresponds with the one used in the authentication center AuC and transmits 214 these to the other parts of the terminal MT (preferably to the control means CM carrying out authentication and the calculation of the second ciphering key K). The MT can check 215 (Check SIGNrand) the check sum SIGNrand sent by the PAC on the basis of the data (Kc) obtained from the SIM and the protection code MT_RAND. If the received SIGNrand corresponds with the value obtained on the basis of the Kc values calculated by the identity module SIM, the MT, or to be more precise, the CM calculates 216 (Calculate SIGNsres) the check response SIGNsres to be transmitted to the GAGW. The SIGNsres is preferably a hash function calculated from one or more first ciphering keys Kc and authentication responses SRES enabling the GAGW to authenticate the MT. The MT may also request the user to approve the billing data possibly sent by the PAC.”); Bhuyan ’491 at Abstract (“A method of providing authentication of a mobile device in a telecommunications network comprising the steps of: providing a user defined first password to an authentication server in the communications network; generating a set of security parameters by an authentication server and provisioning the security parameters to a mobile device, wherein the security parameters are stored at the mobile device and wherein the security

parameters comprises an encryption key; authenticating the mobile device by challenging the integrity of the encryption key stored at the mobile device and verifying a first response generated by the mobile device in response to the challenge, wherein verifying comprises comparing by the network whether the first response matches a second response, wherein the first response is based on the encryption key stored at the mobile device and a second password input by the user, and the second response is generated by the network and is based on the encryption key generated by the authentication server and the user defined first password.”), [0001] (“The present invention relates to a method of authentication in a telecommunications network, in particular a method of authenticating a mobile device using a network provisioned security module and subsequent secure communications between the mobile device and the network.”), [0074]–[0085] (“The authentication server then generates a triplet comprising a random number RAND, an expected response SRES and a key Kc in step 612. Each of these parameters is generated in accordance with the methods…. The values generated for RAND, SRES and Kc are then sent to the access server 506 in step 612…. The access server 506 then uses the received SRES from the authentication server 206 and the password from the data store 208 to generate an adapted expected response SRES1. This is done using cryptographic algorithm F1 taking SRES and the password as inputs and outputting SRES1…. The output generated is SRES 404. This value of SRES 404 is the one transferred from the authentication server 206 to the access server 506 in step 612. The generation of SRES is performed by the authentication server 206 in step 610…. Once the access server 506 has received SRES 404, it calculates SRES1412…. Specifically, SRES 404 is fed into cryptographic algorithm F1 together with the password 406 received from the data store 208…. This value of RAND is taken by the security module application in the mobile device 210 and is sued by the security module to determine the expected response SRES1

and ciphering key Kc1…. Specifically, the methods used to calculate SRES1 and Kc1 used by the security module are the same as those used by the combination of the access server 506 and authentication server 206…. The value of Ki used is the one stored on the mobile device and obtained from the decrypted file in step 604. This is combined with the received value of RAND using to A3 and A8 algorithms to generate SRES and Kc respectively. These are then fed into the F1 and F2 functions together with the password input in step 602 to get SRES1 and Kc1…. The mobile device 210 then sends of the value of SRES1 calculated by the security module to the access server 506 in step 624. The access server 506 then checks the value of SRES1 received from the mobile device 210 with the value of SRES1 calculated itself in step 618. If the two values match, then the mobile device is authenticated and the access server 506 sends the mobile device 210 a SUCCESS message in step 628."); Boyd-Mathuria at Chapter 1.4 ("Data Integrity ensures that data has not been altered by unauthorised entities. This can be achieved through use of hash functions in combination with encryption, or by use of a message authentication code to create a separate check field. Data integrity is essential in most cryptographic protocols to protect elements such as identity fields and nonces."), Chapter 1.4.2 ("*A message authentication code (MAC) is a family of functions parametrised by a key K such that* $MAC_K(m)$ *takes a message m of arbitrary length and outputs a fixed length value and satisfying: 1. it is computationally easy to calculate* $MAC_K(m)$ *given K and m; 2. given any number of MAC values for a given K, it is computationally hard to find any valid MAC value for any new message.* The second mechanism for providing data origin authentication and data integrity is to append a MAC to a message which may be either in plaintext or encrypted. On receipt of the MAC, the recipient who has the correct key is able to recompute the MAC from the message and verify that it is the same as that received." (emphasis in original)), Chapter 1.6.2 ("If any protocol message field is not redundant

then modification of it is a potential attack. Use of cryptographic integrity mechanisms is therefore pervasive in protocols for authentication and key establishment."), Chapter 2.3.1 ("*Key confirmation of A to B is provided if B has assurance that key K is a good key to communicate with A, and that principal A has possession of K.* Key confirmation provides evidence that the partner has the same key but leaves open the possibility that the key is intended by the partner for a different communication session (with the assumption that the partner may be engaged in several conversations). Key confirmation provides evidence that the partner wishes to communicate with some entity, so implies far-end operative, but may not imply entity authentication. Key confirmation is typically achieved by having both parties send each other some fresh data using a cryptographic function depending on the key; this is often referred to as a *handshake*." (emphasis in original)); Farnham '766 at [0001] ("This invention generally relates to secure communications links for data transmission and more particularly relates to data communications links in which asymmetric cryptographic techniques are used to establish a secure link using symmetric cryptography."), [0005]–[0006] ("Asymmetric or so-called public key cryptography uses a pair of keys one "private" and one "public" (although in practice distribution of the public key is also often restricted). A message encrypted with the public key can only be decrypted with the private key, and vice-versa. An individual can thus encrypt data using the private key for decryption by any one with the corresponding public key and, similarly, anyone with the public key can securely send data to the individual by encrypting it with the public key safe in the knowledge that only the private key can be used to decrypt the data. Asymmetric cryptographic systems are generally used within an infrastructure known as Public Key Infrastructure (PKI) which provides key management functions. Asymmetric cryptography can also be used to digitally sign messages by encrypting either the message or a message digest,

using the private key. Providing the recipient has the original message they can compute the same digest and thus authenticate the signature by decrypting the message digest. A message digest is derived from the original message and is generally shorter than the original message making it difficult to compute the original message from the digest; a so-called hash function may be used to generate a message digest.”), [0075] (“Upon decrypting M3, B checks the key k2 recovered from M3 agrees with that sent in M2. The session key may be computed as $f(k_1 \| k_2)$ using an appropriate publicly known non-reversible function f such as MD5 (Message Digest 5, as defined in RFC 1321) and SHA-1 (secure Hash Algorithm-1, see, for example, US National Bureau of Standards Federal Information Processing Standards (FIPS) Publication 180-1.”); Jeong (2010) at Section 1 (“Currently, the 3rd Generation Partnership Project (3GPP) has established the 3GPP-Authentication Key Agreement (3GPP-AKA) standard to provide user authentication, encryption, and message integrity in mobile environments, but the 3GPP-AKA protocol has been criticized for problems such as synchronization issues with SQN (SeQuence number) and attacks using false base stations, privacy issues due to plaintext transmission of IMSI (International Mobile Subscriber Identity), a permanent identifier of the device, and authentication data overhead due to the use of multiple authentication vectors [3, 4, 5].”), Section 2.2 (“Figure 2 illustrates 3GPP-AKA, the USIM authentication process in the wireless Internet environment. When the USIM/MS identifies itself by sending IMSI (International Mobile Subscriber Identity) or TMSI (Temporary Mobile Subscriber Identity) information to the SN (Serving Network), the SN transmits an authentication data request message and the IMSI/TMSI received from the terminal to the AuC (Authentication Center) of the HN (Home Network), which is the authentication center. The HN generates an authentication vector AV (Authentication Vector) for the received IMSI and transmits it to the SN in response to the authentication data request.

The SN selects one of the AVs, generates a random number to extract the authentication token (AUTN) in the AV, and attempts to authenticate the user on the device. The device authenticates this data using the network authentication algorithm of the USIM and transmits a user authentication response to the SN, while generating encrypted session keys CK and IK. The SN authenticates the device and the user by comparing the received RES with the XRES it has stored, and then generates a session key to be used for encrypting the user's data, completing the authentication and key agreement process [10,11,12].”); Nguyen ’985 at [0001] (“The present disclosure relates generally to communication systems and more specifically to a method and apparatus for end-to-end mobile user security in a network.”), [0016] (“The MS 116 can include an identification module 118, such as a secure identification or identity module (e.g., a SIM card), containing subscription information, account data, personal information, and private/public key information. The identification module 118 can have an associated memory (not shown) for storing data associated with a private key. The private key can be used to generate a public key which can be used to securely encrypt data. The private key is kept secret, while the public key may be widely distributed. The keys are related mathematically, but the private key cannot be practically derived from the public key. Data encrypted with the public key can be decrypted only with the corresponding private key. This can be used to ensure confidentiality. Data signed with the sender's private key can be verified by anyone who has access to the sender's public key, thereby proving that the sender signed it and that the message has not been tampered with. This can be used to ensure authenticity.”), [0040]–[0041] (“For example, VLR_1 at step 514 can generate a random number RAND and then encrypt the random number with A_1 to produce an encrypted RAND. VLR_1 can then proceed to send the encrypted RAND to MS_1. At step 516, MS_1 decrypts the encrypted RAND using A_1 to get RAND. MS_1, can apply a message digest

algorithm SHA-1 to RAND to produce a signed response SRES=SHA-1 (RAND), and then sends SRES to VLR_1. VLR_1 can also carry out its own computation of SRES using the same message digest algorithm SHA-1 and then compares its result with the SRES sent from MS_1 at step 518. If at step 520, the SRES generated by VLR_1 matches the SRES received from MS_1, VLR_1 can then authenticate MS_1 with VLR_1, as shown in step 522. That is, VLR_1 authenticates that MS_1 does in fact hold the private key P_1 it claims, and authorizes MS_1 for communication through VLR_1. If however, the SRES generated by VLR_1 does not match the SRES received from MS_1, VLR_1 does not authenticate MS_1 with VLR_1, as shown in step 524. In such regard, VLR_1 cannot confirm that MS_1 does in fact have the private key P_1 it claims to have. Accordingly, VLR_1 cannot confirm to a second VLR_2 desiring to securely communicate with MS_1, that MS_1 is authorized to communicate on the cellular network 113. After authenticating User_1 of MS_1 and User_2 of MS_2, VLR_1, VLR_2 and each MS has the public key of its own subscriber User_1 and User_2, respectively."); Peirce '967 at Abstract ("A system and method for producing cryptographic keys for use by an embedded processing device within a manufactured product. A pseudo random number generator is seeded with entropy data gathered by the embedded device, and the result is used to generate a public-private key pair. The process can be carried out during manufacturing so that the public key of each manufactured product can be stored in a database along with a unique identifier for the embedded device associated with the key. In one particular example, a vehicle having an installed telematics unit uses the key generating process to self-generate keys using entropy data available to the vehicle."), [0001]–[0002] ("The present invention relates generally to techniques for generating cryptographic keys used in secure data communications and, in particular, to such techniques used for manufactured products having embedded processing devices. As computer electronics

continue to reduce in cost and size, the applications for embedded processing devices are continuing to increase, and there now exists many types of manufactured products that contain some type of embedded processing device, whether microprocessor based or otherwise. Some embedded devices are designed to undergo data communication with one or more external, possibly remote devices. In some cases, it is desirable to establish authenticated, secure data communications in which the exchanged data is encrypted. Although various approaches can be used, cryptographic keys are perhaps most commonly used for this purpose. In public key cryptography, a public-private key pair is created with the public key then being available for use by anyone desiring encrypted communication with the holder of the private key. Digital certificates issued by a trusted third party (certificate authority) can also be used to authenticate the public key to a particular entity.”), [0036] (“For the vehicle example shown in FIG. 1, examples of entropy data that can be used are measured transient events occurring on the vehicle, such as features of messages or other communications occurring on the communications bus 44, data from a vehicle system module (VSM) 42 such as data from a sensor 43, or GPS satellite time data (normally used for determining location coordinates) that are received from the GPS module 40. Other, non-transient, but unique data can be used as entropy data, such as serial numbers from onboard devices, the vehicle VIN, an assigned mobile number for the telematics unit or network node address. Other such sources of entropy will become apparent to those skilled in the art.”); Semple ’841 at Abstract (“A mutual authentication method is provided for securely agreeing application-security keys with mobile terminals supporting legacy Subscriber Identity Modules (e.g., GSM SIM and CDMA2000 R-UIM, which do not support 3G AKA mechanisms). A challenge-response key exchange is implemented between a bootstrapping server function (BSF) and mobile terminal (MT). The BSF generates an authentication challenge and sends it to

the MT under a server-authenticated public key mechanism. The MT receives the challenge and determines whether it originates from the BSF based on a bootstrapping server certificate. The MT formulates a response to the authentication challenge based on keys derived from the authentication challenge and a pre-shared secret key. The BSF receives the authentication response and verifies whether it originates from the MT. Once verified, the BSF and MT independently calculate an application security key that the BSF sends to a requesting network application function to establish secure communications with the MT.”), 1:23–29 (“The present invention generally relates to systems and methods for securing wireless communications. More specifically, one feature of the invention provides a novel authentication and key agreement scheme for devices supporting legacy network authentication mechanisms, in order to provide application security keys by taking advantage of legacy wireless authentication and key agreement mechanisms.”), 8:30–9:18 (“For instance, this verification may be performed using a public key or digital server certificate of the BSF which has been provisioned in the MT. If the authentication challenge does not come from the expected BSF, then the process terminates. Otherwise, an authentication response to the challenge is formulated based on a secret key provided by the SIM of the MT 510. For instance, the MT passes the random number RAND to the SIM (in the MT) which calculates one or more secret keys (SRES and Kc) using the pre-shared secret key Ki and random number RAND with the algorithms A3 and A8. The secret keys SRES and Kc are then provided to the MT to formulate the authentication response. In one implementation, the secret keys SRS and Kc may be used to compute a message authentication code, or derive or encrypt one or more parameters, that is sent as part of the authentication response. The authentication response is sent from the MT to the BSF 512. The BSF then verifies the origin of the authentication response based on an independently obtained secret key 514. For

instance, the SRES and Kc obtained from the HLR (in the triplet corresponding to random number RAND and pre-shared secrete key Ki) may be used to validate one or more parameters in the authentication response from the MT. For instance, the BSF may independently calculate the message authentication code (or other parameter in the authentication response) using the random number RAND, SRES, and/or Kc received from the HLR. If the parameters (e.g., message authentication code) calculated by the MT and BSF match, then the origin of the authentication response is verified. In an alternative implementation, the MT may calculate a third key using the one or more secret keys (SRES and Kc obtained from the SIM) and other parameters (obtained from the authentication challenge or response or from the SIM). This third key is then used to formulate the authentication response (e.g., compute the message authentication code). The BSF may also calculate the same key since it knows the same keys and/or parameters as the MT. Thus, the BSF can verify whether the authentication response originated from the MT. Once the authentication response is verified, the BSF and MT independently compute a shared key based on one or more keys and/or parameters (e.g., SRES, Kc, and/or other parameters) known to both the BSF and MT 516. This shared key can then be provided to a requesting NAF to establish secure communications or transactions between the MT and NAF 518. The MT authenticates transmissions from the BSF by means of a public key mechanism. The BSF challenges the MT with a random number RAND and establishes that it is in possession of the corresponding secret keys SRES and/or Kc in order to authenticate the transmissions from the MT. Thus, the BSF and MT are mutually authenticated in order to share information from which keys may be derived for the purpose of bootstrapping.”); Wang ’162 at [0003] (“More particularly, the present invention is related to a method and apparatus for security protection of an original user identity (ID) in an initial access signaling message in a wireless

communication system including third generation (3G) long term evolution (LTE).”), [0007]–[0010] (“Each AV contains a quintet of numbers that includes a random number (RAND), an expected response (XRES) which is used to authenticate the user, a cipher key (CK) for establishing confidentiality, an integrity key (IK), and an authentication token (AUTN). The AUTN comprises a sequence number (SQN) hidden by an anonymity key (AK), an authentication management field (AMP) which specifies certain authentication components, (such as algorithms to be used, key lifetime, etc.), and a message authentication code (MAC) which is functionally dependent on the SQN, the AMF, and the RAND. The VLR/SGSN 20 sends the RAND and the AUTN from the AV that it has selected to the NAS layer 14 via the UTRAN 18 (steps 118, 120). The NAS layer 14 then authenticates the network by calculating an expected MAC (XMAC) and determining whether the XMAC matches the MAC (step 122). The NAS layer 14 also computes session security keys to the WTRU 12, (i.e., the CK and IK in the AV) at step 122. The key generation is performed using predefined UMTS algorithms which take RAND as input and apply the shared secret key K. The NAS layer 14 computes a response (RES) and sends the RES to the VLR/SGSN 20 via the UTRAN 18 (steps 124, 126). The VLR/SGSN 20 determines if the RES matches the XRES to authenticate the WTRU 12 (step 128). An authentication failure occurs if either of these authentication attempts fails at steps 122 and 128. Once mutual authentication has succeeded, the VLR/SGSN 20 sends an authentication complete message to the HLR/AuC 22 (step 130) and a local security activation procedure starts. The VLR/SGSN 20 sends a security mode command to the UTRAN 18 including the negotiated UMTS encryption algorithms (UEAs) and UMTS integrity algorithms (UIAs), and the current session keys, CK and IK (step 132). As secure communication can now begin the UTRAN 18 sends a security mode command to the RRC layer 16 with a message authentication code for

integrity (MAC-I) (step 134). The MAC-I value protects the integrity of the security mode command message. The MAC-I is a type of hash computed by a UIA on the message's contents using the session key IK.”). Thus, a person of ordinary skill in the art would have been motivated to modify any of the primary references to include this feature. A person of ordinary skill in the art would also have had a reasonable expectation of success. A person of ordinary skill in the art would have understood that these references disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach using cryptographic algorithms and an elliptic curve Diffie-Hellman key exchange, based on public/private key pairs, to generate a shared symmetric session key to secure communications between a mobile device and telecommunications network server in a mobile/tele-communications context (in regards to Limitations 1[pre], 1[a], 1[b], 1[d], 1[e], 1[f], and 1[g])[9], it would have been obvious to a person of ordinary skill in the art at the time of the invention to combine the primary reference with any of the prior art that disclose Limitations

[9] Specifically, Limitation 1[pre]: “A mobile device comprising;” Limitation 1[a]: “at least one processor;” Limitation 1[b]: “at least one computer-readable medium operatively connected to the at least one processor and having stored thereon instructions that, when executed by the at least one processor, cause the mobile device to perform a method of authentication with a wireless network;” Limitation 1[d]: “(2) deriving a module private key and a corresponding module public key using the cryptographic algorithms;” Limitation 1[e]: “(3) deriving a symmetric ciphering key using (i) an elliptic curve integrated encryption scheme with the server public key and the module private key and (ii) an American National Standards Institute standard X-9.63 key derivation function;” Limitation 1[f]: “(4) generating a module encrypted data using the symmetric ciphering key and the symmetric ciphering algorithm, wherein the module encrypted data includes the module identity;” and Limitation 1[g]: “(5) sending a message to a server for the wireless network, the message comprising the module encrypted data and the module public key, wherein the server mutually derives the symmetric ciphering key using at least the module public key, and wherein the wireless network selects the pre-shared secret key for the mobile device using the module identity.”

1[pre], 1[a], 1[b], 1[d], 1[e], 1[f], and 1[g] in Exhibits B-01 to B-09 or B-A. For example, several prior art references, including Ala-Laurila ’934, Bhuyan ’491, Boyd-Mathuria, Farnham ’766, Jeong (2010), Nguyen ’985, Peirce ’967, Semple ’841, Wang ’162, and Secondary References explicitly describe or disclose using an elliptic curve Diffie-Hellman key exchange, based on public/private key pairs, to generate a shared symmetric session key to secure communications between a mobile device and telecommunications network server in mobile/tele-communications context. *See, e.g.*, Ala-Laurila ’934 at Abstract, [0002]–[0009], [0025]–[0032], [0041]–[0049], Figs 1–5; Bhuyan ’491 at Abstract, [0001]–[0006], [0045]–[0052], [0062], [0074]–[0091], Figs. 1–6; Boyd-Mathuria at Chapters 1.4, 1.6, 2.3, 2.6, 3.3, 4.1, 4.3.5, 5.1, 5.1.3, 5.2, 5.4.4, 5.7.2, 5.9, 5.11, 6.2.7, 7, 7.8, A; Farnham ’766 at Abstract, [0001]–[0009], [0012]–[0018], [0051]–[0058], [0069]–[0075], [0083]–[0087], Figs. 1–3, Cls. 6, 10, 14; Jeong (2010) at Abstract, Sections 1, 3.1.1, 3.2, 4.1.4, 5, Figs. 2, 4–6; Nguyen ’985 at Abstract, [0001]–[0004], [0010]–[0021], [0036]–[0048], Figs. 1–2, 4–6, Cls. 1, 10, 15; Peirce ’967 at Abstract, [0001]–[0014], [0032]–[0042], Figs. 1–3, Cls. 1, 14–15; Semple ’841 at Abstract, 1:23–2:43, 6:3–7:3, 9:19–59, 9:60–10:24, Figs. 1–7; Wang ’162 at Abstract, [0003]–[0015], [0029]–[0044], [0086], [00129] Figs. 1–7.

A person skilled in the art would have understood the benefits of using an elliptic curve Diffie-Hellman key exchange, based on public/private key pairs, to generate a shared symmetric session key to secure communications between a mobile device and telecommunications network server in a mobile/tele-communications context (in regards to Limitations 1[pre], 1[a], 1[b], 1[d], 1[e], 1[f], and 1[g]), given the well-known and complementary confidentiality and security considerations in that process, and therefore would have been motivated and had a reasonable expectation of success to incorporate this feature into the device or method for a mobile device application according. *See, e.g.*, Ala-Laurila ’934 at [0026] (“The MT requests 202 (IMSI

request) the identity module SIM for the IMSI identifier and the SIM returns 203 the IMSI identifier. The MT sends 204 the authentication starting request (MT_PAC_AUTHSTART_REQ) which preferably comprises a Network Access Identifier NAI. The NAI comprises the IMSI identifier obtained from the identity module SIM. The NAI may be presented, for example, in the form 12345@GSM.org, where 12345 is the IMSI identifier and GSM.org is the domain name of the mobile network, which has conveyed the identity module SIM. The request 204 is preferably sent in ciphered form to the PAC using the Diffie-Hellman algorithm, for example. The MT preferably also sends a specific protection code MT_RAND in the request 204, said code typically being a challenge code. Using the protection code MT_RAND the MT may later be ensured that the party conveying the GSM triplets actually has access to the secret key Ki, which is to be maintained in the GSM home network of the subscriber. However, the use of the protection code is not obligatory.”), [0032] (“The second calculation means included in the MT, preferably the control means CM, calculate 217 (Calculate K) a second ciphering key K using one or more first ciphering keys Kc according to the mobile network GSMNW calculated by the SIM.”), [0042] (“The GAGW informs 222 the PAC about the authentication being accepted (GAGW_PAC_AUTHANSWER_RESP_OK). This message comprises at least the second ciphering key K. Information on services that the MT is authorized to use (such as quality of service QoS data) can also be sent in the message 222. The PAC informs 223 the terminal MT about the authentication being accepted (PAC_MT_AUTHANSWER_RESP_OK). Authentication is then performed and both the terminal MT and the PAC comprise a similar second ciphering key K which can be transmitted to the ciphering means performing ciphering for ciphering traffic.”), [0048] (“After receiving the second ciphering key K, the AP sends 309 (Put_WEP_on) a request to the MT concerning the

use of the WEP algorithm for data ciphering. The MT acknowledges 310 (Put_WEP_on_ack) the request, so that the starting point of data ciphering is correctly timed. After this the second ciphering key K is applied in the MAC layer of the MT, and the MT enciphers the data to be sent and deciphers the received enciphered data 311 (Cipher data with K and WEP) using the K and the WEP algorithm. The AP also starts to use 312 (Cipher data with K and WEP) the K and the WEP algorithm for enciphering data directed to the MT and for deciphering data received from the MT. The AP checks the terminal MT MAC addresses of the received data and performs deciphering for data arriving from the MAC address and correspondingly enciphers the MT data directed to the MAC address. In this case, the K is rapidly initiated and data ciphering can be started."); Bhuyan '491 at [0074] ("In step 608, the access server 506 forwards the authentication request, including the IMSI, to the authentication server 206. The authentication server 206 then uses the IMSI received in the authentication request to retrieve the previously generated (in step 310 in FIG. 3) secret key Ki corresponding to the IMSI. The authentication server then generates a triplet comprising a random number RAND, an expected response SRES and a key Kc in step 612. Each of these parameters is generated in accordance with the methods shown in FIG. 1. The values generated for RAND, SRES and Kc are then sent to the access server 506 in step 612."), [0078]–[0079] ("Once the access server 506 has received SRES 404, it calculates SRES1 412 as illustrated in the remainder of FIG. 4 a. Specifically, SRES 404 is fed into cryptographic algorithm F1 together with the password 406 received from the data store 208. The cryptographic function F1 is operator specific and can be defined by the operator for its specific use in contrast to the GSM algorithms like A3, A5 and A8, which are generally used across service providers and operators. The F1 function can also be tailored and thus be specific to the mobile device 210, as the function F1 is included as part of the security module provided to the mobile device 210

in step 318. Similarly, the access server 506 also uses the received Kc 406 from the authentication server 206 and the password from the data store 208 and feeds both these parameters into cryptographic function F2 to derive Kc1 414. The generation of Kc1 414 is illustrated in FIG. 4 b. It should be noted that like F1, the cryptographic function F2 is also operator specific, but can also be further specified for the individual mobile device 210 in question.”), [0086] (“The mobile device 210 then uses the value of Kc1 generated in step 622 to encrypt and decrypt data transferred to and from the mobile device. The method for ciphering is shown in FIG. 4 c and is the same as that described with reference to FIG. 1 c above, but using Kc1 instead of Kc. In step 630, the access server 506 provides the application server 502 with a copy of Kc1 generated by the access server 506 in step 618. Thus, by mobile device 210 and the application server 502 can communicate securely by ciphering all data using the now shared session key of Kc1 as shown in step 632.”); Boyd-Mathuria at Chapter 5.2 (“Typical sizes in use today are 1024 bits for the length of p and 160 bits for the length of q. Several other algebraic groups have been proposed as the setting for Diffie-Hellman key exchange. Examples are given in Sect. 5.9. In particular, elliptic curve groups are popular today.”), Chapter 5.9 (“Diffie-Hellman key agreement was originally proposed in the algebraic setting of the multiplicative group Z_p^* and we have used this setting in all our descriptions so far. It has long been known that the basic structure can be generalised to any commutative group. In this section we mention some of the most prominent alternative groups that have been proposed. Elliptic curve groups have significant potential advantages over using Z_p^* because of their greater efficiency and compact representation. Many recent protocols have been specially designed with elliptic curve implementation in mind rather than using prime fields. Examples include the MQV (5.11) and Oakley (5.18) protocols. The Oakley specification includes a number of candidate elliptic curves and also provides for

negotiation of new curves during the protocol. It is sometimes possible to avoid certain attacks because of the structure of the curve used. For example, elliptic curve groups can be chosen to have prime order so that there is no need to check whether elements are in a particular subgroup." (emphasis omitted)), Chapter 7.8 ("Since these protocols may well be useful in applications employing mobile computing devices, the computational efficiency and storage gains in using elliptic curve groups can be very attractive. Although it is straightforward to generalise the protocol definitions to different groups, there may be undesirable consequences with respect to security. For example, consider Protocol 7.1 when the Diffie-Hellman exchange takes place in an elliptic curve group."), Farnham '766 at [0056]–[0058] ("In a variant of this technique, the key k is replaced by a Diffie-Hellman public value g^n mod p (see, for example, W. Diffie and D. E. Hellman, ibid), where n is a positive integer satisfying $1 \leqq n \leqq p-2$…. The mobile terminal B or the client can obtain the server's public value $Y_A=g^a$ mod p that is contained in the server key exchange or the SIM may contain the server's public value. The originator (in this example, the server A) chooses a random value n, computes g^n mod p and sends M1 including g^n mod p to the terminal. The server A can then compute a session key $k = Y_A\ n = (g^a)^n = g^{an}$ mod p and the terminal B can compute the same session key using $k = (g^n)^a = g^{na}$ mod p. Encrypted software may then be sent to the terminal B by encrypting the software with the common session key. An eavesdropper does not know the private key of server (that is a) and thus, it is computationally infeasible to determine the session key. This method can be used for distributing system software to mobile equipment for anonymous secure software download, for example for broadcasting a SIM update, because an individual recipient need not be specified."), [0071] ("Under certain circumstances, the Diffie-Hellman and (DH) the related Elliptic Curve Diffie-Hellman (ECDH) key agreement schemes (X9.63, 'Public key cryptography for the financial services industry: Key

agreement and key transport using elliptic curve cryptography', Draft ANSI X9F1, October (1999)) are susceptible to a class of attacks known as "small-subgroup" attacks. Where, if a key belongs to a small subgroup a directed brute-force attack based on guessing keys from the subgroup may succeed. In the anonymous DH and ECDH cases there is a risk that such a small subgroup attack will lead communicating parties to share a session key which is known to an attacker. This threat can be alleviated by using a predetermined group determined 'good' or 'strong' values of g and p and checking that received public keys do not lie in a small subgroup of the group, or by not re-using ordinary DH key pairs. Background information on protection against these attack, can be found in the draft ANSI standards X.9.42 (X.9.42, 'Agreement of symmetric keys using Diffie-Hellman and MQV algorithms', ANSI draft, May (1999)) and. X.9.63 (X9.63, 'Public key cryptography for the financial services industry: Key agreement and key transport using elliptic curve cryptography', Draft ANSI X9F1, October (1999)).''); Jeong (2010) at Section 3.1.1 ("The shared secret key is generated by the EC-DH algorithm, and the shared secret key is used for mutual authentication. Among the component of the mobile payment system, the process of generating a shared secret key between the certificate authority and the store is as follows. (1) The merchant registers the merchant's information when registering with the certificate authority. (2) The certificate authority delivers to the merchant the initial point P, E_p, and the certificate authority's public key $A_{SK}P$, which are necessary for generating the shared secret key. (2) The certificate authority delivers to the merchant the initial point P, E_p, and the certificate authority's public key $A_{SK}P$, which are necessary for generating the shared secret key. (3) The merchant generates a shared secret key $M_{(SK)}\ (A_{(SK)}P)$ with the certificate authority's public key and passes it to the certificate authority as $M_{SK}P$, the merchant's public key. (4) The certificate authority generates a shared secret key $A_{(SK)}\ (M_{(SK)}P)$ with the merchant's public key

and validates it with the shared secret key delivered by the merchant. (5) The merchant checks the validity of the shared secret key received from the certificate authority against the shared secret key generated by the merchant. (6) If the validation is TRUE, the shared secret is used as the shared secret of the merchant and the certificate authority."), Section 4.1.4 ("Since the mobile payment protocol and the AKA module proposed in this paper use SSK and OT-SSK based on EC_DH, even if the initial point P and the public key are disclosed, the SSK and OT-SSK cannot be derived because they do not know each other's secret key, and they satisfy full omnidirectional safety."), Section 5 ("The AKA module proposed in this paper prevents IMSI exposure by generating a shared secret key between the MS and the HN for user authentication and encrypting and transmitting the IMSI value of the USIM, and prevents data replay attack by generating a new OT-SSK for each connection by generating message encryption keys, CK and IK, using a one-time shared secret key, OT-SSK, between the MS and SN."); Nguyen '985 at [0019]–[0020] ("The MSC 123 can include an authentication center (AuC) 231, a Home Location Register (HLR) 232, and/or a Visitor Location Register (VLR) 232 each implementing the key exchange algorithm 117. The key exchange algorithm 117 protects the security of the entire communication channel between any two mobile users. The key exchange algorithm can be based on the Elliptic Curve Diffie-Hellman (ECDH) cryptosystem, which itself is a key exchange algorithm that is based on Elliptic Curve Cryptography (ECC) for public/private key generation. ECC is an approach to public-key cryptography based on an algebraic structure of elliptic curves over finite fields. An elliptic curve is a plane curve defined by an equation of the form $y^2=x^3+ax+b$. The set of points on such a curve can be shown to form a commutative group G, such that a*b=b*a for all a and b in G. Elliptic Curve Diffie-Hellman (ECDH) is a key agreement protocol that allows the two MSs to establish a shared secret key over an insecure channel. The secret key can then

be used to encrypt subsequent communications using a symmetric key cipher.”), [0036] (“Method 500 begins with step 502 in which MS_1 can use its own private key P_1 to compute its own public key Q_1 using a chosen base point B on a specific Elliptic Curve algorithm. The base point “B” can be a random value selected from an elliptic curve algorithm. B does no need to be a secret value and can be available to devices within the communication system 100. In practice, providers within the communication system 100 can determine how the base point B is calculated and distributed among MSs and VLR's. For instance, in one embodiment a unique base point can be used for the entire GSM network that is pre-built into MSs’ SIM cards and VLRs. Another implementation option provides a distinct and temporary base point B for each communication session.”), [0038]–[0039] (“Each MS can use the public key received from the other MS along with its own private key to generate a shared Diffie-Hellman authentication key. For instance, at step 510, MS_1 computes the shared Diffie-Hellman authentication key A_1 using its own private key P_1…. Similarly, at step 512, VLR_1 can compute the shared Diffie-Hellman authentication key A_1 using its own private key P_VLR1, in accordance with the same method steps above. As a result of the elliptic curve algorithm, the authentication key A_1 generated by MS_1 should be the same as the authentication key generated by VLR_1, as shown in the equation above. Although, neither MS_1 nor VLR_1 is aware of the authentication key A_1 value generated by the other, each can perform a subsequent operation together to validate the value.”); Peirce ’967 at [0001] (“The present invention relates generally to techniques for generating cryptographic keys used in secure data communications and, in particular, to such techniques used for manufactured products having embedded processing devices.”), [0038] (“Using the entropy data, the next step 106 in the process is generation of the cryptographic keys using the PRNG within the embedded device. Suitable PRNG software programs are known and

can be incorporated into the embedded processing device. The entropy data is used as a seed value for the PRNG, which will yield a nearly random number suitable for use in generating strong cryptographic keys. Once the keys have been generated, the entropy data used to seed the PRNG process is preferably erased from any memory in which it had been held. The use of the output of the PRNG to generate various types of keys is known, including asymmetric public-private key pairs. These keys can be used either in a web of trust scheme, or can be utilized using public key infrastructure wherein the public key can be issued by a certificate authority."), [0041] ("As shown in FIG. 1, the telematics unit includes a PRNG program (PRNGP) 55 which can be stored in the telematics memory 54 and executed by the processor 52. Thus, at step 212, the PRNG can be seeded with the entropy data and the near-random number that is generated is then used in a known manner at step 214 to generate a public-private key pair. The private key is stored in the vehicle, such as in the telematics memory 54 at step 216, and the public key is transmitted at step 218 to an external database along with at least one unique identifier associated with the telematics unit. Transmission of the public key can be done wirelessly using the cellular chipset 50 or using some other communication approach, as will be known to those skilled in the art. The external database that stores the keys and associated IDs can be, for example, database 84 that is maintained at the call center 20. Once the keys have been generated and stored in their respective locations, the vehicle can then be distributed to a dealer or end customer, as indicated at step 220. The keys can then be used to establish secure communication between, for example, the call center 20 and the vehicle 12."), Cl. 15 ("A vehicle electronics system for self-generating cryptographic keys used for secure wireless communication with the vehicle…."); Semple '841 at 6:3–10 ("A Diffie-Hellman key exchange may be employed as part of the key agreement process between the MT 102 and the BSF 106. The Diffie-Hellman key exchange is a

cryptographic protocol which allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. In one application this shared secret key can then be used to encrypt subsequent communications using a symmetric key cipher."), 6:33–57 ("FIG. 2 is a block diagram illustrating a mobile terminal (MT) 200 configured to perform mutual authentication with bootstrapping server function operational on a communication network. The MT 200 includes a processing circuit 202 (e.g., processor) coupled to a communication interface 202 to communicate with a wireless network, and a Subscriber Identity Module (SIM) card 204. The processing circuit 202 may be configured to perform part or all of the methods illustrated in FIGS. 4, 5, 6, and 7. The SIM 204 may contain a secret key Ki, an implementation of GSM authentication and key agreement algorithms (i.e., the GSM A3/A8 algorithms), and is inserted in a MT 102 containing a public key or digital server certificate of a public key corresponding to a private key in BSF 106. In particular the SIM 204 may be a standard legacy smart card configured for use in a GSM network. The public key or server certificate may correspond to a RSA public key, or other public-key techniques affording digital signatures may also be used, for example, DSA (digital signature algorithm). The BSF 106 and MT 102 may also share a pre-determined generator P of a cyclic group, such as the multiplicative subgroup of a finite field or a point in an elliptic curve, allowing them to employ the Diffie-Hellman key exchange. In alternative embodiments, the MT 200 may include a CDMA2000-compliant authentication module instead of the SIM 204."), 9:35–59 ("In one embodiment, a request for authentication keys may be initiated by MT 606 retrieving its associated International Mobile Subscriber Identity (IMSI) 600 from its SIM 608 and sending it to a bootstrapping server function (BSF) 604. The BSF 604 sends the IMSI 600 to the HLR 602 where it may verify whether the IMSI 600 belongs to a MT that subscribes to the network. The

HLR 602 may be operated by the service provider for the subscriber whose SIM is contained in MT 606. The HLR 602 selects, for example, a 128-bit random challenge RAND and together with pre-shared secret key Ki, uses them as inputs for two algorithms A3 and A8 to yield 32-bit output signed response SRES and 64-bit output secret confidentiality key Kc, respectively. The HLR 602 then provides the triplets (RAND, SRES, Kc) to the BSF 604, corresponding to the identity IMSI 600 of SIM 608. The BSF 604 generates a random secret exponent x and computes a Diffie-Hellman public key P^x, where P is a generator of a cyclic group previously provisioned to both the BSF 604 and MT 606, such as the multiplicative group of a finite field or the additive group of an elliptic curve. The BSF 602 then sends a triplet (RAND, P^x, SIG) 610 to the MT 606, where SIG is a digital signature computed using the BSF 604 RSA private key. The message 610 may be further enhanced to include other server-authenticated parameters such as a transaction identifier."); Wang '162 at [0015] ("The initial security parameters are loaded from a universal subscriber identity module (USIM) and generated from system information broadcast from the network. The system information includes a public key set with at least one public key for asymmetric encryption of the IMSI or information from which the public key(s) can be derived. The initial security parameters for ciphering include a CK. The CK may be a public key or may be selected from the public key set broadcast by or derived from the network system information. An index of the selected public key may be separately encoded. Alternatively, the index may be communicated by using a Diffie-Helman key exchange method."), [0034] ("The aGW 260 sends an authentication request message to the NAS layer 211 of the WTRU 210 including the RAND and the AUTN from the first AV (step 324). The connection response message does not have to be ciphered or integrity protected. Alternatively, the connection response message may be ciphered at the eNode-B 250 with a public key with an index from the HLR/AuC 270 with the

conventional symmetric ciphering algorithm. The NAS layer 211 then authenticates the network by calculating an expected MAC (XMAC) and determining whether the XMAC matches the MAC (step 326). The NAS layer 211 also computes new session keys, (i.e., CK and IK in the AV) at step 326. The key generation is performed using predefined algorithms which take RAND as input and apply the shared secret key K."), [0038] ("Figure 4 shows a ciphering process including conventional f8 ciphering and ciphering parameters. The ciphering algorithm may be a conventional symmetric ciphering algorithm such as f8 or an asymmetric encryption algorithm used for the ciphering with public and private keys."), [0042] ("Alternatively, the public key may be selected using a Diffie-Hellman key exchange method. The LTE network 230 and the WTRU 210 agree on two values, (a very large prime number p and a generator g of the multiplicative group F_p' of the field F_p), that are publicly known. The LTE network 230 broadcasts via system information a set of public keys with a first seed, g_{KI} (where a randomly selected KI is such that $1 < KI \leq p - 2$ and $g \equiv g^{KI} \bmod p$). The set of public keys may be from a larger group of encryption keys with random periodicity and order. The WTRU 210 randomly selects a value $KIn2$, ($1 < KInI < p - 2$), to compute a second seed, $g_{KInl} \equiv g^{KIn2} \bmod p$. The WTRU 210 then computes $k' \equiv (g_{KI})^{KIn2} \bmod p$. The public key index $a \equiv k' \bmod n$, where n is the current number of public keys broadcast from the system information with the first seed, g_{KI} . The computed a is an index to the public key set for the chosen public key k_a . The WTRU 210 ciphers the NAS or the RRC message including the IMSI with the selected public k_a and includes the second seed, g_{KLn2} , in the NAS or RRC message to the LTE network 230. The second seed is not encrypted. The LTE network 230 first takes the unencrypted second seed, g_{KLn2} , and computes $k = (g_{KLn2})^{KI} \bmod p$. The index a is then obtained by $a \equiv k \bmod n$ for the private key index a. The LTE network 230 then decodes the whole message with the private key corresponding to public key ka."). Thus, a

person of ordinary skill in the art would have been motivated to modify any of the primary references to include this feature. A person of ordinary skill in the art would also have had a reasonable expectation of success. A person of ordinary skill in the art would have understood that these references disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

V. U.S. Patent No. 11,916,893 ("the '893 Patent")

A. Identification of Prior Art

Defendants incorporate by reference, as if set forth fully herein, all filings and exhibits from *Inter Partes* Review IPR2026-00119, filed November 26, 2025 with the PTAB, including any subsequent and future filings in that case.

In addition to the prior art cited on the face of the '893 Patent and related patents, the admitted prior art in the specifications of the '893 Patent and related patents, the prior art cited in any file histories, reexaminations, *inter partes* review proceedings, reissue proceedings, or other examination or post-grant proceedings of the '893 Patent and related patents, and the prior art cited in any invalidity contentions or expert reports submitted in any action or proceedings involving the '893 Patent or related patents, Defendants identify the following prior art that anticipates each asserted claim or renders it obvious.

1. Prior Art Patents

The following patents and patent publications are prior art to the asserted claims under at least 35 U.S.C. §§ 102(a)(1) and/or (a)(2), and/or 35 U.S.C. § 103. The identification of any patent or patent publication shall be deemed to include any counterpart patent or application filed, published, or issued anywhere in the world.

Patent or Publication	Country of Origin	Filing Date	Date of Issue or Publication

Number			
U.S. Pat. App. Pub. No. 2013/0301828 ("Gouget")	United States	September 24, 2010 (EP) March 23, 2013 (PCT)	November 14, 2013
U.S. Pat. App. Pub. No. 2013/0227646 ("Haggerty")	United States	February 14, 2013	August 29, 2013
U.S. Pat. App. Pub. No. 2010/0267383 ("Konstantinou")	United States	April 15, 2009	October 21, 2010
U.S. Pat. App. Pub. No. 2016/0127132 ("Lee")	United States	May 30, 2013 (KR) November 30, 2015 (PCT)	May 5, 2016
U.S. Patent No. 9,100,175 ("Nix")	United States	December 6, 2013	August 4, 2015
U.S. Patent No. 8,761,390 ("Peirce")	United States	June 30, 2008	June 24, 2014
U.S. Pat. App. Pub. No. 2015/0350881 ("Weiss")	United States	December 21, 2012 (EP) June 19, 2015 (PCT)	December 3, 2015

2. Prior Art Non-Patent Publications

The following non-patent publications are prior art to the asserted claims under at least 35 U.S.C. §§ 102(a)(1) and/or (a)(2), and/or 35 U.S.C. § 103.

