

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ERICSSON INC.
Petitioner,

v.

KONINKLIJKE KPN N.V.
Patent Owner.

Case No. IPR2023-00902
Patent 9,438,572

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 9,438,572**

TABLE OF CONTENTS

I.	Introduction.....	1
II.	Mandatory Notices Under 37 C.F.R. § 42.8(a)(1).....	2
	A. Real Party-in-Interest under 37 C.F.R. § 42.8(b)(1)	2
	B. Related Matters under 37 C.F.R. § 42.8(b)(2)	2
	C. Lead and Back-Up Counsel under 37 C.F.R. § 42.8(b)(3)	2
	D. Service Information under 37 C.F.R. § 42.8(b)(4).....	3
III.	Fees	4
IV.	Requirements Under 37 C.F.R. § 42.104	4
	A. Grounds for Standing	4
	B. Priority Date	4
	C. Prior Art.....	4
	D. Identification of Challenge and Statement of Precise Relief Requested	7
V.	Institution is Proper under § 314(a).....	7
VI.	Institution is Proper Under § 325(d).....	8
VII.	Overview of the '572 Patent.....	9
	A. Description of the '572 Patent.....	9
	B. The '572 Patent's Prosecution History	10
	C. Level of Ordinary Skill in the Art	11
	D. Claim Listing.....	12
VIII.	Prior Art Summary	12
	A. Teo (EX1005).....	12
	B. Hawkes (EX1006).....	13
	C. RFC 4279 (EX1007)	14
	D. Madoukh (EX1011).....	14
	E. S3-070234 (EX1013)	14
	F. Kumar (EX1016).....	15
	G. Park (EX1017).....	15

H.	Thakare (EX1018).....	15
IX.	Claim Construction.....	15
X.	Asserted Grounds of Invalidity	16
A.	Ground 1: Teo in view of Madoukh Renders Obvious Claims 1-2 and 14.	16
1.	Motivation to Combine	16
2.	Reasonable Expectation of Success.....	17
3.	Claim 1	18
i.	[1p] Method for establishing a device-to-device (D2D) communication session between mobile devices which are mutually connectable via a D2D communication channel and individually connectable to a mobile network, comprising: .	18
ii.	[1a] preloading an initiation key on each of the mobile devices, the initiation key being associated with a validity period; 21	
iii.	[1b] and on each of the mobile devices: verifying a validity of the initiation key based on a current time;	24
iv.	[1c] requesting a further initiation key via the mobile network if no initiation key is deemed valid;.....	26
v.	[1d] if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key agreement procedure between the mobile devices over the D2D communication channel, ...	27
vi.	[1e] the key agreement procedure resulting in the session key based on a match of the respective initiation keys used by each of the mobile devices;	32
vii.	[1f] establishing the D2D communication session over the D2D communication channel based on the session key.	34
4.	Claim 2. Method according to claim 1, wherein the preloading the initiation key comprises providing the initiation key to each of the mobile devices via the mobile network when each respective mobile device is connected to the mobile network.....	35

5.	Claim 14. Method according to claim 1, wherein the key agreement procedure comprises: a three-pass authentication procedure; or a use of the initiation key to encrypt a message exchange between the mobile devices for obtaining a shared secret, and a Diffie-Hellman key exchange procedure which is initiated based on the shared secret.	36
B.	Ground 2: Teo in view of Madoukh and Hawkes Renders Obvious Claims 3-5 and 15-17	39
1.	Motivation to Combine	39
2.	Reasonable Expectation of Success	40
3.	Claim 3. Method according to claim 1, wherein the preloading the initiation key comprises storing the initiation key in a secure storage area of each respective mobile device.	41
4.	Claim 4. Method according to claim 3, wherein the secure storage area is provided by a trusted computing subsystem of each respective mobile device.	42
5.	Claim 5. Method according to claim 4, wherein at least one of the group of: verifying the validity of the initiation key, and using the initiation key in performing the key agreement procedure, is performed by the trusted computing subsystem.	43
6.	Claim 15	44
i.	[15p] A non-transitory computer-readable medium configured to store instructions for, upon execution of the instructions on a mobile device, causing the mobile device to establish a device-to-device (D2D) communication session with a further mobile device, the mobile device and the further mobile device being mutually connectable via a D2D communication channel and individually connectable to a mobile network, by:	44
ii.	[15a]	45
iii.	[15b]	45
iv.	[15c]	45
v.	[15d]	45

vi.	[15e].....	46
7.	Claim 16.....	46
i.	[16p] Mobile device for establishing a device-to-device (D2D) communication session with a further mobile device, the mobile device and the further mobile device being mutually connectable via a D2D communication channel and individually connectable to a mobile network, the mobile device comprising:	46
ii.	[16a].....	46
iii.	[16b].....	46
iv.	[16c].....	46
v.	[16d].....	47
vi.	[16e].....	47
vii.	[16f] a mobile subsystem for establishing the D2D communication session over the D2D communication channel based on the session key.	47
8.	Claim 17.....	48
i.	[17p] Mobile network arranged for preloading an initiation key on a mobile device when the mobile device is connected to the mobile network, the initiation key being associated with a validity period, the mobile device for establishing a device-to-device (D2D) communication session with a further mobile device, the mobile device and the further mobile device being mutually connectable via a D2D communication channel and individually connectable to the mobile network, the mobile device comprising:.....	48
ii.	[17a].....	49
iii.	[17b].....	49
iv.	[17c].....	49
v.	[17d].....	49
vi.	[17e].....	49
C.	Ground 3: Teo in view of Madoukh and RFC 4279 Renders Obvious Claims 6-9.....	50

1.	Motivation to Combine	50
2.	Reasonable Expectation of Success	51
3.	Claim 6.	53
	i. [6a] Method according to claim 1, further comprising: preloading a set of initiation keys on each of the mobile devices, the set of initiation keys key being associated with a respective set of validity periods; and.....	53
	ii. [6b] performing a key synchronization procedure between the mobile devices over the D2D communication channel for selecting a matching one of the set of initiation keys on each of the mobile devices as the initiation key.....	54
4.	Claim 7.	56
	i. [7a] Method according to claim 6, further comprising: preloading a set of key identifiers on each of the mobile devices, each of the set of key identifiers identifying a respective one of the set of initiation keys; and.....	56
	ii. [7b] performing the key synchronization procedure based on an exchange of one or more of the set of key identifiers between the mobile devices.	57
5.	Claim 8. Method according to claim 6, further comprising disabling or removing the initiation key from the set of initiation keys after use in establishing the D2D communication session.	57
6.	Claim 9. Method according to claim 6, wherein the set of validity periods is constituted at least in part by different but overlapping validity periods.	58
D.	Ground 4: Teo in view of Madoukh, RFC 4279, and Kumar Render Obvious Claim 10	59
	1. Motivation to Combine	59
	2. Reasonable Expectation of Success	61
	3. Claim 10. Method according to claim 1, wherein the initiation key is associated with a virtual network identity, and wherein the verifying the validity of the initiation key further comprises determining a match of the virtual	

	network identity on each of the mobile devices via the D2D communication channel.	62
E.	Ground 5: Teo in view of Madoukh and S3-070234 Renders Obvious Claims 11-12.....	63
1.	Motivation to Combine	63
2.	Reasonable Expectation of Success	65
3.	Claim 11. Method according to claim 1, wherein the initiation key is associated with a usage count for limiting a number of uses of the initiation key, and wherein the verifying the validity of the initiation key is further based on the usage count.....	66
4.	Claim 12. Method according to claim 11, further comprising adjusting the usage count after use of the initiation key in establishing the D2D communication session.	67
F.	Ground 6: Teo in view of Madoukh and Thakare Render Obvious Claim 13	68
1.	Motivation to Combine	68
2.	Reasonable Expectation of Success	68
3.	Claim 13. Method according to claim 1, further comprising requesting a further initiation key via the mobile network if the key agreement procedure fails in providing the session key.	69
XI.	Conclusion	70

EXHIBIT LIST

Exhibit No. ¹	Description
1001	U.S. Patent No. 9,549,572 B2 (“the ’572 Patent”)
1002	Prosecution File History for the ’572 Patent
1003	Declaration of Dr. Angelos Keromytis
1004	CV of Dr. Angelos Keromytis
1005	WO 2012/112124 A1 to Teo (“ <i>Teo</i> ”)
1006	U.S. Patent Application Pub. No. 2013/0067552 to Hawkes (“ <i>Hawkes</i> ”)
1007	RFC 4279
1008	Claim Listing
1009	Schneier, “Applied Cryptography: Protocols, Algorithms, and Source Code in C,” Wiley & Sons (Second Edition), 1996
1010	Reserved
1011	U.S. Patent Application Pub. No. 2001/0019614 to Madoukh (“ <i>Madoukh</i> ”)
1012	Reserved
1013	S3-070234, “Key Refresh in SAE/LTE,” 3GPP TSG SA WG3 Security – SA3#46b, 28-29 March, 2007
1014	ETSI TS 133 110 v10.1.0 (2011-07)
1015	RFC 2409
1016	U.S. Patent Application Pub. No. 2007/0171910 to Kumar (“ <i>Kumar</i> ”)
1017	U.S. Patent Application Pub. No. 2009/0016524 to Park (“ <i>Park</i> ”)
1018	U.S. Patent Application Pub. No. 2009/0181643 to Thakare (“ <i>Thakare</i> ”)
1019	Declaration of Craig Bishop

¹ Citations to patents are made by column and line cite; citations to patent publications are made by paragraph number; citations to Exhibit 1002 are made with reference to the Bates-stamped pagination; citations to other exhibits are made to the page number of the document itself.

Exhibit No. ¹	Description
1020	U.S. Patent No. 6,879,825 to Daly

I. INTRODUCTION

Ericsson Inc. (“Petitioner”) submits this Petition for *Inter Partes* Review (“IPR”) of Claims 1-17 of U.S. Patent No. 9,438,572 (the “’572 Patent”). The ’572 Patent relates to “establishing a device-to-device (D2D) communication session between mobile devices.” EX1001, 1:12-14. The independent claims are directed to the basic cryptographic concept that an “initiation key” is loaded onto mobile devices; and, after verifying the validity of the initiation key, using the initiation key to generate a “session key,” which is later used to establish a D2D communication session.

During prosecution, the applicant argued for patentability over the Examiner’s cited art of record (Hakola and Vanderveen), in part, on the basis that the prior art failed to teach the amended claims’ recitation of “*preloading an initiation key on each of the mobile devices, the initiation key being associated with a validity period*” and “*the key agreement procedure resulting in the session key based on a match of the respective initiation keys used by each of the mobile devices.*” EX1002, 66, 72-73. The Examiner found these arguments persuasive and issued a notice of allowance. *Id.*, 25-40. But these concepts are found in the teachings of Petitioner’s primary reference, *Teo*, which discloses a system for loading the same pre-shared key on two mobile communication terminals to facilitate the generation of an encryption key for direct communication between the terminals.

The challenged dependent claims do nothing more than recite rudimentary cryptography concepts either taught or rendered obvious by *Teo*, *Madoukh*, *Hawkes*, RFC 4279, S3-070234, *Kumar*, or *Thakare* cited herein. As a result, the '572 Patent represents no novel or non-obvious advance over the prior art.

Petitioner requests institution of *Inter Partes* Review of Claims 1-17 of the '572 Patent and a finding that all challenged claims are unpatentable.