Title	Author/Publisher	Date of Publication
A Fast and Secure Elliptic Curve Based Authenticated Key Agreement Protocol For Low Power Mobile Communications ("Abi-Char")	Pierre E. Abi-Char, et al., IEEE	2007
Ansi X9.63 Overview Key Agreement and Key Transport Using Elliptic Curve Cryptography ("ANSI X9.63 Overview")	Simon Blake-Wilson, Certicom	2000
Protocols for Authentication and Key Establishment ("Boyd-	Colin Boyd & Anish Mathuria, Springer	2003

Mathuria")		
GlobalPlatform Card Specification Version 2.2.1 Public Release ("GlobalPlatform")	GlobalPlatform, Inc.	January 2011
SGP.22 - RSP Technical Specification Version 2.0 ("SGP.22")	GSM Association	October 14, 2016
Secure Profile Provisioning Architecture for Embedded UICC ("Park (IEEE)")	Jaemin Park, et al., IEEE	November 7, 2013
GlobalPlatform Card Secure Channel Protocol '11' Card Specification v.2.2 – Amendment F Version 1.0 Public Release ("SCP11")	GlobalPlatform, Inc.	May 2015

3. Prior Art Systems

Defendants' investigation into publicly available prior art systems that teach and/or render obvious each element of any asserted claims is ongoing. Fact discovery is at an early stage, and Defendants may require discovery from third parties regarding publicly available prior art systems. On information and belief, prior art systems from the following companies teach and/or render obvious each element of the asserted claims of the '893 Patent: Cinterion (now Telit); Gemalto (now Thales); Giesecke+Devrient; GlobalPlatform; NXP Semiconductors N.V.; Oberthur Technologies (now IDEMIA); and Sierra Wireless. Defendants reserve the right to amend its identification of prior art systems as Defendants become aware of the existence, functionality, and/or characteristics of prior art systems as a result of its investigation and forthcoming discovery. In addition to the prior art products, components, systems, and methods that may be identified as a result of discovery, Defendants also reserve the right to rely on the documents and publications identified in the corresponding claim charts as prior art publications.

B. Primary References

Defendants contend that the primary prior art references identified below and described in the charts attached as Exhibits C-01 to C-08, by themselves, anticipate the asserted claims of the '893 Patent. To the extent that a primary reference is deemed not to anticipate a claim for failing to teach one or more limitations of that claim, Defendants contend that the claim would nonetheless have been obvious to a person of ordinary skill in the art at the time of the invention in view of the prior art reference itself, as described in the attached charts. Defendants' prior art charts (attached as Exhibits C-01 thru C-08) set forth the particular claims that are anticipated under 35 U.S.C. § 102 and/or rendered obvious under 35 U.S.C. § 103 by each item of prior art and identify where specifically in each item of prior art, each element of each asserted claim is found.

Exhibit	Primary References
C-01	*Protocols for Authentication and Key Establishment* ("Boyd-Mathuria")
C-02	*GlobalPlatform Card Specification Version 2.2.1 Public Release* ("GlobalPlatform")
C-03	U.S. Pat. App. Pub. No. 2013/0301828 ("Gouget")
C-04	U.S. Pat. App. Pub. No. 2013/0227646 ("Haggerty")
C-05	U.S. Patent No. 9,100,175 ("Nix")
C-06	*Secure Profile Provisioning Architecture for Embedded UICC* ("Park (IEEE)")
C-07	*SGP.22 - RSP Technical Specification Version 2.0* ("SGP.22")
C-08	U.S. Pat. App. Pub. No. 2015/0350881 ("Weiss")

C. Secondary References

Exhibit C-A lists secondary prior art references and identifies, on a limitation-by-

limitation basis, where specifically each secondary reference teaches the limitations of the asserted claims. To the extent that a primary reference is deemed, by itself, not to anticipate or render obvious a claim for failing to teach one or more limitations, the claim would nonetheless have been obvious to a person of ordinary skill in the art at the time of the invention by the combination of the primary reference with one or more of the other primary references listed above and/or the references listed as disclosing those alleged missing limitations in Exhibit C-A.

D. Obvious Combinations

To the extent that a primary reference is deemed, by itself, not to anticipate or render obvious a claim for failing to teach one or more limitations, the claim would nonetheless have been obvious to a person of ordinary skill in the art at the time of the invention by the combination of the primary reference with one or more other primary references and/or the knowledge of someone skilled in the art. For example, a person of ordinary skill in the art would have been motivated to combine any reference in Exhibits C-01 to C-08 with any other reference(s) in Exhibits C-01 to C-08. Such combinations would be achieved, for example, by merely combining the disclosures described in the respective claim charts for each reference.

Defendants also contend that any of the primary references (or combination of primary references) could be combined with any of the secondary references (or combination of secondary references) in Exhibit C-A to render obvious the asserted claims. Such combinations would be achieved by merely combining the disclosures described in the respective claim charts for each reference.

The obviousness combinations are provided in the alternative to Defendants' anticipation contentions and are not to be construed to suggest that any reference included in the combinations is not itself anticipatory.

1. Exemplary Combinations

Below are examples of prior art references that would have been combined by one of ordinary skill in the art at the time of the alleged invention. These combinations are merely examples. The asserted claims of the '893 Patent are rendered obvious by:

- Park (IEEE) in combination with GlobalPlatform and Abi-Char.
- Park (IEEE) in combination with GlobalPlatform and ANSI X9.63 Overview.
- Park (IEEE) in combination with GlobalPlatform, Abi-Char, and Haggerty.
- Park (IEEE) in combination with GlobalPlatform, ANSI X9.63 Overview, and Haggerty.
- Park (IEEE) in combination with GlobalPlatform, Abi-Char, and Peirce.
- Park (IEEE) in combination with GlobalPlatform, ANSI X9.63 Overview, and Peirce.
- Park (IEEE) in combination with GlobalPlatform, Abi-Char, and Konstantinou.
- Park (IEEE) in combination with GlobalPlatform, ANSI X9.63 Overview, and Konstantinou.
- Nix in combination with Park (IEEE) and GlobalPlatform.
- Boyd-Mathuria alone or in combination with one or more of Abi-Char, ANSI X9.63 Overview, GlobalPlatform, Gouget, Haggerty, Konstantinou, Lee, Nix, Park (IEEE), Peirce, SCP11, SGP.22, and/or Weiss.
- GlobalPlatform alone or in combination with one or more of Abi-Char, ANSI X9.63 Overview, Boyd-Mathuria, Gouget, Haggerty, Konstantinou, Lee, Nix, Park (IEEE), Peirce, SCP11, SGP.22, and/or Weiss.
- Gouget alone or in combination with one or more of Abi-Char, ANSI X9.63

Overview, Boyd-Mathuria, GlobalPlatform, Haggerty, Konstantinou, Lee, Nix, Park (IEEE), Peirce, SCP11, SGP.22, and/or Weiss.

- Haggerty alone or in combination with one or more of Abi-Char, ANSI X9.63 Overview, Boyd-Mathuria, GlobalPlatform, Gouget, Konstantinou, Lee, Nix, Park (IEEE), Peirce, SCP11, SGP.22, and/or Weiss.
- Nix alone or in combination with one or more of Abi-Char, ANSI X9.63 Overview, Boyd-Mathuria, GlobalPlatform, Gouget, Haggerty, Konstantinou, Lee, Park (IEEE), Peirce, SCP11, SGP.22, and/or Weiss.
- Park (IEEE) alone or in combination with one or more of Abi-Char, ANSI X9.63 Overview, Boyd-Mathuria, GlobalPlatform, Gouget, Haggerty, Konstantinou, Lee, Nix, Peirce, SCP11, SGP.22, and/or Weiss.
- SGP.22 alone or in combination with one or more of Abi-Char, ANSI X9.63 Overview, Boyd-Mathuria, GlobalPlatform, Gouget, Haggerty, Konstantinou, Lee, Nix, Park (IEEE), Peirce, SCP11, and/or Weiss.
- Weiss alone or in combination with one or more of Abi-Char, ANSI X9.63 Overview, Boyd-Mathuria, GlobalPlatform, Gouget, Haggerty, Konstantinou, Lee, Nix, Park (IEEE), Peirce, SCP11, and/or SGP.22.

2. Motivations to Combine

To the extent a finder of fact finds that a primary prior art reference does not disclose one or more limitations of an asserted claim, the asserted claim is nevertheless obvious because the allege missing limitations contain nothing beyond ordinary improvements. In other words, the asserted claim combines known elements to achieve predictable results or chooses between clear alternatives known to those of skill in the art, particularly in view of the state of the art as reflected

in the relevant prior art.

Moreover, as explained above, it would have been obvious to a person of skill in the art at the time of the alleged invention of the asserted claims to combine any primary reference with any combination of other primary references or secondary references so as to practice the asserted claims. To the extent that Plaintiff argues that any concept claimed in the asserted claims is not disclosed in a primary reference, it would, at a minimum, have been obvious to adapt the primary reference to include the concept or combine it with other primary references or secondary references that disclose the concept. Each concept described and claimed in the Asserted Patents was known to those of skill in the art as available design choices for the technologies at issue. [10]

The Supreme Court has held that "[t]he combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 416 (2007). "When a work is available in one field of endeavor, design incentives and other market forces can prompt variations of it, either in the same field or a different one." *Id.* at 417. As the Supreme Court made clear, "[f]or the same reason, if a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill." *Id.*

To determine whether there is an apparent reason to combine the known elements in the fashion claimed by the patent at issue, a court can "look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace;

[10] Each concept described and claimed in the '893 Patent was known to those of skill in the art as available design choices for data encryption technology and/or using such technology to provision and/or authenticate mobile devices for use with a wireless network in a wide range of applications for different scenarios and circumstances.

and the background knowledge possessed by a person having ordinary skill in the art." *Id*. at 418. For example, obviousness can be demonstrated by showing "there existed at the time of invention a known problem for which there was an obvious solution encompassed by the patent's claims." *Id*. at 420. "[A]ny need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed." *Id*. Common sense also teaches that "familiar items may have obvious uses beyond their primary purposes, and in many cases a person of ordinary skill will be able to fit the teachings of multiple patents together like pieces of a puzzle." *Id*.

However, the Supreme Court in *KSR* held that a claimed invention can be obvious even if there is no explicit teaching, suggestion, or motivation for combining the prior art to produce that invention. In summary, *KSR* holds that patents that are based on new combinations of elements or components already known in a technical field may be found to be obvious. *See, generally*, *KSR*, 550 U.S. 398. Specifically, the Court in *KSR* rejected a rigid application of the "teaching, suggestion, or motivation [to combine]" test. *Id*. at 418. "In determining whether the subject matter of a patent claim is obvious, neither the particular motivation nor the avowed purpose of the patentee controls. What matters is the objective reach of the claim." *Id*. at 419. "Under the correct analysis, any need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed." *Id*. at 420. A key inquiry is whether the "improvement is more than the predictable use of prior art elements according to their established functions." *Id*. at 417.

The rationale to combine or modify prior art references is significantly stronger when, as here, the references seek to solve the same problem, come from the same field, and correspond well to each other. *In re Inland Steel Co*., 265 F.3d 1354, 1362 (Fed. Cir. 2001). The Federal

Circuit has held that two references may be combined as invalidating art under similar circumstances, namely "[the prior art] focus[es] on the same problem that the … patent addresses: enhancing the magnetic properties of … steel. Moreover, both [prior art references] come from the same field …. Finally, the solutions to the identified problems found in the two references correspond well." *Id*. at 1364 (concerning patents and prior art relating to improving the magnetic and electrical properties of steel).

In view of the Supreme Court's *KSR* decision, the PTO issued a set of Examination Guidelines. Examination Guidelines for Determining Obviousness Under 35 U.S.C. §103 in view of the Supreme Court Decision in *KSR International Co. v. Teleflex, Inc*., 72 Fed. Reg. 57526 (October 10, 2007). Those Guidelines summarized the *KSR* decision and identified various rationales for finding a claim obvious, including those based on other precedents. Those rationales include:

> (A) Combining prior art elements according to known methods to yield predictable results;
> (B) Simple substitution of one known element for another to obtain predictable results;
> (C) Use of known technique to improve similar devices (methods, or products) in the same way;
> (D) Applying a known technique to a known device (method, or product) ready for improvement to yield predictable results;
> (E) "Obvious to try" – choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success;
> (F) Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations would have been predictable to one of ordinary skill in the art;
> (G) Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention.

Id. at 57529. The above rationales likewise apply in rendering obvious the asserted claims of the

Asserted Patents.

The references disclosed herein, alone or in combination, contain an explicit and/or implicit teaching or motivation to combine them due to the following: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference addresses similar problems; and (5) the knowledge of those skilled in the art that the disclosed elements had been or could be used together.

As an example of those reasons and motivations to combine the references, Abi-Char, ANSI X9.63 Overview, Boyd-Mathuria, GlobalPlatform, Gouget, Haggerty, Konstantinou, Lee, Nix, Park (IEEE), Peirce, SCP11, SGP.22 and/or Weiss generally relate to encryption technology, and/or using such technology to provision or authenticate a mobile device for use with a wireless network. *See* Exs. C-01 to C-08 and C-A. The references disclose similar components and techniques for data encryption, and/or using encryption to provision or authenticate mobile devices. *Id.* The attached charts in Exhibits C-01 to C-08 and C-A provide additional reasons and motivations to combine the charted references.

Additionally, the primary and secondary references listed above are analogous art. They are all directed to encryption technology, and in particular, to provisioning and/or authenticating a mobile device for use with a wireless network. *See, e.g.*, Abi-Char at Abstract ("To provide secure communication for mobile devices, authenticated key agreement protocol is an important primitive for establishing session key …. In this paper we present a fast and Secure Authenticated Key Agreement (EC-SAKA) protocol based on Elliptic Curve Cryptography."), ANSI X9.63 Overview at 3 ("Specifies key agreement and key transport schemes using elliptic curve cryptography"), Boyd-Mathuria at VII ("We believe that this book is the first comprehensive

treatment of protocols for authentication and key establishment."), GlobalPlatform at 2-3 ("Its goal is to reduce barriers hindering the growth of cross-industry, multiple Application smart cards …. Although this specification defines card components, command interfaces, transaction sequences, and interfaces that can be common across many different industries, it does not detail the implementation of the lower layers security, which may vary from one industry to the other. This specification is also intended for a more general audience as it describes the generic security concepts and the various actors involved in a multi-Application Card Management System."), Gouget at [0010] ("The purpose of the invention is to provide a method for establishing a secure channel between a client C and a remote server S when the client C and the server S exchange data through an intermediate entity G."), Haggerty at Abstract ("Methods and apparatus for large scale distribution of electronic access control clients. In one aspect, a tiered security software protocol is disclosed. In one exemplary embodiment, a server electronic Universal Integrated Circuit Card (eUICC) and client eUICC software comprise a so-called 'stack' of software layers …. The tiered security software protocol is configured for large scale distribution of electronic Subscriber Identity Modules (eSIMs)."), Lee at Abstract ("The present invention relates to a method and apparatus for installing a profile, and more specifically, to a method for managing mobile communication subscriber information (profile), such as for remotely installing and uninstalling a profile onto a security module (Universal Integrated Circuit Card (UICC)) that is embedded inside a terminal and that is not attachable or detachable, thereby replacing UICC."), Park (IEEE) at Abstract ("In this paper, a novel secure profile provisioning architecture for eUICCs is proposed."), Peirce at Abstract ("A system and method for producing cryptographic keys for use by an embedded processing device within a manufactured product. A pseudo random number generator is seeded with entropy data gathered by the embedded device, and the

result is used to generate a public-private key pair."), SCP11 at 7 ("This document specifies a new secure channel protocol, named Secure Channel Protocol '11' (SCP11), based on Elliptic Curve Cryptography (ECC) for mutual authentication and secure channel initiation and on AES for secure messaging."), SGP.22 at 7 ("This specification provides a technical description of: The eUICC Architecture; The interfaces used within the Remote SIM Provisioning Architecture; and The security functions used within the Remote SIM Provisioning Architecture."), Weiss at Abstract ("A method of providing a secure element of a mobile terminal with a subscription profile…").

A person of ordinary skill in the art would look to the primary and secondary references to improve or tailor the disclosure thereof to tailor to particular settings or particular factors. A person of ordinary skill in the art would have understood the general trend and motivation to optimize the security, effectiveness, and efficiency of profile provisioning, authentication, and data encryption procedures. A POSITA would have understood that doing so could increase system performance, including in terms of, for example, security and/or efficiency. *See, e.g.*, Abi-Char at Abstract ("To provide secure communication for mobile devices, authenticated key agreement protocol is an important primitive for establishing session key …. In this paper we present a fast and Secure Authenticated Key Agreement (EC-SAKA) protocol based on Elliptic Curve Cryptography …. The new protocol achieves many of the required security and performance properties. It can resist dictionary attacks mounted by either passive or active network intruders. It can resist Man-In-The Middle attack. It also offers perfect forward secrecy which protects past sessions and passwords against future compromise. In addition, it can resist known-key and resilience to server attack …. Our proposed protocol offers significantly improved performance in computational and communication load over comparably many

authenticated key agreement protocols…"), ANSI X9.63 Overview at 3 ("Specifies key agreement and key transport schemes using elliptic curve cryptography … Specifies a variety of schemes to meet the diverse security needs of communications protocols"), Boyd-Mathuria at VII ("Authentication and key establishment are fundamental building blocks for securing electronic communications. Cryptographic algorithms for encryption and integrity cannot perform their function unless secure keys have been established and the users know which parties share such keys. It is essential that protocols for providing authentication and key establishment are fit for their purpose."), GlobalPlatform at 2 ("For smart cards to reach their true potential, consumers need to be able to use them for a wide variety of functions. For example, the cards can be used with mobile phones to make purchases over the Internet as well as to securely access a PC. Smart cards should also be cost effective and easily multifunctional …. GlobalPlatform defines a flexible and powerful specification for Card Issuers to create single- and multi-Application chip card systems to meet the evolution of their business needs."), Gouget at [0020]-[0022] ("The invention solves the problem of man-in-the-middle attack in case of the exposure of a permanent secret key used to establish a secure channel. There is neither need for an additional device nor an additional mutual authentication. Thanks to the invention, a secure channel is established between the server S and the client C such that the gateway G cannot access to the plaintext data transmitted into the secure channel, even if the permanent secret key skc has been revealed."), Haggerty at [0013]-[0014] ("Accordingly, new solutions and infrastructure are needed to leverage the enhanced flexibility provided by electronic access clients (e.g., eSIMs), and to support secure and ubiquitous distribution thereof. The present disclosure provides, inter alia, for large scale distribution of electronic access control clients."), Lee at [0010]-[0011] ("Unlike the conventional UICC which is manufactured and distributed for

specific mobile communication operators, the newly introduced embedded security module is capable of allowing for the user who has purchased the terminal to install and maintain the authentication information of various mobile communication operators securely and flexibly in such a way of subscribing and unsubscribing to a specific mobile communication operator or switching the subscription between operators. Thus, the present invention aims to provide a method for installing UICC information of various mobile communication operators in an embedded security module (instead of the conventional detachable UICC) remotely through a network.”), Park (IEEE) at Abstract (“Embedded UICC (eUICC) is a new form of UICC … [T]he profiles necessary for its operations should be provisioned remotely into the eUICC by new entity. For the remote provisioning, SM (Subscription Manager) is newly introduced by the standardization organization. However, this new ecosystem around eUICCs can cause tremendous security issues unless thorough consideration of security is accompanied during standardization because the profiles usually include the security-sensitive information. In this paper, a novel secure profile provisioning architecture for eUICCs is proposed. Our architecture mainly defines the overall architecture of the secure profile provisioning for eUICCs.”), Peirce at 1:50-2:2 (“As applied to embedded processing devices, the generation of the cryptographic keys can be problematic because they typically do not have entropy hardware or software engines of the type found in personal computers. Instead pseudo random number generators (PRNG) are typically used. These PRNGs are generally implemented in software and require a seed value that is used to generate a pseudo-random number. This generated number is then used to produce the cryptographic keys. The generation of strong keys using PRNGs generally necessitates the use of a seed value that cannot later be discovered. For an embedded processing device having restricted computing capabilities, obtaining such a seed value can be problematic …. According

to one aspect of the invention, there is provided a method of producing cryptographic keys for use in communicating with a manufactured product"), SCP11 at 11 ("[T]his protocol allows authentication and secure channel initiation based on certificates instead of pre-shared keys. This provides greater flexibility in cases where the two entities setting up the secure channel are not deployed in strict pairs."), SGP.22 at 7 ("The adoption of this technical solution will provide the basis for global interoperability between different Operator deployment scenarios, for example network equipment (e.g. Subscription Manager Data Preparation (SM-DP+)) and various eUICC platforms."), Weiss at [0005] ("[T]he problem addressed by the present invention is to provide for methods and devices that allow providing the secure element of a mobile terminal over-the-air with a subscription profile.").

One of skill in the art would also have been motivated to combine the different publications and patents that were authored by employees of a given company or assigned to the same assignee and/or related to the same subject matter. The common architect of the references demonstrate that they relate to continued work in a common field of effort and continued related developments in that field. Additionally, based on the teachings of the references and/or the knowledge of one of ordinary skill, one of skill in the art would have been motivated to combine different references from the same company. For example, a POSITA would have been motivated to combine at least GlobalPlatform and SCP11, both of which were published by the same company: GlobalPlatform, Inc. And, one of skill in the art would have been motivated to combine prior art systems or products with any related or applicable documentation or literature for that system, including for the reason that these materials are related.

In addition, below are additional motivations to combine prior art for particular claim limitations. The following discussion of specific claim limitations are merely examples and are

not limiting.

For example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach a secure profile provisioning architecture (*e.g.*, limitations 1[A], 1[C][a], 1[C][b], 1[D], 1[D][b], 1[D][d], 1[D][e], 2, 6, 7, 8, 10, 12, 13), it would have been obvious to a person of ordinary skill in the art at the time of the invention to combine the primary reference with any of the prior art that discloses a secure profile provisioning architecture (*e.g.*, limitations 1[A], 1[C][a], 1[C][b], 1[D], 1[D][b], 1[D][d], 1[D][e], 2, 6, 7, 8, 10, 12, 13) in Exhibits C-01 to C-08 or Exhibit C-A. For example, several prior art references, including at least Abi-Char, ANSI X9.63 Overview, Boyd-Mathuria, GlobalPlatform, Gouget, Haggerty, Konstantinou, Lee, Nix, Park (IEEE), Peirce, SCP11, SGP.22, and/or Weiss explicitly describe or disclose a secure profile provisioning architecture. *See, e.g.*, Abi-Char at 1, 2, 3, 4; ANSI X9.63 Overview at 3, 7, 12; Boyd-Mathuria at 49, 81, 125, 136, 140, 141; GlobalPlatform at 156, 174, 194, 198, 202-203, 216, 234, 246-247, 251-253, 255-256, 258, 260, 264, 266-268, 275-276; Gouget at Abstract; Haggerty at Abstract, [0005], [0008], [0015], [0045]-[0046], [0048], [0084], [0100], [0114], [0121], [0131]-[0133]; Lee at Abstract, [0011], [0062]; Park (IEEE) at 297, 300, 301, 303; Peirce at Abstract, 1:6-9, 2:66-3:54, 8:18-51; SCP11 at 12, 13, 20, 30; SGP.22 at 9, 11, 12, 22, 23, 26-28, 51-54, 62-67, 93-94, 131-132; Weiss at [0002], [0012], [0014], [0015], [0020], [0059]-[0062], [0063].

A person skilled in the art would have understood the benefits of a secure profile provisioning architecture, would have recognized that configuring a system to comprise a secure profile provisioning architecture would provide benefits to the system, and would have been motivated to incorporate these features into a system accordingly. For example, a POSITA would have understood that configuring a system to comprise a secure profile provisioning architecture

would yield a complete, secure, and efficient architecture for eUICC profile provisioning. *See, e.g.*, Abi-Char at Abstract ("To provide secure communication for mobile devices, authenticated key agreement protocol is an important primitive for establishing session key …. In this paper we present a fast and Secure Authenticated Key Agreement (EC-SAKA) protocol based on Elliptic Curve Cryptography …. The new protocol achieves many of the required security and performance properties. It can resist dictionary attacks mounted by either passive or active network intruders. It can resist Man-In-The Middle attack. It also offers perfect forward secrecy which protects past sessions and passwords against future compromise. In addition, it can resist known-key and resilience to server attack …. Our proposed protocol offers significantly improved performance in computational and communication load over comparably many authenticated key agreement protocols…"), ANSI X9.63 Overview at 4 ("Specify schemes capable of meeting common security needs"), Boyd-Mathuria at VII ("We believe that this book is the first comprehensive treatment of protocols for authentication and key establishment …. Authentication and key establishment are fundamental building blocks for securing electronic communications. Cryptographic algorithms for encryption and integrity cannot perform their function unless secure keys have been established and the users know which parties share such keys. It is essential that protocols for providing authentication and key establishment are fit for their purpose."), GlobalPlatform at 18-19 ("The GlobalPlatform architecture is designed to provide Card Issuers with the system management architecture for managing these smart cards …. The GlobalPlatform card architecture is comprised of a number of components that ensure hardware and vendor-neutral interfaces to Applications and off-card management systems."), Gouget at [0020]-[0022] ("The invention solves the problem of man-in-the-middle attack in case of the exposure of a permanent secret key used to establish a secure channel. There is neither

need for an additional device nor an additional mutual authentication. Thanks to the invention, a secure channel is established between the server S and the client C such that the gateway G cannot access to the plaintext data transmitted into the secure channel, even if the permanent secret key skc has been revealed.”), Haggerty at [0009]-[0014] (“Prior SIM card based approaches suffer from a number of disabilities. For instance, traditional UICCs support only a single USIM (or more generally ‘SIM’) access control client. If a user wants to authenticate to a cellular network using a different SIM, the user must physically exchange the SIM card in the device with a different SIM card …. The present disclosure provides, inter alia, for large scale distribution of electronic access control clients.”), Lee at Abstract (“The present invention relates to a method and apparatus for installing a profile, and more specifically, to a method for managing mobile communication subscriber information (profile), such as for remotely installing and uninstalling a profile onto a security module (Universal Integrated Circuit Card (UICC)) that is embedded inside a terminal and that is not attachable or detachable, thereby replacing UICC.”), Park (IEEE) at Abstract (“Embedded UICC (eUICC) is a new form of UICC … [T]he profiles necessary for its operations should be provisioned remotely into the eUICC by new entity. For the remote provisioning, SM (Subscription Manager) is newly introduced by the standardization organization. However, this new ecosystem around eUICCs can cause tremendous security issues unless thorough consideration of security is accompanied during standardization because the profiles usually include the security-sensitive information. In this paper, a novel secure profile provisioning architecture for eUICCs is proposed. Our architecture mainly defines the overall architecture of the secure profile provisioning for eUICCs.”), Peirce at 1:6-9 (“The present invention relates generally to techniques for generating cryptographic keys used in secure data communications and, in particular, to such techniques used for manufactured products

having embedded processing devices."), SCP11 at 11 ("[T]his protocol allows authentication and secure channel initiation based on certificates instead of pre-shared keys. This provides greater flexibility in cases where the two entities setting up the secure channel are not deployed in strict pairs."), SGP.22 at 19 ("This section describes the internal high-level architecture of the eUICC …. Operator Profiles are stored inside security domains within the eUICC and are implemented using GlobalPlatform standards. These ensure that it is impossible for any Profile to access the applications or data of any other Profile stored on the eUICC. The same mechanism is currently in use within SIM cards to ensure payment applications are kept secure."), Weiss at [0003] ("It is foreseeable that at least for some of these devices it will not be possible or at least very difficult to provide the secure element beforehand with the necessary subscription credentials, including for instance an IMSI. This is because in a lot of M2M devices the secure element will most likely be implemented in the form of a surface mounted chip or chip module without the possibility of providing the secure element with the necessary subscription credentials beforehand. Consequently, once in the field, these M2M devices and their non-personalized secure elements require the provision of subscription credentials over-the-air."). Thus, a person of ordinary skill in the art would have been motivated to modify any of the primary references to include this feature. A person of ordinary skill in the art would also have had a reasonable expectation of success. A person of ordinary skill in the art would have understood that these references disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach procedures for mutual authentication and/or sensitive data encryption (*e.g.*, limitations 1[B], 1[C][a], 1[C][b], 1[D][b], 1[D][d], 1[D][e], 9, 12, 13, 14), it would have

been obvious to a person of ordinary skill in the art at the time of the invention to combine the primary reference with any of the prior art that discloses procedures for mutual authentication and/or sensitive data encryption (*e.g.*, limitations 1[B], 1[C][a], 1[C][b], 1[D][b], 1[D][d], 1[D][e], 9, 12, 13, 14) in Exhibits C-01 to C-08 or Exhibit C-A. For example, several prior art references, including at least Abi-Char, ANSI X9.63 Overview, Boyd-Mathuria, GlobalPlatform, Gouget, Haggerty, Konstantinou, Lee, Nix, Park (IEEE), Peirce, SCP11, SGP.22, and/or Weiss explicitly describe or disclose procedures for mutual authentication and/or sensitive data encryption. *See, e.g.*, Abi-Char at 1, 2, 3, 4; ANSI X9.63 Overview at 3, 7, 12; Boyd-Mathuria at 49, 81, 125, 136, 140, 141; GlobalPlatform at 156, 174, 194, 198, 202-203, 216, 234, 246-247, 251-253, 255-256, 258, 260, 264, 266-268, 275-276; Gouget at Abstract; Haggerty at Abstract, [0008], [0015], [0045]-[0046], [0048], [0084], [0100], [0114], [0121], [0131]-[0133]; Lee at Abstract, [0011], [0062]; Park (IEEE) at 297, 300, 301, 303; Peirce at Abstract, 1:6-9, 2:66-3:54, 8:18-51; SCP11 at 12, 13, 20, 30; SGP.22 at 9, 11, 12, 17, 22, 23, 24, 26-28, 51-54, 62-67, 75, 81, 93-94, 131-132, 202, 210; Weiss at [0012], [0014], [0015], [0038], [0042], [0063].

A person skilled in the art would have understood the benefits of procedures for mutual authentication and/or sensitive data encryption, would have recognized that configuring a system to comprise procedures for mutual authentication and/or sensitive data encryption would provide benefits to the system, and would have been motivated to incorporate these features into a system accordingly. For example, a POSITA would have understood that configuring a system to comprise procedures for mutual authentication and/or sensitive data encryption would yield a complete, secure, and efficient architecture for eUICC profile provisioning. Indeed, a POSITA would have recognized that applying procedures for mutual authentication and/or sensitive data encryption would provide an additional layer of protection for the most sensitive data within the

profile, ensuring that even if some aspects were compromised, the critical key materials could remain protected. *See, e.g.*, Abi-Char at Abstract ("To provide secure communication for mobile devices, authenticated key agreement protocol is an important primitive for establishing session key …. In this paper we present a fast and Secure Authenticated Key Agreement (EC-SAKA) protocol based on Elliptic Curve Cryptography …. The new protocol achieves many of the required security and performance properties. It can resist dictionary attacks mounted by either passive or active network intruders. It can resist Man-In-The Middle attack. It also offers perfect forward secrecy which protects past sessions and passwords against future compromise. In addition, it can resist known-key and resilience to server attack …. Our proposed protocol offers significantly improved performance in computational and communication load over comparably many authenticated key agreement protocols…"), ANSI X9.63 Overview at 4 ("Specify schemes capable of meeting common security needs"), Boyd-Mathuria at VII ("We believe that this book is the first comprehensive treatment of protocols for authentication and key establishment …. Authentication and key establishment are fundamental building blocks for securing electronic communications. Cryptographic algorithms for encryption and integrity cannot perform their function unless secure keys have been established and the users know which parties share such keys. It is essential that protocols for providing authentication and key establishment are fit for their purpose."), GlobalPlatform at 23 ("The primary goal of the GlobalPlatform is to ensure the security and integrity of the card's components for the life of the card …. To ensure card security and integrity, the GlobalPlatform is designed to support a range of secure mechanisms for: Data integrity; Resource availability; Confidentiality; Authentication."), Gouget at [0020]-[0022] ("The invention solves the problem of man-in-the-middle attack in case of the exposure of a permanent secret key used to establish a secure channel. There is neither need for an additional

device nor an additional mutual authentication. Thanks to the invention, a secure channel is established between the server S and the client C such that the gateway G cannot access to the plaintext data transmitted into the secure channel, even if the permanent secret key skc has been revealed."), Haggerty at [0009]-[0014] ("Prior SIM card based approaches suffer from a number of disabilities. For instance, traditional UICCs support only a single USIM (or more generally 'SIM') access control client. If a user wants to authenticate to a cellular network using a different SIM, the user must physically exchange the SIM card in the device with a different SIM card …. The present disclosure provides, inter alia, for large scale distribution of electronic access control clients."), Lee at [0005]-[0011] ("The conventional UICC is manufactured on demand as a dedicated card for a specific mobile communication operator. Accordingly, the authentication information (e.g. USIM application, IMSI, and K value) for connection to the corresponding operator network is stored in the UICC in the manufacturing stage. The mobile communication operator provides the subscriber with the manufactured UICC," and "[t]he subscriber may insert the UICC into a mobile communication terminal to use the corresponding mobile communication operator' s network and application services and, if necessary, may detach the UICC from the terminal and attach to another terminal so as to use the authentication information, contacts, and phonebooks stored in the corresponding UICC with the new terminal as they were …. Unlike the conventional UICC which is manufactured and distributed for specific mobile communication operators, the newly introduced embedded security module is capable of allowing for the user who has purchased the terminal to install and maintain the authentication information of various mobile communication operators securely and flexibly in such a way of subscribing and unsubscribing to a specific mobile communication operator or switching the subscription between operators. Thus, the present invention aims to provide a method for installing UICC

information of various mobile communication operators in an embedded security module (instead of the conventional detachable UICC) remotely through a network."), Park (IEEE) at Abstract ("[T]his new ecosystem around eUICCs can cause tremendous security issues unless thorough consideration of security is accompanied during standardization because the profiles usually include the security-sensitive information."), Peirce at 1:21- 25 ("In some cases, it is desirable to establish authenticated, secure data communications in which the exchanged data is encrypted. Although various approaches can be used, cryptographic keys are perhaps most commonly used for this purpose"), SCP11 at 11 ("[T]his protocol allows authentication and secure channel initiation based on certificates instead of pre-shared keys. This provides greater flexibility in cases where the two entities setting up the secure channel are not deployed in strict pairs."), SGP.22 at 33 ("The RSP ecosystem relies on remote secure communication to achieve function execution requests and data exchanges. Any of the remote secure communication defined for RSP SHALL follow the hereunder rules … Mutual authentication[,] Data privacy[,] Communication protection[,] Authorisation[.]"), Weiss at [0014] ("Preferably, the first server decrypts the encrypted version of the identification element IDse, the encrypted version of the session key Kses and the encrypted version of the hardware configuration HWconf of the secure element and/or the mobile terminal using the configuration key Kconf provided by the second server so that the first server can verify the validity of the configuration key Kconf provided by the second server by verifying that the identification element IDse sent in the clear is identical to the identification element IDse resulting from the decryption of the encrypted version of the identification element IDse using the configuration key Kconf."). Thus, a person of ordinary skill in the art would have been motivated to modify any of the primary references to include this feature. A person of ordinary skill in the art would also have had a reasonable expectation of

success. A person of ordinary skill in the art would have understood that these references disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach key exchange and/or agreement protocols or mechanisms (*e.g.*, limitations 1[B], 1[C][a], 1[C][b], 1[D][a], 1[D][c], 1[D][d], 1[D][e], 14), it would have been obvious to a person of ordinary skill in the art at the time of the invention to combine the primary reference with any of the prior art that discloses key exchange and/or agreement protocols or mechanisms (*e.g.*, limitations 1[B], 1[C][a], 1[C][b], 1[D][a], 1[D][c], 1[D][d], 1[D][e], 14) in Exhibits C-01 to C-08 or Exhibit C-A. For example, several prior art references, including at least Abi-Char, ANSI X9.63 Overview, Boyd-Mathuria, GlobalPlatform, Gouget, Haggerty, Konstantinou, Lee, Nix, Park (IEEE), Peirce, SCP11, SGP.22, and/or Weiss explicitly describe or disclose key exchange and/or agreement protocols or mechanisms. *See, e.g.*, Abi-Char at 1, 3; ANSI X9.63 Overview at 3, 7, 12; Boyd-Mathuria at 49, 81, 125, 136, 140, 141; GlobalPlatform at 156, 174, 194, 198, 202-203, 216, 234, 246-247, 251-253, 255-256, 258, 260, 264, 266-268, 275-276; Gouget at Abstract; Haggerty at Abstract, [0008], [0015], [0045]-[0046], [0048], [0084], [0100], [0114], [0121], [0131]-[0133]; Lee at Abstract, [0011], [0062]; Park (IEEE) at 297, 300, 301, 303; Peirce at Abstract, 1:6-9, 2:66-3:54, 8:18-51; SCP11 at 12, 13, 20, 30; SGP.22 at 15, 27-28, 34, 51-53, 62-65, 93-94, 131-132, 140, 210; Weiss at [0002], [0010]-[0011], [0012], [0014], [0015], [0020], [0046], [0063].

A person skilled in the art would have understood the benefits of key exchange and/or agreement protocols or mechanisms, would have recognized that configuring a system to comprise key exchange and/or agreement protocols or mechanisms would provide benefits to the

system, and would have been motivated to incorporate these features into a system accordingly. For example, a POSITA would have understood that configuring a system to comprise key exchange and/or agreement protocols or mechanisms would yield a complete, secure, and efficient architecture for eUICC profile provisioning. Indeed, a POSITA would have recognized that configuring a system to comprise key exchange and/or agreement protocols or mechanisms would provide an additional layer of protection for the most sensitive data within the profile. Key exchange and/or agreement protocols or mechanisms were well-established and known to provide confidentiality, integrity, and mutual authentication. *See, e.g.*, Abi-Char at Abstract ("To provide secure communication for mobile devices, authenticated key agreement protocol is an important primitive for establishing session key …. In this paper we present a fast and Secure Authenticated Key Agreement (EC-SAKA) protocol based on Elliptic Curve Cryptography …. The new protocol achieves many of the required security and performance properties. It can resist dictionary attacks mounted by either passive or active network intruders. It can resist Man-In-The Middle attack. It also offers perfect forward secrecy which protects past sessions and passwords against future compromise. In addition, it can resist known-key and resilience to server attack …. Our proposed protocol offers significantly improved performance in computational and communication load over comparably many authenticated key agreement protocols…"), ANSI X9.63 Overview at 3 ("Specifies key agreement and key transport schemes using elliptic curve cryptography … Specifies a variety of schemes to meet the diverse security needs of communications protocols"), Boyd-Mathuria at VII ("We believe that this book is the first comprehensive treatment of protocols for authentication and key establishment …. Authentication and key establishment are fundamental building blocks for securing electronic communications. Cryptographic algorithms for encryption and integrity cannot perform their

function unless secure keys have been established and the users know which parties share such keys. It is essential that protocols for providing authentication and key establishment are fit for their purpose."), GlobalPlatform at 23 ("The primary goal of the GlobalPlatform is to ensure the security and integrity of the card's components for the life of the card …. Because the cards are only part of a larger card system involving multiple parties and off-card components, the GlobalPlatform also relies upon non-cryptographic, procedural means of protection, such as code testing and verification, physical security, and secure key handling."), Gouget at [0020]-[0022] ("The invention solves the problem of man-in-the-middle attack in case of the exposure of a permanent secret key used to establish a secure channel. There is neither need for an additional device nor an additional mutual authentication. Thanks to the invention, a secure channel is established between the server S and the client C such that the gateway G cannot access to the plaintext data transmitted into the secure channel, even if the permanent secret key skc has been revealed."), Haggerty at [0009]-[0014] ("Prior SIM card based approaches suffer from a number of disabilities. For instance, traditional UICCs support only a single USIM (or more generally 'SIM') access control client. If a user wants to authenticate to a cellular network using a different SIM, the user must physically exchange the SIM card in the device with a different SIM card …. The present disclosure provides, inter alia, for large scale distribution of electronic access control clients."), Lee at [0016] ("According to an embodiment of the present invention, a profile management server for managing the embedded security module of a terminal and a profile provision server for generating a UICC profile in association with a specific mobile communication operator are separated such that the terminal encodes a session key and authenticate the profile with a digital certificate provided by the profile provision server and thus can transfer the encoded profile to the embedded security module of the terminal without

exposing the content of the profile to the profile management server positioned between the profile provision server and the terminal."), Park (IEEE) at 301 ("KAM is software running inside the eUICC to perform the key agreement protocol …. For the security, the SM-DP Credentials should not be revealed to any party, even SM-SR, except for eUICC. To accomplish this, KAM is designed and applied to SPA."), Peirce at 1:50-2:2 ("As applied to embedded processing devices, the generation of the cryptographic keys can be problematic because they typically do not have entropy hardware or software engines of the type found in personal computers. Instead pseudo random number generators (PRNG) are typically used. These PRNGs are generally implemented in software and require a seed value that is used to generate a pseudo-random number. This generated number is then used to produce the cryptographic keys. The generation of strong keys using PRNGs generally necessitates the use of a seed value that cannot later be discovered. For an embedded processing device having restricted computing capabilities, obtaining such a seed value can be problematic …. According to one aspect of the invention, there is provided a method of producing cryptographic keys for use in communicating with a manufactured product"), SCP11 at 11 ("[T]his protocol allows authentication and secure channel initiation based on certificates instead of pre-shared keys. This provides greater flexibility in cases where the two entities setting up the secure channel are not deployed in strict pairs."), SGP.22 at 93-94 ("Public key of the eUICC used to verify an eUICC signature …. Private key of the SM-DS used to provide signatures for authentication to the eUICC …. Public key of the EUM used to verify EUICC Certificates …. One-time public key of the EUICC used for key agreement …. One-time private key of the EUICC used for key agreement."), Weiss at [0002]-[0005] ("[T]he SIM contains subscription credentials for authenticating and identifying the user of the mobile terminal, including in particular an International Mobile Subscriber Identity (IMSI)

and an authentication key Ki. These subscription credentials are generally stored on the SIM by the SIM manufacturer/vendor or the MNO during a SIM personalization process prior to providing the user of the mobile terminal with his SIM …. [T]he problem addressed by the present invention is to provide for methods and devices that allow providing the secure element of a mobile terminal over-the-air with a subscription profile.”). Thus, a person of ordinary skill in the art would have been motivated to modify any of the primary references to include this feature. A person of ordinary skill in the art would also have had a reasonable expectation of success. A person of ordinary skill in the art would have understood that these references disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach random number generation protocols (*e.g.*, limitations 1[B], 4, 5), it would have been obvious to a person of ordinary skill in the art at the time of the invention to combine the primary reference with any of the prior art that discloses random number generation protocols (*e.g.*, limitations 1[B], 4, 5) in Exhibits C-01 to C-08 or Exhibit C-A. For example, several prior art references, including at least Abi-Char, ANSI X9.63 Overview, Boyd-Mathuria, GlobalPlatform, Gouget, Haggerty, Konstantinou, Nix, Park (IEEE), Peirce, SGP.22, and/or Weiss explicitly describe or disclose random number generation protocols. *See, e.g.*, Abi-Char at 3; ANSI X9.63 Overview at 6, 10; Boyd-Mathuria at 9, 136, 140, 141; GlobalPlatform at 194; Gouget at Abstract, [0011]-[0012], [0036], [0040]-[0041]; Haggerty at [0121]; Park (IEEE) at 300, 301; Peirce at Abstract, 8:18-51; SGP.22 at 27-28, 35, 62, 63, 94; Weiss at [0046].

A person skilled in the art would have understood the benefits of random number generation protocols, would have recognized that configuring a system to comprise random

number generation protocols would provide benefits to the system, and would have been motivated to incorporate these features into a system accordingly. For example, a POSITA would have understood that configuring a system to comprise random number generation protocols would improve the security of the system by helping to ensure that the keys used in the exchanges were derived from sufficiently random and unpredictable sources that were readily available to the eUICC-storing devices in these systems. *See, e.g.*, Abi-Char at 2 ("Because round trips and large blocks are critical factors in terms of communication load and because exponentiations and random numbers are to be critical factors in terms of computation load, such properties are listed below: Computational efficiency[,] Communication efficiency[,] Nature of security guarantees[,] Storage of secrets."), ANSI X9.63 Overview at 6 ("A number of primitives (mathematical building blocks) must be specified in order to build schemes …. Curves selected in any manner. Verifiably random selection option"), Boyd-Mathuria at 9 ("There are various mechanisms that may be employed to allow users to check that session keys have not been replayed …. In this method, A will generate a new random value NA commonly known as a nonce (a number used only once). Definition 1.1. A nonce is a random value generated by one party and returned to that party to show that a message is newly generated."), GlobalPlatform at 194 ("The Secure Channel is always initiated … by the off-card entity by passing a 'host' challenge (random data unique to this Secure Channel Session) to the card. The card, on receipt of this challenge, generates its own 'card' challenge (again random data unique to this Secure Channel Session). The card, using the host challenge, the card challenge and its internal static keys, creates new secret Secure Channel session keys and generates a first cryptographic value (card cryptogram) using one of its newly created Secure Channel session keys …. This card cryptogram along with the card challenge, the Secure Channel Protocol identifier, and other data is transmitted back to

the off-card entity. As the off-card entity should now have all the same information that the card used to generate the card cryptogram, it should be able to generate the same Secure Channel session keys and the same card cryptogram and by performing a comparison, it is able to authenticate the card.”), Gouget at [0020]-[0022] (“The invention solves the problem of man-in-the-middle attack in case of the exposure of a permanent secret key used to establish a secure channel. There is neither need for an additional device nor an additional mutual authentication. Thanks to the invention, a secure channel is established between the server S and the client C such that the gateway G cannot access to the plaintext data transmitted into the secure channel, even if the permanent secret key skc has been revealed.”), Haggerty at [0121] (“When the user exports an eSIM, the AP retrieves a list of installed profiles from eUICC; for each profile, eUICC also returns the associated principal and a nonce generated for anti-replay. When the user chooses to export a profile, the AP uses information contained in the principal to obtain a single sign-on (SSO) token from the service provider, where the user would be prompted to enter username and password for the purpose. The SSO token is passed together with principal and nonce to the server broker in export request. The server broker can process the authentication with the service provider, using the SSO token supplied by the device. Once authentication passes, the flow mirrors eSIM delivery to the device, except that the client and server roles are reversed. At a high level, the server broker initiates a session with the eUICC, creates a request BLOB for the export. In the request, it includes the nonce that the eUICC generated, to indicate that the operation has passed L3 authentication. The eUICC verifies the request BLOB, encrypts the eSIM with the server agent’s public key, creates a batch descriptor and L3 owner information for the eSIM. The eSIM together with L3 and L2 information can be sent to the server.”), Park (IEEE) at 301 (“KAM is software running inside the eUICC to perform the key agreement

protocol …. For the security, the SM-DP Credentials should not be revealed to any party, even SM-SR, except for eUICC. To accomplish this, KAM is designed and applied to SPA.”), Peirce at 1:50-2:2 (“As applied to embedded processing devices, the generation of the cryptographic keys can be problematic because they typically do not have entropy hardware or software engines of the type found in personal computers. Instead pseudo random number generators (PRNG) are typically used. These PRNGs are generally implemented in software and require a seed value that is used to generate a pseudo-random number. This generated number is then used to produce the cryptographic keys. The generation of strong keys using PRNGs generally necessitates the use of a seed value that cannot later be discovered. For an embedded processing device having restricted computing capabilities, obtaining such a seed value can be problematic …. According to one aspect of the invention, there is provided a method of producing cryptographic keys for use in communicating with a manufactured product”), SGP.22 at 28 (“Profile protection can optionally be performed using … random keys per Profile…”), Weiss at [0046] (“Preferably, the session key Kses is a nonce, i.e. an arbitrary number used only once. This ensures that for every subscription profile update session, such as the subscription profile update session shown in FIG. 2, a different session key Kses is used. As is well known to the person skilled in the art, such a nonce can be created, for instance, by using a pseudorandom number generator, preferably a cryptographically secure pseudorandom number generator.”). Thus, a person of ordinary skill in the art would have been motivated to modify any of the primary references to include this feature. A person of ordinary skill in the art would also have had a reasonable expectation of success. A person of ordinary skill in the art would have understood that these references disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach specific types or aspects of connected or networked devices (*e.g.*, limitations 1[PRE], 1[A], 1[B], 1[C], 1[D][c], 4, 5, 6, 7, 8, 10, 12, 13, 15, 16, 17), it would have been obvious to a person of ordinary skill in the art at the time of the invention to combine the primary reference with any of the prior art that discloses specific types or aspects of connected or networked devices (*e.g.*, limitations 1[PRE], 1[A], 1[B], 1[C], 1[D][c], 4, 5, 6, 7, 8, 10, 12, 13, 15, 16, 17) in Exhibits C-01 to C-08 or Exhibit C-A. For example, several prior art references, including at least Abi-Char, ANSI X9.63 Overview, Boyd-Mathuria, GlobalPlatform, Gouget, Haggerty, Konstantinou, Lee, Nix, Park (IEEE), Peirce, SGP.22, and/or Weiss explicitly describe or disclose specific types or aspects of connected or networked devices. *See, e.g.*, Abi-Char at Abstract; ANSI X9.63 Overview at 3, 7, 12, 22; Boyd-Mathuria at 23, 24, 126-131, 175, 177, 190-193; GlobalPlatform at 2; Gouget at [0051]; Haggerty at [0017], [0042], [0131]; Lee at Abstract, [0001], [0107]; Park (IEEE) at Abstract, 297, 298; Peirce at Abstract, 3:8-23, 3:64-4:42, 4:43-54, 6:29-65, 7:16-33; SGP.22 at 7, 9, 11, 17, 200; Weiss at [0020], [0031], [0033].

A person skilled in the art would have understood the benefits of applying teachings to specific types or aspects of connected or networked devices, would have recognized that configuring a system to comprise specific types or aspects of connected or networked devices would provide benefits to the system, and would have been motivated to incorporate these features into a system accordingly. For example, a POSITA would have understood that applying teachings to specific types or aspects of connected or networked devices would broaden the applicability of the disclosed systems. Incorporating specific types or aspects of connected or networked devices would have amounted to a straightforward substitution of one known secure element implementation for another, yielding predictable results. *See, e.g.*, Abi-Char at Abstract

("The increased progress in wireless mobile communication has attracted an important amount of attention on the security issue."), ANSI X9.63 Overview at 3 ("Primarily designed to meet the needs of the financial services industry, but also generally applicable"), Boyd-Mathuria at 193 ("Despite the inexorable increase in the availability of computing resources there has been considerable interest in protocols that can be implemented on devices with limited computational power. Typical examples of such devices are mobile terminals and embedded hardware. Very often the low-power device is a client required to establish a key with a computationally powerful server and so an acceptable solution may have unbalanced computational requirements: the server end can bear an increased computational load in order to ease the burden on the client side. Another technique that is effective is to allow the client side to pre-compute values which can be used during the protocol execution; mobile terminals typically have the opportunity to make off-line computations during the idle time between awaiting calls."), GlobalPlatform at 2 ("For smart cards to reach their true potential, consumers need to be able to use them for a wide variety of functions. For example, the cards can be used with mobile phones to make purchases over the Internet as well as to securely access a PC. Smart cards should also be cost effective and easily multifunctional."), Gouget at [0051] ("It will be well understood that a smartcard with a middle-ware installed on a smartcard host is not a limited example. The invention can be advantageously applied to any web service deployment with a client-middleware installed in the dubious environment of a smartcard host such as a user's PC."), Haggerty at [0007] ("Access control is required for secure communication in most prior art wireless radio communication systems."), Lee at [0011] ("Thus, the present invention aims to provide a method for installing UICC information of various mobile communication operators in an embedded security module (instead of the conventional detachable UICC) remotely through a network."), Park (IEEE) at

297 ("The eUICC was initially considered to be utilized as the same roles of UICC [to] be adopted into the small device … These days, the fields of its usages are being considered to be extended to the CEDs (Consumer Electronic Devices) for the smaller form factor to save the physical space of the device."), Peirce at 1:13-30 ("As computer electronics continue to reduce in cost and size, the applications for embedded processing devices are continuing to increase, and there now exists many types of manufactured products that contain some type of embedded processing device, whether microprocessor based or otherwise. Some embedded devices are designed to undergo data communication with one or more external, possibly remote devices. In some cases, it is desirable to establish authenticated, secure data communications in which the exchanged data is encrypted."), SGP.22 at 7 ("This document defines a technical solution for the remote provisioning and management of the Embedded UICC (eUICC) in consumer Devices as defined in RSP Architecture …. The adoption of this technical solution will provide the basis for global interoperability between different Operator deployment scenarios, for example network equipment (e.g. Subscription Manager Data Preparation (SM-DP+)) and various eUICC platforms."), Weiss at [0003] ("One particular field of application of secure elements, such as SIMs, eUICCs, UICCs and the like, which is expected to grow rapidly in the near future is M2M (machine-to-machine) communication, i.e. the communication between machines over a cellular communications network without human intervention, also called the Internet of things …. It is foreseeable that at least for some of these devices it will not be possible or at least very difficult to provide the secure element beforehand with the necessary subscription credentials, including for instance an IMSI. This is because in a lot of M2M devices the secure element will most likely be implemented in the form of a surface mounted chip or chip module without the possibility of providing the secure element with the necessary subscription credentials beforehand.

Consequently, once in the field, these M2M devices and their non-personalized secure elements require the provision of subscription credentials over-the-air.”). Thus, a person of ordinary skill in the art would have been motivated to modify any of the primary references to include this feature. A person of ordinary skill in the art would also have had a reasonable expectation of success. A person of ordinary skill in the art would have understood that these references disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

VI. U.S. Patent No. 11,973,864 (“the ’864 Patent”)

A. Identification of Prior Art

Defendants incorporate by reference, as if set forth fully herein, all filings and exhibits from *Inter Partes* Review IPR2026-00116, filed November 7, 2025 with the PTAB, including any subsequent and future filings in that case.

In addition to the prior art cited on the face of the ’864 Patent and related patents, the admitted prior art in the specifications of the ’864 Patent and related patents, the prior art cited in any file histories, reexaminations, *inter partes* review proceedings, reissue proceedings, or other examination or post-grant proceedings of the ’864 Patent and related patents, and the prior art cited in any invalidity contentions or expert reports submitted in any action or proceedings involving the ’864 Patent or related patents, Defendants identify the following prior art that anticipates each asserted claim or renders it obvious.

1. Prior Art Patents

The following patents and patent publications are prior art to the asserted claims under at least 35 U.S.C. §§ 102(a)(1) and/or (a)(2), and/or 35 U.S.C. § 103. The identification of any patent or patent publication shall be deemed to include any counterpart patent or application filed, published, or issued anywhere in the world.

Patent or Publication Number	Country of Origin	Filing Date	Date of Issue or Publication
U.S. Pat. App. Pub. No. 2012/0300934 ("Ala-Laurila '934")	United States	August 9, 2012	November 29, 2012
U.S. Pat. App. Pub. No. 2010/0135491 ("Bhuyan '491")	United States	January 22, 2008	June 3, 2010
U.S. Pat. App. Pub. No. 2014/0024343 ("Bradley '343")	United States	December 2, 2011	October 10, 2013
U.S. Pat. App. Pub. No. 2007/0083766A1 ("Farnham '766")	United States	October 19, 2006	April 12, 2007
U.S. Pat. App. Pub. No. 2013/0301828 ("Gouget '828")	United States	September 6, 2011	November 14, 2013
U.S. Pat. App. Pub. No. 2004/0221163A1 ("Jorgensen '163")	United States	January 16, 2004	November 4, 2004
U.S. Pat. App. Pub. No. 2009/0323967A1 ("Peirce '967")	United States	June 30, 2008	December 31, 2009
U.S. Pat. App. Pub. No. 2009/0068985 ("Nguyen '985")	United States	September 12, 2007	March 12, 2009
U.S. Pat. No. 8,391,841 ("Semple '841")	United States	May 23, 2011	March 5, 2013
PCT Pat. App. Pub. No. WO2008/005162 ("Wang '162")	World Intellectual Property Organization (Patent Cooperation Treaty)	June 14, 2007	January 10, 2007

2. Prior Art Non-Patent Publications

The following non-patent publications are prior art to the asserted claims under at least 35 U.S.C. §§ 102(a)(1) and/or (a)(2), and/or 35 U.S.C. § 103.

Title	Author/Publisher	Date of Publication
A Design of Safe AKA Module for Adapted Mobile Payment System on Openness Smartphone Environment ("Jeong (2010)")[11]	Jeong et al., Journal of Korea Multimedia Society Vol. 13, No. 11	November 2010
ANSI X9.63 Overview: *Key Agreement and Key Transport Using Elliptic Curve Cryptography* ("ANSI X9.63 Overview")	Blake-Wilson, Certicom Corp.	2000
Protocols for Authentication and Key Establishment ("Boyd-Mathuria")	Colin Boyd & Anish Mathuria, Springer	2003
Certicom Research, Standards for Efficient Cryptography, SEC 1: Elliptic Curve Cryptography ("SEC-1")	Brown, Certicom Corp.	May 2009

3. Prior Art Systems

Defendants' investigation into publicly available prior art systems that teach and/or render obvious each element of any asserted claims is ongoing. Fact discovery is at an early stage, and Defendants may require discovery from third parties regarding publicly available prior art systems. On information and belief, prior art systems from the following companies teach and/or render obvious each element of the asserted claims of the '864 Patent: Cinterion (now Telit); Gemalto (now Thales); Giesecke+Devrient; GlobalPlatform; NXP Semiconductors N.V.; Oberthur Technologies (now IDEMIA); and Sierra Wireless. Defendants reserve the right to amend its identification of prior art systems as Defendants become aware of the existence, functionality, and/or characteristics of prior art systems as a result of its investigation and forthcoming discovery. In addition to the prior art products, components, systems, and methods

[11] Jeong was originally published in Korean. References to Jeong in these contentions are to a certified translation of the original Korean paper. Both the original and the certified translation of Jeong are included in the accompanying document production.

that may be identified as a result of discovery, Defendants also reserve the right to rely on the documents and publications identified in the corresponding claim charts as prior art publications.

B. Primary References

Defendants contend that the primary prior art references identified below and described in the charts attached as Exhibits D-01 to D-09, by themselves, anticipate the asserted claims of the ’864 Patent. To the extent that a primary reference is deemed not to anticipate a claim for failing to teach one or more limitations of that claim, Defendants contend that the claim would nonetheless have been obvious to a person of ordinary skill in the art at the time of the invention in view of the prior art reference itself, as described in the attached charts. Defendants’ prior art charts (attached as Exhibits D-01 to D-09) set forth the particular claims that are anticipated under 35 U.S.C. § 102 and/or rendered obvious under 35 U.S.C. § 103 by each item of prior art and identify where specifically in each item of prior art, each element of each asserted claim is found.

Exhibit	Primary References
D-01	U.S. Pat. App. Pub. No. 2012/0300934 (“Ala-Laurila ’934”)
D-02	U.S. Pat. App. Pub. No. 2010/0135491 (“Bhuyan ’491”)
D-03	Boyd and Mathuria, *Protocols for Authentication and Key Establishment* (“Boyd-Mathuria”)
D-04	U.S. Pat. App. Pub. No. 2007/0083766A1 (“Farnham ’766”)
D-05	Jeong et al., *A Design of Safe AKA Module for Adapted Mobile Payment System on Openness Smartphone Environment* (“Jeong (2010)”)
D-06	U.S. Pat. App. Pub. No. 2009/0323967A1 (“Peirce ’967”)
D-07	U.S. Pat. App. Pub. No. 2009/0068985 (“Nguyen ’985”)
D-08	U.S. Pat. No. 8,391,841 (“Semple ’841”)
D-09	PCT Pat. App. Pub. No. WO2008/005162 (“Wang ’162”)

C. Secondary References

Exhibit D-A lists secondary prior art references and identifies, on a limitation-by-limitation basis, where specifically each secondary reference teaches the limitations of the asserted claims. To the extent that a primary reference is deemed, by itself, not to anticipate or render obvious a claim for failing to teach one or more limitations, the claim would nonetheless have been obvious to a person of ordinary skill in the art at the time of the invention by the combination of the primary reference with one or more of the other primary references listed above and/or the references listed as disclosing those alleged missing limitations in Exhibit D-A.

D. Obvious Combinations

To the extent that a primary reference is deemed, by itself, not to anticipate or render obvious a claim for failing to teach one or more limitations, the claim would nonetheless have been obvious to a person of ordinary skill in the art at the time of the invention by the combination of the primary reference with one or more other primary references and/or the knowledge of someone skilled in the art. For example, a person of ordinary skill in the art would have been motivated to combine any reference in Exhibits D-01 to D-09 with any other reference(s) in Exhibits D-01 to D-09. Such combinations would be achieved, for example, by merely combining the disclosures described in the respective claim charts for each reference.

Defendants also contend that any of the primary references (or combination of primary references) could be combined with any of the secondary references (or combination of secondary references) in Exhibit D-A to render obvious the asserted claims. Such combinations would be achieved by merely combining the disclosures described in the respective claim charts for each reference.

The obviousness combinations are provided in the alternative to Defendants' anticipation contentions and are not to be construed to suggest that any reference included in the combinations is not itself anticipatory.

1. Exemplary Combinations

Below are examples of prior art references that would have been combined by one of ordinary skill in the art at the time of the alleged invention. These combinations are merely examples. The asserted claims of the '864 Patent are rendered obvious by:

- Semple '841 in combination with Wang '162.
- Semple '841 in combination with Bhuyan '491 and/or Wang '162.
- Semple '841 in combination with Peirce '967 and/or Wang '162.
- Semple '841 in combination with Jorgensen '163 and/or Wang '162.
- Semple '841 in combination with SEC-1 and/or Wang '162.
- Semple '841 in combination with Bhuyan '491, SEC-1, and/or Wang '162.
- Semple '841 in combination with Peirce '967, SEC-1, and/or Wang '162.
- Semple '841 in combination with Jorgensen '163, SEC-1, and/or Wang '162.
- Ala-Laurila '934 alone or in combination with one or more of Bhuyan '491, Boyd-Mathuria, Farnham '766, Jeong (2010), Nguyen '985, Peirce '967, Semple '841, Wang '162, Bradley '343, Gouget '828, Jorgensen '163, SEC-1, and/or ANSI X9.63 Overview.
- Bhuyan '491 alone or in combination with one or more of Ala-Laurila '934, Boyd-Mathuria, Farnham '766, Jeong (2010), Nguyen '985, Peirce '967, Semple '841, Wang '162, Bradley '343, Gouget '828, Jorgensen '163, SEC-1, and/or ANSI X9.63 Overview.

- Boyd-Mathuria alone or in combination with one or more of Ala-Laurila ’934, Bhuyan ’491, Farnham ’766, Jeong (2010), Nguyen ’985, Peirce ’967, Semple ’841, Wang ’162, Bradley ’343, Gouget ’828, Jorgensen ’163, SEC-1, and/or ANSI X9.63 Overview.
- Farnham ’766 alone or in combination with one or more of Ala-Laurila ’934, Bhuyan ’491, Boyd-Mathuria, Jeong (2010), Nguyen ’985, Peirce ’967, Semple ’841, Wang ’162, Bradley ’343, Gouget ’828, Jorgensen ’163, SEC-1, and/or ANSI X9.63 Overview.
- Jeong (2010) alone or in combination with one or more of Ala-Laurila ’934, Bhuyan ’491, Boyd-Mathuria, Farnham ’766, Nguyen ’985, Peirce ’967, Semple ’841, Wang ’162, Bradley ’343, Gouget ’828, Jorgensen ’163, SEC-1, and/or ANSI X9.63 Overview.
- Nguyen ’985 alone or in combination with one or more of Ala-Laurila ’934, Bhuyan ’491, Boyd-Mathuria, Farnham ’766, Jeong (2010), Peirce ’967, Semple ’841, Wang ’162, Bradley ’343, Gouget ’828, Jorgensen ’163, SEC-1, and/or ANSI X9.63 Overview.
- Peirce ’967 alone or in combination with one or more of Ala-Laurila ’934, Bhuyan ’491, Boyd-Mathuria, Farnham ’766, Jeong (2010), Nguyen ’985, Semple ’841, Wang ’162, Bradley ’343, Gouget ’828, Jorgensen ’163, SEC-1, and/or ANSI X9.63 Overview.
- Semple ’841 alone or in combination with one or more of Ala-Laurila ’934, Bhuyan ’491, Boyd-Mathuria, Farnham ’766, Jeong (2010), Nguyen ’985, Peirce

’967, Wang ’162, Bradley ’343, Gouget ’828, Jorgensen ’163, SEC-1, and/or ANSI X9.63 Overview.

- Wang ’162 alone or in combination with one or more of Ala-Laurila ’934, Bhuyan ’491, Boyd-Mathuria, Farnham ’766, Jeong (2010), Nguyen ’985, Peirce ’967, Semple ’841, Bradley ’343, Gouget ’828, Jorgensen ’163, SEC-1, and/or ANSI X9.63 Overview.

2. Motivations to Combine

To the extent a finder of fact finds that a primary prior art reference does not disclose one or more limitations of an asserted claim, the asserted claim is nevertheless obvious because the allege missing limitations contain nothing beyond ordinary improvements. In other words, the asserted claim combines known elements to achieve predictable results or chooses between clear alternatives known to those of skill in the art, particularly in view of the state of the art as reflected in the relevant prior art.

Moreover, as explained above, it would have been obvious to a person of skill in the art at the time of the alleged invention of the asserted claims to combine any primary reference with any combination of other primary references or secondary references so as to practice the asserted claims. To the extent that Plaintiff argues that any concept claimed in the asserted claims is not disclosed in a primary reference, it would, at a minimum, have been obvious to adapt the primary reference to include the concept or combine it with other primary references or secondary references that disclose the concept. Each concept described and claimed in the Asserted Patents was known to those of skill in the art as available design choices for the technologies at issue.[12]

[12] Each concept described and claimed in the ’864 Patent was known to those of skill in the art as available design choices for data encryption technology and/or using such technology to

The Supreme Court has held that "[t]he combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 416 (2007). "When a work is available in one field of endeavor, design incentives and other market forces can prompt variations of it, either in the same field or a different one." *Id*. at 417. As the Supreme Court made clear, "[f]or the same reason, if a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill." *Id*.

To determine whether there is an apparent reason to combine the known elements in the fashion claimed by the patent at issue, a court can "look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art." *Id*. at 418. For example, obviousness can be demonstrated by showing "there existed at the time of invention a known problem for which there was an obvious solution encompassed by the patent's claims." *Id*. at 420. "[A]ny need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed." *Id*. Common sense also teaches that "familiar items may have obvious uses beyond their primary purposes, and in many cases a person of ordinary skill will be able to fit the teachings of multiple patents together like pieces of a puzzle." *Id*.

However, the Supreme Court in *KSR* held that a claimed invention can be obvious even if there is no explicit teaching, suggestion, or motivation for combining the prior art to produce

---

provision and/or authenticate mobile devices for use with a wireless network in a wide range of applications for different scenarios and circumstances.

that invention. In summary, *KSR* holds that patents that are based on new combinations of elements or components already known in a technical field may be found to be obvious. *See, generally*, *KSR*, 550 U.S. 398. Specifically, the Court in *KSR* rejected a rigid application of the "teaching, suggestion, or motivation [to combine]" test. *Id*. at 418. "In determining whether the subject matter of a patent claim is obvious, neither the particular motivation nor the avowed purpose of the patentee controls. What matters is the objective reach of the claim." *Id*. at 419. "Under the correct analysis, any need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed." *Id*. at 420. A key inquiry is whether the "improvement is more than the predictable use of prior art elements according to their established functions." *Id*. at 417.

The rationale to combine or modify prior art references is significantly stronger when, as here, the references seek to solve the same problem, come from the same field, and correspond well to each other. *In re Inland Steel Co*., 265 F.3d 1354, 1362 (Fed. Cir. 2001). The Federal Circuit has held that two references may be combined as invalidating art under similar circumstances, namely "[the prior art] focus[es] on the same problem that the … patent addresses: enhancing the magnetic properties of … steel. Moreover, both [prior art references] come from the same field …. Finally, the solutions to the identified problems found in the two references correspond well." *Id*. at 1364 (concerning patents and prior art relating to improving the magnetic and electrical properties of steel).

In view of the Supreme Court's *KSR* decision, the PTO issued a set of Examination Guidelines. Examination Guidelines for Determining Obviousness Under 35 U.S.C. §103 in view of the Supreme Court Decision in *KSR International Co. v. Teleflex, Inc*., 72 Fed. Reg. 57526 (October 10, 2007). Those Guidelines summarized the *KSR* decision and identified various

rationales for finding a claim obvious, including those based on other precedents. Those rationales include:

> (A) Combining prior art elements according to known methods to yield predictable results;
> (B) Simple substitution of one known element for another to obtain predictable results;
> (C) Use of known technique to improve similar devices (methods, or products) in the same way;
> (D) Applying a known technique to a known device (method, or product) ready for improvement to yield predictable results;
> (E) "Obvious to try" – choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success;
> (F) Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations would have been predictable to one of ordinary skill in the art;
> (G) Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention.

Id. at 57529. The above rationales likewise apply in rendering obvious the asserted claims of the Asserted Patents.

The references disclosed herein, alone or in combination, contain an explicit and/or implicit teaching or motivation to combine them due to the following: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference addresses similar problems; and (5) the knowledge of those skilled in the art that the disclosed elements had been or could be used together.

As an example of those reasons and motivations to combine the references, Ala-Laurila '934, Bhuyan '491, Boyd-Mathuria, Farnham '766, Jeong (2010), Nguyen '985, Peirce '967, Semple '841, Wang '162, and the specified secondary references generally relate to encryption

technology, and/or using such technology to provision or authenticate a mobile device for use with a wireless network. *See* Exs. D-01 to D-09 and D-A. The references disclose similar components and techniques for data encryption, and/or using encryption to provision or authenticate mobile devices. *See id.* The attached charts in Exhibits D-01 to D-09 and D-A provide additional reasons and motivations to combine the charted references.

Additionally, the primary and secondary references listed above are analogous art. They are all directed to encryption technology, and in particular, to provisioning and/or authenticating a mobile device for use with a wireless network. *See, e.g.*, Ala-Laurila '934 at Abstract ("Arranging data ciphering in a telecommunication system comprising at least one wireless terminal, a wireless local area network and a public land mobile network. At least one first ciphering key according to the mobile network is calculated in the mobile network and in the terminal for a terminal identifier using a specific secret key for the identifier. Data transmission between the mobile network and the terminal is carried out through the wireless local area network. A second ciphering key is calculated in the terminal and in the mobile network using said at least one first ciphering key. The second ciphering key is sent from the mobile network to the wireless local area network. The data between the terminal and the network is ciphered using said second ciphering key."), [0002] ("The disclosure relates to arranging data ciphering in wireless telecommunication systems and particularly in Wireless Local Area Networks WLAN."); Bhuyan '491 at Abstract ("A method of providing authentication of a mobile device in a telecommunications network comprising the steps of: providing a user defined first password to an authentication server in the communications network; generating a set of security parameters by an authentication server and provisioning the security parameters to a mobile device, wherein the security parameters are stored at the mobile device and wherein the security

parameters comprises an encryption key; authenticating the mobile device by challenging the integrity of the encryption key stored at the mobile device and verifying a first response generated by the mobile device in response to the challenge, wherein verifying comprises comparing by the network whether the first response matches a second response, wherein the first response is based on the encryption key stored at the mobile device and a second password input by the user, and the second response is generated by the network and is based on the encryption key generated by the authentication server and the user defined first password."), [0001] ("The present invention relates to a method of authentication in a telecommunications network, in particular a method of authenticating a mobile device using a network provisioned security module and subsequent secure communications between the mobile device and the network."); Boyd-Mathuria at Chapter 1.2.1 ("The reader is probably already aware of the obvious problem with our first attempt. Nevertheless it is our purpose here to be explicit about our assumptions. The problem is that the session key KAB must be transported to A and B but to no other entities. It is an assumption that the adversary, against whose attacks we are implementing our security, can eavesdrop on all messages that are sent or received. This is a realistic assumption in typical communications systems such as the Internet and corporate networks. Indeed, if this possibility can be discounted then there is probably no need to apply security at all."), Chapter 1.4 ("In this section we highlight the importance of distinguishing the possible different properties that may be provided by cryptographic algorithms. A good understanding of the algorithms and methods of cryptography is highly beneficial in assessing cryptographic protocols…."); Farnham '766 at Abstract ("This invention generally relates to secure communications links for data transmission and more particularly relates to data communications links in which asymmetric cryptographic techniques are used to establish a secure link using symmetric cryptography. A method of

establishing a secure communications link between a terminal and a server, the method comprising, assembling a message comprising a secret number and a digital signature for the secret number, the digital signature being generated using a private key for the server, encrypting the message at the server end of the communications link using a public key for the terminal, sending said encrypted message from the server to the terminal, decrypting said encrypted message at the terminal using a private key for the terminal, validating the message by checking the digital signature using a public key for the server; and establishing said secure communications link using said secret number, wherein the public and private keys for the terminal and server are public and private keys of an asymmetric cryptographic technique. Corresponding software is also provided. The method facilitates fast and if desired, anonymous, download of software to a mobile communications system terminal.”); Jeong (2010) at Abstract (“The USIM-based AKA authentication process is essential to a mobile payment system on smart phone environment. In this paper a payment protocol and an AKA module are designed for mobile payment system which is suitable for openness smart phone environment. The payment protocol designs the cross authentication among components of the mobile payment system to improve the reliability of the components. The AKA module of mobile payment system based on 3GPP-AKA protocol prevents the exposure of IMSI by creating the SSK (Shared safe Key) through advance registration and solves the SQN (SeQuence Number) synchronization problem by using timestamp. Also, by using the SSK instead of authentication vector between SN and authentication center, the existing bandwidth (688×N)×R bit between them is reduced to 320×R bit or 368×R bit. It creates CK and IK which are message encryption keys by using OT-SSK (One-Time SSK) between MS and SN. In addition, creating the new OT-SSK whenever MS is connected to SN, it prevents the data replay attack.”); Nguyen ’985 at Abstract (“A system that

incorporates teachings of the present disclosure may include, for example, a server having a controller to implement an Elliptic Curve Diffie-Hellman (ECDH) cryptosystem and manage a key exchange, authentication, and certificate exchange with a communication device also implementing the ECDH cryptosystem, wherein the server communicates over a network that provides an encrypted communication link for the communication device. Other embodiments are disclosed."), [0001] ("The present disclosure relates generally to communication systems and more specifically to a method and apparatus for end-to-end mobile user security in a network."); Peirce '967 at Abstract ("A system and method for producing cryptographic keys for use by an embedded processing device within a manufactured product. A pseudo random number generator is seeded with entropy data gathered by the embedded device, and the result is used to generate a public-private key pair. The process can be carried out during manufacturing so that the public key of each manufactured product can be stored in a database along with a unique identifier for the embedded device associated with the key. In one particular example, a vehicle having an installed telematics unit uses the key generating process to self-generate keys using entropy data available to the vehicle."), [0001] ("The present invention relates generally to techniques for generating cryptographic keys used in secure data communications and, in particular, to such techniques used for manufactured products having embedded processing devices."); Semple '841 at Abstract ("A mutual authentication method is provided for securely agreeing application-security keys with mobile terminals supporting legacy Subscriber Identity Modules (e.g., GSM SIM and CDMA2000 R-UIM, which do not support 3G AKA mechanisms). A challenge-response key exchange is implemented between a bootstrapping server function (BSF) and mobile terminal (MT). The BSF generates an authentication challenge and sends it to the MT under a server-authenticated public key mechanism. The MT receives the challenge and

determines whether it originates from the BSF based on a bootstrapping server certificate. The MT formulates a response to the authentication challenge based on keys derived from the authentication challenge and a pre-shared secret key. The BSF receives the authentication response and verifies whether it originates from the MT. Once verified, the BSF and MT independently calculate an application security key that the BSF sends to a requesting network application function to establish secure communications with the MT."), 1:23–29 ("The present invention generally relates to systems and methods for securing wireless communications. More specifically, one feature of the invention provides a novel authentication and key agreement scheme for devices supporting legacy network authentication mechanisms, in order to provide application security keys by taking advantage of legacy wireless authentication and key agreement mechanisms."); Wang '162 at Abstract ("A wireless transmit/receive unit (WTRU) includes a control plane (C-plane) packet data convergence protocol (C-PDCP) layer which performs ciphering of a signaling message. The C-PDCP layer is activated upon power up of the WTRU and initial security parameters are loaded to the C-PDCP layer. An initial connection signaling message and a user identity are ciphered using the initial security parameters even before the WTRU is authenticated. The initial security parameters including a ciphering key (CK) may be generated from system information broadcast from the network. The CK may be a public key for asymmetric encryption, and may be selected from a public key set broadcast by or derived from the network system information. An index of the selected public key may be separately encoded. Alternatively, the index may be communicated by using a Diffie-Hellman key exchange method."), [0003] ("More particularly, the present invention is related to a method and apparatus for security protection of an original user identity (ID) in an initial access signaling message in a wireless communication system including third generation (3G) long term evolution (LTE).").

In addition, below are additional motivations to combine prior art for particular claim limitations. The following discussion of specific claim limitations are merely examples and are not limiting.

For example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach using secure methods of authenticating a mobile device with a wireless network employing encryption techniques in a mobile/tele-communications context (in regards to Limitations 1[pre], 1[e], and 1[f])[13], it would have been obvious to a person of ordinary skill in the art at the time of the invention to combine the primary reference with any of the prior art that disclose Limitations 1[pre], 1[e], and 1[f] in Exhibits D-01 to D-09 or D-A. For example, several prior art references, including Ala-Laurila '934, Bhuyan '491, Boyd-Mathuria, Farnham '766, Jeong (2010), Nguyen '985, Peirce '967, Semple '841, Wang '162, and Secondary References explicitly describe or using secure methods of authenticating a mobile device with a wireless network. *See, e.g.*, Ala-Laurila '934 at Abstract, [0002]–[0009], [0018]–[0025], Figs. 1–3; Bhuyan '491 at Abstract, [0001]–[0007], [0045]–[0046], [0059], [0062], [0092], Figs 2–3, 5–6; Boyd-Mathuria at Chapters 1.2.2, 1.4.2, 1.6.1, 2.2.2, 3.2, 4.2, 4.3.6, 5.7.1, 6.3.1, A; Farnham '766 at Abstract, [0001]–[0003], [0007]–[0009], [0021], [0032], [0046]–[0051], [0069]–[0071], Figs 1–3; Jeong (2010) at Abstract, Sections 1, 2.2, 5, Figs 1–6; Nguyen '985 at Abstract, [0001]–[0004], [0024]–[0029], [0036]–[0046], Figs 1–2, 4–6; Peirce '967 at Abstract, [0001]–[0004],

[13] Specifically, Limitation 1[1re]: "A method comprising;" Limitation 1[e]: "(5) sending a message to a server for a wireless network, the message comprising the module encrypted data and the corresponding module public key, wherein the server mutually derives the symmetric ciphering key using at least the module public key, and wherein the wireless network selects the pre-shared secret key for the mobile device using the module identity;" Limitation 1[f]: "(6) authenticating the mobile device with the wireless network using a message digest with the pre-shared secret key."

[0019]–[0020], [0037]–[0039], Figs 1–3; Semple ’841 at Abstract, 1:23–2:43, 5:17–62, 7:4–47, 8:4–9:3, Figs. 1, 4–7; Wang ’162 at [0003], [0007]–[0015], [0026]–[0034], Figs. 1–4

A person skilled in the art would have understood the benefits of using secure methods of authenticating a mobile device with a wireless network (in regards to Limitations 1[pre], 1[e], and 1[f]), given the well-known and complementary weaknesses in that process, and therefore would have been motivated and had a reasonable expectation of success to incorporate this feature into the device or method for a mobile device application according. *See, e.g.*, Ala-Laurila ’934 at Abstract (“Arranging data ciphering in a telecommunication system comprising at least one wireless terminal, a wireless local area network and a public land mobile network. At least one first ciphering key according to the mobile network is calculated in the mobile network and in the terminal for a terminal identifier using a specific secret key for the identifier. Data transmission between the mobile network and the terminal is carried out through the wireless local area network. A second ciphering key is calculated in the terminal and in the mobile network using said at least one first ciphering key. The second ciphering key is sent from the mobile network to the wireless local area network. The data between the terminal and the network is ciphered using said second ciphering key.”), [0002] (“The disclosure relates to arranging data ciphering in wireless telecommunication systems and particularly in Wireless Local Area Networks WLAN.”), [0025] (“FIG. 2 shows the essential functions according to a preferred embodiment of the invention for authenticating the terminal MT and for calculating a ciphering key. The terminal MT is offered an identifier IMSI and a secret key Ki by the subscriber identity application SIM included therein. The authentication process of the terminal MT is typically triggered when the MT starts setting up a connection 201 (Connection setup) with the WLAN network WLAN. Then the MT is provided with an IP address through a DHCP server

(Dynamic Host Configuration Protocol). Before the terminal MT is allowed to establish a connection with other networks than the network WLAN, the authentication must be performed in an acceptable manner."); Bhuyan '491 at [0003] ("The present invention relates to a method of authentication in a telecommunications network, in particular a method of authenticating a mobile device using a network provisioned security module and subsequent secure communications between the mobile device and the network."), [0003] ("Security provisions, including authentication, under GSM are based upon a key sharing principle, where a secure smart card, a SIM (subscriber identity module), is used to store a secret key that is been preloaded onto the card when the card is made. The secret key is thus shared a priori between the mobile phone and the network operator before any communication is initiated. This shared secret key forms the basis for all subsequent key generation used for authentication and ciphering of communications to and from the mobile phone."), [0059] ("In step 308, the provisioning server 204 makes a request to the authentication server 206 for security module parameters. The authentication server 206 receives the request and generates in response to the request a unique identifier for the mobile device 210 in step 310 as well as a secret key Ki. In this example, the identifier is referred to as the IMSI (international mobile subscriber identity). However, the identity is not restricted to having the limitations and format of a GSM IMSI. The term IMSI is used here to provide a simple reference to the unique identity, which is also associated with the subscriber or user."), [0062] ("In step 318, the provisioning server 204 encrypts and sends a file containing the security parameters IMSI and Ki to the mobile device 210 specified by the mobile number given in step 304. The file is encrypted using the password provided by the user in step 304. Also sent with the encrypted file is the software-based security module. The security module is an application that is run by the mobile device 210 that executes the various methods used for

authentication and ciphering which will be described in more detail below. The security module uses security parameters during its operation and also includes operator specific cryptographic functions such as F1 and F2 described below."); Boyd-Mathuria at Chapter 1.6.1 ("Eavesdropping is perhaps the most basic attack on a protocol. Nearly all protocols address eavesdropping by using encryption. It is obvious that encryption must be used to protect confidential information such as session keys. In certain protocols there may be other information that also needs to be protected. An interesting example is that protocols for key establishment in mobile communications usually demand that the identity of the mobile station remain confidential. Eavesdropping is sometimes distinguished as being a passive attack since it does not require the adversary to disturb the communications of legitimate principals. The other attacks we consider all require the adversary to be active. It should be remembered that many sophisticated attacks include eavesdropping of protocol runs as an essential part."), Chapter 4.3.6 ("MSR Protocol … In the following, the notation SCB is a structure known as the secret certificate of the mobile station, B, which is issued by a trusted central authority. This certificate can be checked by anyone using the public key of the central authority in order to verify the mobile's identity. Unlike a usual public key certificate, this certificate must be kept secret from all other mobile users and eavesdroppers, because it is all that is required to masquerade as B. Protocol 4.26 shows the basic MSR protocol [36]…. 1. A à B : A, KA … 2. B à A: EA(KAB), {B, SCB}KAB … Protocol 4.26: Basic MSR protocol of Beller, Chang and Yacobi. … Upon receiving the base A's public key KA, the mobile uses it to encrypt the session key KAB, and sends the encrypted message to A. The mobile also sends its identity and secret certificate encrypted under KAB to authenticate KAB to the base. The symmetric encryption with KAB in message 2 is of negligible computational effort compared to the public key encryption in the

same message; therefore the computational effort at the mobile is effectively limited to that of modulo squaring of the session key.”), Chapter 5.7.1 (“[The] proposed a protocol for use in a wireless environment that is based on the Yacobi-Shmuely protocol, but with a small and significant difference. In Protocol 5.34 the server or base station, A, carries out the exponentiation using U A on behalf of the mobile station, B, with the aim of reducing the computational load on B. Apart from this change in where the computation takes place, the protocol (including the shared secret) is the same as Protocol 5.33.”); Farnham ’766 at Abstract (“This invention generally relates to secure communications links for data transmission and more particularly relates to data communications links in which asymmetric cryptographic techniques are used to establish a secure link using symmetric cryptography. A method of establishing a secure communications link between a terminal and a server, the method comprising, assembling a message comprising a secret number and a digital signature for the secret number, the digital signature being generated using a private key for the server, encrypting the message at the server end of the communications link using a public key for the terminal, sending said encrypted message from the server to the terminal, decrypting said encrypted message at the terminal using a private key for the terminal, validating the message by checking the digital signature using a public key for the server; and establishing said secure communications link using said secret number, wherein the public and private keys for the terminal and server are public and private keys of an asymmetric cryptographic technique. Corresponding software is also provided. The method facilitates fast and if desired, anonymous, download of software to a mobile communications system terminal.”), [0003] (“Secure data transmission is important for m-commerce but, in addition to this, the secure download and installation of software onto mobile terminals will also be important for multimedia entertainment, telle-medicine, upgrades for

programmable mobile terminals, upgrades to different wireless standards, and the like. Reconfigurable mobile terminals are able to provide increased flexibility for end users who can customize the terminals for their personal needs by downloading and installing the desired applications, for example to support different types of radio systems and to allow the integration of different systems. However techniques are needed to protect mobile terminals against hackers maliciously substituting their software for software available from a handset manufacturer, network operator or trusted third party source."), [0046] ("The main objective of both these approaches is to protect terminals against malicious downloaded software. They do not protect against attacks that involve physical modifications of the terminal, such as the replacement of program memory, nor are they are intended to limit the distribution and use of software or to protect a software module against reverse-engineering. The security of the symmetric approach, however, requires that the terminal maintain the secrecy of the cryptographic key that it shares with the ticket server, whereas the asymmetric approach relies on a public-key, i.e. the level of secrecy required to protect the symmetric key is necessary for protecting the public key."); Jeong (2010) at Section 2.2 ("Figure 2 illustrates 3GPP-AKA, the USIM authentication process in the wireless Internet environment. When the USIM/MS identifies itself by sending IMSI (International Mobile Subscriber Identity) or TMSI (Temporary Mobile Subscriber Identity) information to the SN (Serving Network), the SN transmits an authentication data request message and the IMSI/TMSI received from the terminal to the AuC (Authentication Center) of the HN (Home Network), which is the authentication center. The HN generates an authentication vector AV (Authentication Vector) for the received IMSI and transmits it to the SN in response to the authentication data request."), Section 5 ("The user authentication of the mobile payment protocol proposed in this paper eliminates the possibility of USIM exposure by encrypting and

transmitting the USIM from the store to the certifier with each shared secret key, and generates a new session key using the USIM, a random value, the user's master key, the store's master key, and the payment center's master key every time the identity of the user, store, and payment center is verified, so that malicious users cannot attempt to make mobile payments due to the exposure of the previous session key."); Nguyen '985 at Abstract ("A system that incorporates teachings of the present disclosure may include, for example, a server having a controller to implement an Elliptic Curve Diffie-Hellman (ECDH) cryptosystem and manage a key exchange, authentication, and certificate exchange with a communication device also implementing the ECDH cryptosystem, wherein the server communicates over a network that provides an encrypted communication link for the communication device. Other embodiments are disclosed."), [0001] ("The present disclosure relates generally to communication systems and more specifically to a method and apparatus for end-to-end mobile user security in a network."), [0003] ("Although GSM differs significantly from its predecessor technologies with regard to signaling and speech channels, GSM is still vulnerable to basic forms of passive security attack, such as eavesdropping. This is mainly due to a signaling link within the fixed infrastructure part of the GSM signaling network which can expose users' unencrypted phone calls and data to an attacker if the attacker can manage to gain direct access to the signaling network."); Peirce '967 at [0001] ("The present invention relates generally to techniques for generating cryptographic keys used in secure data communications and, in particular, to such techniques used for manufactured products having embedded processing devices."), [0002] ("As computer electronics continue to reduce in cost and size, the applications for embedded processing devices are continuing to increase, and there now exists many types of manufactured products that contain some type of embedded processing device, whether microprocessor based or otherwise.