II. MANDATORY NOTICES UNDER 37 C.F.R. § 42.8(a)(1)

A. *Real Party-in-Interest under 37 C.F.R. § 42.8(b)(1)*

Ericsson Inc. and Telefonaktiebolaget LM Ericsson are the Real Parties-in-Interest. Ericsson Inc. is a wholly-owned subsidiary of Telefonaktiebolaget LM Ericsson. No other parties exercised or could have exercised control over this Petition. No other parties funded or directed this Petition. *See* Office Patent Trial Practice Guide, 77 FR 48756-01, 48759-60, 2012 WL 3276882 (Aug. 14, 2012).

B. *Related Matters under 37 C.F.R. § 42.8(b)(2)*

Petitioner is not aware of any related matters that may affect, or may be affected by, decisions in this proceeding.

C. *Lead and Back-Up Counsel under 37 C.F.R. § 42.8(b)(3)*

Petitioner provides the following designation of counsel.

LEAD COUNSEL	BACK-UP COUNSEL
Chad C. Walters BAKER BOTTS L.L.P. 2001 Ross Ave., Suite 900 Dallas, TX 75201-2980 Phone: (214) 953-6511 Fax: (214) 661-4511 chad.walters@bakerbotts.com USPTO Reg. No. 48,022	Douglas M. Kubehl BAKER BOTTS L.L.P. 2001 Ross Ave., Suite 900 Dallas, TX 75201-2980 Phone: (214) 953-6486 Fax: (214) 661-4486 doug.kubehl@bakerbotts.com USPTO Reg. No. 41,915 Jeffery S. Becker BAKER BOTTS L.L.P. 2001 Ross Ave., Suite 900 Dallas, TX 75201-2980 Phone: 214-953-6526 Fax: 214-661-4526 jeff.becker@bakerbotts.com USPTO Reg. No. 68,533 Joseph Andrew Grado BAKER BOTTS L.L.P. 2001 Ross Ave., Suite 900 Dallas, TX 75201-2980 Phone: (214) 953-6522 Fax: (214) 661-4522 Andrew.grado@bakerbotts.com USPTO Reg. No. 80,316

D. Service Information under 37 C.F.R. § 42.8(b)(4)

A copy of this entire Petition, including all Exhibits and a Power of Attorney, is being served by FEDERAL EXPRESS, costs prepaid, to the address of the attorney or agent of record at the USPTO: Hamilton, Brook, Smith & Reynolds, P.C., 530 Virginia Road, P.O. Box 9133, Concord, MA 01742-9133, United States.

Petitioner consents to electronic service at the address provided above for lead and back-up counsel. A Power of Attorney is filed concurrently herewith under 37 C.F.R. § 42.10(b).

III. FEES

The Office is authorized to charge the fee in 37 C.F.R. § 42.15(a) to Deposit Account No. 02-0384 and any additional fees that are due.

IV. REQUIREMENTS UNDER 37 C.F.R. § 42.104

A. *Grounds for Standing*

Petitioner certifies that the '572 Patent is eligible for IPR and that Petitioner is not barred or otherwise estopped.

B. *Priority Date*

The '572 Patent was filed as PCT No. PCT/EP2013/067904 on August 29, 2013, and claims priority to EP 12183256, filed on September 6, 2012. EX1001, Codes 22, 86, 30. Petitioner assumes without conceding that the '572 Patent is entitled to a priority date of September 6, 2012.

C. *Prior Art*²

Exhibit 1005: WO 2012/112124 A1 to Teo ("*Teo*") was filed as International Application Number PCT/SG2012/000045 on February 14, 2012, designated the

² Petitioner understands that Patent Owner believes the '572 Patent is entitled to pre-AIA treatment. If the '572 Patent is entitled to AIA treatment, *Teo*, RFC 4279,

United States, and was filed and published in English. EX1005, Codes 22, 25, 26. *Teo* has an international publication date of August 23, 2012. *Id.*, Code 43. *Teo* qualifies as prior art under at least (pre-AIA) 35 U.S.C. §§ 102(a) and 102(e).

Exhibit 1006: United States Patent Application Publication No. 2013/0067552 to Hawkes (“*Hawkes*”) was filed as Application No. 13/288,949 on November 3, 2011. *Hawkes* qualifies as prior art under at least (pre-AIA) 35 U.S.C. § 102(e).

Exhibit 1007: RFC 4279 is a standards-track paper entitled “Pre-Shared Key Ciphersuites for Transport Layer Security (TLS),” that was submitted by Nokia and Siemens to the Internet Engineering Task Force. RFC 4279 was published on December 6, 2005. EX1003, ¶ 87 (citing Appendices 1-3 to EX1003). RFC 4279 qualifies as prior art under at least (pre-AIA) 35 U.S.C. §§ 102(a) and 102(b).

Exhibit 1011: United States Patent Application Publication No. 2001/0019614 to Madoukh (“*Madoukh*”) was filed as Application No. 09/693,605 on October 20, 2000. *Madoukh* was published on September 6, 2001. *Madoukh* qualifies as prior art under at least (pre-AIA) 35 U.S.C. §§ 102(a), 102(b), and 102(e).

Madoukh, S3-070234, *Kumar*, *Park*, and *Thakare* are still prior art under at least 35 U.S.C. § 102(a)(1), and *Hawkes* is still prior art under at least 35 U.S.C. § 102(a)(2).

Exhibit 1013: Document number S3-070234 to 3GPP TSG SA WG3 Security meeting #46b (“S3-070234”) is a 3GPP standards submission submitted by Nokia and Siemens to 3GPP. S3-070234 was published on March 21, 2007. EX1019, ¶¶ 45-52. S3-070234 qualifies as prior art under at least (pre-AIA) 35 U.S.C. §§ 102(a) and 102(b).

Exhibit 1016: United States Patent Application Publication No. 2007/0171910 to Kumar (“*Kumar*”) was filed as Application No. 11/538,222 on October 3, 2006. *Kumar* was published on July 26, 2007. *Kumar* qualifies as prior art under at least (pre-AIA) 35 U.S.C. §§ 102(a), 102(b), and 102(e).

Exhibit 1017: United States Patent Application Publication No. 2009/0016524 to Park (“*Park*”) was filed as Application No. 12/147,967 on June 27, 2008. *Park* was published on January 15, 2009. *Park* qualifies as prior art under at least (pre-AIA) 35 U.S.C. §§ 102(a), 102(b), and 102(e).

Exhibit 1018: United States Patent Application Publication No. 2009/0181643 to Thakare (“*Thakare*”) was filed as Application No. 12/255,509 on October 21, 2008. *Thakare* was published on July 16, 2009. *Thakare* qualifies as prior art under at least (pre-AIA) 35 U.S.C. §§ 102(a), 102(b), and 102(e).

D. Identification of Challenge and Statement of Precise Relief Requested

Petitioner requests IPR of Claims 1-17 of the '572 Patent based on the following grounds:

Ground	Claims	Prior Art
1	1-2, 14	<i>Teo</i> in view of <i>Madoukh</i>
2	3-5, 15-17	<i>Teo</i> in view of <i>Madoukh</i> and <i>Hawkes</i>
3	6-9	<i>Teo</i> in view of <i>Madoukh</i> and RFC 4279
4	10	<i>Teo</i> in view of <i>Madoukh</i> , RFC 4279, and <i>Kumar</i>
5	11-12	<i>Teo</i> in view of <i>Madoukh</i> and S3-070234
6	13	<i>Teo</i> in view of <i>Madoukh</i> and <i>Thakare</i>

Submitted with this Petition is a declaration of Dr. Angelos Keromytis (EX1003), a qualified technical expert. EX1003, ¶¶ 61-70. Dr. Keromytis' curriculum vitae is attached as Exhibit 1004.

V. INSTITUTION IS PROPER UNDER § 314(A)

The factors in *General Plastic Industrial Co., Ltd. v. Canon Kabushiki Kaisha*, IPR2016-01357, Paper 19 (P.T.A.B. Sept. 6, 2017) favor institution. This is the first and only petition challenging the '572 Patent. The factors in *Apple Inc.*

v. Fintiv, Inc., IPR2020-00019, Paper 11 at 6 (P.T.A.B. Mar. 20, 2020) (“*Fintiv-I*”) (precedential) also favor institution. Petitioner submits that there is no currently co-pending litigation involving the ’572 Patent which would create any cognizable milestones that may impact the judicial efficiency of the Board issuing a final determination within the statutory one-year limit. To the extent Koninklijke KPN N.V. (“Patent Owner”) raises § 314(a) arguments in a Preliminary Response, Petitioner respectfully requests the opportunity to reply prior to institution to address such arguments.

VI. INSTITUTION IS PROPER UNDER § 325(D)

None of the *Becton, Dickinson* factors weigh in favor of discretionary denial under § 325(d). *Becton, Dickinson & Co. v. B. Braun Melsungen AG*, IPR2017-01586, Paper 8 (P.T.A.B. Dec. 15, 2017) (precedential). *Teo, Hawkes*, RFC 4279, S3-070234, *Madoukh, Kumar, Park*, and *Thakare* are new references that were not disclosed, cited, or considered during prosecution. This Petition thus does not present a situation in which “the same or substantially the same prior art or arguments previously were presented to the Office.” 35 U.S.C. § 325(d). The Board should, therefore, grant this Petition.

VII. OVERVIEW OF THE '572 PATENT

A. *Description of the '572 Patent*

The '572 Patent is directed to “a method for establishing a device-to-device (D2D) communication session between mobile devices.” EX1001, 1:12-14. The '572 Patent explains that it is desirable to have “more control over the D2D communication between mobile devices which are connectable to a mobile network.” *Id.*, 2:11-25.

To this end, the '572 Patent describes using an “*initiation key*” in a “*key agreement procedure*,” which is a procedure performed between the mobile devices “via the D2D communication channel, e.g., by exchanging messages between the mobile devices, with the messages together constituting the key agreement procedure.” *Id.*, 3:64-4:5. This key agreement procedure results in a valid session key “provided that each respective mobile device uses the same initiation key in the key agreement procedure.” *Id.*, 4:8-13. “The session key constitutes a key used for cryptographically protecting messages in a communication session.” *Id.*, 4:13-15.

The initiation key “is associated with a validity period,” which “indicates a period of time in which the initiation key is deemed to be valid for use in establishing the D2D communication session.” *Id.*, 3:47-54. The mobile devices holding the initiation key will check the current time when a D2D communication session is requested; if the current time is “in the validity period, the initiation key is used in

performing a key agreement procedure between the mobile devices.” *Id.*, 3:54-63. Further, the initiation key is “preloaded” in that it is loaded “on a mobile device before establishing the D2D communication session.” *Id.*, 3:32-39.

B. *The ’572 Patent’s Prosecution History*

The PCT application that led to the ’572 Patent was filed as a national stage entry in the U.S. on February 27, 2015. EX1002, 356 (transmittal of application). The Patent Office issued a first office action on December 20, 2015, in which the Examiner rejected then-pending claims 18-34. *Id.*, 88-104. The Examiner rejected Claims 18-27 and 30-34 over U.S. Patent Publication 2013/0013926 to Hakola in view of U.S. Patent Publication 2013/0227655 to Vanderveen. *Id.*, 93-100, and rejected claims 28-29 over Hakola in view of Vanderveen and U.S. Patent Publication 2009/00320102 to Ou. *Id.*, 100-101. In response to the Office Action, applicant filed an amendment to the claims on March 16, 2016, to specify that the recited “key agreement procedure” results in a session key “*based on a match of the respective initiation keys* used by each of the mobile devices”:

18. Method for establishing a device-to-device (D2D) communication session between mobile devices which are mutually connectable via a D2D communication channel and individually connectable to a mobile network, comprising:

preloading an initiation key on each of the mobile devices, the initiation key being associated with a validity period; and on each of the mobile devices;

verifying a validity of the initiation key based on a current time;

if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key agreement procedure between the mobile devices over the D2D communication channel, the key agreement procedure resulting in the session key **based on a match of the respective initiation keys** ~~if the initiation key~~ used by each of the mobile devices ~~matches~~; and

establishing the D2D communication session over the D2D communication channel based on the session key.