Some embedded devices are designed to undergo data communication with one or more external, possibly remote devices. In some cases, it is desirable to establish authenticated, secure data communications in which the exchanged data is encrypted. Although various approaches can be used, cryptographic keys are perhaps most commonly used for this purpose. In public key cryptography, a public-private key pair is created with the public key then being available for use by anyone desiring encrypted communication with the holder of the private key. Digital certificates issued by a trusted third party (certificate authority) can also be used to authenticate the public key to a particular entity."), [0039] ("For public-private key pairs, once the keys are generated, the private key is stored in the manufactured product, such as in memory included within the embedded device. This is shown at step 108. Then, the public key is transmitted electronically (for example, wirelessly) from the manufactured product and stored in an external database, step 110. A unique ID of the manufactured product or its embedded device can also be stored in the database and associated with the public key so that subsequent communications can be targeted individually to that particular product. For example, a serial number or MAC address for the embedded device can be used. At this point, the generation of the keys is complete and the manufactured product can be distributed by, for example, transferring possession of the product to another entity."); Semple '841 at 1:23–29 ("The present invention generally relates to systems and methods for securing wireless communications. More specifically, one feature of the invention provides a novel authentication and key agreement scheme for devices supporting legacy network authentication mechanisms, in order to provide application security keys by taking advantage of legacy wireless authentication and key agreement mechanisms."), 8:4–9:3 ("FIG. 5 illustrates a method of authenticating a mobile terminal using a bootstrapping server function and authentication of the server function according to one embodiment of the invention.

This method may be implemented when a network application function wishes to agree on keys with a mobile terminal (MT) prior to initiating a network application transaction. For example, GSM Authentication and Key Agreement (AKA) are based on a challenge-response protocol. A secret key Ki as well as two algorithms A3 and A8 are stored in a Subscriber Identity Module (SIM) inside the MT as well as the network home location register (HLR)/Authentication Center (AuC). The SIM is designed to be tamper-proof and contains secret data and algorithms that cannot be easily read out by a user. A request for a key is generated and sent from the MT, which has a legacy SIM inside, to a bootstrapping server function (BSF) 502. The BSF obtains authentication information for the MT from a network HLR or AuC 504…. The MT verifies whether the authentication challenge originates from the expected BSF based on a bootstrapping server certificate 508…. The authentication response is sent from the MT to the BSF 512. The BSF then verifies the origin of the authentication response based on an independently obtained secret key 514…. In an alternative implementation, the MT may calculate a third key using the one or more secret keys (SRES and Kc obtained from the SIM) and other parameters (obtained from the authentication challenge or response or from the SIM). This third key is then used to formulate the authentication response (e.g., compute the message authentication code). The BSF may also calculate the same key since it knows the same keys and/or parameters as the MT. Thus, the BSF can verify whether the authentication response originated from the MT.”); Wang ’162 at [0013] (“Therefore, it would be desirable to provide a method and system for protecting initial control signaling messages and especially the WTRU identity, (i.e., IMSI), during the initial connection for attachment and authentication procedure.”), [0015] (“The present invention is related to a method and apparatus for security protection of an original user identity in an initial access signaling message in a wireless communication system including third generation (3G)

LTE. A WTRU includes a control plane (C-plane) packet data convergence protocol (C-PDCP) layer which performs ciphering and integrity protection of a signaling message. The C-PDCP layer is activated upon power up of the WTRU and initial security parameters are loaded to the C-PDCP layer. An initial connection signaling message for network attachment, and a user ID, (e.g., an IMSI), are ciphered using the initial security parameters even before the WTRU is authenticated. The initial security parameters are loaded from a universal subscriber identity module (USIM) and generated from system information broadcast from the network. The system information includes a public key set with at least one public key for asymmetric encryption of the IMSI or information from which the public key(s) can be derived. The initial security parameters for ciphering include a CK. The CK may be a public key or may be selected from the public key set broadcast by or derived from the network system information. An index of the selected public key may be separately encoded. Alternatively, the index may be communicated by using a Diffie-Helhnan key exchange method."), [0031] ("The NAS layer 211 triggers an RRC connection by sending an attach message along with an IMSI to the RRC layer 212 (step 308). The RRC layer 212 sends an LTE RRC connection request to the C-PDCP layer 213 including the attach message and MAC-I and preferably a public land mobile network (PLMN) identity (ID) (step 310). The C-PDCP layer 213 then performs ciphering on the attach message and the IMSI with the initial CK (from USIM or system information broadcast), and sends an LTE RRC connection request message including ciphered attach message and IMSI along with the MAC-I from the RRC layer 212 (steps 312, 314). Unlike the conventional attachment procedure, the attach message and the IMSI are protected with initial CK and IK."). Thus, a person of ordinary skill in the art would have been motivated to modify any of the primary references to include this feature. A person of ordinary skill in the art would also have had a

reasonable expectation of success. A person of ordinary skill in the art would have understood that these references disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach using encryption techniques and a symmetric key to encrypt and decrypt module identity for a mobile device for submission to a server or a mobile network (in regards to Limitations 1[pre],1 [c], 1[d], and 1[e])[14], it would have been obvious to a person of ordinary skill in the art at the time of the invention to combine the primary reference with any of the prior art that disclose Limitations 1[pre], 1[c], 1[d], and 1[e] in Exhibits D-01 to D-09 or D-A. For example, several prior art references, including Ala-Laurila '934, Bhuyan '491, Boyd-Mathuria, Farnham '766, Jeong (2010), Nguyen '985, Peirce '967, Semple '841, Wang '162, and Secondary References explicitly describe or disclose using encryption techniques and a symmetric key to encrypt and decrypt the subscriber identity for a mobile device for submission to the mobile network. *See, e.g.*, Ala-Laurila '934 at Abstract, [0002]–[0007], [0022]–[0028], Figs.1–3; Bhuyan '491 at Abstract, [0001]–[0006], [0045]–[0051], Figs. 2–3, 5–6; Boyd-Mathuria at Chapters 1.4, 1.6.1, 2.3, 3.4, 4.3.6, A; Farnham '766 at Abstract, [0001]–[0009], [0021], [0027]–[0032], [0046]–[0051], [0069]–[0071], Figs. 1–3; Jeong (2010) at Abstract,

[14] Specifically, Limitation 1[pre]: "A method comprising;" Limitation 1[c]: "(3) deriving a symmetric ciphering key using (i) an elliptic curve integrated encryption scheme with the server public key and the module private key and (ii) an American National Standards Institute standard X-9.63 key derivation function;" Limitation 1[d]: "(4) generating module encrypted data using the symmetric ciphering key and the symmetric ciphering algorithm, wherein the module encrypted data includes the module identity;" and Limitation 1[e]: "(5) sending a message to a server for a wireless network, the message comprising the module encrypted data and the corresponding module public key, wherein the server mutually derives the symmetric ciphering key using at least the module public key, and wherein the wireless network selects the pre-shared secret key for the mobile device using the module identity."

Sections 2.2, 3.1.2, 3.2, 4.1.2, 5, Figs. 4–6; Nguyen ’985 at Abstract, [0001]–[0004], [0012]–[0024], [0036]–[0046], Figs. 1–2, 4–6; Peirce ’967 at Abstract, [0001]–[0004], [0034]–[0041] Figs. 1–3; Semple ’841 at Abstract, 1:23–2:43, 9:19-10:43, 10:44-11:35, Figs. 1–3, 6–7; Wang ’162 at [0003], [0012]–[0015], [0031]–[0042], Figs. 1–4.

A person skilled in the art would have understood the benefits of using encryption techniques and a symmetric key to encrypt and decrypt the subscriber identity for a mobile device for submission to a server or mobile network (in regards to Limitations 1[pre], 1[c], 1[d], and 1[e]), given the well-known and complementary confidentiality and security considerations in that process, and therefore would have been motivated and had a reasonable expectation of success to incorporate this feature into the device or method for a mobile device application according. *See, e.g.*, Ala-Laurila ’934 at [0004] (“However, a problem in some wireless telecommunication networks, such as IEEE802.11 WLAN networks, is that the ciphering keys used for ciphering traffic must be stored in advance in the terminal and access point. If the network does not have the same key as the terminal, then the data between the network and the terminal cannot be ciphered. To add different ciphering keys is difficult, and a safe data transmission cannot always be offered for terminals moving in different networks.”), [0025]–[0026] (“FIG. 2 shows the essential functions according to a preferred embodiment of the invention for authenticating the terminal MT and for calculating a ciphering key. The terminal MT is offered an identifier IMSI and a secret key Ki by the subscriber identity application SIM included therein. The authentication process of the terminal MT is typically triggered when the MT starts setting up a connection 201 (Connection setup) with the WLAN network WLAN. Then the MT is provided with an IP address through a DHCP server (Dynamic Host Configuration Protocol). Before the terminal MT is allowed to establish a connection with other networks than

the network WLAN, the authentication must be performed in an acceptable manner. The MT requests 202 (IMSI request) the identity module SIM for the IMSI identifier and the SIM returns 203 the IMSI identifier. The MT sends 204 the authentication starting request (MT_PAC_AUTHSTART_REQ) which preferably comprises a Network Access Identifier NAI. The NAI comprises the IMSI identifier obtained from the identity module SIM. The NAI may be presented, for example, in the form 12345@GSM.org, where 12345 is the IMSI identifier and GSM.org is the domain name of the mobile network, which has conveyed the identity module SIM. The request 204 is preferably sent in ciphered form to the PAC using the Diffie-Hellman algorithm, for example. The MT preferably also sends a specific protection code MT_RAND in the request 204, said code typically being a challenge code. Using the protection code MT_RAND the MT may later be ensured that the party conveying the GSM triplets actually has access to the secret key Ki, which is to be maintained in the GSM home network of the subscriber. However, the use of the protection code is not obligatory."); Bhuyan '491 at [0001]–[0006] ("The present invention relates to a method of authentication in a telecommunications network, in particular a method of authenticating a mobile device using a network provisioned security module and subsequent secure communications between the mobile device and the network. Security in communication systems has always been important and mobile cellular communication systems have been no different. In early 'first generation' analogue mobile phone systems, a third party could eavesdrop on the communications between a mobile terminal and the mobile network relatively easily over the radio interface. These problems were partly mitigated when 'second generation' digital systems, such as GSM (Global System for Mobile communications), were adopted by mobile operators. Security provisions, including authentication, under GSM are based upon a key sharing principle, where a secure smart card, a

SIM (subscriber identity module), is used to store a secret key that is been preloaded onto the card when the card is made. The secret key is thus shared a priori between the mobile phone and the network operator before any communication is initiated. This shared secret key forms the basis for all subsequent key generation used for authentication and ciphering of communications to and from the mobile phone. The SIM also holds other data as well as the shared secret key, commonly referred to as Ki, such as SIM applications, encryption algorithms, and user identifiers such as the IMSI (International mobile subscriber identity). SIM cards have been proven to be reasonably secure and tamper-proof and have been commonly used in both GSM and 3G mobile telecommunications networks for some time. However, SIM cards suffer from a number of drawbacks. In particular, provisioning of SIM cards is a complex process brought about by having to manufacture the tamper resistant modules, initialising the cards with the requisite data (IMSI, Ki and operator secrets) and then distributing and handling of the physical cards to the subscriber. Furthermore, most mobile devices these days also only have the capacity to use a single SIM card, and thus access to networks is limited to those allowed by the single SIM. The few devices that can handle multiple SIM cards are rare and are usually more complex and costly to manufacture as well as being more difficult to use.”); Boyd-Mathuria at Chapter 1.4 (“Confidentiality ensures that data is only available to those authorised to obtain it. This is usually achieved through encryption of the data so that only those with the correct decryption key can recover it. In cryptographic protocols confidentiality is essential to ensure that keys and other data are available only as intended.”), Chapter 4.3.6 (“MSR Protocol…In the following, the notation *SCB* is a structure known as the *secret certificate* of the mobile station, *B,* which is issued by a trusted central authority. This certificate can be checked by anyone using the public key of the central authority in order to verify the mobile's identity. Unlike a usual public key certificate,

this certificate must be kept secret from all other mobile users and eavesdroppers, because it is all that is required to masquerade as *B.* Protocol 4.26 shows the basic MSR protocol [36]…. 1. $A \rightarrow B : A, K_A$ … 2. $B \rightarrow A: E_A(K_{AB}), \{B, SC_B\}K_{AB}$ … Protocol 4.26: Basic MSR protocol of Beller, Chang and Yacobi. … Upon receiving the base *A's* public key K_A, the mobile uses it to encrypt the session key K_{AB}, and sends the encrypted message to *A.* The mobile also sends its identity and secret certificate encrypted under K_{AB} to authenticate K_{AB} to the base. The symmetric encryption with K_{AB} in message 2 is of negligible computational effort compared to the public key encryption in the same message; therefore the computational effort at the mobile is effectively limited to that of modulo squaring of the session key."); Farnham '766 at Abstract ("This invention generally relates to secure communications links for data transmission and more particularly relates to data communications links in which asymmetric cryptographic techniques are used to establish a secure link using symmetric cryptography. A method of establishing a secure communications link between a terminal and a server, the method comprising, assembling a message comprising a secret number and a digital signature for the secret number, the digital signature being generated using a private key for the server, encrypting the message at the server end of the communications link using a public key for the terminal, sending said encrypted message from the server to the terminal, decrypting said encrypted message at the terminal using a private key for the terminal, validating the message by checking the digital signature using a public key for the server; and establishing said secure communications link using said secret number, wherein the public and private keys for the terminal and server are public and private keys of an asymmetric cryptographic technique. Corresponding software is also provided. The method facilitates fast and if desired, anonymous, download of software to a mobile communications system terminal."), [0001] ("This invention generally relates to secure

communications links for data transmission and more particularly relates to data communications links in which asymmetric cryptographic techniques are used to establish a secure link using symmetric cryptography.”), [0007] (“A Public Key Infrastructure normally includes provision for digital identity Certificates. To prevent an individual posing as somebody else an individual may prove his identity to a certification authority which then issues a certificate signed using the authority’s private key and including the public key of the individual. The Certification Authority’s public key is widely known and therefore trusted and since the certificate could only have been encrypted using the authority's private key, the public key of the individual is verified by the certificate. Within the context of a mobile phone network a user or the network operator can authenticate their identity by signing a message with their private key; likewise a public key can be used to verify an identity. Further details of PKI for wireless applications can be found in WPKI, WAP-217-WPKI, version 24—April 2001 available at www.wapforum.org and in the X.509 specifications (PKIX) which can be found at www.ietf.org, all hereby incorporated by reference.”); Jeong (2010) at Section 3.2 (“(1) In the existing AKA, we need to solve the privacy problem and the synchronization problem of SQN by transmitting the IMSI plaintext of the terminal. Therefore, the IMSI, T_{MS}(timestamp), and SN_{ID} located near the terminal are concatenated to generate the authentication value of the MS using the function $f^1_K()$. Also, E-$IMSI_{MS}$, MAC_{MS}, HN_{ID}, and T_{MS}, which are values encrypted with $SSK_{MS\text{-}HN}$, a shared secret key between HN and MS, are transmitted to the SN located near the MS. … $MAC_{MS} = f^1 SSK_{MS\text{-}HN}$ ($IMSI_{MS}$ || T_{MS} || SN_{ID}) … E- $IMSI_{MS}$ = E($SSK_{MS\text{-}HN}$, $IMSI_{MS}$) … (2) The SN forwards the received E-$IMSI_{MS}$, MAC_{MS}, T_{MS} to the corresponding certificate authority (HN).”), Section 5 (“With the rapid development of communication and the widespread use of the Internet, many people are frequently accessing remote servers in a distributed computing environment, but data

transmission over insecure channels without an authenticated protection system is exposed to many problems such as replay attacks, offline password attacks, and impersonation attacks. In this paper, we design a safe Authentication Key Agreement (AKA) module for mobile payment system suitable for openness smartphone environment that can solve these problems. The AKA module proposed in this paper prevents IMSI exposure by generating a shared secret key between the MS and the HN for user authentication and encrypting and transmitting the IMSI value of the USIM, and prevents data replay attack by generating a new OT-SSK for each connection by generating message encryption keys, CK and IK, using a one-time shared secret key, OT-SSK, between the MS and SN.”); Nguyen ’985 at Abstract (“A system that incorporates teachings of the present disclosure may include, for example, a server having a controller to implement an Elliptic Curve Diffie-Hellman (ECDH) cryptosystem and manage a key exchange, authentication, and certificate exchange with a communication device also implementing the ECDH cryptosystem, wherein the server communicates over a network that provides an encrypted communication link for the communication device. Other embodiments are disclosed.”), [0001] (“The present disclosure relates generally to communication systems and more specifically to a method and apparatus for end-to-end mobile user security in a network.”), [0016] (“The MS 116 can include an identification module 118, such as a secure identification or identity module (e.g., a SIM card), containing subscription information, account data, personal information, and private/public key information. The identification module 118 can have an associated memory (not shown) for storing data associated with a private key. The private key can be used to generate a public key which can be used to securely encrypt data. The private key is kept secret, while the public key may be widely distributed. The keys are related mathematically, but the private key cannot be practically derived from the public key. Data

encrypted with the public key can be decrypted only with the corresponding private key. This can be used to ensure confidentiality. Data signed with the sender's private key can be verified by anyone who has access to the sender's public key, thereby proving that the sender signed it and that the message has not been tampered with. This can be used to ensure authenticity.”), [0020] (“ECC is an approach to public-key cryptography based on an algebraic structure of elliptic curves over finite fields. An elliptic curve is a plane curve defined by an equation of the form $y^2=x^3+ax+b$. The set of points on such a curve can be shown to form a commutative group G, such that a*b=b*a for all a and b in G. Elliptic Curve Diffie-Hellman (ECDH) is a key agreement protocol that allows the two MSs to establish a shared secret key over an insecure channel. The secret key can then be used to encrypt subsequent communications using a symmetric key cipher.”); Peirce ’967 at Abstract (“A system and method for producing cryptographic keys for use by an embedded processing device within a manufactured product. A pseudo random number generator is seeded with entropy data gathered by the embedded device, and the result is used to generate a public-private key pair. The process can be carried out during manufacturing so that the public key of each manufactured product can be stored in a database along with a unique identifier for the embedded device associated with the key. In one particular example, a vehicle having an installed telematics unit uses the key generating process to self-generate keys using entropy data available to the vehicle.”), [0001] (“The present invention relates generally to techniques for generating cryptographic keys used in secure data communications and, in particular, to such techniques used for manufactured products having embedded processing devices.”), [0039] (“For public-private key pairs, once the keys are generated, the private key is stored in the manufactured product, such as in memory included within the embedded device. This is shown at step 108. Then, the public key is transmitted

electronically (for example, wirelessly) from the manufactured product and stored in an external database, step 110. A unique ID of the manufactured product or its embedded device can also be stored in the database and associated with the public key so that subsequent communications can be targeted individually to that particular product. For example, a serial number or MAC address for the embedded device can be used. At this point, the generation of the keys is complete and the manufactured product can be distributed by, for example, transferring possession of the product to another entity."); Semple '841 at 1:23–29 ("The present invention generally relates to systems and methods for securing wireless communications. More specifically, one feature of the invention provides a novel authentication and key agreement scheme for devices supporting legacy network authentication mechanisms, in order to provide application security keys by taking advantage of legacy wireless authentication and key agreement mechanisms."), 9:35–59 ("In one embodiment, a request for authentication keys may be initiated by MT 606 retrieving its associated International Mobile Subscriber Identity (IMSI) 600 from its SIM 608 and sending it to a bootstrapping server function (BSF) 604. The BSF 604 sends the IMSI 600 to the HLR 602 where it may verify whether the IMSI 600 belongs to a MT that subscribes to the network. The HLR 602 may be operated by the service provider for the subscriber whose SIM is contained in MT 606. The HLR 602 selects, for example, a 128-bit random challenge RAND and together with pre-shared secret key Ki, uses them as inputs for two algorithms A3 and A8 to yield 32-bit output signed response SRES and 64-bit output secret confidentiality key Kc, respectively. The HLR 602 then provides the triplets (RAND, SRES, Kc) to the BSF 604, corresponding to the identity IMSI 600 of SIM 608. The BSF 604 generates a random secret exponent x and computes a Diffie-Hellman public key P^x, where P is a generator of a cyclic group previously provisioned to both the BSF 604 and MT 606, such as the multiplicative group of a finite field or the additive

group of an elliptic curve. The BSF 602 then sends a triplet (RAND, P^x, SIG) 610 to the MT 606, where SIG is a digital signature computed using the BSF 604 RSA private key. The message 610 may be further enhanced to include other server-authenticated parameters such as a transaction identifier."); Wang '162 at [0003] ("More particularly, the present invention is related to a method and apparatus for security protection of an original user identity (ID) in an initial access signaling message in a wireless communication system including third generation (3G) long term evolution (LTE)."), [0012]–[0013] ("For the process illustrated in Figure 1, the RRC connection request message with the IMSI, the RRC setup request message, the RRC setup complete message, the initial direct transfer message with an optional IMSI, the authentication request message and the authentication response message are not protected, but transmitted in an open environment unprotected. The fact that the important WTRU identity, (i.e., IMSI), is sent over the air unprotected provokes an 'IMSI catching threat.' The caught IMSI could be used by a malignant denial of service (DoS) attack or other possible attacks to the network and users. Therefore, it would be desirable to provide a method and system for protecting initial control signaling messages and especially the WTRU identity, (i.e., IMSI), during the initial connection for attachment and authentication procedure."). Thus, a person of ordinary skill in the art would have been motivated to modify any of the primary references to include this feature. A person of ordinary skill in the art would also have had a reasonable expectation of success. A person of ordinary skill in the art would have understood that these references disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach using a message digest for device authentication in a mobile/tele-

communications context (in regards to Limitations 1[pre] and 1[f])[15], it would have been obvious to a person of ordinary skill in the art at the time of the invention to combine the primary reference with any of the prior art that disclose Limitations 1[pre] and 1[f] in Exhibits D-01 to D-09 or D-A. For example, several prior art references, including Ala-Laurila '934, Bhuyan '491, Boyd-Mathuria, Farnham '766, Jeong (2010), Nguyen '985, Peirce '967, Semple '841, Wang '162, and Secondary References explicitly describe or disclose using a message digest for device authentication with the mobile network. *See, e.g.*, Ala-Laurila '934 at Abstract, [0002]–[0009], [0016]–[0018], [0022]–[0031], [0039]–[0047] Figs 1–5; Bhuyan '491 at Abstract, [0001]–[0006], [0045]–[0052], [0074]–[0091], Figs. 1, 3–4, 6; Boyd-Mathuria at Chapters 1.4, 1.4.2, 1.4.4, 1.6.1, 1.6.2, 2.3, 2.3.1, 2.6.4, 3.3.2, 3.3.3, 3.3.4, 4.3.5, 3.4, 4.3.6, 5.4.8, A; Farnham '766 at Abstract, [0001]–[0009], [0012]–[0018], [0041]–[0045], [0051]–[0052], [0069]–[0075], [0083]–[0087], Figs. 1–3; Jeong (2010) at Abstract, Sections 1, 2, 2.1, 2.2, 3.1.2, 3.2, 4.1.1, 5, Figs. 2, 4–6; Nguyen '985 at Abstract, [0001]–[0004], [0012]–[0024], [0036]–[0046], Figs. 1–2, 4–6; Peirce '967 at Abstract, [0001]–[0014], [0034]–[0042], Figs. 1–3; Semple '841 at Abstract, 1:23–2:43, 7:4–58, 8:30–9:18, 9:60–10:24, Figs. 3–6; Wang '162 at [0003]–[0015], [0027]–[0036], [0045]–[0051], [0064]–[0066], Figs. 1–7.

A person skilled in the art would have understood the benefits of using a message digest for device authentication in a mobile/tele-communications context (in regards to Limitations 1[pre] and 1[f]), given the well-known and complementary confidentiality and security considerations in that process, and therefore would have been motivated and had a reasonable expectation of success to incorporate this feature into the device or method for a mobile device

[15] Specifically, Limitation 1[pre]: "A method comprising;" and Limitation 1[f]: "(6) authenticating the mobile device with the wireless network using a message digest with the pre-shared secret key."

application according. *See, e.g.*, Ala-Laurila '934 at [0002] ("The disclosure relates to arranging data ciphering in wireless telecommunication systems and particularly in Wireless Local Area Networks WLAN."), [0008] ("According to a preferred embodiment of the invention at least one authentication response according to the mobile network is calculated in the terminal and in the mobile network on the basis of at least one challenge code and a ciphering key. A check response is calculated in the terminal on the basis of at least one authentication response and the first ciphering key. The check response is sent to the mobile network. The check response is calculated in the mobile network on the basis of at least one authentication response and at least one first ciphering key. The check response sent by the terminal is compared with the check response calculated by the mobile network. The second ciphering key is sent from the mobile network to the wireless local area network, if the check response sent by the terminal and calculated by the mobile network correspond with one another. This embodiment provides the advantage that a subscriber (identity module) can be reliably authenticated in the mobile network. Consequently a data transmission connection and data ciphering can be allowed only for the authenticated terminals in the wireless local area networks."), [0031]–[0032] ("The GAGW sends 210 the PAC an acknowledgment message of the authentication request GAGW_PAC_AUTHSTART_RESP comprising one or more challenge codes RAND for the terminal MT and preferably also a check sum SIGNrand. This message may also include data associated with billing. The message can also be ciphered using the protection code MT-RAND. The PAC sends 211 the terminal MT an acknowledgment message of the authentication request PAC MT_AUTHSTART_RESP comprising at least one challenge code RAND and preferably the check sum SIGNrand. The terminal MT feeds 212 the challenge code/s RAND into the identity module SIM. The SIM calculates 213 (Calculate Kc(s)) at least one first ciphering key Kc according to the mobile

network GSMNW and an authentication response (responses) SRES in a manner that corresponds with the one used in the authentication center AuC and transmits 214 these to the other parts of the terminal MT (preferably to the control means CM carrying out authentication and the calculation of the second ciphering key K). The MT can check 215 (Check SIGNrand) the check sum SIGNrand sent by the PAC on the basis of the data (Kc) obtained from the SIM and the protection code MT_RAND. If the received SIGNrand corresponds with the value obtained on the basis of the Kc values calculated by the identity module SIM, the MT, or to be more precise, the CM calculates 216 (Calculate SIGNsres) the check response SIGNsres to be transmitted to the GAGW. The SIGNsres is preferably a hash function calculated from one or more first ciphering keys Kc and authentication responses SRES enabling the GAGW to authenticate the MT. The MT may also request the user to approve the billing data possibly sent by the PAC.”); Bhuyan ’491 at Abstract (“A method of providing authentication of a mobile device in a telecommunications network comprising the steps of: providing a user defined first password to an authentication server in the communications network; generating a set of security parameters by an authentication server and provisioning the security parameters to a mobile device, wherein the security parameters are stored at the mobile device and wherein the security parameters comprises an encryption key; authenticating the mobile device by challenging the integrity of the encryption key stored at the mobile device and verifying a first response generated by the mobile device in response to the challenge, wherein verifying comprises comparing by the network whether the first response matches a second response, wherein the first response is based on the encryption key stored at the mobile device and a second password input by the user, and the second response is generated by the network and is based on the encryption key generated by the authentication server and the user defined first password.”), [0001] (“The present invention

relates to a method of authentication in a telecommunications network, in particular a method of authenticating a mobile device using a network provisioned security module and subsequent secure communications between the mobile device and the network.”), [0074]–[0085] (“The authentication server then generates a triplet comprising a random number RAND, an expected response SRES and a key Kc in step 612. Each of these parameters is generated in accordance with the methods…. The values generated for RAND, SRES and Kc are then sent to the access server 506 in step 612…. The access server 506 then uses the received SRES from the authentication server 206 and the password from the data store 208 to generate an adapted expected response SRES1. This is done using cryptographic algorithm F1 taking SRES and the password as inputs and outputting SRES1…. The output generated is SRES 404. This value of SRES 404 is the one transferred from the authentication server 206 to the access server 506 in step 612. The generation of SRES is performed by the authentication server 206 in step 610…. Once the access server 506 has received SRES 404, it calculates SRES1412…. Specifically, SRES 404 is fed into cryptographic algorithm F1 together with the password 406 received from the data store 208…. This value of RAND is taken by the security module application in the mobile device 210 and is sued by the security module to determine the expected response SRES1 and ciphering key Kc1…. Specifically, the methods used to calculate SRES1 and Kc1 used by the security module are the same as those used by the combination of the access server 506 and authentication server 206…. The value of Ki used is the one stored on the mobile device and obtained from the decrypted file in step 604. This is combined with the received value of RAND using to A3 and A8 algorithms to generate SRES and Kc respectively. These are then fed into the F1 and F2 functions together with the password input in step 602 to get SRES1 and Kc1…. The mobile device 210 then sends of the value of SRES1 calculated by the security module to

the access server 506 in step 624. The access server 506 then checks the value of SRES1 received from the mobile device 210 with the value of SRES1 calculated itself in step 618. If the two values match, then the mobile device is authenticated and the access server 506 sends the mobile device 210 a SUCCESS message in step 628."); Boyd-Mathuria at Chapter 1.4 ("Data Integrity ensures that data has not been altered by unauthorised entities. This can be achieved through use of hash functions in combination with encryption, or by use of a message authentication code to create a separate check field. Data integrity is essential in most cryptographic protocols to protect elements such as identity fields and nonces."), Chapter 1.4.2 ("*A message authentication code (MAC) is a family of functions parametrised by a key K such that* $MAC_K(m)$ *takes a message m of arbitrary length and outputs a fixed length value and satisfying: 1. it is computationally easy to calculate* $MAC_K(m)$ *given K and m; 2. given any number of MAC values for a given K, it is computationally hard to find any valid MAC value for any new message.* The second mechanism for providing data origin authentication and data integrity is to append a MAC to a message which may be either in plaintext or encrypted. On receipt of the MAC, the recipient who has the correct key is able to recompute the MAC from the message and verify that it is the same as that received." (emphasis in original)), Chapter 1.6.2 ("If any protocol message field is not redundant then modification of it is a potential attack. Use of cryptographic integrity mechanisms is therefore pervasive in protocols for authentication and key establishment."), Chapter 2.3.1 ("*Key confirmation of A to B is provided if B has assurance that key K is a good key to communicate with A, and that principal A has possession of K.* Key confirmation provides evidence that the partner has the same key but leaves open the possibility that the key is intended by the partner for a different communication session (with the assumption that the partner may be engaged in several conversations). Key confirmation provides evidence that the partner wishes to

communicate with some entity, so implies far-end operative, but may not imply entity authentication. Key confirmation is typically achieved by having both parties send each other some fresh data using a cryptographic function depending on the key; this is often referred to as a *handshake*." (emphasis in original)); Farnham '766 at [0001] ("This invention generally relates to secure communications links for data transmission and more particularly relates to data communications links in which asymmetric cryptographic techniques are used to establish a secure link using symmetric cryptography."), [0005]–[0006] ("Asymmetric or so-called public key cryptography uses a pair of keys one "private" and one "public" (although in practice distribution of the public key is also often restricted). A message encrypted with the public key can only be decrypted with the private key, and vice-versa. An individual can thus encrypt data using the private key for decryption by any one with the corresponding public key and, similarly, anyone with the public key can securely send data to the individual by encrypting it with the public key safe in the knowledge that only the private key can be used to decrypt the data. Asymmetric cryptographic systems are generally used within an infrastructure known as Public Key Infrastructure (PKI) which provides key management functions. Asymmetric cryptography can also be used to digitally sign messages by encrypting either the message or a message digest, using the private key. Providing the recipient has the original message they can compute the same digest and thus authenticate the signature by decrypting the message digest. A message digest is derived from the original message and is generally shorter than the original message making it difficult to compute the original message from the digest; a so-called hash function may be used to generate a message digest."), [0075] ("Upon decrypting M3, B checks the key k2 recovered from M3 agrees with that sent in M2. The session key may be computed as $f(k_1 \| k_2)$ using an appropriate publicly known non-reversible function f such as MD5 (Message Digest 5, as defined

in RFC 1321) and SHA-1 (secure Hash Algorithm-1, see, for example, US National Bureau of Standards Federal Information Processing Standards (FIPS) Publication 180-1."); Jeong (2010) at Section 1 ("Currently, the 3rd Generation Partnership Project (3GPP) has established the 3GPP-Authentication Key Agreement (3GPP-AKA) standard to provide user authentication, encryption, and message integrity in mobile environments, but the 3GPP-AKA protocol has been criticized for problems such as synchronization issues with SQN (SeQuence number) and attacks using false base stations, privacy issues due to plaintext transmission of IMSI (International Mobile Subscriber Identity), a permanent identifier of the device, and authentication data overhead due to the use of multiple authentication vectors [3, 4, 5]."), Section 2.2 ("Figure 2 illustrates 3GPP-AKA, the USIM authentication process in the wireless Internet environment. When the USIM/MS identifies itself by sending IMSI (International Mobile Subscriber Identity) or TMSI (Temporary Mobile Subscriber Identity) information to the SN (Serving Network), the SN transmits an authentication data request message and the IMSI/TMSI received from the terminal to the AuC (Authentication Center) of the HN (Home Network), which is the authentication center. The HN generates an authentication vector AV (Authentication Vector) for the received IMSI and transmits it to the SN in response to the authentication data request. The SN selects one of the AVs, generates a random number to extract the authentication token (AUTN) in the AV, and attempts to authenticate the user on the device. The device authenticates this data using the network authentication algorithm of the USIM and transmits a user authentication response to the SN, while generating encrypted session keys CK and IK. The SN authenticates the device and the user by comparing the received RES with the XRES it has stored, and then generates a session key to be used for encrypting the user's data, completing the authentication and key agreement process [10,11,12]."); Nguyen '985 at [0001] ("The present

disclosure relates generally to communication systems and more specifically to a method and apparatus for end-to-end mobile user security in a network.”), [0016] (“The MS 116 can include an identification module 118, such as a secure identification or identity module (e.g., a SIM card), containing subscription information, account data, personal information, and private/public key information. The identification module 118 can have an associated memory (not shown) for storing data associated with a private key. The private key can be used to generate a public key which can be used to securely encrypt data. The private key is kept secret, while the public key may be widely distributed. The keys are related mathematically, but the private key cannot be practically derived from the public key. Data encrypted with the public key can be decrypted only with the corresponding private key. This can be used to ensure confidentiality. Data signed with the sender's private key can be verified by anyone who has access to the sender's public key, thereby proving that the sender signed it and that the message has not been tampered with. This can be used to ensure authenticity.”), [0040]–[0041] (“For example, VLR_1 at step 514 can generate a random number RAND and then encrypt the random number with A_1 to produce an encrypted RAND. VLR_1 can then proceed to send the encrypted RAND to MS_1. At step 516, MS_1 decrypts the encrypted RAND using A_1 to get RAND. MS_1, can apply a message digest algorithm SHA-1 to RAND to produce a signed response SRES=SHA-1 (RAND), and then sends SRES to VLR_1. VLR_1 can also carry out its own computation of SRES using the same message digest algorithm SHA-1 and then compares its result with the SRES sent from MS_1 at step 518. If at step 520, the SRES generated by VLR_1 matches the SRES received from MS_1, VLR_1 can then authenticate MS_1 with VLR_1, as shown in step 522. That is, VLR_1 authenticates that MS_1 does in fact hold the private key P_1 it claims, and authorizes MS_1 for communication through VLR_1. If however, the SRES generated by VLR_1 does not match the

SRES received from MS_1, VLR_1 does not authenticate MS_1 with VLR_1, as shown in step 524. In such regard, VLR_1 cannot confirm that MS_1 does in fact have the private key P_1 it claims to have. Accordingly, VLR_1 cannot confirm to a second VLR_2 desiring to securely communicate with MS_1, that MS_1 is authorized to communicate on the cellular network 113. After authenticating User_1 of MS_1 and User_2 of MS_2, VLR_1, VLR_2 and each MS has the public key of its own subscriber User_1 and User_2, respectively."); Peirce '967 at Abstract ("A system and method for producing cryptographic keys for use by an embedded processing device within a manufactured product. A pseudo random number generator is seeded with entropy data gathered by the embedded device, and the result is used to generate a public-private key pair. The process can be carried out during manufacturing so that the public key of each manufactured product can be stored in a database along with a unique identifier for the embedded device associated with the key. In one particular example, a vehicle having an installed telematics unit uses the key generating process to self-generate keys using entropy data available to the vehicle."), [0001]–[0002] ("The present invention relates generally to techniques for generating cryptographic keys used in secure data communications and, in particular, to such techniques used for manufactured products having embedded processing devices. As computer electronics continue to reduce in cost and size, the applications for embedded processing devices are continuing to increase, and there now exists many types of manufactured products that contain some type of embedded processing device, whether microprocessor based or otherwise. Some embedded devices are designed to undergo data communication with one or more external, possibly remote devices. In some cases, it is desirable to establish authenticated, secure data communications in which the exchanged data is encrypted. Although various approaches can be used, cryptographic keys are perhaps most commonly used for this purpose. In public key

cryptography, a public-private key pair is created with the public key then being available for use by anyone desiring encrypted communication with the holder of the private key. Digital certificates issued by a trusted third party (certificate authority) can also be used to authenticate the public key to a particular entity."), [0036] ("For the vehicle example shown in FIG. 1, examples of entropy data that can be used are measured transient events occurring on the vehicle, such as features of messages or other communications occurring on the communications bus 44, data from a vehicle system module (VSM) 42 such as data from a sensor 43, or GPS satellite time data (normally used for determining location coordinates) that are received from the GPS module 40. Other, non-transient, but unique data can be used as entropy data, such as serial numbers from onboard devices, the vehicle VIN, an assigned mobile number for the telematics unit or network node address. Other such sources of entropy will become apparent to those skilled in the art."); Semple '841 at Abstract ("A mutual authentication method is provided for securely agreeing application-security keys with mobile terminals supporting legacy Subscriber Identity Modules (e.g., GSM SIM and CDMA2000 R-UIM, which do not support 3G AKA mechanisms). A challenge-response key exchange is implemented between a bootstrapping server function (BSF) and mobile terminal (MT). The BSF generates an authentication challenge and sends it to the MT under a server-authenticated public key mechanism. The MT receives the challenge and determines whether it originates from the BSF based on a bootstrapping server certificate. The MT formulates a response to the authentication challenge based on keys derived from the authentication challenge and a pre-shared secret key. The BSF receives the authentication response and verifies whether it originates from the MT. Once verified, the BSF and MT independently calculate an application security key that the BSF sends to a requesting network application function to establish secure communications with the MT."), 1:23–29 ("The present

invention generally relates to systems and methods for securing wireless communications. More specifically, one feature of the invention provides a novel authentication and key agreement scheme for devices supporting legacy network authentication mechanisms, in order to provide application security keys by taking advantage of legacy wireless authentication and key agreement mechanisms.”), 8:30–9:18 (“For instance, this verification may be performed using a public key or digital server certificate of the BSF which has been provisioned in the MT. If the authentication challenge does not come from the expected BSF, then the process terminates. Otherwise, an authentication response to the challenge is formulated based on a secret key provided by the SIM of the MT 510. For instance, the MT passes the random number RAND to the SIM (in the MT) which calculates one or more secret keys (SRES and Kc) using the pre-shared secret key Ki and random number RAND with the algorithms A3 and A8. The secret keys SRES and Kc are then provided to the MT to formulate the authentication response. In one implementation, the secret keys SRS and Kc may be used to compute a message authentication code, or derive or encrypt one or more parameters, that is sent as part of the authentication response. The authentication response is sent from the MT to the BSF 512. The BSF then verifies the origin of the authentication response based on an independently obtained secret key 514. For instance, the SRES and Kc obtained from the HLR (in the triplet corresponding to random number RAND and pre-shared secrete key Ki) may be used to validate one or more parameters in the authentication response from the MT. For instance, the BSF may independently calculate the message authentication code (or other parameter in the authentication response) using the random number RAND, SRES, and/or Kc received from the HLR. If the parameters (e.g., message authentication code) calculated by the MT and BSF match, then the origin of the authentication response is verified. In an alternative implementation, the MT may calculate a

third key using the one or more secret keys (SRES and Kc obtained from the SIM) and other parameters (obtained from the authentication challenge or response or from the SIM). This third key is then used to formulate the authentication response (e.g., compute the message authentication code). The BSF may also calculate the same key since it knows the same keys and/or parameters as the MT. Thus, the BSF can verify whether the authentication response originated from the MT. Once the authentication response is verified, the BSF and MT independently compute a shared key based on one or more keys and/or parameters (e.g., SRES, Kc, and/or other parameters) known to both the BSF and MT 516. This shared key can then be provided to a requesting NAF to establish secure communications or transactions between the MT and NAF 518. The MT authenticates transmissions from the BSF by means of a public key mechanism. The BSF challenges the MT with a random number RAND and establishes that it is in possession of the corresponding secret keys SRES and/or Kc in order to authenticate the transmissions from the MT. Thus, the BSF and MT are mutually authenticated in order to share information from which keys may be derived for the purpose of bootstrapping."); Wang '162 at [0003] ("More particularly, the present invention is related to a method and apparatus for security protection of an original user identity (ID) in an initial access signaling message in a wireless communication system including third generation (3G) long term evolution (LTE)."), [0007]–[0010] ("Each AV contains a quintet of numbers that includes a random number (RAND), an expected response (XRES) which is used to authenticate the user, a cipher key (CK) for establishing confidentiality, an integrity key (IK), and an authentication token (AUTN). The AUTN comprises a sequence number (SQN) hidden by an anonymity key (AK), an authentication management field (AMP) which specifies certain authentication components, (such as algorithms to be used, key lifetime, etc.), and a message authentication code (MAC)

which is functionally dependent on the SQN, the AMF, and the RAND. The VLR/SGSN 20 sends the RAND and the AUTN from the AV that it has selected to the NAS layer 14 via the UTRAN 18 (steps 118, 120). The NAS layer 14 then authenticates the network by calculating an expected MAC (XMAC) and determining whether the XMAC matches the MAC (step 122). The NAS layer 14 also computes session security keys to the WTRU 12, (i.e., the CK and IK in the AV) at step 122. The key generation is performed using predefined UMTS algorithms which take RAND as input and apply the shared secret key K. The NAS layer 14 computes a response (RES) and sends the RES to the VLR/SGSN 20 via the UTRAN 18 (steps 124, 126). The VLR/SGSN 20 determines if the RES matches the XRES to authenticate the WTRU 12 (step 128). An authentication failure occurs if either of these authentication attempts fails at steps 122 and 128. Once mutual authentication has succeeded, the VLR/SGSN 20 sends an authentication complete message to the HLR/AuC 22 (step 130) and a local security activation procedure starts. The VLR/SGSN 20 sends a security mode command to the UTRAN 18 including the negotiated UMTS encryption algorithms (UEAs) and UMTS integrity algorithms (UIAs), and the current session keys, CK and IK (step 132). As secure communication can now begin the UTRAN 18 sends a security mode command to the RRC layer 16 with a message authentication code for integrity (MAC-I) (step 134). The MAC-I value protects the integrity of the security mode command message. The MAC-I is a type of hash computed by a UIA on the message's contents using the session key IK.”). Thus, a person of ordinary skill in the art would have been motivated to modify any of the primary references to include this feature. A person of ordinary skill in the art would also have had a reasonable expectation of success. A person of ordinary skill in the art would have understood that these references disclose interrelated teachings based on routine

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

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach using cryptographic algorithms and an elliptic curve Diffie-Hellman key exchange, based on public/private key pairs, to generate a shared symmetric session key to secure communications between a mobile device and telecommunications network server (in regards to Limitations 1[pre], 1[b], 1[c], 1[d], and 1[e])[16], it would have been obvious to a person of ordinary skill in the art at the time of the invention to combine the primary reference with any of the prior art that disclose Limitations 1[pre], 1[b], 1[c], 1[d], and 1[e] in Exhibits D-01 to D-09 or D-A. For example, several prior art references, including Ala-Laurila '934, Bhuyan '491, Boyd-Mathuria, Farnham '766, Jeong (2010), Nguyen '985, Peirce '967, Semple '841, Wang '162, and Secondary References explicitly describe or disclose using an elliptic curve Diffie-Hellman key exchange, based on public/private key pairs, to generate a shared symmetric session key to secure communications between a mobile device and telecommunications network server in mobile/tele-communications context. *See, e.g.*, Ala-Laurila '934 at Abstract, [0002]–[0009], [0025]–[0032], [0041]–[0049], Figs 1–5; Bhuyan '491 at Abstract, [0001]–[0006], [0045]–

[16] Specifically, Limitation 1[pre]: "A method comprising;" Limitation 1[b]: "(2) deriving a module private key and a corresponding module public key associated with the mobile device using the cryptographic algorithms;" Limitation 1[c]: "(3) deriving a symmetric ciphering key using (i) an elliptic curve integrated encryption scheme with the server public key and the module private key and (ii) an American National Standards Institute standard X-9.63 key derivation function;" Limitation 1[d]: "(4) generating module encrypted data using the symmetric ciphering key and the symmetric ciphering algorithm, wherein the module encrypted data includes the module identity;" and Limitation 1[e]: "(5) sending a message to a server for a wireless network, the message comprising the module encrypted data and the corresponding module public key, wherein the server mutually derives the symmetric ciphering key using at least the module public key, and wherein the wireless network selects the pre-shared secret key for the mobile device using the module identity."

[0052], [0062], [0074]–[0091], Figs. 1–6; Boyd-Mathuria at Chapters 1.4, 1.6, 2.3, 2.6, 3.3, 4.1, 4.3.5, 5.1, 5.1.3, 5.2, 5.4.4, 5.7.2, 5.9, 5.11, 6.2.7, 7, 7.8, A; Farnham '766 at Abstract, [0001]–[0009], [0012]–[0018], [0051]–[0058], [0069]–[0075], [0083]–[0087], Figs. 1–3, Cls. 6, 10, 14; Jeong (2010) at Abstract, Sections 1, 3.1.1, 3.2, 4.1.4, 5, Figs. 2, 4–6; Nguyen '985 at Abstract, [0001]–[0004], [0010]–[0021], [0036]–[0048], Figs. 1–2, 4–6, Cls. 1, 10, 15; Peirce '967 at Abstract, [0001]–[0014], [0032]–[0042], Figs. 1–3, Cls. 1, 14–15; Semple '841 at Abstract, 1:23–2:43, 6:3–7:3, 9:19–59, 9:60–10:24, Figs. 1–7; Wang '162 at Abstract, [0003]–[0015], [0029]–[0044], [0086], [00129] Figs. 1–7.

A person skilled in the art would have understood the benefits of using an elliptic curve Diffie-Hellman key exchange, based on public/private key pairs, to generate a shared symmetric session key to secure communications between a mobile device and telecommunications network server (in regards to Limitations 1[pre], 1[b], 1[c], 1[d], and 1[e]), given the well-known and complementary confidentiality and security considerations in that process, and therefore would have been motivated and had a reasonable expectation of success to incorporate this feature into the device or method for a mobile device application according. *See, e.g.*, Ala-Laurila '934 at [0026] ("The MT requests 202 (IMSI request) the identity module SIM for the IMSI identifier and the SIM returns 203 the IMSI identifier. The MT sends 204 the authentication starting request (MT_PAC_AUTHSTART_REQ) which preferably comprises a Network Access Identifier NAI. The NAI comprises the IMSI identifier obtained from the identity module SIM. The NAI may be presented, for example, in the form 12345@GSM.org, where 12345 is the IMSI identifier and GSM.org is the domain name of the mobile network, which has conveyed the identity module SIM. The request 204 is preferably sent in ciphered form to the PAC using the Diffie-Hellman algorithm, for example. The MT preferably also sends a specific protection code MT_RAND in

the request 204, said code typically being a challenge code. Using the protection code MT_RAND the MT may later be ensured that the party conveying the GSM triplets actually has access to the secret key Ki, which is to be maintained in the GSM home network of the subscriber. However, the use of the protection code is not obligatory.”), [0032] (“The second calculation means included in the MT, preferably the control means CM, calculate 217 (Calculate K) a second ciphering key K using one or more first ciphering keys Kc according to the mobile network GSMNW calculated by the SIM.”), [0042] (“The GAGW informs 222 the PAC about the authentication being accepted (GAGW_PAC_AUTHANSWER_RESP_OK). This message comprises at least the second ciphering key K. Information on services that the MT is authorized to use (such as quality of service QoS data) can also be sent in the message 222. The PAC informs 223 the terminal MT about the authentication being accepted (PAC_MT_AUTHANSWER_RESP_OK). Authentication is then performed and both the terminal MT and the PAC comprise a similar second ciphering key K which can be transmitted to the ciphering means performing ciphering for ciphering traffic.”), [0048] (“After receiving the second ciphering key K, the AP sends 309 (Put_WEP_on) a request to the MT concerning the use of the WEP algorithm for data ciphering. The MT acknowledges 310 (Put_WEP_on_ack) the request, so that the starting point of data ciphering is correctly timed. After this the second ciphering key K is applied in the MAC layer of the MT, and the MT enciphers the data to be sent and deciphers the received enciphered data 311 (Cipher data with K and WEP) using the K and the WEP algorithm. The AP also starts to use 312 (Cipher data with K and WEP) the K and the WEP algorithm for enciphering data directed to the MT and for deciphering data received from the MT. The AP checks the terminal MT MAC addresses of the received data and performs deciphering for data arriving from the MAC address and correspondingly enciphers the MT data

directed to the MAC address. In this case, the K is rapidly initiated and data ciphering can be started.”); Bhuyan ’491 at [0074] (“In step 608, the access server 506 forwards the authentication request, including the IMSI, to the authentication server 206. The authentication server 206 then uses the IMSI received in the authentication request to retrieve the previously generated (in step 310 in FIG. 3) secret key Ki corresponding to the IMSI. The authentication server then generates a triplet comprising a random number RAND, an expected response SRES and a key Kc in step 612. Each of these parameters is generated in accordance with the methods shown in FIG. 1. The values generated for RAND, SRES and Kc are then sent to the access server 506 in step 612.”), [0078]–[0079] (“Once the access server 506 has received SRES 404, it calculates SRES1 412 as illustrated in the remainder of FIG. 4 a. Specifically, SRES 404 is fed into cryptographic algorithm F1 together with the password 406 received from the data store 208. The cryptographic function F1 is operator specific and can be defined by the operator for its specific use in contrast to the GSM algorithms like A3, A5 and A8, which are generally used across service providers and operators. The F1 function can also be tailored and thus be specific to the mobile device 210, as the function F1 is included as part of the security module provided to the mobile device 210 in step 318. Similarly, the access server 506 also uses the received Kc 406 from the authentication server 206 and the password from the data store 208 and feeds both these parameters into cryptographic function F2 to derive Kc1 414. The generation of Kc1 414 is illustrated in FIG. 4 b. It should be noted that like F1, the cryptographic function F2 is also operator specific, but can also be further specified for the individual mobile device 210 in question.”), [0086] (“The mobile device 210 then uses the value of Kc1 generated in step 622 to encrypt and decrypt data transferred to and from the mobile device. The method for ciphering is shown in FIG. 4 c and is the same as that described with reference to FIG. 1 c above, but using Kc1 instead of Kc. In step

630, the access server 506 provides the application server 502 with a copy of Kc1 generated by the access server 506 in step 618. Thus, by mobile device 210 and the application server 502 can communicate securely by ciphering all data using the now shared session key of Kc1 as shown in step 632."); Boyd-Mathuria at Chapter 5.2 ("Typical sizes in use today are 1024 bits for the length of p and 160 bits for the length of q. Several other algebraic groups have been proposed as the setting for Diffie-Hellman key exchange. Examples are given in Sect. 5.9. In particular, elliptic curve groups are popular today."), Chapter 5.9 ("Diffie-Hellman key agreement was originally proposed in the algebraic setting of the multiplicative group Z_p^* and we have used this setting in all our descriptions so far. It has long been known that the basic structure can be generalised to any commutative group. In this section we mention some of the most prominent alternative groups that have been proposed. Elliptic curve groups have significant potential advantages over using Z_p^* because of their greater efficiency and compact representation. Many recent protocols have been specially designed with elliptic curve implementation in mind rather than using prime fields. Examples include the MQV (5.11) and Oakley (5.18) protocols. The Oakley specification includes a number of candidate elliptic curves and also provides for negotiation of new curves during the protocol. It is sometimes possible to avoid certain attacks because of the structure of the curve used. For example, elliptic curve groups can be chosen to have prime order so that there is no need to check whether elements are in a particular subgroup." (emphasis omitted)), Chapter 7.8 ("Since these protocols may well be useful in applications employing mobile computing devices, the computational efficiency and storage gains in using elliptic curve groups can be very attractive. Although it is straightforward to generalise the protocol definitions to different groups, there may be undesirable consequences with respect to security. For example, consider Protocol 7.1 when the Diffie-Hellman exchange takes place in

an elliptic curve group."), Farnham '766 at [0056]–[0058] ("In a variant of this technique, the key k is replaced by a Diffie-Hellman public value g^n mod p (see, for example, W. Diffie and D. E. Hellman, ibid), where n is a positive integer satisfying $1 \leqq n \leqq p-2$…. The mobile terminal B or the client can obtain the server's public value $Y_A=g^a$ mod p that is contained in the server key exchange or the SIM may contain the server's public value. The originator (in this example, the server A) chooses a random value n, computes g^n mod p and sends M1 including g^n mod p to the terminal. The server A can then compute a session key $k = Y_A\ n = (g^a)^n = g^{an}$ mod p and the terminal B can compute the same session key using $k = (g^n)^a = g^{na}$ mod p. Encrypted software may then be sent to the terminal B by encrypting the software with the common session key. An eavesdropper does not know the private key of server (that is a) and thus, it is computationally infeasible to determine the session key. This method can be used for distributing system software to mobile equipment for anonymous secure software download, for example for broadcasting a SIM update, because an individual recipient need not be specified."), [0071] ("Under certain circumstances, the Diffie-Hellman and (DH) the related Elliptic Curve Diffie-Hellman (ECDH) key agreement schemes (X9.63, 'Public key cryptography for the financial services industry: Key agreement and key transport using elliptic curve cryptography', Draft ANSI X9F1, October (1999)) are susceptible to a class of attacks known as "small-subgroup" attacks. Where, if a key belongs to a small subgroup a directed brute-force attack based on guessing keys from the subgroup may succeed. In the anonymous DH and ECDH cases there is a risk that such a small subgroup attack will lead communicating parties to share a session key which is known to an attacker. This threat can be alleviated by using a predetermined group determined 'good' or 'strong' values of g and p and checking that received public keys do not lie in a small subgroup of the group, or by not re-using ordinary DH key pairs. Background information on protection

against these attack, can be found in the draft ANSI standards X.9.42 (X.9.42, 'Agreement of symmetric keys using Diffie-Hellman and MQV algorithms', ANSI draft, May (1999)) and. X.9.63 (X9.63, 'Public key cryptography for the financial services industry: Key agreement and key transport using elliptic curve cryptography', Draft ANSI X9F1, October (1999)).”); Jeong (2010) at Section 3.1.1 (“The shared secret key is generated by the EC-DH algorithm, and the shared secret key is used for mutual authentication. Among the component of the mobile payment system, the process of generating a shared secret key between the certificate authority and the store is as follows. (1) The merchant registers the merchant's information when registering with the certificate authority. (2) The certificate authority delivers to the merchant the initial point P, E_p, and the certificate authority's public key $A_{SK}P$, which are necessary for generating the shared secret key. (2) The certificate authority delivers to the merchant the initial point P, E_p, and the certificate authority's public key $A_{SK}P$, which are necessary for generating the shared secret key. (3) The merchant generates a shared secret key $M_{(SK)}\ (A_{(SK)}P)$ with the certificate authority's public key and passes it to the certificate authority as $M_{SK}P$, the merchant's public key. (4) The certificate authority generates a shared secret key $A_{(SK)}\ (M_{(SK)}P)$ with the merchant's public key and validates it with the shared secret key delivered by the merchant. (5) The merchant checks the validity of the shared secret key received from the certificate authority against the shared secret key generated by the merchant. (6) If the validation is TRUE, the shared secret is used as the shared secret of the merchant and the certificate authority.”), Section 4.1.4 (“Since the mobile payment protocol and the AKA module proposed in this paper use SSK and OT-SSK based on EC_DH, even if the initial point P and the public key are disclosed, the SSK and OT-SSK cannot be derived because they do not know each other's secret key, and they satisfy full omnidirectional safety.”), Section 5 (“The AKA module proposed in this paper prevents IMSI exposure by

generating a shared secret key between the MS and the HN for user authentication and encrypting and transmitting the IMSI value of the USIM, and prevents data replay attack by generating a new OT-SSK for each connection by generating message encryption keys, CK and IK, using a one-time shared secret key, OT-SSK, between the MS and SN."); Nguyen '985 at [0019]–[0020] ("The MSC 123 can include an authentication center (AuC) 231, a Home Location Register (HLR) 232, and/or a Visitor Location Register (VLR) 232 each implementing the key exchange algorithm 117. The key exchange algorithm 117 protects the security of the entire communication channel between any two mobile users. The key exchange algorithm can be based on the Elliptic Curve Diffie-Hellman (ECDH) cryptosystem, which itself is a key exchange algorithm that is based on Elliptic Curve Cryptography (ECC) for public/private key generation. ECC is an approach to public-key cryptography based on an algebraic structure of elliptic curves over finite fields. An elliptic curve is a plane curve defined by an equation of the form $y^2=x^3+ax+b$. The set of points on such a curve can be shown to form a commutative group G, such that a*b=b*a for all a and b in G. Elliptic Curve Diffie-Hellman (ECDH) is a key agreement protocol that allows the two MSs to establish a shared secret key over an insecure channel. The secret key can then be used to encrypt subsequent communications using a symmetric key cipher."), [0036] ("Method 500 begins with step 502 in which MS_1 can use its own private key P_1 to compute its own public key Q_1 using a chosen base point B on a specific Elliptic Curve algorithm. The base point "B" can be a random value selected from an elliptic curve algorithm. B does no need to be a secret value and can be available to devices within the communication system 100. In practice, providers within the communication system 100 can determine how the base point B is calculated and distributed among MSs and VLR's. For instance, in one embodiment a unique base point can be used for the entire GSM network that is pre-built into MSs' SIM cards and

VLRs. Another implementation option provides a distinct and temporary base point B for each communication session.”), [0038]–[0039] (“Each MS can use the public key received from the other MS along with its own private key to generate a shared Diffie-Hellman authentication key. For instance, at step 510, MS_1 computes the shared Diffie-Hellman authentication key A_1 using its own private key P_1…. Similarly, at step 512, VLR_1 can compute the shared Diffie-Hellman authentication key A_1 using its own private key P_VLR1, in accordance with the same method steps above. As a result of the elliptic curve algorithm, the authentication key A_1 generated by MS_1 should be the same as the authentication key generated by VLR_1, as shown in the equation above. Although, neither MS_1 nor VLR_1 is aware of the authentication key A_1 value generated by the other, each can perform a subsequent operation together to validate the value.”); Peirce ’967 at [0001] (“The present invention relates generally to techniques for generating cryptographic keys used in secure data communications and, in particular, to such techniques used for manufactured products having embedded processing devices.”), [0038] (“Using the entropy data, the next step 106 in the process is generation of the cryptographic keys using the PRNG within the embedded device. Suitable PRNG software programs are known and can be incorporated into the embedded processing device. The entropy data is used as a seed value for the PRNG, which will yield a nearly random number suitable for use in generating strong cryptographic keys. Once the keys have been generated, the entropy data used to seed the PRNG process is preferably erased from any memory in which it had been held. The use of the output of the PRNG to generate various types of keys is known, including asymmetric public-private key pairs. These keys can be used either in a web of trust scheme, or can be utilized using public key infrastructure wherein the public key can be issued by a certificate authority.”), [0041] (“As shown in FIG. 1, the telematics unit includes a PRNG program (PRNGP) 55 which can be

stored in the telematics memory 54 and executed by the processor 52. Thus, at step 212, the PRNG can be seeded with the entropy data and the near-random number that is generated is then used in a known manner at step 214 to generate a public-private key pair. The private key is stored in the vehicle, such as in the telematics memory 54 at step 216, and the public key is transmitted at step 218 to an external database along with at least one unique identifier associated with the telematics unit. Transmission of the public key can be done wirelessly using the cellular chipset 50 or using some other communication approach, as will be known to those skilled in the art. The external database that stores the keys and associated IDs can be, for example, database 84 that is maintained at the call center 20. Once the keys have been generated and stored in their respective locations, the vehicle can then be distributed to a dealer or end customer, as indicated at step 220. The keys can then be used to establish secure communication between, for example, the call center 20 and the vehicle 12."), Cl. 15 ("A vehicle electronics system for self-generating cryptographic keys used for secure wireless communication with the vehicle…."); Semple '841 at 6:3–10 ("A Diffie-Hellman key exchange may be employed as part of the key agreement process between the MT 102 and the BSF 106. The Diffie-Hellman key exchange is a cryptographic protocol which allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. In one application this shared secret key can then be used to encrypt subsequent communications using a symmetric key cipher."), 6:33–57 ("FIG. 2 is a block diagram illustrating a mobile terminal (MT) 200 configured to perform mutual authentication with bootstrapping server function operational on a communication network. The MT 200 includes a processing circuit 202 (e.g., processor) coupled to a communication interface 202 to communicate with a wireless network, and a Subscriber Identity Module (SIM) card 204. The processing circuit 202 may be configured to perform part

or all of the methods illustrated in FIGS. 4, 5, 6, and 7. The SIM 204 may contain a secret key Ki, an implementation of GSM authentication and key agreement algorithms (i.e., the GSM A3/A8 algorithms), and is inserted in a MT 102 containing a public key or digital server certificate of a public key corresponding to a private key in BSF 106. In particular the SIM 204 may be a standard legacy smart card configured for use in a GSM network. The public key or server certificate may correspond to a RSA public key, or other public-key techniques affording digital signatures may also be used, for example, DSA (digital signature algorithm). The BSF 106 and MT 102 may also share a pre-determined generator P of a cyclic group, such as the multiplicative subgroup of a finite field or a point in an elliptic curve, allowing them to employ the Diffie-Hellman key exchange. In alternative embodiments, the MT 200 may include a CDMA2000-compliant authentication module instead of the SIM 204.”), 9:35–59 (“In one embodiment, a request for authentication keys may be initiated by MT 606 retrieving its associated International Mobile Subscriber Identity (IMSI) 600 from its SIM 608 and sending it to a bootstrapping server function (BSF) 604. The BSF 604 sends the IMSI 600 to the HLR 602 where it may verify whether the IMSI 600 belongs to a MT that subscribes to the network. The HLR 602 may be operated by the service provider for the subscriber whose SIM is contained in MT 606. The HLR 602 selects, for example, a 128-bit random challenge RAND and together with pre-shared secret key Ki, uses them as inputs for two algorithms A3 and A8 to yield 32-bit output signed response SRES and 64-bit output secret confidentiality key Kc, respectively. The HLR 602 then provides the triplets (RAND, SRES, Kc) to the BSF 604, corresponding to the identity IMSI 600 of SIM 608. The BSF 604 generates a random secret exponent x and computes a Diffie-Hellman public key P^x, where P is a generator of a cyclic group previously provisioned to both the BSF 604 and MT 606, such as the multiplicative group of a finite field or the additive

group of an elliptic curve. The BSF 602 then sends a triplet (RAND, P^x, SIG) 610 to the MT 606, where SIG is a digital signature computed using the BSF 604 RSA private key. The message 610 may be further enhanced to include other server-authenticated parameters such as a transaction identifier."); Wang '162 at [0015] ("The initial security parameters are loaded from a universal subscriber identity module (USIM) and generated from system information broadcast from the network. The system information includes a public key set with at least one public key for asymmetric encryption of the IMSI or information from which the public key(s) can be derived. The initial security parameters for ciphering include a CK. The CK may be a public key or may be selected from the public key set broadcast by or derived from the network system information. An index of the selected public key may be separately encoded. Alternatively, the index may be communicated by using a Diffie-Helman key exchange method."), [0034] ("The aGW 260 sends an authentication request message to the NAS layer 211 of the WTRU 210 including the RAND and the AUTN from the first AV (step 324). The connection response message does not have to be ciphered or integrity protected. Alternatively, the connection response message may be ciphered at the eNode-B 250 with a public key with an index from the HLR/AuC 270 with the conventional symmetric ciphering algorithm. The NAS layer 211 then authenticates the network by calculating an expected MAC (XMAC) and determining whether the XMAC matches the MAC (step 326). The NAS layer 211 also computes new session keys, (i.e., CK and IK in the AV) at step 326. The key generation is performed using predefined algorithms which take RAND as input and apply the shared secret key K."), [0038] ("Figure 4 shows a ciphering process including conventional f8 ciphering and ciphering parameters. The ciphering algorithm may be a conventional symmetric ciphering algorithm such as f8 or an asymmetric encryption algorithm used for the ciphering with public and private keys."), [0042] ("Alternatively, the public key may

be selected using a Diffie-Hellman key exchange method. The LTE network 230 and the WTRU 210 agree on two values, (a very large prime number p and a generator g of the multiplicative group F_p' of the field F_p), that are publicly known. The LTE network 230 broadcasts via system information a set of public keys with a first seed, g_{KI} (where a randomly selected KI is such that $1 < KI \leq p - 2$ and $g \equiv g^{KI} \bmod p$). The set of public keys may be from a larger group of encryption keys with random periodicity and order. The WTRU 210 randomly selects a value $KIn2$, ($1 < KInI < p - 2$), to compute a second seed, $g_{KInl} \equiv g^{KIn2} \bmod p$. The WTRU 210 then computes $k' \equiv (g_{KI})^{KIn2} \bmod p$. The public key index $a \equiv k' \bmod n$, where n is the current number of public keys broadcast from the system information with the first seed, g_{KI} . The computed a is an index to the public key set for the chosen public key k_a . The WTRU 210 ciphers the NAS or the RRC message including the IMSI with the selected public k_a and includes the second seed, g_{KLn2} , in the NAS or RRC message to the LTE network 230. The second seed is not encrypted. The LTE network 230 first takes the unencrypted second seed, g_{KLn2} , and computes $k = (g_{KLn2})^{KI} \bmod p$. The index a is then obtained by $a \equiv k \bmod n$ for the private key index a. The LTE network 230 then decodes the whole message with the private key corresponding to public key ka.”). Thus, a person of ordinary skill in the art would have been motivated to modify any of the primary references to include this feature. A person of ordinary skill in the art would also have had a reasonable expectation of success. A person of ordinary skill in the art would have understood that these references disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

VII. U.S. Patent No. 12,166,869 ("the '869 Patent")

A. Identification of Prior Art

Defendants incorporate by reference, as if set forth fully herein, all filings and exhibits from *Inter Partes* Review IPR2026-00117, filed November 20, 2025 with the PTAB, including any subsequent and future filings in that case.

In addition to the prior art cited on the face of the '869 Patent and related patents, the admitted prior art in the specifications of the '869 Patent and related patents, the prior art cited in any file histories, reexaminations, *inter partes* review proceedings, reissue proceedings, or other examination or post-grant proceedings of the '869 Patent and related patents, and the prior art cited in any invalidity contentions or expert reports submitted in any action or proceedings involving the '869 Patent or related patents, Defendants identify the following prior art that anticipates each asserted claim or renders it obvious.

1. Prior Art Patents

The following patents and patent publications are prior art to the asserted claims under at least 35 U.S.C. §§ 102(a)(1) and/or (a)(2), and/or 35 U.S.C. § 103. The identification of any patent or patent publication shall be deemed to include any counterpart patent or application filed, published, or issued anywhere in the world.

Patent or Publication Number	Country of Origin	Filing Date	Date of Issue or Publication
U.S. Pat. No. 9,210,138 ("Nakhjiri '138")	United States	April 17, 2013	December 8, 2015
U.S. Pat. App. Pub. No. 2012/0300934 ("Ala-Laurila '934")	United States	August 9, 2012	November 29, 2012
U.S. Pat. App. Pub. No. 2014/0024343 ("Bradley '343")	United States	December 2, 2011	October 10, 2013
U.S. Pat. App. Pub. No.	United States	September 6, 2011	November 14, 2013

Patent or Publication Number	Country of Origin	Filing Date	Date of Issue or Publication
2013/0301828 ("Gouget '828")			
U.S. Pat. No. 8,761,390 ("Peirce")	United States	June 30, 2008	June 24, 2014
U.S. Pat. App. No. 2013/0012168 ("Rajadurai '168")	United States	March 15, 2011	January 10, 2013
U.S. Pat. No. 8,391,841 ("Semple '841")	United States	May 23, 2011	March 5, 2013
U.S. Pat. No. 9,807,605 ("Gao '605")	United States	October 15, 2013	October 31, 2017

2. Prior Art Non-Patent Publications

The following non-patent publications are prior art to the asserted claims under at least 35 U.S.C. §§ 102(a)(1) and/or (a)(2), and/or 35 U.S.C. § 103.

Title	Author/Publisher	Date of Publication
A Design of Safe AKA Module for Adapted Mobile Payment System on Openness Smartphone Environment ("Jeong (2010)")[17]	Jeong et al., Journal of Korea Multimedia Society Vol. 13, No. 11	November 2010
Certicom Research, Standards for Efficient Cryptography, SEC 1: Elliptic Curve Cryptography ("SEC-1")	Brown, Certicom Corp.	May 2009
GlobalPlatform Remote Application Management over HTTP Card Specification V2.2 – Amendment B ("GlobalPlatform (Amendment B)")	GlobalPlatform, Inc.	March 2012
ANSI X9.63 Overview: *Key Agreement and Key Transport Using Elliptic Curve Cryptography* ("ANSI X9.63 Overview")	Blake-Wilson, Certicom Corp.	2000

[17] Jeong was originally published in Korean. References to Jeong in these contentions are to a certified translation of the original Korean paper. Both the original and the certified translation of Jeong are included in the accompanying document production.

Title	Author/Publisher	Date of Publication
Secure Profile Provisioning Architecture for Embedded UICC ("Park (IEEE)")	Park et al., 2013 International Conference on Availability, Reliability and Security, 297-303 IEEE	November 7, 2013
Protocols for Authentication and Key Establishment ("Boyd-Mathuria")	Colin Boyd & Anish Mathuria, Springer	2003

3. Prior Art Systems

Defendants' investigation into publicly available prior art systems that teach and/or render obvious each element of any asserted claims is ongoing. Fact discovery is at an early stage, and Defendants may require discovery from third parties regarding publicly available prior art systems. On information and belief, prior art systems from the following companies teach and/or render obvious each element of the asserted claims of the '869 Patent: Cinterion (now Telit); Gemalto (now Thales); Giesecke+Devrient; GlobalPlatform; NXP Semiconductors N.V.; Oberthur Technologies (now IDEMIA); and Sierra Wireless. Defendants reserve the right to amend its identification of prior art systems as Defendants become aware of the existence, functionality, and/or characteristics of prior art systems as a result of its investigation and forthcoming discovery. In addition to the prior art products, components, systems, and methods that may be identified as a result of discovery, Defendants also reserve the right to rely on the documents and publications identified in the corresponding claim charts as prior art publications.

B. Primary References

Defendants contend that the primary prior art references identified below and described in the charts attached as Exhibits E-01 to E-10, by themselves, anticipate the asserted claims of the '869 Patent. To the extent that a primary reference is deemed not to anticipate a claim for failing to teach one or more limitations of that claim, Defendants contend that the claim would

nonetheless have been obvious to a person of ordinary skill in the art at the time of the invention in view of the prior art reference itself, as described in the attached charts. Defendants' prior art charts (attached as Exhibits E-01 thru E-10) set forth the particular claims that are anticipated under 35 U.S.C. § 102 and/or rendered obvious under 35 U.S.C. § 103 by each item of prior art and identify where specifically in each item of prior art, each element of each asserted claim is found.

Exhibit	Primary References
E-01	U.S. Pat. No. 9,210,138 ("Nakhjiri '138")
E-02	U.S. Pat. App. Pub. No. 2012/0300934 ("Ala-Laurila '934")
E-03	U.S. Pat. App. Pub. No. 2014/0024343 ("Bradley '343")
E-04	Jeong et al., *A Design of Safe AKA Module for Adapted Mobile Payment System on Openness Smartphone Environment* ("Jeong (2010)")
E-05	U.S. Pat. App. Pub. No. 2013/0301828 ("Gouget '828")
E-06	U.S. Pat. App. No. 2013/0012168 ("Rajadurai '168")
E-07	U.S. Pat. No. 8,391,841 ("Semple '841")
E-08	U.S. Pat. No. 9,807,605 ("Gao '605")
E-09	Park et al., *Secure Profile Provisioning Architecture for Embedded UICC* ("Park (IEEE)")
E-10	Boyd and Mathuria, *Protocols for Authentication and Key Establishment* ("Boyd-Mathuria")

C. Secondary References

Exhibit E-A lists secondary prior art references and identifies, on a limitation-by-limitation basis, where specifically each secondary reference teaches the limitations of the asserted claims. To the extent that a primary reference is deemed, by itself, not to anticipate or render obvious a claim for failing to teach one or more limitations, the claim would nonetheless

have been obvious to a person of ordinary skill in the art at the time of the invention by the combination of the primary reference with one or more of the other primary references listed above and/or the references listed as disclosing those alleged missing limitations in Exhibit E-A.

D. Obvious Combinations

To the extent that a primary reference is deemed, by itself, not to anticipate or render obvious a claim for failing to teach one or more limitations, the claim would nonetheless have been obvious to a person of ordinary skill in the art at the time of the invention by the combination of the primary reference with one or more other primary references and/or the knowledge of someone skilled in the art. For example, a person of ordinary skill in the art would have been motivated to combine any reference in Exhibits E-01 to E-10 with any other reference(s) in Exhibits E-01 to E-10. Such combinations would be achieved, for example, by merely combining the disclosures described in the respective claim charts for each reference.

Defendants also contend that any of the primary references (or combination of primary references) could be combined with any of the secondary references (or combination of secondary references) in Exhibit E-A to render obvious the asserted claims. Such combinations would be achieved by merely combining the disclosures described in the respective claim charts for each reference.

The obviousness combinations are provided in the alternative to Defendants' anticipation contentions and are not to be construed to suggest that any reference included in the combinations is not itself anticipatory.

1. Exemplary Combinations

Below are examples of prior art references that would have been combined by one of ordinary skill in the art at the time of the alleged invention. These combinations are merely examples. The asserted claims of the '869 Patent are rendered obvious by:

- Nakhjiri ’138 in combination with Bradley ’343 and Jeong (2010).
- Nakhjiri ’138 in combination with Bradley ’343 and Ala-Laurila ’934.
- Nakhjiri ’138 in combination with Bradley ’343, Jeong (2010), and ANSI X9.63 Overview.
- Nakhjiri ’138 in combination with Bradley ’343, Ala-Laurila ’934, and ANSI X9.63 Overview.
- Nakhjiri ’138 in combination with Bradley ’343, Jeong (2010), and Peirce ’390.
- Nakhjiri ’138 in combination with Bradley ’343, Ala-Laurila ’934, and Peirce ’390.
- Nakhjiri ’138 in combination with Bradley ’343, Jeong (2010), and GlobalPlatform (Amendment B).
- Nakhjiri ’138 in combination with Bradley ’343, Ala-Laurila ’934, and GlobalPlatform (Amendment B).
- Nakhjiri ’138 alone or in combination with one or more of Ala-Laurila ’934, Bradley ’343, Jeong (2010), Gouget ’828, Rajadurai ’168, Semple ’841, Gao ’605, Park (IEEE), Boyd-Mathuria, GlobalPlatform (Amendment B), Peirce ’390, ANSI X9.63 Overview, and/or SEC-1.
- Ala-Laurila ’934 alone or in combination with one or more of Nakhjiri ’138, Bradley ’343, Jeong (2010), Gouget ’828, Rajadurai ’168, Semple ’841, Gao ’605, Park (IEEE), Boyd-Mathuria, GlobalPlatform (Amendment B), Peirce ’390, ANSI X9.63 Overview, and/or SEC-1.
- Bradley ’343 alone or in combination with one or more of Nakhjiri ’138, Ala-Laurila ’934, Jeong (2010), Gouget ’828, Rajadurai ’168, Semple ’841, Gao ’605,

Park (IEEE), Boyd-Mathuria, GlobalPlatform (Amendment B), Peirce ’390, ANSI X9.63 Overview, and/or SEC-1.

- Jeong (2010) alone or in combination with one or more of Nakhjiri ’138, Ala-Laurila ’934, Bradley ’343, Gouget ’828, Rajadurai ’168, Semple ’841, Gao ’605, Park (IEEE), Boyd-Mathuria, GlobalPlatform (Amendment B), Peirce ’390, ANSI X9.63 Overview, and/or SEC-1.
- Gouget ’828 alone or in combination with one or more of Nakhjiri ’138, Ala-Laurila ’934, Bradley ’343, Jeong (2010), Rajadurai ’168, Semple ’841, Gao ’605, Park (IEEE), Boyd-Mathuria, GlobalPlatform (Amendment B), Peirce ’390, ANSI X9.63 Overview, and/or SEC-1.
- Rajadurai ’168 alone or in combination with one or more of Nakhjiri ’138, Ala-Laurila ’934, Bradley ’343, Jeong (2010), Gouget ’828, Semple ’841, Gao ’605, Park (IEEE), Boyd-Mathuria, GlobalPlatform (Amendment B), Peirce ’390, ANSI X9.63 Overview, and/or SEC-1.
- Semple ’841 alone or in combination with one or more of Nakhjiri ’138, Ala-Laurila ’934, Bradley ’343, Jeong (2010), Gouget ’828, Rajadurai ’168, Gao ’605, Park (IEEE), Boyd-Mathuria, GlobalPlatform (Amendment B), Peirce ’390, ANSI X9.63 Overview, and/or SEC-1.
- Gao ’605 alone or in combination with one or more of Nakhjiri ’138, Ala-Laurila ’934, Bradley ’343, Jeong (2010), Gouget ’828, Rajadurai ’168, Semple ’841, Park (IEEE), Boyd-Mathuria, GlobalPlatform (Amendment B), Peirce ’390, ANSI X9.63 Overview, and/or SEC-1.

- Park (IEEE) alone or in combination with one or more of Nakhjiri '138, Ala-Laurila '934, Bradley '343, Jeong (2010), Gouget '828, Rajadurai '168, Semple '841, Gao '605, Boyd-Mathuria, GlobalPlatform (Amendment B), Peirce '390, ANSI X9.63 Overview, and/or SEC-1.
- Boyd-Mathuria alone or in combination with one or more of Nakhjiri '138, Ala-Laurila '934, Bradley '343, Jeong (2010), Gouget '828, Rajadurai '168, Semple '841, Gao '605, Park (IEEE), GlobalPlatform (Amendment B), Peirce '390, ANSI X9.63 Overview, and/or SEC-1.

2. Motivations to Combine

To the extent a finder of fact finds that a primary prior art reference does not disclose one or more limitations of an asserted claim, the asserted claim is nevertheless obvious because the allege missing limitations contain nothing beyond ordinary improvements. In other words, the asserted claim combines known elements to achieve predictable results or chooses between clear alternatives known to those of skill in the art, particularly in view of the state of the art as reflected in the relevant prior art.

Moreover, as explained above, it would have been obvious to a person of skill in the art at the time of the alleged invention of the asserted claims to combine any primary reference with any combination of other primary references or secondary references so as to practice the asserted claims. To the extent that Plaintiff argues that any concept claimed in the asserted claims is not disclosed in a primary reference, it would, at a minimum, have been obvious to adapt the primary reference to include the concept or combine it with other primary references or secondary

references that disclose the concept. Each concept described and claimed in the Asserted Patents was known to those of skill in the art as available design choices for the technologies at issue.[18]

The Supreme Court has held that "[t]he combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 416 (2007). "When a work is available in one field of endeavor, design incentives and other market forces can prompt variations of it, either in the same field or a different one." *Id*. at 417. As the Supreme Court made clear, "[f]or the same reason, if a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill." *Id*.

To determine whether there is an apparent reason to combine the known elements in the fashion claimed by the patent at issue, a court can "look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art." *Id*. at 418. For example, obviousness can be demonstrated by showing "there existed at the time of invention a known problem for which there was an obvious solution encompassed by the patent's claims." *Id*. at 420. "[A]ny need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed." *Id*. Common sense also teaches that "familiar items may have obvious uses beyond their primary

[18] Each concept described and claimed in the '869 Patent was known to those of skill in the art as available design choices for data encryption technology and/or using such technology to provision and/or authenticate mobile devices for use with a wireless network in a wide range of applications for different scenarios and circumstances.

purposes, and in many cases a person of ordinary skill will be able to fit the teachings of multiple patents together like pieces of a puzzle." *Id*.

However, the Supreme Court in *KSR* held that a claimed invention can be obvious even if there is no explicit teaching, suggestion, or motivation for combining the prior art to produce that invention. In summary, *KSR* holds that patents that are based on new combinations of elements or components already known in a technical field may be found to be obvious. *See, generally*, *KSR*, 550 U.S. 398. Specifically, the Court in *KSR* rejected a rigid application of the "teaching, suggestion, or motivation [to combine]" test. *Id*. at 418. "In determining whether the subject matter of a patent claim is obvious, neither the particular motivation nor the avowed purpose of the patentee controls. What matters is the objective reach of the claim." *Id*. at 419. "Under the correct analysis, any need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed." *Id*. at 420. A key inquiry is whether the "improvement is more than the predictable use of prior art elements according to their established functions." *Id*. at 417.

The rationale to combine or modify prior art references is significantly stronger when, as here, the references seek to solve the same problem, come from the same field, and correspond well to each other. *In re Inland Steel Co*., 265 F.3d 1354, 1362 (Fed. Cir. 2001). The Federal Circuit has held that two references may be combined as invalidating art under similar circumstances, namely "[the prior art] focus[es] on the same problem that the … patent addresses: enhancing the magnetic properties of … steel. Moreover, both [prior art references] come from the same field …. Finally, the solutions to the identified problems found in the two references correspond well." *Id*. at 1364 (concerning patents and prior art relating to improving the magnetic and electrical properties of steel).

In view of the Supreme Court's *KSR* decision, the PTO issued a set of Examination Guidelines. Examination Guidelines for Determining Obviousness Under 35 U.S.C. §103 in view of the Supreme Court Decision in *KSR International Co. v. Teleflex, Inc*., 72 Fed. Reg. 57526 (October 10, 2007). Those Guidelines summarized the *KSR* decision and identified various rationales for finding a claim obvious, including those based on other precedents. Those rationales include:

> (A) Combining prior art elements according to known methods to yield predictable results;
> (B) Simple substitution of one known element for another to obtain predictable results;
> (C) Use of known technique to improve similar devices (methods, or products) in the same way;
> (D) Applying a known technique to a known device (method, or product) ready for improvement to yield predictable results;
> (E) "Obvious to try" – choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success;
> (F) Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations would have been predictable to one of ordinary skill in the art;
> (G) Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention.

Id. at 57529. The above rationales likewise apply in rendering obvious the asserted claims of the Asserted Patents.

The references disclosed herein, alone or in combination, contain an explicit and/or implicit teaching or motivation to combine them due to the following: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved;

(4) the fact that each prior art reference addresses similar problems; and (5) the knowledge of those skilled in the art that the disclosed elements had been or could be used together.

As an example of those reasons and motivations to combine the references, Nakhjiri '138, Ala-Laurila '934, Bradley '343, Jeong (2010), Gouget '828, Rajadurai '168, Semple '841, Gao '605, Park (IEEE), and Boyd-Mathuria generally relate to encryption technology, and/or using such technology to provision or authenticate a mobile device for use with a wireless network. *See* Exs. E-01 to E-10 and E-A. The references disclose similar components and techniques for data encryption, and/or using encryption to provision or authenticate mobile devices. *Id.* The attached charts in Exhibits E-01 to E-10 and E-A provide additional reasons and motivations to combine the charted references.