Id., 66. In the remarks accompanying this amendment, applicant argued that Hakola “discloses different keys for each mobile device”—thus, Hakola fails to teach “preloading an initiation key on each of the mobile devices,” and “the key agreement procedure resulting in the session key based on a match of the respective initiation keys used by each of the mobile devices.” *Id.*, 72-73 (emphasis original).

The Examiner found these remarks persuasive and issued a notice of allowance on May 11, 2016. *Id.*, 25. The Examiner also suggested an additional amendment adding the claim limitation “*requesting a further initiation key via the mobile network if no initiation key is deemed valid*,” which applicant authorized. *Id.*, 30-31, 40.

C. *Level of Ordinary Skill in the Art*

A person of ordinary skill in the art at the time of the alleged invention of the ’572 Patent would have had a degree in electrical engineering, computer science, or a similar discipline, with at least 2-4 years of relevant industry or research experience in the network security industry. EX1003, ¶¶ 66, 68. A POSITA would also have

familiarity with the wireless standards and protocols relating to mobile communications and the security of such communications. *Id.*, ¶¶ 65, 68. This definition is approximate, and more education may substitute for industry experience or vice versa. *Id.*

D. Claim Listing

Exhibit 1008 is a claim listing that enumerates each claim limitation. Bracketed notations (*e.g.*, [a], [b], etc.) will be used to refer to individual limitations.

VIII. PRIOR ART SUMMARY

A. Teo (EX1005)

Teo describes a system and method for establishing, between two mobile communication terminals, direct, secure communications that are encrypted using a “determined encryption key.” EX1005, 8:1-21. *Teo* describes a “Pre-shared key scenario” for generating the “encryption key,” wherein the terminals that want to establish a direct communication first receive the same pre-shared key, called “DMK” (Direct Communications Master Key), from a base station to which the terminals are connected. *Id.*, 31:6-15, 62:29-30. The base station also sends a “key_lifetime” parameter associated with the DMK to the terminals. *Id.*, 14:21-15:2, Fig. 5 (Step 505). As discussed above in Section VII.B, applicant argued during prosecution that the ’572 Patent was novel over the prior art because the prior art “discloses different keys for each mobile device.” *See supra*, Section VII.B;

EX1002, 72-73 (emphasis original). *Teo* does not have this deficiency, because it discloses sending the same DMK to the two mobile communication terminals. EX1005, 13:4-14:19, Fig. 5 (Step 504).

Once the terminals receive the DMK, they are able to establish direct communication with each other. In doing so, the terminals use the DMK to generate a set of additional keys—DAK, DCMAC (Direct Communication Cipher-based Message Authentication Code), and DTEK (Direct Communication Traffic Encryption Key). EX1005, 32:16-21. The terminals then use the keys to generate, and subsequently check, “message digests.” *Id.*, 32:16-30, 35 (θ_{HR-MS1} entry). Successful checks of the message digests indicate that the terminals have received the same DMK and that the terminals have computed the same DAK, DCMAC, and DTEK. EX1003, ¶ 80. The DAK, DCMAC, and DTEK are then used for direct communications. For example, the DTEK is “used to encrypt data in direct communications.” *Id.*, 38:24-25.

B. *Hawkes* (EX1006)

Hawkes is directed to a system for managing security credentials associated with a mobile device, where the security credential is later used to authenticate the mobile device for network services. EX1006, Abstract. *Hawkes* describes hardware components that store the security credential, such as a “universal integrated circuit card (UICC).” *Id.*, [0098]. *Hawkes* also describes the hardware components that

facilitate wireless communication with other entities, such as a “system-in-package or system-on-chip device (e.g., a mobile station modem (MSM)).” *Id.*, [0099]-[0100].

C. RFC 4279 (EX1007)

RFC 4279 describes protocols to support authentication of clients to servers using pre-shared keys (PSKs). When using PSK-based authentication, the client and server must first agree to a particular PSK that is to be used. EX1007, 4-5. Accordingly, the client may send a “PSK identity” to the server, thereby “indicat[ing] which key to use.” *Id.*, 5.

D. *Madoukh* (EX1011)

Madoukh describes a computer system that includes a number of components for managing encrypted data, security information, and keys. EX1011, Abstract. For example, the disclosed computer system “includes a key lifetime manager operable to monitor encryption key expiration dates and request new encryption keys upon the expiration of old encryption keys.” *Id.*, [0007].

E. S3-070234 (EX1013)

S3-070234 describes implementing “counters related to limiting key usage, e.g. to limit the number of key derivations from one parent key.” EX1013, 1-2.

F. *Kumar* (EX1016)

Kumar describes peer-to-peer communication in an ad-hoc wireless network using pre-shared keys to generate session keys. EX1016, Abstract. *Kumar* explains that the pre-shared keys may be associated with a service set identifier (SSID), which identifies an 802.11 wireless network. *Id.*, [0057], Fig. 2.

G. *Park* (EX1017)

Park describes distributing keys within an ad-hoc peer-to-peer network, wherein the keys may have different validity periods (*e.g.*, one month, six hours, one hour), after which the key expires. EX1017, Abstract, [0050], [0052], [0059], [0064].

H. *Thakare* (EX1018)

Thakare describes packet-based communication wherein data packets are encrypted according to an encryption key. EX1018, [0008], [0032]. *Thakare* explains that a new encryption key may be requested if data packets are not successfully authenticated. *Id.*, [0008]-[0009].

IX. CLAIM CONSTRUCTION

Without conceding that the claims satisfy 35 U.S.C. § 112, Petitioner respectfully submits that the Board need not expressly construe any term because the prior art invalidates the claims under any plausible construction, in accordance with 37 C.F.R. § 41.100(b). EX1003, ¶ 60.

X. ASSERTED GROUNDS OF INVALIDITY

A. Ground 1: *Teo* in view of *Madoukh* Renders Obvious Claims 1-2 and 14.

1. Motivation to Combine

A POSITA would have been motivated to combine *Teo* with *Madoukh*.

Teo discloses a system wherein two mobile communication terminals receive both a pre-shared key, called “DMK,” and the DMK’s lifetime, called “key_lifetime.” EX1005, 13:19-15:2. *Madoukh* discloses a computer system that “includes a key lifetime manager operable to monitor encryption key expiration dates and request new encryption keys upon the expiration of old encryption keys,” as well as “deactivate the expired keys.” EX1011, [0007]-[0008].

A POSITA would have been motivated to combine *Teo*’s system for receiving and using keys with associated lifetimes with *Madoukh*’s “key lifetime manager” for monitoring the expiration of keys, requesting new keys when old keys have expired, and deactivating expired keys. Such a combination would have involved combining prior art elements according to known methods to yield predictable results. *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 416 (2007); EX1003, ¶ 103. A POSITA would have understood that *Madoukh*’s key lifetime manager could be implemented in any device that stores keys with some designated lifetime, such as *Teo*’s mobile communication terminals. EX1003, ¶ 103. The combination of *Teo* with *Madoukh* would have been predictable and foreseeable because the combination merely

involves incorporating known features that are explicitly disclosed by *Madoukh* and would have been understood by a POSITA as likely present if not explicitly disclosed by *Teo*. *Id.* A POSITA would have understood that *Teo*'s DMK would expire (as indicated by the `key_lifetime` value associated with the DMK) and one would need to implement a component for tracking the DMK's expiration, requesting a new DMK upon such expiration, and deactivating the expired DMK, such as *Madoukh*'s key lifetime manager. *Id.*

2. Reasonable Expectation of Success

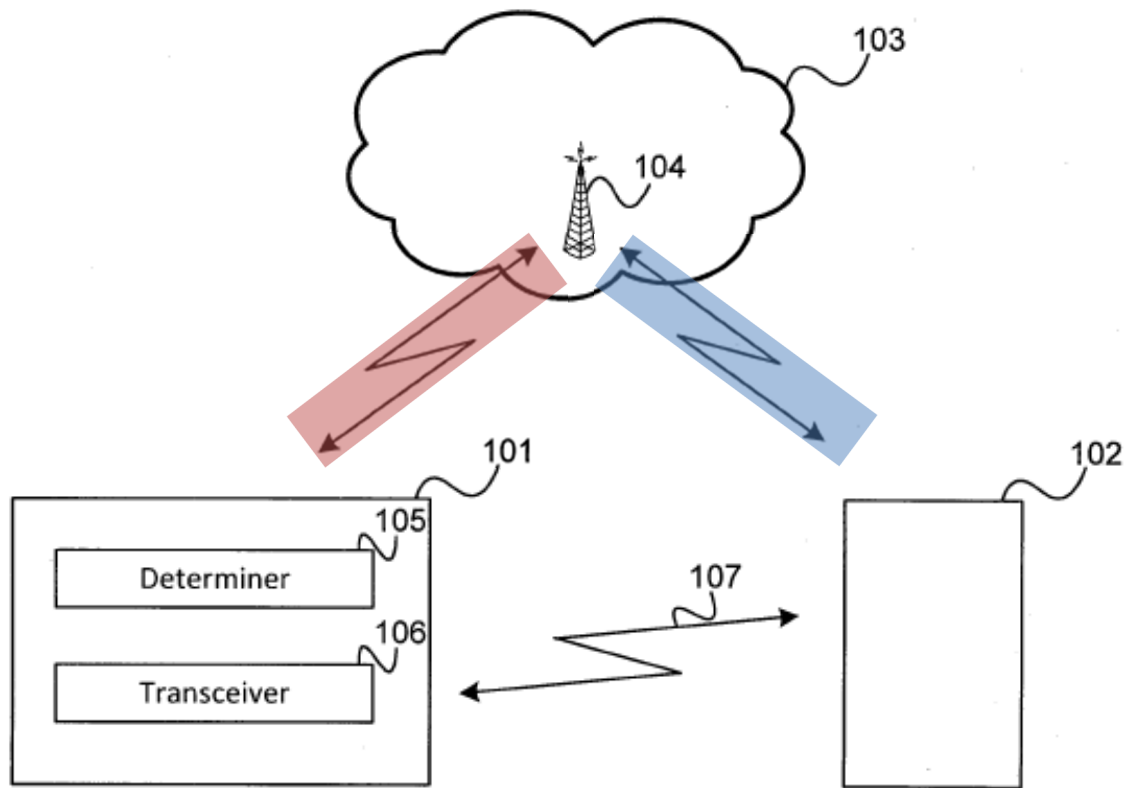
A POSITA would have reasonably expected success when combining *Teo* with *Madoukh*. EX1003, ¶ 104. As discussed above in Section X.A.1, a POSITA would have recognized that *Madoukh*'s key lifetime manager could be implemented in any device that stores keys with some designated lifetime, such as *Teo*'s mobile communication terminals. *Id.*; see also *supra*, Section X.A.1. Indeed, a POSITA would have understood that *Teo*'s terminals would need to some sort of component for managing DMKs and their lifetime, as it is a fundamental aspect of cryptographic key management that keys should expire and be replaced. EX1003, ¶ 104 (citing EX1009, 183). Thus, a POSITA would have reasonably expected success in implementing the key lifetime manager as detailed by *Madoukh*. *Id.*

3. Claim 1

i. [1p] Method for establishing a device-to-device (D2D) communication session between mobile devices which are mutually connectable via a D2D communication channel and individually connectable to a mobile network, comprising:

To the extent the preamble is limiting, *Teo* discloses the preamble. *Teo* discloses “a method for setting up a communication between a communication terminal of a cellular mobile communication system and another communication terminal of the cellular mobile communication system.” EX1005, 8:1-4. Figure 1 of *Teo*, copied and annotated below, shows an example of *Teo*’s cellular mobile communication system, which comprises communication terminals 101 and 102 and communication network 103:

FIG 1



Id., Fig. 1 (annotated), 4:11-17.