Additionally, the primary and secondary references listed above are analogous art. They are all directed to encryption technology, and in particular, to provisioning and/or authenticating a mobile device for use with a wireless network. *See, e.g.*, Nakhjiri '138 at Abstract ("A method provides end-to-end security for transport of a profile to a target device (e.g., a mobile computing device) over at least one communications network … [T]he profile is encrypted for transport between the target device and an initial node of the network through which the profile is transported"); Ala-Laurila '934 at [0025] ("FIG. 2 shows the essential functions according to a preferred embodiment of the invention for authenticating the terminal MT and for calculating a ciphering key. The terminal MT is offered an identifier IMSI and a secret key Ki by the subscriber identity application SIM included therein."); Bradley '343 at [0002] ("The present invention concerns a method for downloading a subscription in an UICC (Universal Integrated Circuit Card) embedded in a terminal for example a mobile terminal (mobile phone) or a machine (for M2M (Machine to Machine) applications"); Jeong (2010) at Section 5 ("The user

authentication of the mobile payment protocol proposed in this paper eliminates the possibility of USIM exposure by encrypting and transmitting the USIM from the store to the certifier with each shared secret key, and generates a new session key using the USIM, a random value, the user's master key, the store's master key, and the payment center's master key every time the identity of the user, store, and payment center is verified, so that malicious users cannot attempt to make mobile payments due to the exposure of the previous session key."); Gouget '828 at Abstract ("The present invention provides a method for establishing a secure communication channel between a client (C) and a remote server (S), said client (C) and remote server (S) exchanging data through an intermediate entity (G), said client (C) having a long-term key pair (sk_c,pk_c), said remote server generating an ephemeral key (sk_s,pk_s), the method comprising a mutual authentication step wherein the client (C) sends a public key (pk_c) of said long-term key pair (sk_c, pk_c) and the proof that said public key (pk_c) is valid to the server (S), and wherein the remote server (S) sends the public key (pk_s) of said ephemeral key pair (sk_s,pk_s) to the client (C)."); Rajadurai '168 at Abstract ("The present invention provides a method and system for secured remote provisioning of a universal integrated circuit card of a user equipment. A system includes a user equipment for initiating a request for remote provisioning of an universal integrated circuit card (UICC) in the user equipment, where the request for remote provisioning includes a machine identifier (MID) associated with the user equipment and a public land mobile network (PLMN) identifier (ID) associated with an network operator."); Semple '841 at Abstract ("A mutual authentication method is provided for securely agreeing application-security keys with mobile terminals supporting legacy Subscriber Identity Modules (e.g., GSM SIM and CDMA2000 R-UIM, which do not support 3G AKA mechanisms). A challenge-response key exchange is implemented between a bootstrapping server function (BSF) and mobile terminal

(MT). The BSF generates an authentication challenge and sends it to the MT under a server-authenticated public key mechanism."); Gao '605 at Abstract ("The present invention provides a method and a device for switching a subscription manager-secure routing device. The method includes: acquiring, by a second SM-SR from a first SM-SR, a PIC corresponding to an eUICC; acquiring, by the second SM-SR from a second SM-DP, a second PP that is encrypted by using the PIC; generating, by the second SM-SR, a key pair including a public key and a private key; sending, by the second SM-SR, the second PP and the public key to the eUICC through the first SM-SR, so that the eUICC accesses the second SM-SR after deactivating a first PP and activating the second PP; and encrypting, by the second SM-SR, a second PMC by using the private key, and sending an encrypted second PMC to the eUICC, so that the eUICC accesses the mobile network through the second SM-SR."); Park (IEEE) at Section II.A ("A. eUICC Provisioning Ecosystem… The eUICC provisioning ecosystem mainly consists of eUICCs, eUICC Vendors, Devices and SMs (SM-SRs and SM-DPs) [2], [4] as shown in Fig. 1. SM is divided into two parties; one is SM-SR for secure routing and the other is SM-DP, the owner or generator of security-sensitive information, for data preparation. As shown in Fig. 1, small numbers of SM-SRs are interworking with each other and SM-DPs delegate the roles of secure routing of the sensitive information to their trusted SM-SRs. For the provisioning and management, one eUICC usually interworks with one SM-SR. Because of their specific roles, one SM-SR can interwork with several SM-DPs for secure routing of profiles generated by SM-DPs to eUICCs. For scalability, several SM-SRs can interwork each other to extend the manageability to other eUICCs associated with other SM-SRs. For secure routing, SM-SRs usually utilize the SM-SR Credentials, installed in eUICCs during the manufacturing and shared by eUICC Vendors."); and Boyd-Mathuria at Chapter 1.6.1 ("Eavesdropping is perhaps the most basic attack on a protocol.

Nearly all protocols address eavesdropping by using encryption. It is obvious that encryption must be used to protect confidential information such as session keys. In certain protocols there may be other information that also needs to be protected. An interesting example is that protocols for key establishment in mobile communications usually demand that the identity of the mobile station remain confidential. Eavesdropping is sometimes distinguished as being a passive attack since it does not require the adversary to disturb the communications of legitimate principals. The other attacks we consider all require the adversary to be active. It should be remembered that many sophisticated attacks include eavesdropping of protocol runs as an essential part.").

In addition, below are additional motivations to combine prior art for particular claim limitations. The following discussion of specific claim limitations are merely examples and are not limiting.

For example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach using an embedded universal integrated circuit card (eUICC) to facilitate secure, wireless communication with a mobile device (in regards to Limitation 1[pre][19]) it would have been obvious to a person of ordinary skill in the art at the time of the invention to combine the primary reference with any of the prior art that disclose Limitation 1[pre] in Exhibits E-01 to E-10 or E-A. For example, several prior art references, including Nakhjiri '138, Ala-Laurila '934, Bradley '343, Jeong (2010), Gouget '828, Rajadurai '168, Semple '841, SEC-1, Gao '605, and Park (IEEE) explicitly describe or disclose using an eUICC to facilitate secure, wireless communication with a mobile device. *See, e.g.*, Nakhjiri at 1:1–6, 1:18–26, 1:57–2:24; Ala-Laurila '934 at [0016], [0018]; Bradley '343 at [0002], [0012]-[0013]; Jeong (2010) at Section

[19] Specifically, Limitation 1[pre]: "A method for a mobile device with an embedded universal integrated circuit card (eUICC) to securely communicate with a wireless network, the method performed by the mobile device."

1, Section 5; Gouget ’828 at [0003]-[0005]; Rajadurai ’168 at [0002]-[0003]; Semple ’841 at 2:10–43, 4:58-5:10; Gao ’605 at Abstract, 1:19-31, 7:48-55, Fig. 1; Park (IEEE) at Abstract, Section I, Section IV.C, Fig. 5; and Boyd-Mathuria at Chapter 1.6.1, Chapter 4.3.

A person skilled in the art would have understood the benefits of using an eUICC to facilitate secure, wireless communication with a mobile device, and would have been motivated to incorporate this feature into the method for a mobile device accordingly. *See, e.g.*, Nakhjiri at 1:18-26 (“Current smart-card technologies are moving towards non-removable embedded smart cards for use in mobile computing devices, such as mobile phones, tablet computers, and automobile navigation systems. Recent examples include embedded Universal Integrated Circuit Cards (UICC), which are used to host security-sensitive functions. Aside from smart cards, there is also a trend to use trusted environments to perform functions similar to functions currently performed by smart cards”); Ala-Laurila at [0018], (“A Subscriber Identity Module SIM, which is specific for the GSM network, is connected to the terminal equipment TE of the terminal MT, meaning that the terminal MT comprises both the TE and the SIM. Different identity modules can be used in the terminal MT depending on the mobile network; the UMTS network, for example, employs an identity module USIM (UMTS Subscriber Identity Module). The SIM is typically stored on an IC card (Integrated Circuit), which can be changed from one equipment TE to another. The SIM is provided by the mobile network GSMNW operator, and data concerning the SIM is stored in the mobile network GSMNW. The SIM comprises an International Mobile Subscriber Identity IMSI which represents the subscriber in the network, thus operating as an identifier of the terminal MT. The terminal equipment TE of the terminal MT may also include a specific International Mobile Equipment Identity IMEI, which is not really relevant for the invention. The SIM also comprises a secret key Ki, an algorithm A8 for

forming a ciphering key Kc and an algorithm A3 for forming an authentication response SRES (Signed Response)."); Bradley '343 at [0002] ("The present invention concerns a method for downloading a subscription in an UICC (Universal Integrated Circuit Card) embedded in a terminal for example a mobile terminal (mobile phone) or a machine (for M2M (Machine to Machine) applications). A UICC can be in the format of a smart card, or may be in any other format such as for example but not limited to a packaged chip as described in PCT/SE2008/050380, or any other format. It can be used in mobile terminals in GSM and UMTS networks for instance. The UICC ensures network authentication, integrity and security of all kinds of personal data."); Jeong (2010) at Section 1 ("In addition, the advancement of mobile networks and the rapid development of terminals have led to the emergence of smartphones that meet the diverse needs of users, and from the third generation of mobile terminals, USIM cards, called Universal Subscriber Identity Modules (USIM), are used to provide network authentication and additional functions. In other words, smartphones can provide various additional services such as communication, finance, transportation, and other mobile services that users want anytime and anywhere through various interfaces, and this has brought tremendous opportunities to our business and life [2]."); Gouget '828 at [0005] ("As shown in FIG. 1, a first secure channel between the client C and the gateway G and a second secure channel between the gateway G and the sever S may have been established. When the client C sends data to the remote server S through the gateway G, the gateway G has to decrypt and then encrypt data from a first protocol, used between the client C and the gateway G, to a second protocol used between the remote server S and the gateway G. The same happens when the remote server S sends data to the client C though the gateway G, which gateway G has to decrypt and then encrypt data from the second protocol used between the remote server S and the gateway G, to

the first protocol used between the client C and the gateway G."); Rajadurai '168 at [0002] ("Recent developments in Machine-to-Machine (M2M) applications has given rise to the possibility of having a universal integrated circuit card (UICC) that is embedded in a communication device in such a way that the UICC is not easily accessible or replaceable. The ability to change network subscriptions on such devices becomes problematic, thus necessitating mechanisms for securely and remotely provisioning access credentials on these embedded UICCs (eUICC) and managing subscription changes from one network operator to another. These mechanisms shall take into account that the change of subscription may involve provisioning of a new eUICC network access application as well as operator specific applications. Any changes must preserve the industry and end-user benefits that the non-embedded UICC provides today for GSM, 3GPP, 3GPP2 and other systems employing it, particularly in terms of security, flexibility in business relationships, logistics, and end-user experience."); Semple '841 at 4:58-5:10 ("In the following description, certain terminology is used to describe certain features of one or more embodiments of the invention. For instance, the terms "mobile terminal", "user equipment", "mobile device", "wireless device", and "wireless mobile device" are interchangeably used to refer to mobile phones, pagers, wireless modems, personal digital assistants, personal information managers (PIMs), palmtop computers, laptop computers, and/or other mobile communication/computing devices which communicate, at least partially, through a cellular network. The terms "legacy" is used to refer to networks, protocols, and/or mobile devices which are pre-3G, operate a pre-3G protocol, or employ a GSM-compliant SIM or a CDMA-compliant Authentication Module or MN-AAA Authentication Module. Additionally, the term subscriber identification module is used to refer to a GSM-compliant Subscriber Identity Module (SIM), a CDMA-compliant Authentication Module or MN-AAA Authentication

Module, or any other module typically included in a mobile terminal to identify the mobile terminal to a wireless network."); Gao '605 at 1:24-31 ("An embedded UICC (embedded UICC, eUICC for short) is a UICC embedded into a terminal, and it can be implemented that an operator and a corresponding subscription manager-secure routing unit (Subscription Manager-Secure Routing, SM-SR for short) perform remote management on the eUICC, for example, downloading data of the operator, handing over to or accessing a mobile network of the operator, and the like."); Park (IEEE) at Abstract ("Embedded UICC (eUICC) is a new form of UICC, soldered into a device during manufacturing. On the contrary to the traditional UICC, the eUICC is not fully controlled by one specific MNO (Mobile Network Operator) since not removable physically from the device and not issued by the MNO. Thus, the profiles necessary for its operations should be provisioned remotely into the eUICC by new entity. For this remote provisioning, SM (Subscription Manager) is newly introduced by the standardization organization. However, this new ecosystem around eUICCs can cause tremendous security issues unless thorough consideration of security is accompanied during the standardization because the profiles usually include the security-sensitive information."); and Boyd-Mathuria at Chapter 4.3.6 ("Beller, Chang and Yacobi (BCY) [34,35,36]' and Beller and Yacobi (BY) [37] proposed hybrid protocols using a combination of asymmetric and symmetric cryptographic algorithms. These protocols are designed to satisfy the requirements of the mobile communications environment. They are intended to provide security between a mobile station and a base station of the fixed network, rather than to provide end-to-end security between mobile users. There are at least two requirements in addition to those usually needed for authentication and key establishment protocols…• The computational load on the mobile station must be minimised, even at the expense of increased load on the base station. … • The identity of the

mobile station must remain hidden from the adversary."). Thus, a person of ordinary skill in the art would have been motivated to modify any of the primary references to include this feature. A person of ordinary skill in the art would also have had a reasonable expectation of success. A person of ordinary skill in the art would have understood that these references disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach using a key exchange algorithm to create a secure key for encrypting a profile, in connection with provisioning the profile from a first server to a mobile device (in regards to Limitations 1[a], 1[b], 1[c], and 1[d][20]) it would have been obvious to a person of ordinary skill in the art at the time of the invention to combine the primary reference with any of the prior art that disclose Limitations 1[a], 1[b], 1[c], and 1[d] in Exhibits E-01 to E-10 or E-A. For example, several prior art references, including Nakhjiri '138, Ala-Laurila '934, Bradley '343, Jeong (2010), Gouget '828, Rajadurai '168, Semple '841, SEC-1, Gao '605, and Park (IEEE) explicitly describe or disclose using a key exchange algorithm to create a secure key for encrypting a profile, in connection with provisioning the profile from a first server to a mobile device. *See, e.g.*, Nakhjiri at Abstract, 1:57-2:24, 2:34–67, 3:11-41, 5:38-58, 5:59-6:16 Fig. 1; Ala-Laurila '934 at [0022]-[0026]; Bradley '343 at [0029]–[0033], claim 1; Jeong (2010) at Section 2.2, Section 3.2, Figs. 3-4; Gouget '828 at [0010]-[0011], [0012]-[0019], [0032], Fig. 2;

[20]Specifically, Limitation 1[a]: "a) storing, in the eUICC, a first module private key, a corresponding first module public key, and a network public key"; Limitation 1[b]: "b) receiving, from a first server associated with the wireless network, an encrypted profile for the eUICC comprising cryptographic parameters, a module identity, and a key K"; Limitation 1[c]: "c) generating a shared secret key using a first elliptic curve Diffie-Hellman (ECDH) key exchange with the first module private key and the network public key"; and Limitation 1[d]: "d) decrypting, with the shared secret key, at least a portion of the encrypted profile for the eUICC."

Rajadurai ’168 at Abstract, [0001]-[0003], [0016]-[0019], [0023]-[0028], Figs. 2a-b, claim 1; Semple ’841 at Abstract, 2:47-62, 6:33-57, Fig. 2; Gao ’605 at 1:32-44, 6:64-7:9, 7:56-8:3, Figs. 1-2; Park (IEEE) at Section II.A, Section IV.B.1; and Boyd-Mathuria at Chapter 1.6.1, Chapter 3.4, and Chapter 4.3.

A person skilled in the art would have understood the benefits of using a key exchange algorithm to create a secure key for encrypting a profile, in connection with provisioning the profile from a first server to a mobile device (in regards to Limitations 1[a], 1[b], 1[c], and 1[d]), and would have been motivated to incorporate this feature into the method for a mobile device accordingly. *See, e.g.*, Nakhjiri at 1:57-2:24 (“Application service providers such as a mobile network operator (MNO), for example, generally need to remotely provision sensitive data into a secure execution environment of a target device such as a mobile computing device… As detailed below, techniques and arrangements are provided which allow multiple application service providers to provision sensitive data, referred to herein as a profile, in a target device. A profile may include, by way of example, security application algorithm codes, data and cryptographic keys. Such provisioning may include the transport of encrypted profiles through the network, decryption of encrypted profiles within the secure execution environment, and installation of the profiles within a secure storage for later execution within the secure execution environment. Because profiles from multiple application service providers are to be resident in the same secure execution environment, knowledge of each profile should be isolated within a security domain (e.g., a logical segmentation of hardware resources segmented and isolated from other segments by a firewall or the like) designated for the application service provider that is associated with that profile.”); Ala-Laurila ’934 at [0022] (“The mobile network GSMNW comprises one or more Mobile Switching Centers MSC/VLR typically comprising a Visitor

Location Register VLR and/or GPRS operating nodes SGSN (Serving (General Packet Radio Service) Support Nodes). The mobile network GSMNW also comprises a GSM/GPRS Authentication and Billing Gateway GAGW, which is connected to the Internet. The GAGW is an entity in the mobile network GSMNW offering authentication services of mobile subscribers to the WLAN networks WLAN and preferably also collects billing information. Hence, the subscriber data and the authentication services of the mobile network GSMNW can be used for serving the terminals MT comprising the identity module SIM in the WLAN network WLAN. The terminal MT user does not need to have a pre-agreed agreement with the operator of the WLAN network WLAN. A visiting terminal MT may use the identity module SIM and the mobile network GSMNW for implementing authentication and billing when visiting the network WLAN. In such a case the wireless connection offered by the network WLAN can be billed through the GAGW of the mobile network GSMNW. The WLAN operator may later compensate the mobile operator for the use of the network."); Bradley '343 at [0029]–[0030] ("If for example, a user has a pre-activated device X and want to buy a subscription from operator A, the flow would be as follows: Device X is touched against NFC token Y. The token contains the ICCID and preferably also the ICCID's activation code. Device X reads the ICCID from token Y as well as (preferably) the ICCID's secret activation code which is unique (this code prevents brute-force guessing of ICCID requests to the provisioning centre)."); Jeong (2010) at Section 2.2 ("Figure 2 illustrates 3GPP-AKA, the USIM authentication process in the wireless Internet environment. When the USIM/MS identifies itself by sending IMSI (International Mobile Subscriber Identity) or TMSI (Temporary Mobile Subscriber Identity) information to the SN (Serving Network), the SN transmits an authentication data request message and the IMSI/TMSI received from the terminal to the AuC (Authentication Center) of the HN (Home Network),

which is the authentication center. The HN generates an authentication vector AV (Authentication Vector) for the received IMSI and transmits it to the SN in response to the authentication data request."); Gouget '828 at [0011] ("For this purpose, an object of the invention is a method for establishing a secure communication channel between a client (C) and a remote server (S), said client (C) and remote server (S) exchanging data through an intermediate entity (G), said client (C) having a long-term key pair (sk_c,pk_c), said remote server generating an ephemeral key (sk_s,pk_s), the method comprising a mutual authentication step wherein the client (C) sends a public key (pk_c) of said long-term key pair (sk_c,pk_c) and the proof that said public key (pk_c) is valid to the server (S), and wherein the remote server (S) sends the public key (pk_s) of said ephemeral key pair (sk_s,pk_s) to the client (C), characterized in that the client (C) generates an ephemeral key pair (sk_{cc},pk_{cc}) and sends the public key (pk_{cc}) of said ephemeral key pair (sk_{cc},pk_{cc}) to the server (S) so as to generate a secret common to the client (C) and to the remote server (S) for opening the secure communication channel."); Rajadurai '168 at [0023] ("FIGS. 2a and 2b are flow diagrams 200 illustrating an exemplary method of secured remote provisioning of the UICC 112 in the user equipment 102A, according to one embodiment. At step 202, the user equipment 102A initiates a request for remote provisioning of the UICC 112. At step 204, the authentication and authorization server 104 forwards the request for remote provisioning along with a network type to the shared key management server 106A based on the MID. At step 206, the shared key management server 106A generates an authentication vector based on the request for remote provisioning received from the user equipment 102A. The authentication vector includes an authentication token, a random number, response expected from the user equipment 102A. At step 208, the shared key management server 106A derives an operator shared key using the security keys (ciphering key (CK), and integrity protection key

(IK)) based on the MID."); Semple '841 at 2:47-62 ("An aspect of the present invention can be regarded as a method for authenticating a bootstrapping server function to a mobile terminal supporting a legacy subscriber identification module, comprising provisioning the mobile terminal with a digital certificate associated with the bootstrapping server function, receiving an authentication challenge at the mobile terminal including a random number, authenticating, at the mobile terminal, the bootstrapping server function based on the digital certificate associated with the bootstrapping server function, being provided with a first secret key by the legacy subscriber identification module in response to passing the random number received in the authentication challenge to the legacy subscriber identification module, and formulating an authentication response based on the first secret key provided by the legacy subscriber identification module to the mobile terminal."); Gao '605 at 7:56-8:3 ("101: A second SM-SR acquires, from a first SM-SR, a profile installer credential corresponding to an eUICC. 102: The second SM-SR transmits the profile installer credential to a second SM-DP, and sends a provisioning profile (Provisioning Profile, PP for short) generation request, where the PP generation request is used for instructing the second SM-DP to generate a second PP corresponding to the second SM-SR, and encrypt the second PP by using the profile installer credential. It should be noted that, the eUICC can access the second SM-SR by using the second PP. The profile installer credential (Profile Installer Credential, PLC for short) is unique for the eUICC, and is used for ensuring that a profile downloaded from an external entity can be correctly decrypted and installed."); Park (IEEE) at Section IV.B.1 ("B. Secure Profile Provisioning Architecture (SPA). SPA mainly consists of two procedures; Pre-Provisioning Procedure and Secure Profile Provisioning Procedure. 1) Pre-Provisioning Procedure: SPA involves the pre-provisioning procedure, conducted during the eUICC-based device

manufacturing. Through this procedure, SM can collect the necessary information for SPA, and the verification of the capability information of the eUICC can be possible when performing the secure profile provisioning in the field. The detail of this pre-provisioning procedure is depicted in Fig. 3…. Step P1 - The eUICC Vendor develops eUICCs. During this, the SM-SR Credentials (key_{SM-SR}) and the capability information ($CI_{installed}$) of each eUICC are installed into each eUICC. Then, the eUICC Vendor generates the public key pair, and installs the private key ($Priv_{vendor}$) into the eUICCs. …Step P2 - The eUICC Vendor requests the evaluation of the eUICCs to the eUICC Certification Center with the public key (Pub_{vendor}) of Step P1…. Step P3 - Only after the successful evaluation, the eUICC Certification Center responses the results with the certificate ($Cert_{vendor}$)by using Pub_{vendor}. … Step P4 - The eUICC Vendor can install the received certificate into the eUICCs, and sends the developed and evaluated eUICCs to the device manufacturers. Simultaneously, the eUICC Vendor sends the information to SM-SR required for SPA such as the certificate, the eUICC IDs, the SM-SR Credentials, the mapping table between eUICC IDs and SM-SR Credential indexes, etc. in the secure manner. … Step P5 - The Device Manufacturer develops the eUICC-based devices using the received eUICCs."); and Boyd-Mathuria at Chapter 4.3.6 ("MSR Protocol…In the following, the notation *SCB* is a structure known as the *secret certificate* of the mobile station, *B,* which is issued by a trusted central authority. This certificate can be checked by anyone using the public key of the central authority in order to verify the mobile's identity. Unlike a usual public key certificate, this certificate must be kept secret from all other mobile users and eavesdroppers, because it is all that is required to masquerade as *B.* Protocol 4.26 shows the basic MSR protocol [36]…. 1. *A* à *B* : A, K_A … 2. *B* à *A:* $E_A(K_{AB}), \{B, SC_B\}K_{AB}$ … Protocol 4.26: Basic MSR protocol of Beller, Chang and Yacobi. … Upon receiving the base *A's* public key K_A, the mobile uses it to encrypt the session key K_{AB}, and

sends the encrypted message to *A*. The mobile also sends its identity and secret certificate encrypted under K_{AB} to authenticate K_{AB} to the base. The symmetric encryption with K_{AB} in message 2 is of negligible computational effort compared to the public key encryption in the same message; therefore the computational effort at the mobile is effectively limited to that of modulo squaring of the session key."). Thus, a person of ordinary skill in the art would have been motivated to modify any of the primary references to include this feature. A person of ordinary skill in the art would also have had a reasonable expectation of success. A person of ordinary skill in the art would have understood that these references disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach using a shared secret key to decrypt part of a provisioned, encrypted profile (in regards to Limitation 1[d]) it would have been obvious to a person of ordinary skill in the art at the time of the invention to combine the primary reference with any of the prior art that disclose Limitation 1[d] in Exhibits E-01 to E-10 or E-A. For example, several prior art references, including Nakhjiri '138, Ala-Laurila '934, Bradley '343, Jeong (2010), Gouget '828, Rajadurai '168, Semple '841, SEC-1, Gao '605, and Park (IEEE) explicitly describe or disclose using a shared secret key to decrypt part of a provisioned, encrypted network profile. *See, e.g.*, Nakhjiri at 1:57-2:24, 5:59-6:16, 6:50-60, Figs 3-4; Ala-Laurila '934 at [0022]-[0023], [0027]-[0028]; Bradley '343 at [0029]-[0033]; Jeong (2010) at Section 3.1.2, Section 3.2; Gouget '828 at [0003]-[0005], [0010]-[0011], [0012]-[0019], Fig. 1; Rajadurai '168 at [0023]-[0028], [0029]-[0032], Figs. 2a-2b, Fig. 3; Semple '841 at Abstract, 2:47-62; Gao '605 at 7:3-9, 7:56-8:3; Park

(IEEE) at Section II.C and Section IV.B.2; and Boyd-Mathuria at Chapter 1.4.1, Chapter 4.3.6, and Chapter 5.1.

A person skilled in the art would have understood the benefits of using a shared secret key to decrypt part of a provisioned, encrypted network profile (in regards to Limitation 1[d]), and would have been motivated to incorporate this feature into the method for a mobile device accordingly. *See, e.g.*, Nakhjiri at 5:59-6:16 ("Once the UICC receives the inner layer encrypted profile it performs a decryption process to remove the inner layer encryption, as illustrated in FIG. 4. As shown, the UICC uses its private seed and the MNO identifier (MN_ID) to generate its own ECC private key (MNO_ECC_PVKDEV) using the pre-configured key generator function (KGF) 510. The UICC then creates the PEK to perform decryption. To create the PEK, the UICC uses the device ECC private key for this particular MNO (MNO_ECC_PVKDEV) and the MNO ECC public key (MNO_ECC_PLKOP) to perform a local ECDH key agreement process 520. As discussed above in connection with FIG. 3, the UICC can obtain the MNO ECC public key (MNO_ECC_PLKOP) from the MNO along with the encrypted data, especially in cases where the MNO uses a unique public key for each UICC. Alternatively, the MNO ECC public key may be obtained by the UICC through other means. For example, the MNO ECC public key may be pre-provisioned in the UICC. The local ECDH key agreement process 520 creates the PEK 530 from a shared ECDH secret 540. In some cases a key size reduction process 550 may be performed when generating the PEK 530, depending on the key size that is needed to encrypt the profile. The UICC then uses the PEK 530 to perform a symmetric key decryption process 560 to decrypt the profile, which is stored in secure storage device 570 associated with the UICC."); Ala-Laurila '934 at [0028] ("The GAGW requests 206 (Send Parameters) at least one triplet from the mobile network GSMNW. This can be arranged so that the GAGW transmits

the request to the nearest mobile services switching center MSC/VLR (or to the operation node SGSN). The MSC/VLR checks the IMSI identifier and sends a request to the home location register HLR of the network possessing the identity module SIM, the HLR typically comprising an Authentication Center AuC (the GSMNW AuC in the Figure). In the first calculation means included in the mobile network GSMNW, i.e. when the GSM network is concerned, the authentication center AuC forms 207 (Calculate Kc(s)) one or more GSM triplets (RAND, SRES, Kc) in a known manner using the secret key Ki according to the IMSI identifier. A GSM triplet comprises a challenge code, i.e. a random number, RAND, an authentication response SRES formed on the basis of the RAND and a secret key Ki using an algorithm A3, and a first ciphering key Kc formed on the basis of the RAND and the secret key Ki using an algorithm A8. The HLR sends the triplet to the MSC/VLR which forwards the triplet to the GAGW 208 (Send_Parameters_Result). The mobile network GSMNW can also send several triplets, whereby the GAGW preferably selects one and stores the other triplets for later use."); Bradley '343 at [0032]-[0033] ("The secure vault transmits the above personalisation script to device X encrypted for Device X's embedded secure element (and with an anti-replay counter mechanism included) over the IP link. Device X (including its embedded secure element) decrypts and runs the personalisation script thus provisioning the subscription onto the embedded secure element "); Jeong (2010) at Section 3.2 ("The MS decrypts the received $ERAND_{HN}$ using the shared secret key SSK_{MS-HN} to extract the random value $RAND_{HN}$ of the certificate authority (HN). Using this value, $XMAC_{HN}$ is calculated and compared with the MAC_{HN} received to verify the identity of the certificate authority (HN). At this time, the MS generates $OT\text{-}SSK_{MS-SN}$ With its own secret key to the public key received from the SN. Then, it transmits its public key, MSP, and a one-time shared secret key, $OT\text{-}SSK_{MS-SN}$ to the SN… $E(SSK_{MS-HN}, ERAND_{HN}) = RAND_{HN}$ …

$XMAC_{HN} = f^2SSK_{MS\text{-}HN}(IMSI_{MS} \| RAND_{HN})$… OT- $SSK_{MS\text{-}SN}$ = EC-DH(P, MS, SNP).”); Gouget ’828 at [0011] (“For this purpose, an object of the invention is a method for establishing a secure communication channel between a client (C) and a remote server (S), said client (C) and remote server (S) exchanging data through an intermediate entity (G), said client (C) having a long-term key pair (sk_c,pk_c), said remote server generating an ephemeral key (sk_s,pk_s), the method comprising a mutual authentication step wherein the client (C) sends a public key (pk_c) of said long-term key pair (sk_c,pk_c) and the proof that said public key (pk_c) is valid to the server (S), and wherein the remote server (S) sends the public key (pk_s) of said ephemeral key pair (sk_s,pk_s) to the client (C), characterized in that the client (C) generates an ephemeral key pair (sk_{cc},pk_{cc}) and sends the public key (pk_{cc}) of said ephemeral key pair (sk_{cc},pk_{cc}) to the server (S) so as to generate a secret common to the client (C) and to the remote server (S) for opening the secure communication channel.”); Rajadurai ’168 at [0032] (“At step 318, the authentication and authorization server 108 provides the IMSI, the random number, the security profile, the encrypted operator shared key, and the shared key management server certificate to the user equipment 102A via a secured channel. At step 320, the user equipment 102A verifies the shared key management server certificate using the root certificate in the UICC 112. Upon successful verification, at step 322, the user equipment 102A decrypts the encrypted operator shared key and derives the subscription key using the decrypted operator shared key and the random number. At step 324, the user equipment 102A stores the subscription key and the IMSI along with the security profile in the storage space of the UICC 112.”); Semple ’841 at 2:47-62 (“An aspect of the present invention can be regarded as a method for authenticating a bootstrapping server function to a mobile terminal supporting a legacy subscriber identification module, comprising provisioning the mobile terminal with a digital certificate associated with the bootstrapping

server function, receiving an authentication challenge at the mobile terminal including a random number, authenticating, at the mobile terminal, the bootstrapping server function based on the digital certificate associated with the bootstrapping server function, being provided with a first secret key by the legacy subscriber identification module in response to passing the random number received in the authentication challenge to the legacy subscriber identification module, and formulating an authentication response based on the first secret key provided by the legacy subscriber identification module to the mobile terminal."); Gao '605 at 7:3-9 ("The subscription manager-data preparing unit (Subscription Manager-Data Preparing, SM-DP for short) is configured to generate a profile, and encrypt the generated profile by using a profile installer credential, that is, perform data preparation for the profile, for example, encrypt the profile, so that only a specified eUICC/a terminal in which the eUICC is located can decrypt the profile."); Park (IEEE) at Section IV.B.2 ("Step 7 - Using the agreed SM-DP Credentials and the selected cryptographic algorithms, SM-DP encrypts each block of profile ($Profile_i$) and generates its MACed value. Then, SM-DP sends the protected profile blocks to the eUICC via the secure communication channel of SM-SR. PM of eUICC performs the necessary cryptographic operations for the secure communication channel, and then PI of eUICC decrypts and verifies the received profile blocks. If no problem found, the profile blocks are provisioned inside the eUICC by PI. Then, PI sends the acknowledge for each block of profile with its MACed value to SM-DP. This step continues recursively until the provisioning is completed.); and Boyd-Mathuria at Chapter 1.4.1 ("Definition 1.5. *An* encryption scheme *consists of three sets: a key set K, a message set M, and a ciphertext set* C *together with three algorithms….1. A key generation algorithm, which outputs a valid encryption key* $K \in K$ *and a valid decryption key* $K^{-1} \in K$*…. 2. An encryption algorithm, which takes an element* $m \in M$ *and an encryption key* $K \in K$ *and outputs*

an element c ∈ C *defined as* c = ∈ *K* { m }. *The encryption algorithm may be randomised so that a different* c *will result given the same* m…. *3. A decryption junction, which takes an element* c E C *and a decryption key* K^{-1} ∈ *K and outputs an element* m∈ *M defined as* m = $D_K^{-1}\{c\}$. *We require that* $D_K^{-1}\{E_K\{m\}\}$ = m."). Thus, a person of ordinary skill in the art would have been motivated to modify any of the primary references to include this feature. A person of ordinary skill in the art would also have had a reasonable expectation of success. A person of ordinary skill in the art would have understood that these references disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach using a key exchange algorithm based on public / private keys to derive a secure session key, in connection with authenticating a mobile device with a second server (in regards to Limitations 1[e], 1[f], 1[g], 1[h], and 1[i][21]) it would have been obvious to a person of ordinary skill in the art at the time of the invention to combine the primary reference with any of the prior art that disclose Limitations 1[e], 1[f], 1[g], 1[h], and 1[i] in Exhibits E-01 to E-10 or E-A. For example, several prior art references, including Nakhjiri '138, Ala-Laurila '934, Bradley '343, Jeong (2010), Gouget '828, Rajadurai '168, Semple '841, SEC-1, Gao '605, and Park (IEEE) explicitly describe or disclose using a key exchange algorithm based on public / private keys to derive a secure session key, in connection with authenticating a mobile device

[21] Specifically, Limitation 1[e]: "e) generating, by the eUICC, a second module public key and a corresponding second module private key;"; Limitation 1[f]: "f) sending, to a second server associated with the wireless network, the second module public key;"; Limitation 1[g]: "g) generating a symmetric key using a second ECDH key exchange with the second module private key and the cryptographic parameters;"; Limitation 1[h]: "h) generating, with the symmetric key, module encrypted data, the module encrypted data comprising the module identity;"; and Limitation 1[i]: "i) sending, to the second server, the module encrypted data."

with a second server. *See, e.g.*, Nakhjiri at 5:38-58 and 9:21–31; Ala-Laurila '934 at [0022]-[0028] and Figs. 2-3; Bradley '343 at [0002] and [0029]-[0034]; Jeong (2010) at Section 2.2, Section 3.1.2, Section 3.2, and Figs. 4, 6; Gouget '828 at [0010]–[0011], [0012]-[0019]; Rajadurai '168 at [0003]-[0004] and [0021]-[0022]; Semple '841 at Abstract, 7:4-8:3, 8:4-9:18, 9:19-10:43, 10:44-11:35, and Figs. 4-7; Gao '605 at 7:48-55, 8:4-14, and Fig. 2; Park (IEEE) at Section III.B, Section IV.C., and Table 1; and Boyd-Mathuria at Chapter 3.4, Chapter 4.3.6, and Chapter 5.1.

A person skilled in the art would have understood the benefits of using a key exchange algorithm based on public / private keys to derive a secure session key, in connection with authenticating a mobile device with a second server (in regards to Limitations 1[e], 1[f], 1[g], 1[h], and 1[i]), and would have been motivated to incorporate this feature into the method for a mobile device accordingly. *See, e.g.*, Nakhjiri at 9:21-31 ("Target device 106 may include a nonvolatile memory (NV) component 618. In an aspect, the NV may contain subscription, connection, or any information related to establishing a connection with a wireless network or authenticating a user to such a network. By non-limiting example, such a wireless network may utilize an access technology and/or communication protocol or standard such as, but not limited to, CDMA2000 1X (IS-2000), 1x, 1xRTT, CDMA2000, and/or 1xEV-DO (Evolution-Data Optimized), also known as EV-DO or EV, or any other access technology that is part of the 3G access technology family."); Ala-Laurila '934 at [0025] ("FIG. 2 shows the essential functions according to a preferred embodiment of the invention for authenticating the terminal MT and for calculating a ciphering key. The terminal MT is offered an identifier IMSI and a secret key Ki by the subscriber identity application SIM included therein. The authentication process of the terminal MT is typically triggered when the MT starts setting up a connection 201 (Connection

setup) with the WLAN network WLAN. Then the MT is provided with an IP address through a DHCP server (Dynamic Host Configuration Protocol). Before the terminal MT is allowed to establish a connection with other networks than the network WLAN, the authentication must be performed in an acceptable manner."); Bradley '343 at [0002] ("The present invention concerns a method for downloading a subscription in an UICC (Universal Integrated Circuit Card) embedded in a terminal for example a mobile terminal (mobile phone) or a machine (for M2M (Machine to Machine) applications). A UICC can be in the format of a smart card, or may be in any other format such as for example but not limited to a packaged chip as described in PCT/SE2008/050380, or any other format. It can be used in mobile terminals in GSM and UMTS networks for instance. The UICC ensures network authentication, integrity and security of all kinds of personal data."); Jeong (2010) at Section 3.2 ("Figure 6 shows the user authentication process using USIM, and each step is described as follows. (1) In the existing AKA, we need to solve the privacy problem and the synchronization problem of SQN by transmitting the IMSI plaintext of the terminal. Therefore, the IMSI, T_{MS}(timestamp), and SN_{ID} located near the terminal are concatenated to generate the authentication value of the MS using the function $f^{l}_{K}()$. Also, E-$IMSI_{MS}$, MAC_{MS}, HN_{ID}, and T_{MS}, which are values encrypted with $SSK_{MS\text{-}HN}$, a shared secret key between HN and MS, are transmitted to the SN located near the MS. … MAC_{MS} = $f^{l}SSK_{MS\text{-}HN}$ ($IMSI_{MS}$ || T_{MS} || SN_{ID}) … E- $IMSI_{MS}$ = E($SSK_{MS\text{-}HN}$, $IMSI_{MS}$) … (7) Since the mutual authentication of the MS and the HN is completed, mutual authentication between the MS and the SN is performed for safe information transmission. The SN generates a one-time shared secret key, OT-$SSK_{MS\text{-}SN}$, using the MS public key, MSP, received from the MS, and mutually authenticates the identity of the MS by checking whether it matches the OT-$SSK_{MS\text{-}SN}$ received from the MS. … OT-$SSK_{ms\text{-}sn}$= EC- DH(P, SN, MSP)"); Gouget '828 at [0011] ("For

this purpose, an object of the invention is a method for establishing a secure communication channel between a client (C) and a remote server (S), said client (C) and remote server (S) exchanging data through an intermediate entity (G), said client (C) having a long-term key pair (sk_c,pk_c), said remote server generating an ephemeral key (sk_s,pk_s), the method comprising a mutual authentication step wherein the client (C) sends a public key (pk_c) of said long-term key pair (sk_c,pk_c) and the proof that said public key (pk_c) is valid to the server (S), and wherein the remote server (S) sends the public key (pk_s) of said ephemeral key pair (sk_s,pk_s) to the client (C), characterized in that the client (C) generates an ephemeral key pair (sk_{cc},pk_{cc}) and sends the public key (pk_{cc}) of said ephemeral key pair (sk_{cc},pk_{cc}) to the server (S) so as to generate a secret common to the client (C) and to the remote server (S) for opening the secure communication channel."); Rajadurai '168 at [0021] ("The shared key management server 106A generates authentication vectors, security keys (e.g., ciphering key (CK), and integrity protection key (IK)), an operator shared key using the security keys (CK and IK) and other parameters for mutual authentication based on the MID. The shared key management server 106A provides the operator shared key to the HSS 110 via the server 108. Alternatively, the operator shared key may be generated at the authentication and authorization server 108 using the security keys. The HSS 110 then generates an international mobile subscriber identity, a random number (Nonce), and a subscription key using the operator shared key and selects a security profile upon authenticating the user equipment 102A by the authentication and authorization server 108."); Semple '841 at 9:19-10:43 ("In one embodiment, a request for authentication keys may be initiated by MT 606 retrieving its associated International Mobile Subscriber Identity (IMSI) 600 from its SIM 608 and sending it to a bootstrapping server function (BSF) 604. The BSF 604 sends the IMSI 600 to the HLR 602 where it may verify whether the IMSI 600 belongs to a MT that subscribes to

the network. The HLR 602 may be operated by the service provider for the subscriber whose SIM is contained in MT 606. The HLR 602 selects, for example, a 128-bit random challenge RAND and together with pre-shared secret key Ki, uses them as inputs for two algorithms A3 and A8 to yield 32-bit output signed response SRES and 64-bit output secret confidentiality key Kc, respectively. The HLR 602 then provides the triplets (RAND, SRES, Kc) to the BSF 604, corresponding to the identity IMSI 600 of SIM 608. The BSF 604 generates a random secret exponent x and computes a Diffie-Hellman public key P^x, where P is a generator of a cyclic group previously provisioned to both the BSF 604 and MT 606, such as the multiplicative group of a finite field or the additive group of an elliptic curve. The BSF 602 then sends a triplet (RAND, P^x, SIG) 610 to the MT 606, where SIG is a digital signature computed using the BSF 604 RSA private key. The message 610 may be further enhanced to include other server-authenticated parameters such as a transaction identifier."); Gao '605 at 8:4-14 ("103: After receiving an encrypted second PP sent by the second SM-DP, the second SM-SR generates a key pair including a first key and a second key…. 104: The second SM-SR sends a third request message to the first SM-SR, where the third request message includes: the encrypted second PP and the first key, and the third request message is used for instructing the first SM-SR to send the encrypted second PP and the first key to the eUICC, so that the eUICC replaces an internally preset first SM-SR according to an SM-SR replacement message sent by the first SM-SR."); Park (IEEE) at Section III.B ("The following security requirements should be guaranteed in accordance with the requirements in [5]: … Mutual Authentication - eUICC and SM-DP prove their authenticities each other through cryptographic exchanges. … Confidentiality - profiles being transmitted to eUICC by SM-DP are only available to those authorized entities. … Data Integrity - data being exchanged between eUICC and SM-DP has not been altered by

unauthorized entities. … Data Origin Authentication - eUICC and SM-DP ensure that data actually came from the authorized entities, SM-DP and eUICC, respectively."); and Boyd-Mathuria at Chapter 4.3.6 ("MSR Protocol…In the following, the notation *SCB* is a structure known as the *secret certificate* of the mobile station, *B,* which is issued by a trusted central authority. This certificate can be checked by anyone using the public key of the central authority in order to verify the mobile's identity. Unlike a usual public key certificate, this certificate must be kept secret from all other mobile users and eavesdroppers, because it is all that is required to masquerade as *B.* Protocol 4.26 shows the basic MSR protocol [36]…. 1. *A* à *B* : A, K_A … *2. B* à $A: E_A(K_{AB}), \{B, SC_B\}K_{AB}$ … Protocol 4.26: Basic MSR protocol of Beller, Chang and Yacobi. … Upon receiving the base *A's* public key K_A, the mobile uses it to encrypt the session key K_{AB}, and sends the encrypted message to *A.* The mobile also sends its identity and secret certificate encrypted under K_{AB} to authenticate K_{AB} to the base. The symmetric encryption with K_{AB} in message 2 is of negligible computational effort compared to the public key encryption in the same message; therefore the computational effort at the mobile is effectively limited to that of modulo squaring of the session key."). Thus, a person of ordinary skill in the art would have been motivated to modify any of the primary references to include this feature. A person of ordinary skill in the art would also have had a reasonable expectation of success. A person of ordinary skill in the art would have understood that these references disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach using an elliptic curve Diffie-Hellman key exchange, an asymmetric technique involving public / private key pairs, to generate a shared key (i.e., symmetric key) in

the mobile communications context (in regards to Limitations 1[c] and 1[g]) it would have been obvious to a person of ordinary skill in the art at the time of the invention to combine the primary reference with any of the prior art that disclose Limitations 1[c] and 1[g] in Exhibits E-01 to E-10 or E-A. For example, several prior art references, including Nakhjiri '138, Ala-Laurila '934, Bradley '343, Jeong (2010), Gouget '828, Rajadurai '168, Semple '841, SEC-1, Gao '605, and Park (IEEE) explicitly describe or disclose using an elliptic curve Diffie-Hellman key exchange, an asymmetric technique involving public / private key pairs, to generate a shared key (i.e., symmetric key) in the mobile communications context. *See, e.g.*, Nakhjiri at 5:25–37, 5:38-58, 11:10-13, and Fig. 3; Ala-Laurila '934 at [0022]-[0028]; Bradley '343 at [0031]-[0034]; Jeong (2010) at Section 3.1.2, Section 3.2, and Section 4.1.1; Gouget '828 at [0012]-[0019], [0040]-[0045], and claim 3; Rajadurai '168 at [0003]-[0004] and [0021]-[0022]; Semple '841 at 7:4-8:3, 9:19-10:43, 11:37-60, and Figs. 4, 6; Gao '605 at Abstract, 7:56-8:14, Fig. 2, and Figs. 5A-5B; Park (IEEE) at Section IV.B.2, Table 1, and Fig. 4; and Boyd-Mathuria at Chapter 3.4, Chapter 4.3.6, and Chapter 5.2.