Teo's communication terminals disclose "*mobile devices.*" *Teo* explains that "communication terminal 101 is a (mobile) communication terminal." *Id.*, 4:10-11, 10:4-6 (describing a communication system that comprises "a first mobile terminal...[and] a second mobile terminal."). And *Teo*'s terminals are "*mutually connectable via a D2D communication channel,*" at least because these terminals are able to directly communicate with each other via a radio interface. *Id.*, 4:26-30 ("The communication terminal 101 further comprises a transceiver 106 configured to *perform secure communication with the other communication terminals [102]*

via the radio interface 107 between the communication terminal 101 and the other communication terminal 102....” (emphasis added)), 5:11-13. Because *Teo*’s radio interface 107 facilitates direct communication between the communication terminals, the radio interface 107 is a “*a D2D communication channel.*”

Teo’s terminals are “*individually connectable to a mobile network,*” at least because these terminals are each connected to communication network 103 via base station 104. As shown above in annotated Figure 1 of *Teo*, terminal 101 is connected with communication network 103 via a first connection with base station 104 (as shown with the red annotation), and terminal 102 is connected with communication network 103 via a second connection with base station 104 (as shown with the blue annotation).

Teo’s method for setting up direct communication between the terminals discloses a “[*m*]ethod for establishing a device-to-device (D2D) communication session between mobile devices.” *Teo*’s method includes first determining an encryption key for secure communication. *Id.*, 8:12-15, Fig. 2 (step 201). The terminals then perform secure communication with each other via the radio interface between the two terminals by using the determined encryption key. *Id.*, 8:17-21, Fig. 2 (step 202). “[T]he secure communication is ***direct communication*** between the communication terminal and the other communication terminal.” *Id.*, 5:11-13 (emphasis added).

For at least these reasons, *Teo* discloses the preamble.

ii. [1a] preloading an initiation key on each of the mobile devices, the initiation key being associated with a validity period;

Teo discloses Claim Element [1a] through at least its disclosure of a base station transmitting a “pre-shared key DMK” (Direct Communication Master Key) (*i.e.*, “*initiation key*”) and its associated “lifetime” (*i.e.*, “*validity period*”) to different mobile communication terminals before the terminals establish a direct communication session. *See, e.g.*, EX1005, 18:7-19:3 (referring to the “Pre-shared key scenario” for establishing a direct communication session “where it is assumed that HR-MS1 and HR-MS2 shares a ***key prior to direct communications.***” (emphasis added)).

Teo explains that the mobile communication terminals obtain the pre-shared DMK from the base station to which the terminals are connected. After a first mobile communication terminal (*i.e.*, HR-MS1) and a second communication terminal (*i.e.*, HR-MS2) agree to directly communicate, the base station to which the terminals are connected (*i.e.*, HR-BS) “generates the DMK” and sends the DMK to both HR-MS1 and HR-MS2. *Id.*, Fig. 5 (Step 504), 13:4-14:19. HR-MS1 and HR-MS2 each decrypt the message it received from HR-BS and “obtains DMK and its lifetime key_lifetime.” *Id.*, 14:21-15:2, Fig. 5 (Step 505).

Teo's DMK is an "*initiation key*" because the DMK is necessary for the devices to initiate D2D communications. As will be discussed in more detail below with respect to Claim Element [1d], *Teo* uses the DMK to derive another key, the DTEK, which is used to encrypt messages during direct communication between the mobile communication terminals. *See, e.g., id.*, 37:20-23, 38:1-7, 38:24-25. The DMK is therefore an "*initiation key*" because it initiates the terminals' ability to directly communicate with each other by facilitating the generation of other keys necessary for direct communication, such as the DTEK. EX1003, ¶ 141. This is consistent with the '572 Patent, which states that the "*initiation key*" "essentially functions as an authorization token in that a mobile device needs the initiation key to establish the D2D communication session." EX1001, 4:28-30.

Teo's DMK is "*preload[ed]*" because it is obtained by the terminals before a direct communication session is established. Indeed, *Teo* refers to the DMK as a "*pre-shared* key DMK." EX1005, 10:27-28 (emphasis added). Further, *Teo* describes that the mobile communication terminals may establish a direct communication only after they obtain the DMK. *See, e.g., id.*, 18:7-19:3 (referring to the "Pre-shared key scenario...where it is assumed that HR-MS1 and HR-MS2 shares a *key prior to direct communications*." (emphasis added)); 63:9-13. This is because other keying materials used during direct communications, such as the DTEK, are derived from the DMK. *See id.*, 37:20-25. This is consistent with the

'572 Patent, which states that “the term preloading refers to a loading of the initiation key on a mobile device before establishing the D2D communication session.” EX1001, 3:34-37.

And *Teo*'s DMK is “*preload[ed]...on each of the mobile devices*” because the base station transmits the same DMK to each of the two mobile communication terminals. As discussed above, *Teo* explains that the base station “generates *the* DMK” and sends the DMK to both HR-MS1 and HR-MS2 in encrypted messages. *Id.*, Fig. 5 (Step 504) (emphasis added), 13:4-14:19. As will be discussed in more detail below with regard to Claim Element [1d], the same DMK being loaded to each of the mobile communication terminals allows the terminals to establish direct communication with each other. *See infra*, Section X.A.3.v. Thus, *Teo* discloses the very element of the '572 Patent that applicant argued was novel over the prior art. *See supra*, Section VII.B (explaining that applicant argued during prosecution that the '572 Patent was novel over the prior art because the prior art “discloses different keys for each mobile device.” (emphasis original)); *see also* EX1002, 72-73.

Finally, *Teo*'s DMK is “*associated with a validity period*” because the DMK has an associated lifetime, “key_lifetime.” When *Teo*'s terminals decrypt the messages from the base station containing the DMK, the terminals obtain both the DMK “and its lifetime key_lifetime.” *Id.*, 14:25-26, 15:1-2. A POSITA would have

understood the “key_lifetime” to be some value that represents the duration (*e.g.*, in seconds) for which the DMK is valid. EX1003, ¶ 144 (citing EX1015, 35). The terminals also receive timestamps from the base station (*i.e.*, $T_{HR-BS'}$ and $T_{HR-BS''}$) in the messages containing the DMK. EX1005., 13:19-14:19, 17, 18. A POSITA would have understood that the DMK is valid from the period starting at the time indicated by the received timestamp through the expiration of the DMK’s lifetime as indicated by the “key_lifetime” value. EX1003, ¶ 144. This understanding is consistent with the ’572 Patent, which states that the “validity period indicates a period in time in which the initiation key is deemed to be valid for use in establishing the D2D communication session.” EX1001, 3:52-54.

iii. [1b] and on each of the mobile devices: verifying a validity of the initiation key based on a current time;

Teo renders obvious Claim Element [1b] in light of *Madoukh*. *Teo* teaches that its pre-shared DMK (*i.e.*, the “initiation key”) has an associated lifetime, “key_lifetime.” EX1005, 14:21-15:2, Fig. 5 (Step 505). And *Madoukh* discloses a “key lifetime manager operable to monitor encryption key expiration dates and request new encryption keys upon the expiration of old encryption keys.” EX1011, [0007].

A POSITA would have understood that *Teo*’s “key_lifetime” reflects the duration for which the DMK is valid. *See supra*, Section X.A.3.ii. Accordingly, a

POSITA would have understood that in implementing *Teo*, one would need to verify the validity of the DMK based on the current time before using the DMK. EX1003, ¶ 146. And it would have been obvious to use the teachings of *Madoukh* in doing so. *Id.* Thus, a POSITA would have found it obvious to implement *Madoukh*'s key lifetime manager to monitor whether *Teo*'s DMK has expired by checking whether the current time falls within the range of the DMK's lifetime (*i.e.*, the time period starting at the time of the received timestamp (*e.g.*, T_{HR-BS}) through the expiration of the associated "key_lifetime"). *Id.* A POSITA would have understood that when the key lifetime manager determines that the DMK is not expired because the current time falls within the DMK's lifetime, the DMK has been verified as valid (*i.e.*, not expired). *Id.*

A POSITA would have found obvious that each mobile communication terminal that receives a DMK and associated key_lifetime value from a base station (*e.g.*, HR-MS1 and HR-MS2) would have performed this verification to validate the DMK before using it. EX1003, ¶ 147. Thus, the *Teo-Madoukh* combination renders obvious this claim element. This combination would have been obvious for additional the reasons explained above in Sections X.A.1-2.

iv. [1c] requesting a further initiation key via the mobile network if no initiation key is deemed valid;

Teo renders obvious Claim Element [1c] in light of *Madoukh*. The *Teo-Madoukh* combination renders obvious verifying the validity of *Teo*'s DMKs by using a key lifetime manager (as taught by *Madoukh*) to compare the current time to the DMKs' lifetime, "key_lifetime." See *supra*, Section X.A.3.iii. *Madoukh* also explains that the key lifetime manager is operable to "request new encryption keys upon the expiration of old encryption keys." EX1011, [0007]. It would have been obvious to a POSITA to implement *Madoukh*'s key lifetime manager in *Teo*'s mobile communication terminals such that the terminals request a new DMK from the base station (e.g., HR-BS) upon determining that a currently-held DMK has expired (i.e., is not "deemed valid") (as disclosed by *Madoukh*). EX1003, ¶ 149. This implementation would have been obvious, because a POSITA would have recognized that *Teo*'s DMKs would eventually expire and thus need to be replaced. *Id.* (citing EX1009, 183). And because *Teo* teaches that the base station is part of a "communication network" that provides service to mobile terminals, a POSITA would have understood that this request would be made "via the mobile network." EX1005, 4:14-17; EX1003, ¶ 149.

Further, it would have been obvious to a POSITA that both terminals (e.g., both HR-MS1 and HR-MS2) would have requested a new DMK upon determining

that a currently-held DMK is expired. EX1003, ¶ 150. *Teo* teaches that the base station transmits the same DMK value and associated lifetime, *key_lifetime*, to the two terminals that agree to establish direct communication. *See supra*, Section X.A.3.ii. Because both terminals would have received the same *key_lifetime* value, a POSITA would have understood that both terminals would detect the expiration of the DMK at the same or similar times. EX1003, ¶ 150. Accordingly, a POSITA would have understood that when the DMK expires, both terminals would have determined that the DMK is no longer valid and would therefore have requested a new DMK value from the base station. *Id.*

Thus, the *Teo-Madoukh* combination renders obvious Claim Element [1c]. This combination would have been obvious for the additional reasons explained above in Sections X.A.1-2.

v. [1d] if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key agreement procedure between the mobile devices over the D2D communication channel,

The *Teo-Madoukh* combination renders obvious this claim element, at least through its disclosure of generating an encryption key, DTEK (*i.e.*, “*session key*”) using the pre-shared DMK (*i.e.*, “*initiation key*”) in a “pre-shared key approach” (*i.e.*, “*key agreement procedure*”) over radio interface 107 (*i.e.*, “*D2D communication channel*”). *Teo* discloses a method for establishing direct

communication between two mobile communication terminals. *See supra*, Section X.A.3.i; EX1005, 5:11-13, 8:1-4. Establishing the direct communication involves generating an encryption key, which later encrypts the direct communications to ensure their security. *See supra*, Section X.A.3.i; EX1005, 8:17-21, 38:24-25. *Teo* discloses a “pre-shared key approach,” which is an “AKE [Authenticated Key Exchange] protocol[]” for generating the encryption key. EX1005, 18:7-19:3, 31:6-8.

In the pre-shared key approach, a first mobile communication terminal (*e.g.*, HR-MS1) and a second mobile communication terminal (*e.g.*, HR-MS2) each use the pre-shared DMK to compute three new keys, DAK, DCMAC, and DTEK. EX1005, 32:16-21 (describing HR-MS1 computing these keys), 33:1-7 (describing HR-MS2 computing these keys). The DAK is derived from the DMK. *Id.*, 37:23-25, 32:17-18. The DCMAC and DTEK are then derived from the DAK. *Id.*, 38:1-7, 32:19, 32:21. Because HR-MS1 and HR-MS2 have received the same DMK value, and use the same formulas and parameters to compute DAK, DCMAC, and DTEK, respectively, *Teo* discloses that the HR-MS2 generates the same DAK, DCMAC, and DTEK values as those generated by the HR-MS1. EX1003, ¶ 154; EX1005, 32:15-33:7 (showing HR-MS1 and HR-MS2 use the same formulas and parameters to compute DAK, DCMAC, and DTEK, respectively).

The terminals then exchange a series of messages and perform a series of checks to verify that they have computed the same sets of keys. That is, the terminals use the DCMAC key to generate, and subsequently check, “message digests,” (e.g., $\theta_{\text{HR-MS1}}$, $\theta_{\text{HR-MS2}}$, and $\theta_{\text{HR-MS1}}$). For example, HR-MS1 generates a first message digest $\theta_{\text{HR-MS1}}$ “using the DCMAC key,” and sends $\theta_{\text{HR-MS1}}$ to HR-MS2 in a message called “DirectComms_KeyAgreement_MSG_#1.” *Id.*, 32:23-30, 35 (explaining that $\theta_{\text{HR-MS1}}$ is a “[m]essage digest calculated using DCMAC key.”). Upon receiving the “DirectComms_KeyAgreement_MSG_#1” message, HR-MS2 then uses the DCMAC it computed “to check $\theta_{\text{HR-MS1}}$.” *Id.*, 33:7-8. As Dr. Keromytis explains in more detail in his declaration, HR-MS2 performs this “check” by independently computing $\theta_{\text{HR-MS1}}$ using the DCMAC calculated by the second terminal. EX1003, ¶¶ 154-155; *see also* EX1005, 38:14-16. Because the DCMACs held by the HR-MS1 and HR-MS2 are expected to have the same value (because these keys are derived from the DAK, which is derived from the pre-shared DMK), a POSITA would have understood that HR-MS2 would have successfully “checked” $\theta_{\text{HR-MS1}}$ if its independent calculation of $\theta_{\text{HR-MS1}}$ matched the value received from HR-MS1. EX1003, ¶ 155. This match indicates that the two terminals share the same DMK value and have generated the same DAK, DCMAC, and DTEK keys. *Id.*

After verifying the received $\theta_{\text{HR-MS1}}$, HR-MS2 uses the DCMAC to compute a second message digest, $\theta_{\text{HR-MS2}}$, which is then sent to, and checked by, HR-MS1 in

the same manner described in the previous paragraph. EX1005, 33:8-30, 36. Fig. 12 (Step 1203); EX1003, ¶¶ 156-157. And after verifying the received $\theta_{\text{HR-MS2}}$, HR-MS1 uses the DCMAC to compute a third and final message digest, $\theta_{\text{HR-MS1}}$, which is then sent to, and checked by, HR-MS2 in the same manner described in the previous paragraph. EX1005, 33:30-34:19, 36, Fig. 12 (Step 1204); EX1003, ¶¶ 157-158. Upon a successful check, HR-MS2 “is ready for direct communications with HR-MS1” (*i.e.*, the first mobile communication terminal). EX1005, 34:19-21.

*Teo's pre-shared key approach just discussed discloses “generating a session key using the initiation key by using the initiation key in performing a key agreement procedure between the mobile devices over the D2D communication channel,” as recited in Claim 1. As discussed above, Teo describes how the mobile communication terminals (e.g., HR-MS1 and HR-MS2) use the DMK (i.e., the “initiation key”) to generate a DTEK (i.e., the “session key”) during the pre-shared key approach. EX1005, 32:17-21, 38:1-7. Teo's pre-shared key approach is a “key agreement procedure” because the pre-shared key approach involves the two mobile communication terminals agreeing to keys used for direct communications (i.e., DAK, DCMAC, and DTEK) by confirming that the two mobile communication terminals have generated the same keys. EX1003, ¶ 159. Indeed, the messages exchanged during this procedure, called “DirectComms_***KeyAgreement**” messages

(emphasis added), confirm that the pre-shared key approach would be considered a “*key agreement procedure*.” *Id.*; EX1005, 32:23-30, 33:14-24, 34:5-15.

Further, *Teo* explains that the DTEK “is used to encrypt data in direct communications.” *Id.*, 38:24-25. Accordingly, a POSITA would have understood the DTEK to be a “*session key*” because it facilitates a direct communication session between the two terminals by encrypting the communications of that session. EX1003, ¶ 159. This encryption functionality is consistent with the ’572 Patent’s description of the “*session key*.” *See* EX1001, 4:13-17 (“The session key constitutes a key used for cryptographically protecting messages in a communication session, such as confidentiality protection using encryption....”).

Teo discloses that the “encryption key” (*i.e.*, DTEK) is determined “by exchanging messages with the other communication terminal via the radio interface between the communication terminal and the other communication terminal” (*i.e.*, via “*the D2D communication channel*”). EX1005, 5:23-27. Thus, *Teo*’s disclosure of the mobile communication terminals generating the DTEK (*i.e.*, “*session key*”) during the pre-shared key approach (*i.e.*, “*key agreement procedure*”) based on the pre-shared DMK (*i.e.*, “*initiation key*”) teaches “*generating a session key using the initiation key by using the initiation key in performing a key agreement procedure between the mobile devices over the D2D communication channel.*”

Further, a POSITA would have understood that the pre-shared key approach discussed above would have occurred only after the mobile communication terminals determine that the DMK (*i.e.*, “*initiation key*”) is valid, *e.g.*, based on comparing the current time with the DMK’s key_lifetime relative to the time stamp indicating the start of DMK’s validity period (*e.g.*, T_{HR-BS}). EX1003, ¶ 162; *see supra*, Sections X.A.3.iii-iv. Thus, a POSITA would have understood that the pre-shared key approach is performed only “*if the initiation key is deemed valid,*” as recited in Claim 1. EX1003, ¶ 162.

vi. [1e] the key agreement procedure resulting in the session key based on a match of the respective initiation keys used by each of the mobile devices;

Teo discloses this claim element. *Teo* describes using the DCMAC to generate and verify message digests (*e.g.*, θ_{HR-MS1} , θ_{HR-MS2} , and θ_{HR-MS1}') sent by one mobile communication terminal to the other. *See supra*, Section X.A.3.v. A POSITA would have understood that these message digests are verified by the receiving terminal only if said receiving terminal has independently generated the same DCMAC value as the DCMAC value used to generate the message digest at the sending mobile communication terminal. *See supra*, Section X.A.3.v; EX1005, 37:7-8 (explaining that the second mobile communication terminal “uses DCMAC to check θ_{HR-MS1} ”); EX1003, ¶ 163. A POSITA would have understood that successful verification of these messages indicates that the mobile communication

terminals have received and used matching DMK values, because the terminals use the DMK in the same formulas to generate the DAK, and then use the DAK in the same formulas to generate the DCMAC, as well as the DTEK. *Id.*, ¶ 164; EX1005, 37:23-25, 38:1-6, 32:16-33:8 (showing that HR-MS1 and HR-MS2 (i) use the same formula and parameters to compute the DAK using the DMK, (ii) use the same formula and parameters to compute the DCMAC using the DAK, and (iii) use the same formula and parameters to compute the DTEK using the DAK).

Thus, *Teo*'s pre-shared key approach for generating the DTEK is successfully completed only if the DMKs held by each of the mobile communication terminals match. EX1003, ¶ 165. If the DMKs do not match, the various “checks” made by the mobile communication terminals on the received message digests (*e.g.*, $\theta_{\text{HR-MS1}}$, $\theta_{\text{HR-MS2}}$, and $\theta_{\text{HR-MS1}}'$) would fail. *Id.* Accordingly, *Teo*'s pre-shared key approach to generating the DTEK (*i.e.*, “*session key*”) results in a valid DTEK only when the DMK (*i.e.*, “*initiation key*”) held by each terminal is the same value (*i.e.*, “*match[es]*”). *Id.* *Teo* therefore discloses this claim element.

Applicant argued that the '572 Patent was novel over the prior art cited during prosecution because Hakola “discloses different keys for each mobile device”—thus, Hakola fails to teach “preloading an initiation key on each of the mobile devices,” and “the key agreement procedure resulting in the session key based on a match of the respective initiation keys used by each of the mobile devices.” *See*

supra, Section VII.B; EX1002, 72-73 (emphasis original). As with Claim Element [1a], *Teo* discloses sending the same pre-shared key DMK to two mobile communication terminals (*i.e.*, “*preloading an initiation key on each of the mobile devices*”). And *Teo* discloses “*the key agreement procedure resulting in the session key based on a match of the respective initiation keys used by each of the mobile devices,*” at least because it discloses a pre-shared key approach for generating an encryption key DTEK that is dependent on both mobile communication terminals having received the *same* DMK.

vii. [1f] establishing the D2D communication session over the D2D communication channel based on the session key.

Teo discloses this claim element at least because of its teaching that the encryption key, DTEK (*i.e.*, “*session key*”), is used to establish direct communication between mobile communication terminals (*i.e.*, a “*D2D communication session*”). *Teo* generally discloses a two-step method wherein (1) an encryption key for secure direct communication is determined and (2) mobile communication terminals perform secure direct communication with each other based on the determined encryption key. *See supra*, Section X.A.3.i; *see also* EX1005, 8:12-21. As with Claim Element [1d], *Teo* discloses the generation of the DTEK (*i.e.*, “*session key*”), which is “used to encrypt data in direct communications.” EX1005, 38:24-25. A POSITA would have therefore understood

Teo's DTEK to be the “encryption key” used during secure communication between the mobile communication terminals. EX1003, ¶ 166. And *Teo* discloses that the secure direct communication between the two mobile communication terminals occurs via a radio interface (*i.e.*, “D2D communication channel”). *See supra*, Section X.A.3.i.

Thus, *Teo* discloses establishing a secure direct communication between mobile communication terminals (*i.e.*, “establishing the D2D communication session”) via a radio interface (*i.e.*, “over the D2D communication channel”) based on a determined encryption key, DTEK (*i.e.*, “based on the session key”). *Teo* therefore discloses this claim element.

4. Claim 2. Method according to claim 1, wherein the preloading the initiation key comprises providing the initiation key to each of the mobile devices via the mobile network when each respective mobile device is connected to the mobile network.