A person skilled in the art would have understood the benefits of using an elliptic curve Diffie-Hellman key exchange, an asymmetric technique involving public / private key pairs, to generate a shared key (i.e., symmetric key) in the mobile communications context (in regards to Limitations 1[c] and 1[g]), and would have been motivated to incorporate this feature into the method for a mobile device accordingly. *See, e.g.*, Nakhjiri at 5:25-37 ("To be able to establish a profile encryption key (PEK) using ECC, a key agreement exchange may take place between the MNO SM-DP and each UICC. One example of a key exchange algorithm that may be employed is an Elliptic Curve Diffie-Hellman exchange (ECDH) algorithm where both the UICC and the MNO end up with exactly the same Shared ECDH secret (using Elliptic Curve

multiplication operation): … Calculated by UICC: Shared ECDH Secret=MNO_ECC_PLK*MNO_ECC_PVKDEV … Calculated by MNO: Shared ECDH Secret=MNO_ECC_PLKDEV*MNO_ECC_PVK."); Ala-Laurila '934 at [0028] ("The GAGW requests 206 (Send Parameters) at least one triplet from the mobile network GSMNW. This can be arranged so that the GAGW transmits the request to the nearest mobile services switching center MSC/VLR (or to the operation node SGSN). The MSC/VLR checks the IMSI identifier and sends a request to the home location register HLR of the network possessing the identity module SIM, the HLR typically comprising an Authentication Center AuC (the GSMNW AuC in the Figure). In the first calculation means included in the mobile network GSMNW, i.e. when the GSM network is concerned, the authentication center AuC forms 207 (Calculate Kc(s)) one or more GSM triplets (RAND, SRES, Kc) in a known manner using the secret key Ki according to the IMSI identifier. A GSM triplet comprises a challenge code, i.e. a random number, RAND, an authentication response SRES formed on the basis of the RAND and a secret key Ki using an algorithm A3, and a first ciphering key Kc formed on the basis of the RAND and the secret key Ki using an algorithm A8. The HLR sends the triplet to the MSC/VLR which forwards the triplet to the GAGW 208 (Send_Parameters_Result). The mobile network GSMNW can also send several triplets, whereby the GAGW preferably selects one and stores the other triplets for later use"); Bradley '343 at [0031] ("Device X sends this ICCID over an IP link to a secure vault. The secure vault verifies the ICCID/secret activation code pairing and if valid it securely packages, encrypts and signs the entire personalisation script for the related embedded UICC (containing SIM application, USIM application, ISIM application, CSIM application, any other network authentication applications as well as any SIM application Toolkit applications and Operating System Customisations/mechanisms related to that specific MNO) as well as the relevant

subscription information such as the IMSI, K, Opc, IMPU and algorithm constants. The contents of the profile would be known to the secure vault using the ICCID range or alternatively a profile code could be submitted to the system."); Jeong (2010) at Section 3.2 ("(7) Since the mutual authentication of the MS and the HN is completed, mutual authentication between the MS and the SN is performed for safe information transmission. The SN generates a one-time shared secret key, $OT\text{-}SSK_{MS\text{-}SN}$, using the MS public key, MSP, received from the MS, and mutually authenticates the identity of the MS by checking whether it matches the $OT\text{-}SSK_{MS\text{-}SN}$ received from the MS. … $OT\text{-}SSK_{ms\text{-}sn}$= EC-DH(P, SN, MSP) … (8) Finally, generate CK and IK for safe information transmission, and in this paper, $OT\text{-}SSK_{MS\text{-}SN}$ using EC-DH's algorithm is utilized to generate CK and IK. …CK= $f^3 OT\text{-}SSK_{MS\text{-}SN}(OT\text{-}SSK_{MS\text{-}SN} \| SN_{ID})$ … IK= $f^4 OT\text{-}SSK_{MS\text{-}SN}(OT\text{-}SSK_{MS\text{-}SN} \| SN_{ID})$"); Gouget '828 at [0012]-[0014] ("According to other aspects of the invention, the method for establishing a secure communication channel between a client (C) and a remote server (S) may comprise generating said common secret by the client (C) and by the server (S), said common secret being based on the ephemeral secret key (sk_{cc}) of said ephemeral key pair (sk_{cc},pk_{cc}) of the client (C); the method may comprise generating the common secret according to the Diffie-Hellman protocol;"); Rajadurai '168 at [0021] ("The shared key management server 106A generates authentication vectors, security keys (e.g., ciphering key (CK), and integrity protection key (IK)), an operator shared key using the security keys (CK and IK) and other parameters for mutual authentication based on the MID. The shared key management server 106A provides the operator shared key to the HSS 110 via the server 108. Alternatively, the operator shared key may be generated at the authentication and authorization server 108 using the security keys. The HSS 110 then generates an international mobile subscriber identity, a random number (Nonce), and a subscription key using the operator shared

key and selects a security profile upon authenticating the user equipment 102A by the authentication and authorization server 108."); Semple '841 at 9:19-10:43 ("In one embodiment, a request for authentication keys may be initiated by MT 606 retrieving its associated International Mobile Subscriber Identity (IMSI) 600 from its SIM 608 and sending it to a bootstrapping server function (BSF) 604. The BSF 604 sends the IMSI 600 to the HLR 602 where it may verify whether the IMSI 600 belongs to a MT that subscribes to the network. The HLR 602 may be operated by the service provider for the subscriber whose SIM is contained in MT 606. The HLR 602 selects, for example, a 128-bit random challenge RAND and together with pre-shared secret key Ki, uses them as inputs for two algorithms A3 and A8 to yield 32-bit output signed response SRES and 64-bit output secret confidentiality key Kc, respectively. The HLR 602 then provides the triplets (RAND, SRES, Kc) to the BSF 604, corresponding to the identity IMSI 600 of SIM 608. The BSF 604 generates a random secret exponent x and computes a Diffie-Hellman public key P^x, where P is a generator of a cyclic group previously provisioned to both the BSF 604 and MT 606, such as the multiplicative group of a finite field or the additive group of an elliptic curve. The BSF 602 then sends a triplet (RAND, P^x, SIG) 610 to the MT 606, where SIG is a digital signature computed using the BSF 604 RSA private key. The message 610 may be further enhanced to include other server-authenticated parameters such as a transaction identifier."); Gao '605 at Abstract ("The present invention provides a method and a device for switching a subscription manager-secure routing device. The method includes: acquiring, by a second SM-SR from a first SM-SR, a PIC corresponding to an eUICC; acquiring, by the second SM-SR from a second SM-DP, a second PP that is encrypted by using the PIC; generating, by the second SM-SR, a key pair including a public key and a private key; sending, by the second SM-SR, the second PP and the public key to the eUICC through the first SM-SR,

so that the eUICC accesses the second SM-SR after deactivating a first PP and activating the second PP; and encrypting, by the second SM-SR, a second PMC by using the private key, and sending an encrypted second PMC to the eUICC, so that the eUICC accesses the mobile network through the second SM-SR."); Park (IEEE) at Section IV.B.2 ("Step 4 - Then, SM-DP sends the message including the selected capabilities ($CI_{selected}$, the cryptographic algorithms, the key agreement protocol, the secure communication protocol and so forth) and its hashed value to the eUICC via SM-SR if the decision is completed based on the received capability information. The capability information about the secure communication protocol can be chosen through the interworking between SM-SR and SM-DP…. Step 5 – PM of eUICC and the SM-SR establish the secure communication channel based on the selected protocol. The SM-SR Credential can be same as or derived from the master secret installed in Step P1. … Step 5 - The blocks of KAM from SM-DP and the acknowledgement from the eUICC can be sent through the secure communication channel established in Step 5 and installed to the eUICC if the message of Step 2 indicates that the installation is necessary. This can be happened when the change of security policy is required, the vulnerabilities of the cryptographic algorithm used in that module are found, or other reasons are happened."); and Boyd-Mathuria at Chapter 5.2 ("In the basic Diffie-Hellman protocol, two principals A and B agree publicly on an element g that generates a multiplicative group G. They then select random values, r_A and r_B respectively, in the range between 1 and the order of G. A calculates $tA = g^R{}_a$ and B calculates $t_B = g^{r}{}_B$ and they exchange these values as shown in Protocol 5.1. The shared secret is $Z_{AB} = g^{r}{}_A{}^{r}{}_B$. This value can be calculated by both A and B due to the homomorphic property of exponentiation: $Z_{AB} = t_A{}^{rB} = t_B{}^{rA}$."). Thus, a person of ordinary skill in the art would have been motivated to modify any of the primary references to include this feature. A person of ordinary skill in the art would also

have had a reasonable expectation of success. A person of ordinary skill in the art would have understood that these references disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach using a symmetric key to encrypt the subscriber identity for a mobile device for submission to the mobile network (in regards to Limitations 1[h] and 1[i]) it would have been obvious to a person of ordinary skill in the art at the time of the invention to combine the primary reference with any of the prior art that disclose Limitation 1[h] and 1[i] in Exhibits E-01 to E-10 or E-A. For example, several prior art references, including Nakhjiri '138, Ala-Laurila '934, Bradley '343, Jeong (2010), Gouget '828, Rajadurai '168, Semple '841, SEC-1, Gao '605, and Park (IEEE) explicitly describe or disclose using a symmetric key to encrypt the subscriber identity for a mobile device for submission to the mobile network. *See, e.g.*, Nakhjiri at 5:38-58, 9:21-31, and Fig. 3; Ala-Laurila '934 at [0022]-[0028]; Bradley '343 at [0031]-[0034]; Jeong (2010) at Section 2.2, Section 3.1.2, Section 3.2, Section 4.1.2, and Fig. 6; Gouget '828 at [0010]-[0011] and [0012]-[0019]; Rajadurai '168 at [0021]-[0022] and [0033]-[0035]; Semple '841 at 9:19-10:43, 10:44-11:35, and Figs. 6-7; Gao '605 3:24–42, 7:39-43, 9:29-49, Fig.2, and Fig. 3A; Park (IEEE) at Section I, Section IV.B.2, and Table 1; and Boyd-Mathuria at Chapter 1.6.1, Chapter 3.4, and Chapter 4.3.6.

A person skilled in the art would have understood the benefits of using a symmetric key to encrypt the subscriber identity for a mobile device for submission to the mobile network (in regards to Limitations 1[h] and 1[i]), and would have been motivated to incorporate this feature into the method for a mobile device accordingly. *See, e.g.*, Nakhjiri at 5:38-58 ("The key generation process shown in FIG. 3 may be used to encrypt a profile using a key agreement

exchange process performed by the MNO's SM-DP. As part of this process the SM-DP generates its own ECC private, public key pair (denoted MNO_ECC_PVKOP and MNO_ECC_PLKOP, respectively). This key pair may be unique for each UICC, a population of UICCs, or each ECDH process that is performed. The SM-DP will then use its own ECC private key (MNO_ECC_PVKOP) and the UICC public key (MNO_ECC_PLKDEV), which is provided by the public key list from UICC manufacturer or vendor, to perform a local ECDH key agreement 410 and create the PEK 430 from a shared ECDH secret 420. In some cases a key size reduction process 440 may be performed when generating the PEK 430, depending on the key size that is needed to encrypt the profile. The SM-DP then uses the PEK to perform a symmetric key encryption process 450 to encrypt the profile for the UICC. Finally, the encrypted profile, along with the MNO device identifier (MNO_ID) and the MNO ECC public key (MNO_ECC_PLKOP) are delivered to the target device of the provisioning infrastructure shown in FIG. 1."); Ala-Laurila '934 at [0026] ("The MT requests 202 (IMSI request) the identity module SIM for the IMSI identifier and the SIM returns 203 the IMSI identifier. The MT sends 204 the authentication starting request (MT_PAC_AUTHSTART_REQ) which preferably comprises a Network Access Identifier NAI. The NAI comprises the IMSI identifier obtained from the identity module SIM. The NAI may be presented, for example, in the form 12345@GSM.org, where 12345 is the IMSI identifier and GSM.org is the domain name of the mobile network, which has conveyed the identity module SIM. The request 204 is preferably sent in ciphered form to the PAC using the Diffie-Hellman algorithm, for example. The MT preferably also sends a specific protection code MT_RAND in the request 204, said code typically being a challenge code. Using the protection code MT_RAND the MT may later be ensured that the party conveying the GSM triplets actually has access to the secret key Ki, which is to be maintained in

the GSM home network of the subscriber. However, the use of the protection code is not obligatory."); Bradley '343 at [0031] ("Device X sends this ICCID over an IP link to a secure vault. The secure vault verifies the ICCID/secret activation code pairing and if valid it securely packages, encrypts and signs the entire personalisation script for the related embedded UICC (containing SIM application, USIM application, ISIM application, CSIM application, any other network authentication applications as well as any SIM application Toolkit applications and Operating System Customisations/mechanisms related to that specific MNO) as well as the relevant subscription information such as the IMSI, K, Opc, IMPU and algorithm constants. The contents of the profile would be known to the secure vault using the ICCID range or alternatively a profile code could be submitted to the system."); Jeong (2010) at Section 3.2 ("(1) In the existing AKA, we need to solve the privacy problem and the synchronization problem of SQN by transmitting the IMSI plaintext of the terminal. Therefore, the IMSI, T_{MS}(timestamp), and SN_{ID} located near the terminal are concatenated to generate the authentication value of the MS using the function $f^1_K()$. Also, E-$IMSI_{MS}$, MAC_{MS}, HN_{ID}, and T_{MS}, which are values encrypted with $SSK_{MS\text{-}HN}$, a shared secret key between HN and MS, are transmitted to the SN located near the MS. … $MAC_{MS} = f^1 SSK_{MS\text{-}HN}$ ($IMSI_{MS}$ || T_{MS} || SN_{ID}) … E- $IMSI_{MS}$ = E($SSK_{MS\text{-}HN}$, $IMSI_{MS}$) … (2) The SN forwards the received E-$IMSI_{MS}$, MAC_{MS}, T_{MS} to the corresponding certificate authority (HN)."); Gouget '828 at [0011] ("For this purpose, an object of the invention is a method for establishing a secure communication channel between a client (C) and a remote server (S), said client (C) and remote server (S) exchanging data through an intermediate entity (G), said client (C) having a long-term key pair (sk_c,pk_c), said remote server generating an ephemeral key (sk_s,pk_s), the method comprising a mutual authentication step wherein the client (C) sends a public key (pk_c) of said long-term key pair (sk_c,pk_c) and the proof that said public key (pk_c) is

valid to the server (S), and wherein the remote server (S) sends the public key (pk_s) of said ephemeral key pair (sk_s,pk_s) to the client (C), characterized in that the client (C) generates an ephemeral key pair (sk_{cc},pk_{cc}) and sends the public key (pk_{cc}) of said ephemeral key pair (sk_{cc},pk_{cc}) to the server (S) so as to generate a secret common to the client (C) and to the remote server (S) for opening the secure communication channel."); Rajadurai '168 at [0033] ("FIG. 4 is a flow diagram 400 illustrating an exemplary method of establishing a communication session with the operator network using the IMSI assigned to the user equipment 102A, according to one embodiment. At step 402, the user equipment 102A sends a non-access stratum message including the assigned IMSI to the operator network 104. At step 404, the authentication and authorization server 108 requests the HSS 110 for an authentication vector to authenticate the user equipment 102A. At step 406, the HSS 110 generates the authentication vector using the subscription key. At step 408, the HSS 110 provides the authentication vector to the authentication and authorization server 108."); Semple '841 at 9:35-59 ("In one embodiment, a request for authentication keys may be initiated by MT 606 retrieving its associated International Mobile Subscriber Identity (IMSI) 600 from its SIM 608 and sending it to a bootstrapping server function (BSF) 604. The BSF 604 sends the IMSI 600 to the HLR 602 where it may verify whether the IMSI 600 belongs to a MT that subscribes to the network. The HLR 602 may be operated by the service provider for the subscriber whose SIM is contained in MT 606. The HLR 602 selects, for example, a 128-bit random challenge RAND and together with pre-shared secret key Ki, uses them as inputs for two algorithms A3 and A8 to yield 32-bit output signed response SRES and 64-bit output secret confidentiality key Kc, respectively. The HLR 602 then provides the triplets (RAND, SRES, Kc) to the BSF 604, corresponding to the identity IMSI 600 of SIM 608. The BSF 604 generates a random secret exponent x and computes a Diffie-Hellman public

key P^x, where P is a generator of a cyclic group previously provisioned to both the BSF 604 and MT 606, such as the multiplicative group of a finite field or the additive group of an elliptic curve. The BSF 602 then sends a triplet (RAND, P^x, SIG) 610 to the MT 606, where SIG is a digital signature computed using the BSF 604 RSA private key. The message 610 may be further enhanced to include other server-authenticated parameters such as a transaction identifier."); Gao '605 at 3:24-42 ("According to a fourth aspect, an embodiment of the present invention provides a method for switching a subscription manager-secure routing device, where a mobile network is a mobile network corresponding to a second SM-SR, including: receiving, by the mobile network, a first request message that is sent by an SP after the SP activates an eUICC, where the first request message includes: information about the first SM-SR, and an eID of the eUICC and/or an IMEI of a terminal in which the eUICC is located; and sending, by the mobile network, a second request message to the second SM-SR, where the second request message includes: the information about the first SM-SR, and information that the mobile network provides a service for the eUICC activated by the SP, and further includes the eID of the eUICC and/or the IMEI of the terminal in which the eUICC is located, so that the eUICC switches an internally preset first SM-SR to the second SM-SR, and accesses the mobile network through the second SM-SR."); Park (IEEE) at Section IV.B.2 ("Step 2 - After the establishment of the communication channel, the eUICC sends the message including the eUICC ID (eICCID) and its capability information (CIproposal) to SM-SR for the capability negotiation. The eUICC ID and capability information are signed by the eUICC Vendors private key, and this signed value needs to be added to the message. If there is no KAM installed onto the eUICC, the eUICC can replace the key agreement protocol of the CI message with proper value such as null, blank, error message, etc. to inform SM that the installation is required. Simultaneously, the eUICC can also send the

eUICC Vendors certificate if necessary."); and Boyd-Mathuria at Chapter 4.3.6 ("MSR Protocol…In the following, the notation *SCB* is a structure known as the *secret certificate* of the mobile station, *B,* which is issued by a trusted central authority. This certificate can be checked by anyone using the public key of the central authority in order to verify the mobile's identity. Unlike a usual public key certificate, this certificate must be kept secret from all other mobile users and eavesdroppers, because it is all that is required to masquerade as *B.* Protocol 4.26 shows the basic MSR protocol [36]…. 1. *A* à *B* : A, K_A … 2. *B* à *A:* $E_A(K_{AB}), \{B, SC_B\}K_{AB}$ … Protocol 4.26: Basic MSR protocol of Beller, Chang and Yacobi. … Upon receiving the base *A's* public key K_A, the mobile uses it to encrypt the session key K_{AB}, and sends the encrypted message to *A.* The mobile also sends its identity and secret certificate encrypted under K_{AB} to authenticate K_{AB} to the base. The symmetric encryption with K_{AB} in message 2 is of negligible computational effort compared to the public key encryption in the same message; therefore the computational effort at the mobile is effectively limited to that of modulo squaring of the session key."). Thus, a person of ordinary skill in the art would have been motivated to modify any of the primary references to include this feature. A person of ordinary skill in the art would also have had a reasonable expectation of success. A person of ordinary skill in the art would have understood that these references disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

VIII. U.S. Patent No. 12,207,094 ("the '094 Patent")

A. Identification of Prior Art

Defendants incorporate by reference, as if set forth fully herein, all filings and exhibits from *Inter Partes* Review IPR2026-00118, filed November 26, 2025 with the PTAB, including any subsequent and future filings in that case.

In addition to the prior art cited on the face of the '094 Patent and related patents, the

admitted prior art in the specifications of the ’094 Patent and related patents, the prior art cited in any file histories, reexaminations, *inter partes* review proceedings, reissue proceedings, or other examination or post-grant proceedings of the ’094 Patent and related patents, and the prior art cited in any invalidity contentions or expert reports submitted in any action or proceedings involving the ’094 Patent or related patents, Defendants identify the following prior art that anticipates each asserted claim or renders it obvious.

1. Prior Art Patents

The following patents and patent publications are prior art to the asserted claims under at least 35 U.S.C. §§ 102(a)(1) and/or (a)(2), and/or 35 U.S.C. § 103. The identification of any patent or patent publication shall be deemed to include any counterpart patent or application filed, published, or issued anywhere in the world.

Patent or Publication Number	Country of Origin	Filing Date	Date of Issue or Publication
U.S. Pat. App. Pub. No. 2013/0301828 (“Gouget”)	United States	September 24, 2010 (EP) March 23, 2013 (PCT)	November 14, 2013
U.S. Pat. App. Pub. No. 2013/0227646 (“Haggerty”)	United States	February 14, 2013	August 29, 2013
U.S. Pat. App. Pub. No. 2010/0267383 (“Konstantinou”)	United States	April 15, 2009	October 21, 2010
U.S. Pat. App. Pub. No. 2016/0127132 (“Lee”)	United States	May 30, 2013 (KR) November 30, 2015 (PCT)	May 5, 2016
U.S. Patent No. 9,100,175 (“Nix”)	United States	December 6, 2013	August 4, 2015
U.S. Patent No. 8,761,390 (“Peirce”)	United States	June 30, 2008	June 24, 2014
U.S. Pat. App. Pub. No. 2015/0350881	United	December 21, 2012 (EP)	December 3, 2015

("Weiss")	States	June 19, 2015 (PCT)	

2. Prior Art Non-Patent Publications

The following non-patent publications are prior art to the asserted claims under at least 35 U.S.C. §§ 102(a)(1) and/or (a)(2), and/or 35 U.S.C. § 103.

Title	Author/Publisher	Date of Publication
A Fast and Secure Elliptic Curve Based Authenticated Key Agreement Protocol For Low Power Mobile Communications ("Abi-Char")	Pierre E. Abi-Char, et al., IEEE	2007
Ansi X9.63 Overview Key Agreement and Key Transport Using Elliptic Curve Cryptography ("ANSI X9.63 Overview")	Simon Blake-Wilson, Certicom	2000
Protocols for Authentication and Key Establishment ("Boyd-Mathuria")	Colin Boyd & Anish Mathuria, Springer	2003
GlobalPlatform Card Specification Version 2.2.1 Public Release ("GlobalPlatform")	GlobalPlatform, Inc.	January 2011
SGP.22 - RSP Technical Specification Version 2.0 ("SGP.22")	GSM Association	October 14, 2016
Secure Profile Provisioning Architecture for Embedded UICC ("Park (IEEE)")	Jaemin Park, et al., IEEE	November 7, 2013
GlobalPlatform Card Secure Channel Protocol '11' Card Specification v.2.2 – Amendment F Version 1.0 Public Release ("SCP11")	GlobalPlatform, Inc.	May 2015

3. Prior Art Systems

Defendants' investigation into publicly available prior art systems that teach and/or

render obvious each element of any asserted claims is ongoing. Fact discovery is at an early stage, and Defendants may require discovery from third parties regarding publicly available prior art systems. On information and belief, prior art systems from the following companies teach and/or render obvious each element of the asserted claims of the ’094 Patent: Cinterion (now Telit); Gemalto (now Thales); Giesecke+Devrient; GlobalPlatform; NXP Semiconductors N.V.; Oberthur Technologies (now IDEMIA); and Sierra Wireless. Defendants reserve the right to amend its identification of prior art systems as Defendants become aware of the existence, functionality, and/or characteristics of prior art systems as a result of its investigation and forthcoming discovery. In addition to the prior art products, components, systems, and methods that may be identified as a result of discovery, Defendants also reserve the right to rely on the documents and publications identified in the corresponding claim charts as prior art publications.

B. Primary References

Defendants contend that the primary prior art references identified below and described in the charts attached as Exhibits F-01 to F-08, by themselves, anticipate the asserted claims of the ’094 Patent. To the extent that a primary reference is deemed not to anticipate a claim for failing to teach one or more limitations of that claim, Defendants contend that the claim would nonetheless have been obvious to a person of ordinary skill in the art at the time of the invention in view of the prior art reference itself, as described in the attached charts. Defendants’ prior art charts (attached as Exhibits F-01 thru F-08) set forth the particular claims that are anticipated under 35 U.S.C. § 102 and/or rendered obvious under 35 U.S.C. § 103 by each item of prior art and identify where specifically in each item of prior art, each element of each asserted claim is found.

Exhibit	Primary References

F-01	*Protocols for Authentication and Key Establishment* ("Boyd-Mathuria")
F-02	*GlobalPlatform Card Specification Version 2.2.1 Public Release* ("GlobalPlatform")
F-03	U.S. Pat. App. Pub. No. 2013/0301828 ("Gouget")
F-04	U.S. Pat. App. Pub. No. 2013/0227646 ("Haggerty")
F-05	U.S. Patent No. 9,100,175 ("Nix")
F-06	*Secure Profile Provisioning Architecture for Embedded UICC* ("Park (IEEE)")
F-07	*SGP.22 - RSP Technical Specification Version 2.0* ("SGP.22")
F-08	U.S. Pat. App. Pub. No. 2015/0350881 ("Weiss")

C. Secondary References

Exhibit F-A lists secondary prior art references and identifies, on a limitation-by-limitation basis, where specifically each secondary reference teaches the limitations of the asserted claims. To the extent that a primary reference is deemed, by itself, not to anticipate or render obvious a claim for failing to teach one or more limitations, the claim would nonetheless have been obvious to a person of ordinary skill in the art at the time of the invention by the combination of the primary reference with one or more of the other primary references listed above and/or the references listed as disclosing those alleged missing limitations in Exhibit F-A.

D. Obvious Combinations

To the extent that a primary reference is deemed, by itself, not to anticipate or render obvious a claim for failing to teach one or more limitations, the claim would nonetheless have been obvious to a person of ordinary skill in the art at the time of the invention by the combination of the primary reference with one or more other primary references and/or the knowledge of someone skilled in the art. For example, a person of ordinary skill in the art would have been

motivated to combine any reference in Exhibits F-01 to F-08 with any other reference(s) in Exhibits F-01 to F-08. Such combinations would be achieved, for example, by merely combining the disclosures described in the respective claim charts for each reference.

Defendants also contend that any of the primary references (or combination of primary references) could be combined with any of the secondary references (or combination of secondary references) in Exhibit F-A to render obvious the asserted claims. Such combinations would be achieved by merely combining the disclosures described in the respective claim charts for each reference.

The obviousness combinations are provided in the alternative to Defendants' anticipation contentions and are not to be construed to suggest that any reference included in the combinations is not itself anticipatory.

1. **Exemplary Combinations**

Below are examples of prior art references that would have been combined by one of ordinary skill in the art at the time of the alleged invention. These combinations are merely examples. The asserted claims of the '094 Patent are rendered obvious by:

- Park (IEEE) in combination with GlobalPlatform and Abi-Char.
- Park (IEEE) in combination with GlobalPlatform and ANSI X9.63 Overview.
- Park (IEEE) in combination with GlobalPlatform, Abi-Char, and Weiss.
- Park (IEEE) in combination with GlobalPlatform, ANSI X9.63 Overview, and Weiss.
- Nix in combination with Park (IEEE) and GlobalPlatform.
- Boyd-Mathuria alone or in combination with one or more of Abi-Char, ANSI X9.63 Overview, GlobalPlatform, Gouget, Haggerty, Konstantinou, Lee, Nix,

Park (IEEE), Peirce, SCP11, SGP.22, and/or Weiss.

- GlobalPlatform alone or in combination with one or more of Abi-Char, ANSI X9.63 Overview, Boyd-Mathuria, Gouget, Haggerty, Konstantinou, Lee, Nix, Park (IEEE), Peirce, SCP11, SGP.22, and/or Weiss.
- Gouget alone or in combination with one or more of Abi-Char, ANSI X9.63 Overview, Boyd-Mathuria, GlobalPlatform, Haggerty, Konstantinou, Lee, Nix, Park (IEEE), Peirce, SCP11, SGP.22, and/or Weiss.
- Haggerty alone or in combination with one or more of Abi-Char, ANSI X9.63 Overview, Boyd-Mathuria, GlobalPlatform, Gouget, Konstantinou, Lee, Nix, Park (IEEE), Peirce, SCP11, SGP.22, and/or Weiss.
- Nix alone or in combination with one or more of Abi-Char, ANSI X9.63 Overview, Boyd-Mathuria, GlobalPlatform, Gouget, Haggerty, Konstantinou, Lee, Park (IEEE), Peirce, SCP11, SGP.22, and/or Weiss.
- Park (IEEE) alone or in combination with one or more of Abi-Char, ANSI X9.63 Overview, Boyd-Mathuria, GlobalPlatform, Gouget, Haggerty, Konstantinou, Lee, Nix, Peirce, SCP11, SGP.22, and/or Weiss.
- SGP.22 alone or in combination with one or more of Abi-Char, ANSI X9.63 Overview, Boyd-Mathuria, GlobalPlatform, Gouget, Haggerty, Konstantinou, Lee, Nix, Park (IEEE), Peirce, SCP11, and/or Weiss.
- Weiss alone or in combination with one or more of Abi-Char, ANSI X9.63 Overview, Boyd-Mathuria, GlobalPlatform, Gouget, Haggerty, Konstantinou, Lee, Nix, Park (IEEE), Peirce, SCP11, and/or SGP.22.

2. Motivations to Combine

To the extent a finder of fact finds that a primary prior art reference does not disclose one or more limitations of an asserted claim, the asserted claim is nevertheless obvious because the allege missing limitations contain nothing beyond ordinary improvements. In other words, the asserted claim combines known elements to achieve predictable results or chooses between clear alternatives known to those of skill in the art, particularly in view of the state of the art as reflected in the relevant prior art.

Moreover, as explained above, it would have been obvious to a person of skill in the art at the time of the alleged invention of the asserted claims to combine any primary reference with any combination of other primary references or secondary references so as to practice the asserted claims. To the extent that Plaintiff argues that any concept claimed in the asserted claims is not disclosed in a primary reference, it would, at a minimum, have been obvious to adapt the primary reference to include the concept or combine it with other primary references or secondary references that disclose the concept. Each concept described and claimed in the Asserted Patents was known to those of skill in the art as available design choices for the technologies at issue.[22]

The Supreme Court has held that "[t]he combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 416 (2007). "When a work is available in one field of endeavor, design incentives and other market forces can prompt variations of it, either in the same field or a different one." *Id.* at 417. As the Supreme Court made clear, "[f]or the same reason, if a technique has been used to improve one device, and a person of ordinary skill in the

[22] Each concept described and claimed in the '094 Patent was known to those of skill in the art as available design choices for data encryption technology and/or using such technology to provision and/or authenticate mobile devices for use with a wireless network in a wide range of applications for different scenarios and circumstances.

art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill." *Id*.

To determine whether there is an apparent reason to combine the known elements in the fashion claimed by the patent at issue, a court can "look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art." *Id*. at 418. For example, obviousness can be demonstrated by showing "there existed at the time of invention a known problem for which there was an obvious solution encompassed by the patent's claims." *Id*. at 420. "[A]ny need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed." *Id*. Common sense also teaches that "familiar items may have obvious uses beyond their primary purposes, and in many cases a person of ordinary skill will be able to fit the teachings of multiple patents together like pieces of a puzzle." *Id*.

However, the Supreme Court in *KSR* held that a claimed invention can be obvious even if there is no explicit teaching, suggestion, or motivation for combining the prior art to produce that invention. In summary, *KSR* holds that patents that are based on new combinations of elements or components already known in a technical field may be found to be obvious. *See, generally*, *KSR*, 550 U.S. 398. Specifically, the Court in *KSR* rejected a rigid application of the "teaching, suggestion, or motivation [to combine]" test. *Id*. at 418. "In determining whether the subject matter of a patent claim is obvious, neither the particular motivation nor the avowed purpose of the patentee controls. What matters is the objective reach of the claim." *Id*. at 419. "Under the correct analysis, any need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the

manner claimed." *Id*. at 420. A key inquiry is whether the "improvement is more than the predictable use of prior art elements according to their established functions." *Id*. at 417.

The rationale to combine or modify prior art references is significantly stronger when, as here, the references seek to solve the same problem, come from the same field, and correspond well to each other. *In re Inland Steel Co*., 265 F.3d 1354, 1362 (Fed. Cir. 2001). The Federal Circuit has held that two references may be combined as invalidating art under similar circumstances, namely "[the prior art] focus[es] on the same problem that the … patent addresses: enhancing the magnetic properties of … steel. Moreover, both [prior art references] come from the same field …. Finally, the solutions to the identified problems found in the two references correspond well." *Id*. at 1364 (concerning patents and prior art relating to improving the magnetic and electrical properties of steel).

In view of the Supreme Court's *KSR* decision, the PTO issued a set of Examination Guidelines. Examination Guidelines for Determining Obviousness Under 35 U.S.C. §103 in view of the Supreme Court Decision in *KSR International Co. v. Teleflex, Inc*., 72 Fed. Reg. 57526 (October 10, 2007). Those Guidelines summarized the *KSR* decision and identified various rationales for finding a claim obvious, including those based on other precedents. Those rationales include:

> (A) Combining prior art elements according to known methods to yield predictable results;
> (B) Simple substitution of one known element for another to obtain predictable results;
> (C) Use of known technique to improve similar devices (methods, or products) in the same way;
> (D) Applying a known technique to a known device (method, or product) ready for improvement to yield predictable results;
> (E) "Obvious to try" – choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success;

> (F) Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations would have been predictable to one of ordinary skill in the art;
>
> (G) Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention.

Id. at 57529. The above rationales likewise apply in rendering obvious the asserted claims of the Asserted Patents.

The references disclosed herein, alone or in combination, contain an explicit and/or implicit teaching or motivation to combine them due to the following: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference addresses similar problems; and (5) the knowledge of those skilled in the art that the disclosed elements had been or could be used together.

As an example of those reasons and motivations to combine the references, Abi-Char, ANSI X9.63 Overview, Boyd-Mathuria, GlobalPlatform, Gouget, Haggerty, Konstantinou, Lee, Nix, Park (IEEE), Peirce, SCP11, SGP.22 and/or Weiss generally relate to encryption technology, and/or using such technology to provision or authenticate a mobile device for use with a wireless network. *See* Exs. F-01 to F-08 and F-A. The references disclose similar components and techniques for data encryption, and/or using encryption to provision or authenticate mobile devices. *Id.* The attached charts in Exhibits F-01 to F-08 and F-A provide additional reasons and motivations to combine the charted references.

Additionally, the primary and secondary references listed above are analogous art. They are all directed to encryption technology, and in particular, to provisioning and/or authenticating a mobile device for use with a wireless network. *See, e.g.*, Abi-Char at Abstract ("To provide

secure communication for mobile devices, authenticated key agreement protocol is an important primitive for establishing session key …. In this paper we present a fast and Secure Authenticated Key Agreement (EC-SAKA) protocol based on Elliptic Curve Cryptography."), ANSI X9.63 Overview at 3 ("Specifies key agreement and key transport schemes using elliptic curve cryptography"), Boyd-Mathuria at VII ("We believe that this book is the first comprehensive treatment of protocols for authentication and key establishment."), GlobalPlatform at 2-3 ("Its goal is to reduce barriers hindering the growth of cross-industry, multiple Application smart cards …. Although this specification defines card components, command interfaces, transaction sequences, and interfaces that can be common across many different industries, it does not detail the implementation of the lower layers security, which may vary from one industry to the other. This specification is also intended for a more general audience as it describes the generic security concepts and the various actors involved in a multi-Application Card Management System."), Gouget at [0010] ("The purpose of the invention is to provide a method for establishing a secure channel between a client C and a remote server S when the client C and the server S exchange data through an intermediate entity G."), Haggerty at Abstract ("Methods and apparatus for large scale distribution of electronic access control clients. In one aspect, a tiered security software protocol is disclosed. In one exemplary embodiment, a server electronic Universal Integrated Circuit Card (eUICC) and client eUICC software comprise a so-called 'stack' of software layers …. The tiered security software protocol is configured for large scale distribution of electronic Subscriber Identity Modules (eSIMs)."), Lee at Abstract ("The present invention relates to a method and apparatus for installing a profile, and more specifically, to a method for managing mobile communication subscriber information (profile), such as for remotely installing and uninstalling a profile onto a security module (Universal Integrated Circuit Card (UICC)) that is

embedded inside a terminal and that is not attachable or detachable, thereby replacing UICC.”), Park (IEEE) at Abstract (“In this paper, a novel secure profile provisioning architecture for eUICCs is proposed.”), Peirce at Abstract (“A system and method for producing cryptographic keys for use by an embedded processing device within a manufactured product. A pseudo random number generator is seeded with entropy data gathered by the embedded device, and the result is used to generate a public-private key pair.”), SCP11 at 7 (“This document specifies a new secure channel protocol, named Secure Channel Protocol '11' (SCP11), based on Elliptic Curve Cryptography (ECC) for mutual authentication and secure channel initiation and on AES for secure messaging.”), SGP.22 at 7 (“This specification provides a technical description of: The eUICC Architecture; The interfaces used within the Remote SIM Provisioning Architecture; and The security functions used within the Remote SIM Provisioning Architecture.”), Weiss at Abstract (“A method of providing a secure element of a mobile terminal with a subscription profile…”).

A person of ordinary skill in the art would look to the primary and secondary references to improve or tailor the disclosure thereof to tailor to particular settings or particular factors. A person of ordinary skill in the art would have understood the general trend and motivation to optimize the security, effectiveness, and efficiency of profile provisioning, authentication, and data encryption procedures. A POSITA would have understood that doing so could increase system performance, including in terms of, for example, security and/or efficiency. *See, e.g.*, Abi-Char at Abstract (“To provide secure communication for mobile devices, authenticated key agreement protocol is an important primitive for establishing session key …. In this paper we present a fast and Secure Authenticated Key Agreement (EC-SAKA) protocol based on Elliptic Curve Cryptography …. The new protocol achieves many of the required security and

performance properties. It can resist dictionary attacks mounted by either passive or active network intruders. It can resist Man-In-The Middle attack. It also offers perfect forward secrecy which protects past sessions and passwords against future compromise. In addition, it can resist known-key and resilience to server attack …. Our proposed protocol offers significantly improved performance in computational and communication load over comparably many authenticated key agreement protocols…"), ANSI X9.63 Overview at 3 ("Specifies key agreement and key transport schemes using elliptic curve cryptography … Specifies a variety of schemes to meet the diverse security needs of communications protocols"), Boyd-Mathuria at VII ("Authentication and key establishment are fundamental building blocks for securing electronic communications. Cryptographic algorithms for encryption and integrity cannot perform their function unless secure keys have been established and the users know which parties share such keys. It is essential that protocols for providing authentication and key establishment are fit for their purpose."), GlobalPlatform at 2 ("For smart cards to reach their true potential, consumers need to be able to use them for a wide variety of functions. For example, the cards can be used with mobile phones to make purchases over the Internet as well as to securely access a PC. Smart cards should also be cost effective and easily multifunctional …. GlobalPlatform defines a flexible and powerful specification for Card Issuers to create single- and multi-Application chip card systems to meet the evolution of their business needs."), Gouget at [0020]-[0022] ("The invention solves the problem of man-in-the-middle attack in case of the exposure of a permanent secret key used to establish a secure channel. There is neither need for an additional device nor an additional mutual authentication. Thanks to the invention, a secure channel is established between the server S and the client C such that the gateway G cannot access to the plaintext data transmitted into the secure channel, even if the permanent secret key

skc has been revealed.”), Haggerty at [0013]-[0014] (“Accordingly, new solutions and infrastructure are needed to leverage the enhanced flexibility provided by electronic access clients (e.g., eSIMs), and to support secure and ubiquitous distribution thereof. The present disclosure provides, inter alia, for large scale distribution of electronic access control clients.”), Lee at [0010]-[0011] (“Unlike the conventional UICC which is manufactured and distributed for specific mobile communication operators, the newly introduced embedded security module is capable of allowing for the user who has purchased the terminal to install and maintain the authentication information of various mobile communication operators securely and flexibly in such a way of subscribing and unsubscribing to a specific mobile communication operator or switching the subscription between operators. Thus, the present invention aims to provide a method for installing UICC information of various mobile communication operators in an embedded security module (instead of the conventional detachable UICC) remotely through a network.”), Park (IEEE) at Abstract (“Embedded UICC (eUICC) is a new form of UICC … [T]he profiles necessary for its operations should be provisioned remotely into the eUICC by new entity. For the remote provisioning, SM (Subscription Manager) is newly introduced by the standardization organization. However, this new ecosystem around eUICCs can cause tremendous security issues unless thorough consideration of security is accompanied during standardization because the profiles usually include the security-sensitive information. In this paper, a novel secure profile provisioning architecture for eUICCs is proposed. Our architecture mainly defines the overall architecture of the secure profile provisioning for eUICCs.”), Peirce at 1:50-2:2 (“As applied to embedded processing devices, the generation of the cryptographic keys can be problematic because they typically do not have entropy hardware or software engines of the type found in personal computers. Instead pseudo random number generators (PRNG) are

typically used. These PRNGs are generally implemented in software and require a seed value that is used to generate a pseudo-random number. This generated number is then used to produce the cryptographic keys. The generation of strong keys using PRNGs generally necessitates the use of a seed value that cannot later be discovered. For an embedded processing device having restricted computing capabilities, obtaining such a seed value can be problematic …. According to one aspect of the invention, there is provided a method of producing cryptographic keys for use in communicating with a manufactured product"), SCP11 at 11 ("[T]his protocol allows authentication and secure channel initiation based on certificates instead of pre-shared keys. This provides greater flexibility in cases where the two entities setting up the secure channel are not deployed in strict pairs."), SGP.22 at 7 ("The adoption of this technical solution will provide the basis for global interoperability between different Operator deployment scenarios, for example network equipment (e.g. Subscription Manager Data Preparation (SM-DP+)) and various eUICC platforms."), Weiss at [0005] ("[T]he problem addressed by the present invention is to provide for methods and devices that allow providing the secure element of a mobile terminal over-the-air with a subscription profile.").