Teo discloses Claim 2 because it teaches a base station (*i.e.*, “mobile network”) sending the pre-shared DMK (*i.e.*, “initiation key”) to the mobile communication terminals (*i.e.*, “mobile devices”). *Teo* discloses a process whereby two mobile communication terminals (*e.g.*, HR-MS1 and HR-MS2) obtain a DMK from a base station after the terminals agree to establish direct communication with each other. *See supra*, Section X.A.3.ii. Because *Teo* teaches that the base station is part of the “communication network” of *Teo*, the DMK is provided “*via the mobile network.*”

EX1005, 4:14-17. Further, the base station's ability to send the DMK to the terminals indicates that the base station provides the DMK (*i.e.*, “*initiation key*”) “*when each respective mobile device is connected to the mobile network.*” If the terminals were not connected to the base station (*i.e.*, the “*mobile network*”), the base station would be unable to send the messages that contain the DMK to the terminals. EX1003, ¶ 168.

Thus, *Teo*'s disclosure of a base station sending the DMK to two terminals teaches Claim 2.

5. Claim 14. Method according to claim 1, wherein the key agreement procedure comprises: a three-pass authentication procedure; or a use of the initiation key to encrypt a message exchange between the mobile devices for obtaining a shared secret, and a Diffie-Hellman key exchange procedure which is initiated based on the shared secret.

Teo discloses Claim 14, at least because *Teo* teaches “*wherein the key agreement procedure comprises: a three-pass authentication procedure.*”³ *Teo*'s pre-shared key approach (*i.e.*, “*key agreement procedure*”) comprises “*a three-pass authentication procedure*” at least because the pre-shared key approach involves the

³ Petitioner does not address the alternative limitation, “*or a use of the initiation key to encrypt a message exchange between the mobile devices for obtaining a shared secret, and a Diffie-Hellman key exchange procedure which is initiated based on the shared secret.*”

exchange of three messages before the mobile communication terminals are authorized for direct communication.

As with Claim Element [1d], *Teo's* pre-shared key approach involves the mobile communication terminals exchanging, in three messages (*i.e.*, “DirectComms_KeyAgreement_MSG_#1,” “DirectComms_KeyAgreement_MSG_#2,” and “DirectComms_KeyAgreement_MSG_#3”), “message digests” and subsequently “checking” the message digests. *See supra*, Section X.A.3.v; *see also* EX1005, 32:26-33, 33:17-30, 34:8-19. A POSITA would have understood that a successful “check” indicates that the terminals have generated the same DCMAC, which indicates that the terminals have received the same DMK and are thereby authenticating each other for direct communication. *See supra*, Section X.A.3.v; EX1003, ¶ 170. Thus, *Teo's* pre-shared key approach, wherein three messages are exchanged to authenticate terminals for direct communications, discloses “*a three-pass authentication procedure.*”

This understanding is consistent with the '572 Patent, which characterizes Figure 7 of the '572 Patent, copied and annotated below, as example of the “three-pass authentication procedure.”

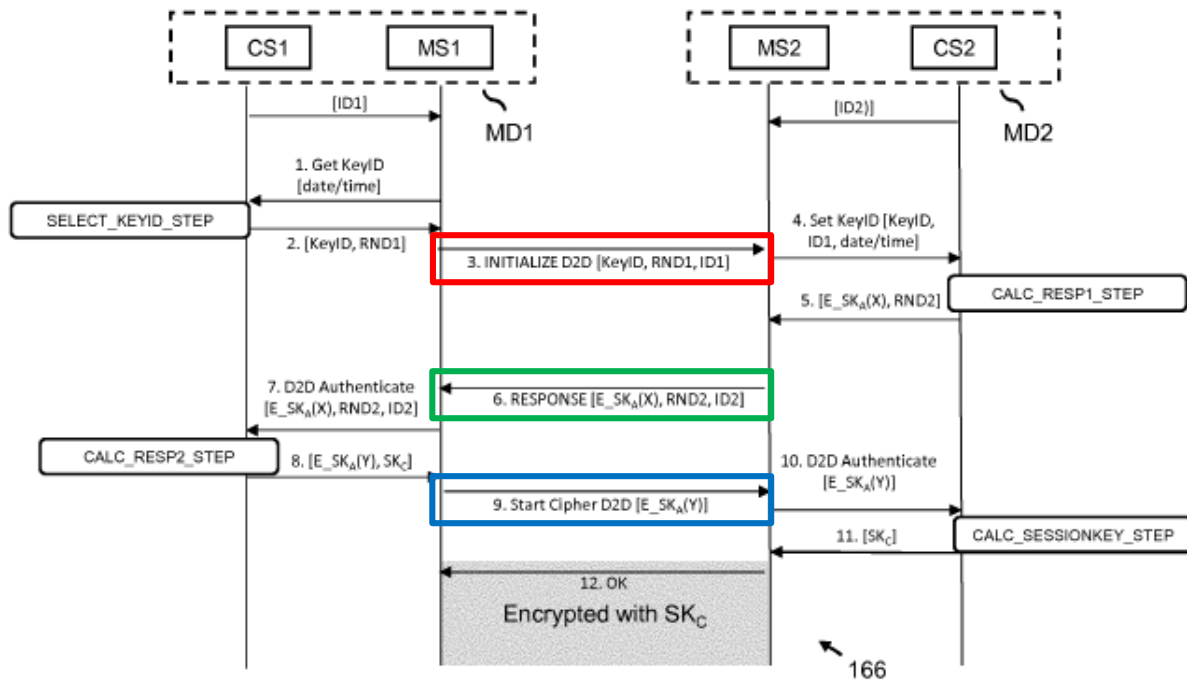
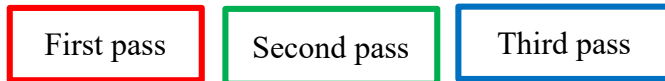


Fig. 7



EX1001, Fig. 7 (annotations added), 13:64-14:6. As shown, Figure 7, like *Teo*, involves the exchange of three messages between mobile devices attempting to authenticate each other for D2D communication. The '572 Patent's characterization of this procedure as a "three-pass authentication procedure" is consistent with a POSITA's understanding that a "three-pass" procedure is one in which three messages are exchanged. EX1003, ¶ 172 (citing EX1009, 516-517 (describing the well-known Shamir's *three-pass* protocol which involves the exchange of three messages)).

Teo therefore discloses Claim 14.

B. Ground 2: *Teo* in view of *Madoukh* and *Hawkes* Renders Obvious Claims 3-5 and 15-17

1. Motivation to Combine

As discussed above in Ground 1, a POSITA would have been motivated to combine *Teo* with *Madoukh*. A POSITA would have motivated to further combine those references with *Hawkes*.

Teo describes sending a “pre-shared” direct communication master key (DMK) to mobile communication terminals to facilitate their direct communication. EX1005, 7:24-27, 10:19-28. *Hawkes* describes mobile devices that include memory components that securely store authorization credentials, such as public keys, needed to verify a mobile device’s access to certain network services. For example, *Hawkes* states that its mobile device includes a “card interface 1170” that is configured to “accommodate a card 1172 (e.g., a subscriber identity module (SIM) card, a universal integrated circuit card (UICC), or other card) storing security credential(s)” of the mobile device. EX1006, [0098]; see also *id.*, [0032]. *Hawkes* further discloses a “system-in-package or system-on-chip device (e.g., a mobile station modem (MSM))” that includes components such as a processor, a display controller, a memory, and a wireless controller. *Id.*, [0099]. *Hawkes* explains that these components are used to facilitate the transmission of data. *Id.*, [0100].

A POSITA would have been motivated to implement *Hawkes*’ UICC and system-on-chip device hardware components into *Teo*’s mobile communication

terminals. EX1003, ¶ 109. Such a combination would have involved combining prior art elements according to known methods to yield predictable results. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 416; EX1003, ¶ 109. A POSITA would have understood that *Hawkes*'s memory components (*e.g.*, the UICC) and communication components (*e.g.*, the system-on-chip device) could be implemented in any mobile device that stores information and exchanges messages with other devices, such as *Teo*'s mobile communication terminals. EX1003, ¶ 109. The combination of *Teo* with *Hawkes* would have been predictable and foreseeable because the combination merely involves incorporating known features that are explicitly disclosed by *Hawkes* and would have been understood by a POSITA as likely present if not explicitly disclosed by *Teo*. *Id.*

2. Reasonable Expectation of Success

As discussed above in Ground 1, a POSITA would have reasonably expected success when combining *Teo* with *Madoukh*. A POSITA would have reasonably expected success when further combining those references with *Hawkes*. EX1003, ¶ 110. A POSITA would have recognized that the components taught by *Hawkes*, such as the UICC and the system-on-chip device, could be implemented in any mobile device that stores information and exchanges messages with other devices, such as *Teo*'s mobile communication terminals. EX1003, ¶ 110; *see also supra*, Section X.B.1. Such an understanding would have been readily apparent in light of

Hawkes' inclusion of these components in a "wireless communication device" such as "mobile device 120." EX1006, [0096]. Indeed, a POSITA would have understood that *Teo*'s mobile communication terminals would need to implement memory and communication components to operate as disclosed in *Teo*, and therefore would have reasonably expected success in implementing the components expressly detailed by *Hawkes*. EX1003, ¶ 110.

3. Claim 3. Method according to claim 1, wherein the preloading the initiation key comprises storing the initiation key in a secure storage area of each respective mobile device.

The *Teo-Madoukh-Hawkes* combination discloses Claim 3. *Teo* discloses mobile communication terminals (*i.e.*, "mobile device[s]") that receive a pre-shared key, DMK (*i.e.*, "initiation key"), from a base station. *See supra*, Section X.A.3.ii. *Hawkes* discloses a mobile device that stores security credentials, such as a "public key," in a "universal integrated circuit card (UICC)." EX1006, [0098] ("The card interface 1170 may be configured to accommodate a card 1172 (describing a UICC used to store "security credentials"), [0032] (describing a "public key" as being a part of a "security credential"). *Hawkes* further explains that the UICC may include a "secure storage area." *See id.*, [1278] ("If the H-SLP address can not be found in the *secure storage area of the UICC* (USIM/SIM),..." (emphasis added)).

A POSITA would have understood that the *Teo-Madoukh-Hawkes* combination discloses mobile communication terminals that each include UICCs for

storing the pre-shared DMK. EX1003, ¶ 176. A POSITA would have understood that the received DMK could have been stored in the “secure storage area” of the respective UICCs, because *Hawkes* teaches using the UICC to store keys. *Id.* This understanding is confirmed by the ’572 Patent, which states that “[t]he secure storage area provided by such a trusted computing subsystem, e.g., the memory of the UICC, is well suited for securely storing the initiation key on the mobile device.” EX1001, 5:22-25.

Thus, the *Teo-Madoukh-Hawkes* combination discloses Claim 3. This combination would have been obvious for the additional reasons explained above in Sections X.B.1-2.

4. Claim 4. Method according to claim 3, wherein the secure storage area is provided by a trusted computing subsystem of each respective mobile device.

The *Teo-Madoukh-Hawkes* combination discloses Claim 4. The *Teo-Madoukh-Hawkes* combination teaches a mobile communication terminal that implements a UICC that includes a “secure storage area” (as taught by *Hawkes*) which a POSITA would have understood could be used to store a key, such as *Teo*’s DMK. *See supra*, Section X.B.3. *Hawkes*’ UICC discloses a “*trusted computing subsystem*.” A POSITA would have understood the UICC to be a well-known component used in mobile devices not only to securely store sensitive information, but also to perform computations with that information. EX1003, ¶ 178 (citing

EX1014, 5 (describing the UICC as a “smart card” that has “a primary role of storing credentials and performing sensitive cryptographic computations”). Accordingly, a POSITA would have understood the UICC is a “*trusted computing subsystem*.” EX1003, ¶ 178. This understanding is confirmed by the ’572 Patent, which acknowledges that a UICC is “[a]n example of a removable trusted computing subsystem.” EX1001, 5:17-22. Thus, the *Teo-Madoukh-Hawkes* combination discloses Claim 4. This combination would have been obvious for the additional reasons explained above in Sections X.B.1-2.

5. Claim 5. Method according to claim 4, wherein at least one of the group of: verifying the validity of the initiation key, and using the initiation key in performing the key agreement procedure, is performed by the trusted computing subsystem.

The *Teo-Madoukh-Hawkes* combination renders obvious Claim 5. The *Teo-Madoukh-Hawkes* combination teaches a mobile communication terminal that implements a UICC (as taught by *Hawkes*) that stores *Teo*’s DMK. *See supra*, Sections X.B.3-4. The UICC is a well-known component that is used not only for “storing credentials” but also “*performing sensitive cryptographic computations*” (emphasis added). *See* EX1014, 5. Under the *Teo-Madoukh-Hawkes* combination, it would have been obvious to a POSITA that the UICC implemented in *Teo*’s mobile communication terminal would have verified the validity of the DMK (*i.e.*, “*initiation key*”) and performed the pre-shared key approach for generating an

encryption key (*i.e.*, “*performing a key agreement procedure*”) as discussed above with reference to Claim 1. EX1003, ¶ 179. Because these operations involve the use of the security-sensitive pre-shared key DMK, a POSITA would have found it obvious to use the UICC, which was well known for “performing sensitive cryptographic computations.” *Id.* (citing EX1014, 5). Thus, the *Teo-Madoukh-Hawkes* combination renders obvious Claim 5. This combination would have been obvious for the additional reasons explained above in Sections X.B.1-2.

6. Claim 15

i. [15p] A non-transitory computer-readable medium configured to store instructions for, upon execution of the instructions on a mobile device, causing the mobile device to establish a device-to-device (D2D) communication session with a further mobile device, the mobile device and the further mobile device being mutually connectable via a D2D communication channel and individually connectable to a mobile network, by:

If the preamble is limiting, the *Teo-Madoukh-Hawkes* combination discloses the preamble. The Petition explains above how *Teo* discloses Claim Element [1p]. *See supra*, Section X.A.3.i. The only difference between Claim Element [1p] and Claim Element [15p] is that this element adds that a mobile device includes “[a] *non-transitory computer-readable medium configured to store instructions for, upon execution of the instructions on a mobile device, causing the mobile device to*

establish a device-to-device (D2D) communication session with a further mobile device,...” This element was well known.

Teo’s mobile communication terminals store a pre-shared key DMK (*i.e.*, “*initiation key*”) and perform a “pre-shared key approach” (*i.e.*, “*key agreement procedure*”) to establish an encryption key DTEK (*i.e.*, “*session key*”). *See* Claim Elements [1p]-[1f]. A POSITA would have known that a mobile communication terminal is a hardware component in a communications network, and that it would have would have required a non-transitory memory storing instructions that allow the mobile communications terminal to perform its tasks. EX1003, ¶¶ 181-182 (citing EX1005, 1:14-23, Figs. 3, 6, 9; EX1006, [0032], [0098]; EX1014, 5 (explaining that *Hawkes’* UICC would have been understood to be a component that performs the memory functions); EX1020, 5:53-6:16, Fig. 3, 9:5-14).

ii. [15a]

See Claim Element [1a] and Claim 3.

iii. [15b]

See Claim Element [1b].

iv. [15c]

See Claim Element [1c].

v. [15d]

See Claim Elements [1d]-[1e].

vi. [15e]

See Claim Element [1f].

7. Claim 16

i. [16p] Mobile device for establishing a device-to-device (D2D) communication session with a further mobile device, the mobile device and the further mobile device being mutually connectable via a D2D communication channel and individually connectable to a mobile network, the mobile device comprising:

If the preamble is limiting, the *Teo-Madoukh-Hawkes* combination discloses the preamble. Claim Element [16p]’s recitation of a “[m]obile device for establishing a device-to-device (D2D) communication session with a further mobile device,...” corresponds to Claim Element [1p]’s recitation of “mobile devices which are mutually connectable via a D2D communication channel and individually connectable to a mobile network” and is disclosed for the same reasons explained in Claim Element [1p]. *See* Claim Element [1p].

ii. [16a]

See Claim Element [1a] and Claim 3.

iii. [16b]

See Claim 5.

iv. [16c]

See Claim 5 and Claim Element [1b].

v. [16d]

See Claim 5 and Claim Element [1c].

vi. [16e]

See Claim Elements [1d]-[1e].

vii. [16f] a mobile subsystem for establishing the D2D communication session over the D2D communication channel based on the session key.

The Petition explains above how *Teo* discloses Claim Element [1f]. *See supra*, Section X.A.3.vii. The only difference between Claim Element [1f] and Claim Element [16f] is that this element adds that the “*establishing*” is performed by “*a mobile subsystem*.” This element was well known.

Teo’s mobile communication terminals establish a direct communication session with each other based on a computed encryption key, DTEK (*i.e.*, “*session key*”). *See supra*, Section X.A.3.vii. A POSITA would have known that a mobile communication terminal is a hardware component in a communications network, and that it would have required a subsystem that facilitates the exchange of messages necessary to establish the direct communication session. EX1003, ¶¶ 195-196 (citing EX1005, 1:14-23, Figs. 3, 6, 9; EX1020, 6:3-12, Fig. 3, 9:5-14. It would have been obvious to a POSITA that *Hawkes*’ system-on-chip device and the components included therein (*e.g.*, the wireless controller, processor, and memory), which are taught by *Hawkes* as facilitating the transmission of data, teaches such a

subsystem. EX1003, ¶ 196; EX1006, [0098]-[0100]. Accordingly, a POSITA would have known that *Teo*'s mobile communication terminals would include “*a mobile subsystem*” for establishing a direct communication session between the mobile communication terminals. EX1003, ¶ 196. This understanding is confirmed by the '572 Patent, which explains that “[a]n example of a mobile subsystem is a mobile System on a Chip (SoC) comprising an application processor, a display processor, one or more modems, an integrated LTE radio.” EX1001, 9:15-18.

8. Claim 17

i. [17p] Mobile network arranged for preloading an initiation key on a mobile device when the mobile device is connected to the mobile network, the initiation key being associated with a validity period, the mobile device for establishing a device-to-device (D2D) communication session with a further mobile device, the mobile device and the further mobile device being mutually connectable via a D2D communication channel and individually connectable to the mobile network, the mobile device comprising:

If the preamble is limiting, the *Teo-Madoukh-Hawkes* combination discloses the preamble. The Petition explains above how *Teo* discloses Claim Element [1p]. *See supra*, Section X.A.3.i. The Petition explains above in Claim Element [1a] how *Teo* discloses “*preloading an initiation key on each of the mobile devices, the initiation key being associated with a validity period.*” The Petition explains above in Claim 2 how *Teo* discloses “*wherein the preloading the initiation key comprises providing the initiation key to each of the mobile devices via the mobile network*

when each respective mobile device is connected to the mobile network.” Claim Element [17p] is written from the perspective of the “[*m*]obile network” that is “*arranged for preloading an initiation key*”; this “[*m*]obile network” corresponds to the “*mobile network*” of Claim Element [1p]. Thus, Claim Element [17p] is disclosed for the same reasons explained in Claim Elements [1p] and [1a] and Claim 2.

ii. [17a]

See Claim 5 and Claim Element [16b].

iii. [17b]

See Claim 5 and Claim Elements [1b] and [16c].

iv. [17c]

See Claim 5 and Claim Elements [1c] and [16d].

v. [17d]

See Claim Elements [1d]-[1e].

vi. [17e]

See Claim Elements [1f] and [16f].

C. Ground 3: *Teo* in view of *Madoukh* and RFC 4279 Renders Obvious Claims 6-9

1. Motivation to Combine

As discussed above in Ground 1, a POSITA would have been motivated to combine *Teo* with *Madoukh*. A POSITA would have motivated to combine those references with RFC 4279.

Teo describes sending a “pre-shared” direct communication master key (DMK) that is used to facilitate the direct communications between mobile communication terminals. EX1005, 7:24-27, 10:19-28. *Teo* explains that its system may be applied, for example, in the event of a disaster such that “rescue teams (e.g. firemen and police officers) would have to communicate directly with each other without a backbone network in order to provide disaster recovery.” EX1005, 1:18-23.

RFC 4279 describes “how to use symmetric keys (later called pre-shared keys or PSKs), shared in advance among the communicating parties, to establish a TLS [Transport Layer Security] connection” between a client and a server. EX1007, 2. RFC 4279 explains that “[b]oth clients and servers may have pre-shared keys with several different parties.” *Id.*, 5. Accordingly, RFC 4279 discloses a procedure whereby the client and server agree on the pre-shared key that they wish to use for a TLS connection. *Id.*, 4-5. In particular, RFC 4279 explains that after the client and server agree to use pre-shared key authentication, the client includes “PSK identity”

information in a “ClientKeyExchange message,” which thereby “indicates which key to use.” *Id.*

A POSITA would have been motivated to modify *Teo*’s procedure for establishing direct communications between terminals based on a pre-shared key DMK to include a procedure whereby the terminals agree on the pre-shared DMK to be used, as taught by RFC 4279. EX1003, ¶ 115. Including such a procedure would have been a matter of common sense and a needed step in a communications system. A POSITA would have recognized that the terminals operating according to *Teo*’s system could receive several pre-shared DMKs, as suggested by *Teo*, which envisions a communications environment wherein several “firemen and police officers,” for example, would need to communicate directly with each other. *Id.*; EX1005, 1:20-23. Accordingly, a POSITA would have recognized the need for implementing a system that allows the terminals to agree on a pre-shared key DMK before attempting to establish a direct communication session. EX1003, ¶ 115. Such a system would allow for a more efficient coordination of pre-shared keys between terminals, as the terminals could avoid wasteful trial-and-error procedures for selecting a common pre-shared key. *Id.*

2. Reasonable Expectation of Success

As discussed above in Ground 1, a POSITA would have reasonably expected success when combining *Teo* with *Madoukh*. A POSITA would have had a

reasonable expectation of success when further combining those references with RFC 4279. EX1003, ¶ 116. Both *Teo* and RFC 4279 relate to the use and management of pre-shared keys, and a POSITA would have recognized that the procedure for identifying pre-shared keys using a generic “PSK identifier” for agreement between entities could be applied in any system where two entities have pre-shared keys, such as *Teo*. *Id.* Although RFC 4279 describes its procedure in the context of TLS connection setup between a client and a server, nothing in RFC 4279 restricts the application of its teachings to any particular system or environment, and a POSITA would have had a reasonable expectation of success in applying RFC 4279’s procedure, which generally teaches how to choose a particular key between two entities that have received several keys, in the context of *Teo*’s device-to-device communication system, which suggests the sharing of several keys amongst several mobile terminals. *Id.* Such a modification would not have involved undue experimentation and instead would have required only basic network design ability. *Id.*

3. Claim 6.

i. [6a] Method according to claim 1, further comprising: preloading a set of initiation keys on each of the mobile devices, the set of initiation keys key being associated with a respective set of validity periods; and

The *Teo-Madoukh*-RFC 4279 combination renders obvious this claim element. *Teo* discloses a base station (*e.g.*, HR-BS) sending a pre-shared DMK (*i.e.*, “*initiation key*”) and its associated “*key_lifetime*” (*i.e.*, “*validity period*”) to two mobile communication terminals. *See supra*, Section X.A.3.ii. *Teo* explains that its system may be applied when several emergency rescue personnel need to directly communicate with each other in the event of a disaster, for example. EX1005, 1:18-23. It would have been obvious to a POSITA that in such a scenario, there would be many terminals that would need to communicate with each other. EX1003, ¶ 203. Accordingly, a POSITA would have found it obvious that *Teo*’s base station would have transmitted several DMKs (*i.e.*, “*preloading a set of initiation keys*”) to the terminals to facilitate their direct communication with each other. *Id.* (citing EX1007, 5 (“Both clients and servers may have pre-shared keys with several different parties.”)). And it would have been obvious to a POSITA that each of the respective keys sent by the base station would have its own “*key_lifetime*” value and, therefore, its own “*validity period*” indicated by the time period between the time stamp included in the message carrying the pre-shared DMK (and the

associated key_lifetime) and the expiration of the key_lifetime value. EX1003, ¶ 203; *see also supra*, Section X.A.3.ii.