One of skill in the art would also have been motivated to combine the different publications and patents that were authored by employees of a given company or assigned to the same assignee and/or related to the same subject matter. The common architect of the references demonstrate that they relate to continued work in a common field of effort and continued related developments in that field. Additionally, based on the teachings of the references and/or the knowledge of one of ordinary skill, one of skill in the art would have been motivated to combine different references from the same company. For example, a POSITA would have been motivated to combine at least GlobalPlatform and SCP11, both of which were published by the

same company: GlobalPlatform, Inc. And, one of skill in the art would have been motivated to combine prior art systems or products with any related or applicable documentation or literature for that system, including for the reason that these materials are related.

In addition, below are additional motivations to combine prior art for particular claim limitations. The following discussion of specific claim limitations are merely examples and are not limiting.

For example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach a secure profile provisioning architecture (*e.g.*, limitations 1[A], 1[B], 1[C], 1[D], 1[E], 1[F], 1[G], 1[H], 1[I], 1[J], 2, 7, 10, 19, 20), it would have been obvious to a person of ordinary skill in the art at the time of the invention to combine the primary reference with any of the prior art that discloses a secure profile provisioning architecture (*e.g.*, limitations 1[A], 1[B], 1[C], 1[D], 1[E], 1[F], 1[G], 1[H], 1[I], 1[J], 2, 7, 10, 19, 20) in Exhibits F-01 to F-08 or Exhibit F-A. For example, several prior art references, including at least Abi-Char, ANSI X9.63 Overview, Boyd-Mathuria, GlobalPlatform, Gouget, Haggerty, Konstantinou, Lee, Nix, Park (IEEE), Peirce, SCP11, SGP.22, and/or Weiss explicitly describe or disclose a secure profile provisioning architecture. *See, e.g.*, Abi-Char at 1, 2, 3, 4; ANSI X9.63 Overview at 3, 7, 12; Boyd-Mathuria at 49, 81, 125, 136, 140, 141; GlobalPlatform at 156, 174, 194, 198, 202-203, 216, 234, 246-247, 251-253, 255-256, 258, 260, 264, 266-268, 275-276; Gouget at Abstract; Haggerty at Abstract, [0005], [0008], [0015], [0045]-[0046], [0048], [0084], [0100], [0114], [0121], [0131]-[0133]; Lee at Abstract, [0011], [0062]; Park (IEEE) at 297, 300, 301, 303; Peirce at Abstract, 1:6-9, 2:66-3:54, 8:18-51; SCP11 at 12, 13, 20, 30; SGP.22 at 9, 11, 12, 22, 23, 26-28, 51-54, 62-67, 93-94, 131-132; Weiss at [0002], [0012], [0014], [0015], [0020], [0059]-[0062], [0063].

A person skilled in the art would have understood the benefits of a secure profile provisioning architecture, would have recognized that configuring a system to comprise a secure profile provisioning architecture would provide benefits to the system, and would have been motivated to incorporate these features into a system accordingly. For example, a POSITA would have understood that configuring a system to comprise a secure profile provisioning architecture would yield a complete, secure, and efficient architecture for eUICC profile provisioning. *See, e.g.*, Abi-Char at Abstract ("To provide secure communication for mobile devices, authenticated key agreement protocol is an important primitive for establishing session key …. In this paper we present a fast and Secure Authenticated Key Agreement (EC-SAKA) protocol based on Elliptic Curve Cryptography …. The new protocol achieves many of the required security and performance properties. It can resist dictionary attacks mounted by either passive or active network intruders. It can resist Man-In-The Middle attack. It also offers perfect forward secrecy which protects past sessions and passwords against future compromise. In addition, it can resist known-key and resilience to server attack …. Our proposed protocol offers significantly improved performance in computational and communication load over comparably many authenticated key agreement protocols…"), ANSI X9.63 Overview at 4 ("Specify schemes capable of meeting common security needs"), Boyd-Mathuria at VII ("We believe that this book is the first comprehensive treatment of protocols for authentication and key establishment …. Authentication and key establishment are fundamental building blocks for securing electronic communications. Cryptographic algorithms for encryption and integrity cannot perform their function unless secure keys have been established and the users know which parties share such keys. It is essential that protocols for providing authentication and key establishment are fit for their purpose."), GlobalPlatform at 18-19 ("The GlobalPlatform architecture is designed to

provide Card Issuers with the system management architecture for managing these smart cards …. The GlobalPlatform card architecture is comprised of a number of components that ensure hardware and vendor-neutral interfaces to Applications and off-card management systems.”), Gouget at [0020]-[0022] (“The invention solves the problem of man-in-the-middle attack in case of the exposure of a permanent secret key used to establish a secure channel. There is neither need for an additional device nor an additional mutual authentication. Thanks to the invention, a secure channel is established between the server S and the client C such that the gateway G cannot access to the plaintext data transmitted into the secure channel, even if the permanent secret key skc has been revealed.”), Haggerty at [0009]-[0014] (“Prior SIM card based approaches suffer from a number of disabilities. For instance, traditional UICCs support only a single USIM (or more generally ‘SIM’) access control client. If a user wants to authenticate to a cellular network using a different SIM, the user must physically exchange the SIM card in the device with a different SIM card …. The present disclosure provides, inter alia, for large scale distribution of electronic access control clients.”), Lee at Abstract (“The present invention relates to a method and apparatus for installing a profile, and more specifically, to a method for managing mobile communication subscriber information (profile), such as for remotely installing and uninstalling a profile onto a security module (Universal Integrated Circuit Card (UICC)) that is embedded inside a terminal and that is not attachable or detachable, thereby replacing UICC.”), Park (IEEE) at Abstract (“Embedded UICC (eUICC) is a new form of UICC … [T]he profiles necessary for its operations should be provisioned remotely into the eUICC by new entity. For the remote provisioning, SM (Subscription Manager) is newly introduced by the standardization organization. However, this new ecosystem around eUICCs can cause tremendous security issues unless thorough consideration of security is accompanied during standardization because

the profiles usually include the security-sensitive information. In this paper, a novel secure profile provisioning architecture for eUICCs is proposed. Our architecture mainly defines the overall architecture of the secure profile provisioning for eUICCs.”), Peirce at 1:6-9 (“The present invention relates generally to techniques for generating cryptographic keys used in secure data communications and, in particular, to such techniques used for manufactured products having embedded processing devices.”), SCP11 at 11 (“[T]his protocol allows authentication and secure channel initiation based on certificates instead of pre-shared keys. This provides greater flexibility in cases where the two entities setting up the secure channel are not deployed in strict pairs.”), SGP.22 at 19 (“This section describes the internal high-level architecture of the eUICC …. Operator Profiles are stored inside security domains within the eUICC and are implemented using GlobalPlatform standards. These ensure that it is impossible for any Profile to access the applications or data of any other Profile stored on the eUICC. The same mechanism is currently in use within SIM cards to ensure payment applications are kept secure.”), Weiss at [0003] (“It is foreseeable that at least for some of these devices it will not be possible or at least very difficult to provide the secure element beforehand with the necessary subscription credentials, including for instance an IMSI. This is because in a lot of M2M devices the secure element will most likely be implemented in the form of a surface mounted chip or chip module without the possibility of providing the secure element with the necessary subscription credentials beforehand. Consequently, once in the field, these M2M devices and their non-personalized secure elements require the provision of subscription credentials over-the-air.”). Thus, a person of ordinary skill in the art would have been motivated to modify any of the primary references to include this feature. A person of ordinary skill in the art would also have had a reasonable expectation of success. A person of ordinary skill in the art would have understood that these references disclose

interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach procedures for mutual authentication and/or sensitive data encryption (*e.g.*, limitations 1[PRE], 1[A], 1[B], 1[C], 1[D], 1[E], 1[F], 1[G], 1[H], 1[I], 1[J], 6, 8, 9, 10, 19, 20, 21), it would have been obvious to a person of ordinary skill in the art at the time of the invention to combine the primary reference with any of the prior art that discloses procedures for mutual authentication and/or sensitive data encryption (*e.g.*, limitations 1[PRE], 1[A], 1[B], 1[C], 1[D], 1[E], 1[F], 1[G], 1[H], 1[I], 1[J], 6, 8, 9, 10, 19, 20, 21) in Exhibits F-01 to F-08 or Exhibit F-A. For example, several prior art references, including at least Abi-Char, ANSI X9.63 Overview, Boyd-Mathuria, GlobalPlatform, Gouget, Haggerty, Konstantinou, Lee, Nix, Park (IEEE), Peirce, SCP11, SGP.22, and/or Weiss explicitly describe or disclose procedures for mutual authentication and/or sensitive data encryption. *See, e.g.*, Abi-Char at 1, 2, 3, 4; ANSI X9.63 Overview at 3, 7, 12; Boyd-Mathuria at 49, 81, 125, 136, 140, 141; GlobalPlatform at 156, 174, 194, 198, 202-203, 216, 234, 246-247, 251-253, 255-256, 258, 260, 264, 266-268, 275-276; Gouget at Abstract; Haggerty at Abstract, [0008], [0015], [0045]-[0046], [0048], [0084], [0100], [0114], [0121], [0131]-[0133]; Lee at Abstract, [0011], [0062]; Park (IEEE) at 297, 300, 301, 303; Peirce at Abstract, 1:6-9, 2:66-3:54, 8:18-51; SCP11 at 12, 13, 20, 30; SGP.22 at 9, 11, 12, 17, 22, 23, 24, 26-28, 51-54, 62-67, 75, 81, 93-94, 131-132, 202, 210; Weiss at [0012], [0014], [0015], [0038], [0042], [0063].

A person skilled in the art would have understood the benefits of procedures for mutual authentication and/or sensitive data encryption, would have recognized that configuring a system to comprise procedures for mutual authentication and/or sensitive data encryption would provide

benefits to the system, and would have been motivated to incorporate these features into a system accordingly. For example, a POSITA would have understood that configuring a system to comprise procedures for mutual authentication and/or sensitive data encryption would yield a complete, secure, and efficient architecture for eUICC profile provisioning. Indeed, a POSITA would have recognized that applying procedures for mutual authentication and/or sensitive data encryption would provide an additional layer of protection for the most sensitive data within the profile, ensuring that even if some aspects were compromised, the critical key materials could remain protected. *See, e.g.*, Abi-Char at Abstract ("To provide secure communication for mobile devices, authenticated key agreement protocol is an important primitive for establishing session key …. In this paper we present a fast and Secure Authenticated Key Agreement (EC-SAKA) protocol based on Elliptic Curve Cryptography …. The new protocol achieves many of the required security and performance properties. It can resist dictionary attacks mounted by either passive or active network intruders. It can resist Man-In-The Middle attack. It also offers perfect forward secrecy which protects past sessions and passwords against future compromise. In addition, it can resist known-key and resilience to server attack …. Our proposed protocol offers significantly improved performance in computational and communication load over comparably many authenticated key agreement protocols…"), ANSI X9.63 Overview at 4 ("Specify schemes capable of meeting common security needs"), Boyd-Mathuria at VII ("We believe that this book is the first comprehensive treatment of protocols for authentication and key establishment …. Authentication and key establishment are fundamental building blocks for securing electronic communications. Cryptographic algorithms for encryption and integrity cannot perform their function unless secure keys have been established and the users know which parties share such keys. It is essential that protocols for providing authentication and key establishment are fit for

their purpose."), GlobalPlatform at 23 ("The primary goal of the GlobalPlatform is to ensure the security and integrity of the card's components for the life of the card …. To ensure card security and integrity, the GlobalPlatform is designed to support a range of secure mechanisms for: Data integrity; Resource availability; Confidentiality; Authentication."), Gouget at [0020]-[0022] ("The invention solves the problem of man-in-the-middle attack in case of the exposure of a permanent secret key used to establish a secure channel. There is neither need for an additional device nor an additional mutual authentication. Thanks to the invention, a secure channel is established between the server S and the client C such that the gateway G cannot access to the plaintext data transmitted into the secure channel, even if the permanent secret key skc has been revealed."), Haggerty at [0009]-[0014] ("Prior SIM card based approaches suffer from a number of disabilities. For instance, traditional UICCs support only a single USIM (or more generally 'SIM') access control client. If a user wants to authenticate to a cellular network using a different SIM, the user must physically exchange the SIM card in the device with a different SIM card …. The present disclosure provides, inter alia, for large scale distribution of electronic access control clients."), Lee at [0005]-[0011] ("The conventional UICC is manufactured on demand as a dedicated card for a specific mobile communication operator. Accordingly, the authentication information (e.g. USIM application, IMSI, and K value) for connection to the corresponding operator network is stored in the UICC in the manufacturing stage. The mobile communication operator provides the subscriber with the manufactured UICC," and "[t]he subscriber may insert the UICC into a mobile communication terminal to use the corresponding mobile communication operator' s network and application services and, if necessary, may detach the UICC from the terminal and attach to another terminal so as to use the authentication information, contacts, and phonebooks stored in the corresponding UICC with the new terminal as they were …. Unlike the

conventional UICC which is manufactured and distributed for specific mobile communication operators, the newly introduced embedded security module is capable of allowing for the user who has purchased the terminal to install and maintain the authentication information of various mobile communication operators securely and flexibly in such a way of subscribing and unsubscribing to a specific mobile communication operator or switching the subscription between operators. Thus, the present invention aims to provide a method for installing UICC information of various mobile communication operators in an embedded security module (instead of the conventional detachable UICC) remotely through a network.”), Park (IEEE) at Abstract (“[T]his new ecosystem around eUICCs can cause tremendous security issues unless thorough consideration of security is accompanied during standardization because the profiles usually include the security-sensitive information.”), Peirce at 1:21- 25 (“In some cases, it is desirable to establish authenticated, secure data communications in which the exchanged data is encrypted. Although various approaches can be used, cryptographic keys are perhaps most commonly used for this purpose”), SCP11 at 11 (“[T]his protocol allows authentication and secure channel initiation based on certificates instead of pre-shared keys. This provides greater flexibility in cases where the two entities setting up the secure channel are not deployed in strict pairs.”), SGP.22 at 33 (“The RSP ecosystem relies on remote secure communication to achieve function execution requests and data exchanges. Any of the remote secure communication defined for RSP SHALL follow the hereunder rules … Mutual authentication[,] Data privacy[,] Communication protection[,] Authorisation[.]”), Weiss at [0014] (“Preferably, the first server decrypts the encrypted version of the identification element IDse, the encrypted version of the session key Kses and the encrypted version of the hardware configuration HWconf of the secure element and/or the mobile terminal using the configuration key Kconf provided by the second

server so that the first server can verify the validity of the configuration key Kconf provided by the second server by verifying that the identification element IDse sent in the clear is identical to the identification element IDse resulting from the decryption of the encrypted version of the identification element IDse using the configuration key Kconf."). Thus, a person of ordinary skill in the art would have been motivated to modify any of the primary references to include this feature. A person of ordinary skill in the art would also have had a reasonable expectation of success. A person of ordinary skill in the art would have understood that these references disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach key exchange and/or agreement protocols or mechanisms (*e.g.*, limitations 1[PRE], 1[A], 1[B], 1[C], 1[D], 1[E], 1[F], 1[G], 1[H], 1[I], 1[J], 5, 19, 20), it would have been obvious to a person of ordinary skill in the art at the time of the invention to combine the primary reference with any of the prior art that discloses key exchange and/or agreement protocols or mechanisms (*e.g.*, limitations 1[PRE], 1[A], 1[B], 1[C], 1[D], 1[E], 1[F], 1[G], 1[H], 1[I], 1[J], 5, 19, 20) in Exhibits F-01 to F-08 or Exhibit F-A. For example, several prior art references, including at least Abi-Char, ANSI X9.63 Overview, Boyd-Mathuria, GlobalPlatform, Gouget, Haggerty, Konstantinou, Lee, Nix, Park (IEEE), Peirce, SCP11, SGP.22, and/or Weiss explicitly describe or disclose key exchange and/or agreement protocols or mechanisms. *See, e.g.*, Abi-Char at 1, 3; ANSI X9.63 Overview at 3, 7, 12; Boyd-Mathuria at 49, 81, 125, 136, 140, 141; GlobalPlatform at 156, 174, 194, 198, 202-203, 216, 234, 246-247, 251-253, 255-256, 258, 260, 264, 266-268, 275-276; Gouget at Abstract; Haggerty at Abstract, [0008], [0015], [0045]-[0046], [0048], [0084], [0100], [0114], [0121], [0131]-[0133]; Lee at Abstract, [0011],

[0062]; Park (IEEE) at 297, 300, 301, 303; Peirce at Abstract, 1:6-9, 2:66-3:54, 8:18-51; SCP11 at 12, 13, 20, 30; SGP.22 at 15, 27-28, 34, 51-53, 62-65, 93-94, 131-132, 140, 210; Weiss at [0002], [0010]-[0011], [0012], [0014], [0015], [0020], [0046], [0063].

A person skilled in the art would have understood the benefits of key exchange and/or agreement protocols or mechanisms, would have recognized that configuring a system to comprise key exchange and/or agreement protocols or mechanisms would provide benefits to the system, and would have been motivated to incorporate these features into a system accordingly. For example, a POSITA would have understood that configuring a system to comprise key exchange and/or agreement protocols or mechanisms would yield a complete, secure, and efficient architecture for eUICC profile provisioning. Indeed, a POSITA would have recognized that configuring a system to comprise key exchange and/or agreement protocols or mechanisms would provide an additional layer of protection for the most sensitive data within the profile. Key exchange and/or agreement protocols or mechanisms were well-established and known to provide confidentiality, integrity, and mutual authentication. *See, e.g.*, Abi-Char at Abstract ("To provide secure communication for mobile devices, authenticated key agreement protocol is an important primitive for establishing session key …. In this paper we present a fast and Secure Authenticated Key Agreement (EC-SAKA) protocol based on Elliptic Curve Cryptography …. The new protocol achieves many of the required security and performance properties. It can resist dictionary attacks mounted by either passive or active network intruders. It can resist Man-In-The Middle attack. It also offers perfect forward secrecy which protects past sessions and passwords against future compromise. In addition, it can resist known-key and resilience to server attack …. Our proposed protocol offers significantly improved performance in computational and communication load over comparably many authenticated key agreement

protocols…"), ANSI X9.63 Overview at 3 ("Specifies key agreement and key transport schemes using elliptic curve cryptography … Specifies a variety of schemes to meet the diverse security needs of communications protocols"), Boyd-Mathuria at VII ("We believe that this book is the first comprehensive treatment of protocols for authentication and key establishment …. Authentication and key establishment are fundamental building blocks for securing electronic communications. Cryptographic algorithms for encryption and integrity cannot perform their function unless secure keys have been established and the users know which parties share such keys. It is essential that protocols for providing authentication and key establishment are fit for their purpose."), GlobalPlatform at 23 ("The primary goal of the GlobalPlatform is to ensure the security and integrity of the card's components for the life of the card …. Because the cards are only part of a larger card system involving multiple parties and off-card components, the GlobalPlatform also relies upon non-cryptographic, procedural means of protection, such as code testing and verification, physical security, and secure key handling."), Gouget at [0020]-[0022] ("The invention solves the problem of man-in-the-middle attack in case of the exposure of a permanent secret key used to establish a secure channel. There is neither need for an additional device nor an additional mutual authentication. Thanks to the invention, a secure channel is established between the server S and the client C such that the gateway G cannot access to the plaintext data transmitted into the secure channel, even if the permanent secret key skc has been revealed."), Haggerty at [0009]-[0014] ("Prior SIM card based approaches suffer from a number of disabilities. For instance, traditional UICCs support only a single USIM (or more generally 'SIM') access control client. If a user wants to authenticate to a cellular network using a different SIM, the user must physically exchange the SIM card in the device with a different SIM card …. The present disclosure provides, inter alia, for large scale distribution of electronic access control

clients.”), Lee at [0016] (“According to an embodiment of the present invention, a profile management server for managing the embedded security module of a terminal and a profile provision server for generating a UICC profile in association with a specific mobile communication operator are separated such that the terminal encodes a session key and authenticate the profile with a digital certificate provided by the profile provision server and thus can transfer the encoded profile to the embedded security module of the terminal without exposing the content of the profile to the profile management server positioned between the profile provision server and the terminal.”), Park (IEEE) at 301 (“KAM is software running inside the eUICC to perform the key agreement protocol …. For the security, the SM-DP Credentials should not be revealed to any party, even SM-SR, except for eUICC. To accomplish this, KAM is designed and applied to SPA.”), Peirce at 1:50-2:2 (“As applied to embedded processing devices, the generation of the cryptographic keys can be problematic because they typically do not have entropy hardware or software engines of the type found in personal computers. Instead pseudo random number generators (PRNG) are typically used. These PRNGs are generally implemented in software and require a seed value that is used to generate a pseudo-random number. This generated number is then used to produce the cryptographic keys. The generation of strong keys using PRNGs generally necessitates the use of a seed value that cannot later be discovered. For an embedded processing device having restricted computing capabilities, obtaining such a seed value can be problematic …. According to one aspect of the invention, there is provided a method of producing cryptographic keys for use in communicating with a manufactured product”), SCP11 at 11 (“[T]his protocol allows authentication and secure channel initiation based on certificates instead of pre-shared keys. This provides greater flexibility in cases where the two entities setting up the secure channel are not deployed in strict pairs.”),

SGP.22 at 93-94 ("Public key of the eUICC used to verify an eUICC signature …. Private key of the SM-DS used to provide signatures for authentication to the eUICC …. Public key of the EUM used to verify EUICC Certificates …. One-time public key of the EUICC used for key agreement …. One-time private key of the EUICC used for key agreement."), Weiss at [0002]-[0005] ("[T]he SIM contains subscription credentials for authenticating and identifying the user of the mobile terminal, including in particular an International Mobile Subscriber Identity (IMSI) and an authentication key Ki. These subscription credentials are generally stored on the SIM by the SIM manufacturer/vendor or the MNO during a SIM personalization process prior to providing the user of the mobile terminal with his SIM …. [T]he problem addressed by the present invention is to provide for methods and devices that allow providing the secure element of a mobile terminal over-the-air with a subscription profile."). Thus, a person of ordinary skill in the art would have been motivated to modify any of the primary references to include this feature. A person of ordinary skill in the art would also have had a reasonable expectation of success. A person of ordinary skill in the art would have understood that these references disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach random number generation protocols (*e.g.*, limitations 1[A], 1[C]), it would have been obvious to a person of ordinary skill in the art at the time of the invention to combine the primary reference with any of the prior art that discloses random number generation protocols (*e.g.*, limitations 1[A], 1[C]) in Exhibits F-01 to F-08 or Exhibit F-A. For example, several prior art references, including at least Abi-Char, ANSI X9.63 Overview, Boyd-Mathuria, GlobalPlatform, Gouget, Haggerty, Konstantinou, Nix, Park (IEEE), Peirce, SGP.22, and/or

Weiss explicitly describe or disclose random number generation protocols. *See, e.g.*, Abi-Char at 3; ANSI X9.63 Overview at 6, 10; Boyd-Mathuria at 9, 136, 140, 141; GlobalPlatform at 194; Gouget at Abstract, [0011]-[0012], [0036], [0040]-[0041]; Haggerty at [0121]; Park (IEEE) at 300, 301; Peirce at Abstract, 8:18-51; SGP.22 at 27-28, 35, 62, 63, 94; Weiss at [0046].

A person skilled in the art would have understood the benefits of random number generation protocols, would have recognized that configuring a system to comprise random number generation protocols would provide benefits to the system, and would have been motivated to incorporate these features into a system accordingly. For example, a POSITA would have understood that configuring a system to comprise random number generation protocols would improve the security of the system by helping to ensure that the keys used in the exchanges were derived from sufficiently random and unpredictable sources that were readily available to the eUICC-storing devices in these systems. *See, e.g.*, Abi-Char at 2 ("Because round trips and large blocks are critical factors in terms of communication load and because exponentiations and random numbers are to be critical factors in terms of computation load, such properties are listed below: Computational efficiency[,] Communication efficiency[,] Nature of security guarantees[,] Storage of secrets."), ANSI X9.63 Overview at 6 ("A number of primitives (mathematical building blocks) must be specified in order to build schemes …. Curves selected in any manner. Verifiably random selection option"), Boyd-Mathuria at 9 ("There are various mechanisms that may be employed to allow users to check that session keys have not been replayed …. In this method, A will generate a new random value NA commonly known as a nonce (a number used only once). Definition 1.1. A nonce is a random value generated by one party and returned to that party to show that a message is newly generated."), GlobalPlatform at 194 ("The Secure Channel is always initiated … by the off-card entity by passing a 'host' challenge (random data

unique to this Secure Channel Session) to the card. The card, on receipt of this challenge, generates its own 'card' challenge (again random data unique to this Secure Channel Session). The card, using the host challenge, the card challenge and its internal static keys, creates new secret Secure Channel session keys and generates a first cryptographic value (card cryptogram) using one of its newly created Secure Channel session keys …. This card cryptogram along with the card challenge, the Secure Channel Protocol identifier, and other data is transmitted back to the off-card entity. As the off-card entity should now have all the same information that the card used to generate the card cryptogram, it should be able to generate the same Secure Channel session keys and the same card cryptogram and by performing a comparison, it is able to authenticate the card."), Gouget at [0020]-[0022] ("The invention solves the problem of man-in-the-middle attack in case of the exposure of a permanent secret key used to establish a secure channel. There is neither need for an additional device nor an additional mutual authentication. Thanks to the invention, a secure channel is established between the server S and the client C such that the gateway G cannot access to the plaintext data transmitted into the secure channel, even if the permanent secret key skc has been revealed."), Haggerty at [0121] ("When the user exports an eSIM, the AP retrieves a list of installed profiles from eUICC; for each profile, eUICC also returns the associated principal and a nonce generated for anti-replay. When the user chooses to export a profile, the AP uses information contained in the principal to obtain a single sign-on (SSO) token from the service provider, where the user would be prompted to enter username and password for the purpose. The SSO token is passed together with principal and nonce to the server broker in export request. The server broker can process the authentication with the service provider, using the SSO token supplied by the device. Once authentication passes, the flow mirrors eSIM delivery to the device, except that the client and server roles are

reversed. At a high level, the server broker initiates a session with the eUICC, creates a request BLOB for the export. In the request, it includes the nonce that the eUICC generated, to indicate that the operation has passed L3 authentication. The eUICC verifies the request BLOB, encrypts the eSIM with the server agent's public key, creates a batch descriptor and L3 owner information for the eSIM. The eSIM together with L3 and L2 information can be sent to the server."), Park (IEEE) at 301 ("KAM is software running inside the eUICC to perform the key agreement protocol …. For the security, the SM-DP Credentials should not be revealed to any party, even SM-SR, except for eUICC. To accomplish this, KAM is designed and applied to SPA."), Peirce at 1:50-2:2 ("As applied to embedded processing devices, the generation of the cryptographic keys can be problematic because they typically do not have entropy hardware or software engines of the type found in personal computers. Instead pseudo random number generators (PRNG) are typically used. These PRNGs are generally implemented in software and require a seed value that is used to generate a pseudo-random number. This generated number is then used to produce the cryptographic keys. The generation of strong keys using PRNGs generally necessitates the use of a seed value that cannot later be discovered. For an embedded processing device having restricted computing capabilities, obtaining such a seed value can be problematic …. According to one aspect of the invention, there is provided a method of producing cryptographic keys for use in communicating with a manufactured product"), SGP.22 at 28 ("Profile protection can optionally be performed using … random keys per Profile…"), Weiss at [0046] ("Preferably, the session key Kses is a nonce, i.e. an arbitrary number used only once. This ensures that for every subscription profile update session, such as the subscription profile update session shown in FIG. 2, a different session key Kses is used. As is well known to the person skilled in the art, such a nonce can be created, for instance, by using a pseudorandom number generator, preferably a

cryptographically secure pseudorandom number generator.”). Thus, a person of ordinary skill in the art would have been motivated to modify any of the primary references to include this feature. A person of ordinary skill in the art would also have had a reasonable expectation of success. A person of ordinary skill in the art would have understood that these references disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

As another example, to the extent that any primary reference is deemed not to anticipate a claim for failing to teach specific types or aspects of connected or networked devices (*e.g.*, limitations 2, 10, 14, 15), it would have been obvious to a person of ordinary skill in the art at the time of the invention to combine the primary reference with any of the prior art that discloses specific types or aspects of connected or networked devices (*e.g.*, limitations 2, 10, 14, 15) in Exhibits F-01 to F-08 or Exhibit F-A. For example, several prior art references, including at least Abi-Char, ANSI X9.63 Overview, Boyd-Mathuria, GlobalPlatform, Gouget, Haggerty, Konstantinou, Lee, Nix, Park (IEEE), Peirce, SGP.22, and/or Weiss explicitly describe or disclose specific types or aspects of connected or networked devices. *See, e.g.*, Abi-Char at Abstract; ANSI X9.63 Overview at 3, 7, 12, 22; Boyd-Mathuria at 23, 24, 126-131, 175, 177, 190-193; GlobalPlatform at 2; Gouget at [0051]; Haggerty at [0017], [0042], [0131]; Lee at Abstract, [0001], [0107]; Park (IEEE) at Abstract, 297, 298; Peirce at Abstract, 3:8-23, 3:64-4:42, 4:43-54, 6:29-65, 7:16-33; SGP.22 at 7, 9, 11, 17, 200; Weiss at [0020], [0031], [0033].

A person skilled in the art would have understood the benefits of applying teachings to specific types or aspects of connected or networked devices, would have recognized that configuring a system to comprise specific types or aspects of connected or networked devices would provide benefits to the system, and would have been motivated to incorporate these

features into a system accordingly. For example, a POSITA would have understood that applying teachings to specific types or aspects of connected or networked devices would broaden the applicability of the disclosed systems. Incorporating specific types or aspects of connected or networked devices would have amounted to a straightforward substitution of one known secure element implementation for another, yielding predictable results. *See, e.g.*, Abi-Char at Abstract ("The increased progress in wireless mobile communication has attracted an important amount of attention on the security issue."), ANSI X9.63 Overview at 3 ("Primarily designed to meet the needs of the financial services industry, but also generally applicable"), Boyd-Mathuria at 193 ("Despite the inexorable increase in the availability of computing resources there has been considerable interest in protocols that can be implemented on devices with limited computational power. Typical examples of such devices are mobile terminals and embedded hardware. Very often the low-power device is a client required to establish a key with a computationally powerful server and so an acceptable solution may have unbalanced computational requirements: the server end can bear an increased computational load in order to ease the burden on the client side. Another technique that is effective is to allow the client side to pre-compute values which can be used during the protocol execution; mobile terminals typically have the opportunity to make off-line computations during the idle time between awaiting calls."), GlobalPlatform at 2 ("For smart cards to reach their true potential, consumers need to be able to use them for a wide variety of functions. For example, the cards can be used with mobile phones to make purchases over the Internet as well as to securely access a PC. Smart cards should also be cost effective and easily multifunctional."), Gouget at [0051] ("It will be well understood that a smartcard with a middle-ware installed on a smartcard host is not a limited example. The invention can be advantageously applied to any web service deployment with a client-middleware installed in the dubious

environment of a smartcard host such as a user's PC."), Haggerty at [0007] ("Access control is required for secure communication in most prior art wireless radio communication systems."), Lee at [0011] ("Thus, the present invention aims to provide a method for installing UICC information of various mobile communication operators in an embedded security module (instead of the conventional detachable UICC) remotely through a network."), Park (IEEE) at 297 ("The eUICC was initially considered to be utilized as the same roles of UICC [to] be adopted into the small device … These days, the fields of its usages are being considered to be extended to the CEDs (Consumer Electronic Devices) for the smaller form factor to save the physical space of the device."), Peirce at 1:13-30 ("As computer electronics continue to reduce in cost and size, the applications for embedded processing devices are continuing to increase, and there now exists many types of manufactured products that contain some type of embedded processing device, whether microprocessor based or otherwise. Some embedded devices are designed to undergo data communication with one or more external, possibly remote devices. In some cases, it is desirable to establish authenticated, secure data communications in which the exchanged data is encrypted."), SGP.22 at 7 ("This document defines a technical solution for the remote provisioning and management of the Embedded UICC (eUICC) in consumer Devices as defined in RSP Architecture …. The adoption of this technical solution will provide the basis for global interoperability between different Operator deployment scenarios, for example network equipment (e.g. Subscription Manager Data Preparation (SM-DP+)) and various eUICC platforms."), Weiss at [0003] ("One particular field of application of secure elements, such as SIMs, eUICCs, UICCs and the like, which is expected to grow rapidly in the near future is M2M (machine-to-machine) communication, i.e. the communication between machines over a cellular communications network without human intervention, also called the Internet of things …. It is

foreseeable that at least for some of these devices it will not be possible or at least very difficult to provide the secure element beforehand with the necessary subscription credentials, including for instance an IMSI. This is because in a lot of M2M devices the secure element will most likely be implemented in the form of a surface mounted chip or chip module without the possibility of providing the secure element with the necessary subscription credentials beforehand. Consequently, once in the field, these M2M devices and their non-personalized secure elements require the provision of subscription credentials over-the-air."). Thus, a person of ordinary skill in the art would have been motivated to modify any of the primary references to include this feature. A person of ordinary skill in the art would also have had a reasonable expectation of success. A person of ordinary skill in the art would have understood that these references disclose interrelated teachings based on routine technologies and would have been amenable to various well-understood and predictable combinations.

IX. Invalidity Contentions Under 35 U.S.C. § 112

Defendants include below the grounds on which Defendants contend the asserted claims are invalid for failure to meet the requirements of the first two paragraphs of 35 U.S.C. § 112.

Plaintiff has not yet provided a claim construction for many of the terms and phrases that Defendants anticipate will be in dispute. Defendants, therefore, cannot provide a complete list of its § 112 defenses because Defendants do not know whether Plaintiff will proffer a construction for certain terms and phrases that is broader than, or inconsistent with, the construction that would be supportable by the disclosure set forth in the specification.

To the extent the following contentions reflect constructions of claim limitations consistent with or implicit in Plaintiff's Infringement Contentions, no inference is intended nor should any be drawn that Defendants agree with Plaintiff's claim constructions, and Defendants expressly reserve the right to contest such claim constructions. Defendants offer these

contentions in response to Plaintiff's Infringement Contentions and without prejudice to any position it may ultimately take as to any claim construction issues.

Accordingly, Defendants reserve the right to amend or supplement these § 112 Invalidity Contentions as discovery progresses.

A. Indefiniteness Under 35 U.S.C. § 112, ¶ 2

35 U.S.C. § 112, ¶ 2 requires that a patent claim "particularly point[] out and distinctly claim[] the subject matter which the applicant regards as his invention." 35 U.S.C. § 112, ¶ 2. Claim terms that fail to inform those skilled in the art "with reasonable certainty … about the scope of the invention" fail the definiteness requirement of 35 U.S.C. § 112, ¶ 2. *Nautilus, Inc. v. Biosig Instruments, Inc*., 572 U.S. 898, 901 (2014).

Each of the asserted claims are invalid as indefinite under 35 U.S.C. § 112 because they fail to particularly point out and distinctly claim the subject matter which the applicant regards as his invention. In particular, the following limitations, read in light of the intrinsic evidence, fail to inform those skilled in the art with reasonable certainty about the scope of the claimed inventions:

1. '780 Patent

- Limitation 1[J]: "(h) decrypting, by the embedded universal integrated circuit card, at least a portion of the encrypted profile using the profile key;"
- Limitation 1[K]: "(i) decrypting, by the embedded universal integrated circuit card, at least a portion of the ciphertext using the symmetric key;"

2. '204 Patent

- Limitation 1[f]: "generating a module encrypted data using the symmetric ciphering key and the symmetric ciphering algorithm, wherein the module encrypted data includes the module identity;"

3. '893 Patent

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

4. '864 Patent

- Limitation 1[d]: "generating module encrypted data using the symmetric ciphering key and the symmetric ciphering algorithm, wherein the module encrypted data includes the module identity;"

5. '869 Patent

- Limitation 1[d]: "decrypting, with the shared secret key, at least a portion of the encrypted profile for the eUICC"
- Limitation 1[h]: "generating, with the symmetric key, module encrypted data, the module encrypted data comprising the module identity"
- Claim 4: "wherein the cryptographic parameters comprise an identifier for a set of cryptographic parameters"

6. '094 Patent

- Limitation 1[H]: "(h) decrypting, by the embedded universal integrated circuit card, at least a portion of the encrypted profile using the profile key;"
- Limitation 1[I]: "(i) decrypting, by the embedded universal integrated circuit card, at least a portion of the ciphertext using the symmetric key."

B. Lack of Enablement/Lack of Written Description Under 35 U.S.C. § 112, ¶ 1

The asserted claims of the Patents-In-Suit are further invalid under 35 U.S.C. § 112, ¶ 1 because the specifications do not contain an adequate written description of the subject matter of

these claims and would not enable one of skill in the relevant art to make and use the alleged invention.

For a claim to be valid, the specification must contain a written description of the invention. 35 U.S.C. § 112, ¶ 1. To fulfill the written description requirement, it "must clearly allow persons of ordinary skill in the art to recognize that the inventor invented what is claimed." *Ariad Pharm., Inc. v. Eli Lilly & Co*., 598 F.3d 1336, 1351 (Fed. Cir. 2010) (citation and internal quotation marks omitted). "[T]he applicant must 'convey with reasonable clarity to those skilled in the art that, as of the filing date sought, he or she was in possession of the invention,' and demonstrate that by disclosure in the specification of the patent." *Carnegie Mellon Univ. v. Hoffmann-La Roche Inc*., 541 F.3d 1115, 1122 (Fed. Cir. 2008) (quoting *Vas-Cath Inc. v. Mahurkar*, 935 F.2d 1555, 1563–64 (Fed. Cir. 1991)).

The specification must also describe "the manner and process of making and using [the invention], in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains … to make and use the" invention. *Ariad*, 598 F.3d at 1343; *see also* 35 U.S.C. § 112 ¶ 1. "The enablement requirement is satisfied when one skilled in the art, after reading the specification, could practice the claimed invention without undue experimentation." *AK Steel Corp. v. Sollac & Ugine*, 344 F.3d 1234, 1244 (Fed. Cir. 2003) (citation omitted). "[T]he scope of the claims must be less than or equal to the scope of the enablement." *Nat'l Recovery Tech., Inc. v. Magnetic Separation Sys., Inc*., 166 F.3d 1190, 1196 (Fed. Cir. 1999).

Each of the asserted claims below are invalid because the specifications fail to provide written description and/or an enabling disclosure of at least the following limitations:

1. ’780 Patent

- Limitation 1[C]: “(a) generating a first message comprising: (1) an identity of 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;”
- Limitation 1[E]: “(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;”
- Limitation 1[I]: “(g) receiving the symmetric key;”
- Limitation 1[J]: “(h) decrypting, by the embedded universal integrated circuit card, at least a portion of the encrypted profile using the profile key;”
- Limitation 1[K]: “(i) decrypting, by the embedded universal integrated circuit card, at least a portion of the ciphertext using the symmetric key;”

2. ’204 Patent

- Limitation 1[f]: “generating a module encrypted data using the symmetric ciphering key and the symmetric ciphering algorithm, wherein the module encrypted data includes the module identity;”

3. ’893 Patent

- Limitation 1[C][b]: “b. receive, from the subscription manager, i) an eUICC profile comprising network parameters, a key K, and a subscriber identity and ii) a symmetric key;”
- Limitation 1[D][b]: “b. decrypt a first portion of the eUICC profile using the profile key;”

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

4. '864 Patent

- Limitation 1[d]: "generating module encrypted data using the symmetric ciphering key and the symmetric ciphering algorithm, wherein the module encrypted data includes the module identity;"

5. '869 Patent

- Limitation 1[d]: "decrypting, with the shared secret key, at least a portion of the encrypted profile for the eUICC"
- Limitation 1[h]: "generating, with the symmetric key, module encrypted data, the module encrypted data comprising the module identity"
- Claim 4: "wherein the cryptographic parameters comprise an identifier for a set of cryptographic parameters"

6. '094 Patent

- Limitation 1[A]: "(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;"
- Limitation 1[C]: "(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;"
- Limitation 1[G]: "(g) receiving the symmetric key;"

- Limitation 1[H]: "(h) decrypting, by the embedded universal integrated circuit card, at least a portion of the encrypted profile using the profile key;"
- Limitation 1[I]: "(i) decrypting, by the embedded universal integrated circuit card, at least a portion of the ciphertext using the symmetric key."

X. Document Production

Pursuant to Patent Local Rule 3-4, Defendants are concurrently producing the prior art identified in these Invalidity Contentions, but Defendants are not required to produce the prior art in the file history of the Asserted Patents.

In addition, based on its investigations to date, and to the extent not already produced, Defendants are concurrently producing source code, specifications, schematics, flow charts, artwork, formulas, or other documentation sufficient to show the operation of any aspects or elements of the Accused Instrumentalities identified by Plaintiff in its P. R. 3-1(c) chart.

Defendants reserve the right to supplement these productions with additional documentation, in accordance with the Federal Rules of Civil Procedure, the Local Rules, the Court's orders and other applicable rules and statutes.

Dated: December 9, 2025

Respectfully submitted,

/s/ Ryan K. Yagura

Ryan K. Yagura (Tex. Bar No. 24075933)
ryagura@omm.com
O'MELVENY & MYERS LLP
400 S. Hope Street
Los Angeles, CA 90071
Telephone: 213-430-6000
Facsimile: 213-430-6407

Marc J. Pensabene (*Pro Hac Vice*)
New York State Bar No. 2656361

mpensabene@omm.com
Laura Gore (*Pro Hac Vice*)
New York State Bar No. 5172879
lgore@omm.com
O'MELVENY & MYERS LLP
1301 Avenue of the Americas, Suite 1700
New York, NY 10019
Telephone: 212-326-2000
Facsimile: 212-326-2061

Melissa R. Smith (Tex. Bar. No. 24001351)
melissa@gillamsmithlaw.com
GILLAM & SMITH, LLP
Marshall, Texas 75670
Telephone: 903-934-8450
Facsimile: 903-934-9257

Attorneys for Defendants Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc.

CERTIFICATE OF SERVICE

Pursuant to the Federal Rules of Civil Procedure, I hereby certify that, on December 9, 2025, all counsel of record who have appeared in this case are being served with a copy of the foregoing via the electronic mail.

/s/ Brian A. Treggs
Brian A. Treggs
Case Manager
O'Melveny & Myers LLP