The *Teo-Madoukh*-RFC 4279 combination therefore renders obvious this claim element. This combination would have been obvious for the additional reasons discussed above in Sections X.C.1-2.

ii. [6b] performing a key synchronization procedure between the mobile devices over the D2D communication channel for selecting a matching one of the set of initiation keys on each of the mobile devices as the initiation key.

The *Teo-Madoukh*-RFC 4279 combination renders obvious this claim element. RFC 4279 describes a procedure for coordinating a pre-shared key to be used to establish a connection between a client and a server when “[b]oth clients and servers [] have pre-shared keys with several different parties.” EX1007, 4-5. In particular, RFC 4279 explains that the “client indicates which key to use” to establish a connection by “including a ‘PSK identity’ in the ClientExchange message” sent from the client to the server. *Id.*, 4-5, 1 (explaining that pre-shared keys are used to establish a TLS connection). If the server does not recognize the “PSK identity,” the server can send an alert message back to the client. *Id.*, 5. A POSITA would have understood that if the server does recognize the PSK identity, the server would understand that it possesses the same pre-shared key as the one selected by the client and that it can commence connection establishment with the client. EX1003, ¶ 205.

A POSITA would have understood that the *Teo-Madoukh*-RFC 4279 combination teaches a system whereby a base station transmits both a set of pre-shared DMKs and a set of “PSK identities” associated with the DMKs to mobile communication terminals, where each DMK is associated with a “PSK identity” that identifies the DMK, as taught by RFC 4279. *Id.*, ¶ 206; EX1007, 4-5. When a first terminal wishes to directly communicate with a second terminal, the first terminal transmits to the second terminal the “PSK identity” associated with the DMK that the first terminal wants to use, as suggested by RFC 4279. EX1003, ¶ 206; *see* EX1007, 4-5. Upon receiving the “PSK identity,” the second terminal determines if it received a DMK associated with the received “PSK identity;” if a positive determination is made, the second terminal determines that the first and second terminals have received matching pre-shared DMKs and that they may proceed with the pre-shared key approach for generating an encryption key, as described in *Teo*. EX1003, ¶ 206; EX1007, 4-5.

A POSITA would have understood that this procedure whereby the terminals agree to a pre-shared DMK for future use discloses a “*key synchronization procedure between the mobile devices.*” EX1003, ¶ 207. Further, it would have been obvious to a POSITA that this agreement procedure would occur via direct communication between the terminals (as suggested by RFC 4279), thereby rendering obvious “*over the D2D communication channel.*” *Id.* And because the agreement procedure would

result in the terminals each agreeing the use the same pre-shared DMK from the several received DMKs for later procedures, the *Teo-Madoukh*-RFC 4279 combination renders obvious “*for selecting a matching one of the set of initiation keys on each of the mobile devices as the initiation key.*” *Id.* This combination would have been obvious for the additional reasons discussed above in Sections X.C.1-2.

4. Claim 7.

i. [7a] Method according to claim 6, further comprising: preloading a set of key identifiers on each of the mobile devices, each of the set of key identifiers identifying a respective one of the set of initiation keys; and

The *Teo-Madoukh*-RFC 4279 combination renders obvious a system wherein a base station sends a set of “PSK identities” that are associated with, and uniquely identify, a set of pre-shared DMKs. *See supra*, Section X.C.3.i. For the same reasons discussed above with reference to Claim Element [6a], the *Teo-Madoukh*-RFC 4279 combination renders obvious Claim Element [7a]. EX1003, ¶ 208. This combination would have been obvious for the additional reasons discussed above in Sections X.C.1-2.

ii. [7b] performing the key synchronization procedure based on an exchange of one or more of the set of key identifiers between the mobile devices.

The *Teo-Madoukh*-RFC4279 combination renders obvious a system wherein a first mobile communication terminal and a second mobile communication terminal agree to a common pre-shared DMK based on the exchange of a “PSK identifier” associated with a selected pre-shared DMK. *See supra*, Section X.C.3.ii. For the same reasons discussed above with reference to Claim Element [6b], the *Teo-Madoukh*-RFC 4279 combination renders obvious Claim Element [7b]. EX1003, ¶ 209. This combination would have been obvious for the additional reasons discussed above in Sections X.C.1-2.

5. Claim 8. Method according to claim 6, further comprising disabling or removing the initiation key from the set of initiation keys after use in establishing the D2D communication session.

The *Teo-Madoukh*-RFC 4279 combination renders obvious Claim 8. As discussed above in Ground 1, a POSITA would have found it obvious to implement *Madoukh*’s key lifetime manager to monitor the lifetime of *Teo*’s DMK (*i.e.*, “*initiation key*”), and deactivate the DMK after it expires. *See supra*, Sections X.A.1-2; EX1011, [0008] (“...the key lifetime manager is operable to flag the expired keys *and to change or deactivate the expired keys...*” (emphasis added)). And it would have been obvious to a POSITA that in the emergency scenario described in *Teo*, there would be many mobile communication terminals that would

need to communicate with each other, and, therefore, that several pre-shared DMKs (*i.e.*, a “*set of initiation keys*”) would be transmitted to the terminals to facilitate their direct communication with each other. *See supra*, Section X.C.3.i; EX1003, ¶ 210. A POSITA would have understood that when direct communication between terminals is desired in such a scenario, one of the several DMKs would be selected for establishing direct communication. EX1003, ¶ 210. Further, a POSITA would have understood that after the DMK is used to establish direct communication, the DMK would eventually expire (*i.e.*, as indicated by the expiration of the DMK’s “*key_lifetime*”). *Id.*, ¶ 210 (citing EX1009, 183).

It would have been obvious to a POSITA that in such a scenario, one could implement *Madoukh*’s key lifetime manage to flag and “deactivate” a DMK after the DMK is used and expires, as taught by *Madoukh*. EX1003, ¶ 211. A POSITA would have understood that the deactivated DMK is “*disable[ed]*” from further use. *Id.* The *Teo-Madoukh*-RFC 4279 combination therefore renders obvious Claim 8. This combination would have been obvious for the additional reasons discussed above in Sections X.C.1-2.

6. Claim 9. Method according to claim 6, wherein the set of validity periods is constituted at least in part by different but overlapping validity periods.

The *Teo-Madoukh*-RFC 4279 combination renders obvious Claim 9. As discussed above with reference to Claim 6, it would have been obvious to a POSITA

that the *Teo-Madoukh*-RFC 4279 combination renders obvious preloading a set of DMKs (*i.e.*, “*initiation keys*”) and associated key_lifetime values on each of *Teo*’s mobile communication terminals (*i.e.*, “*mobile devices*”). *See supra*, Section X.C.3.i. A POSITA would have considered it a natural occurrence in a system that deploys several DMKs with a corresponding set of “*validity periods*” (*i.e.*, the time periods extending from the time indicated by the time stamp of the received messages from the base station through the end of the key_lifetime value), that the set of validity periods would include some different but overlapping time periods. EX1003, ¶ 212 (citing, as an example of such an occurrence, EX1017, [0050], [0052], [0059], [0064], which discloses that a set of keys may be generated with different validity periods (*e.g.*, one year, one month, six hours, three hours, or one hour), and distributed simultaneously such that the different validity periods overlap). Thus, the *Teo-Madoukh*-RFC 4279 combination renders obvious Claim 9. This combination would have been obvious for the additional reasons discussed above in Sections X.C.1-2.

D. Ground 4: *Teo in view of Madoukh, RFC 4279, and Kumar Render Obvious Claim 10*

1. Motivation to Combine

As discussed above in Ground 3, a POSITA would have been motivated to combine *Teo* with *Madoukh* and RFC 4279. A POSITA would have motivated to combine those references with *Kumar*. EX1003, ¶ 117.

Teo describes sending a “pre-shared” direct communication master key (DMK) that is used to facilitate the direct communications between mobile communication terminals. EX1005, 7:24-27, 10:19-28. RFC 4279 discloses a procedure whereby a client device includes “PSK identity” information in a “ClientKeyExchange message” sent to a server, which thereby “indicates which key to use” for a Transport Layer Security connection. EX1007, 4-5. And *Kumar* describes associating a “Preshare Key” (PSK) with an “SSID,” which identifies an 802.11 wireless network associated with the PSK. EX1016, Fig. 2, [0057].

A POSITA would have been motivated to modify the *Teo-Madoukh*-RFC 4279 combination with *Kumar* such that RFC 4279’s “PSK identity” is implemented using *Kumar*’s SSID value. EX1003, ¶ 119. Such a combination would have involved a simple substitution of one known element for another to obtain predictable results. *See KSR Int’l*, 550 U.S. at 416; EX1003, ¶ 119. A POSITA would have recognized RFC 4279’s “PSK identity” to be a generic value that anonymously identifies a “preshare[d] key,” such as *Teo*’s DMK, and could take any value that distinguishes one key from another, such as *Kumar*’s SSID value, which identifies a wireless network with which a key is associated. EX1003, ¶ 119. Indeed, as shown in Figure 2 of *Kumar*, different SSID values are associated with different “Preshare Key[s].” EX1016, Fig. 2.

A POSITA would have recognized that applying such a basic technique, using an SSID value associated with a key to identify the key, would have yielded predictable results and an improved system, such as mobile communication terminals that can efficiently identify a pre-shared key (*e.g.*, DMK) to establish direct communication by exchanging SSID values associated with the pre-shared key. EX1003, ¶ 120.

2. Reasonable Expectation of Success

As discussed above in Ground 3, a POSITA would have reasonably expected success when combining *Teo* with *Madoukh* and RFC 4279. A POSITA would have had a reasonable expectation of success when further combining those references with *Kumar*. *Id.*, ¶ 121. As discussed above, POSITA would have recognized RFC 4279's "PSK identity" to be a generic value that anonymously identifies a "preshare[d] key," and could take any value that distinguishes one key from another. Accordingly, a POSITA would have reasonably expected success in implementing *Kumar*'s SSID value as the "PSK identity," because *Kumar* associates different SSID values with different "Preshare Key[s]." *Id.*, ¶ 122; EX1016, Fig. 2. Such a modification would not have involved undue experimentation and instead would have required only basic network security design ability. EX1003, ¶ 122.

3. Claim 10. Method according to claim 1, wherein the initiation key is associated with a virtual network identity, and wherein the verifying the validity of the initiation key further comprises determining a match of the virtual network identity on each of the mobile devices via the D2D communication channel.

The *Teo-Madoukh*-RFC 4279-*Kumar* combination renders obvious Claim 10. The *Teo-Madoukh*-RFC 4279 combination teaches a system wherein mobile communication terminals exchange a “PSK identity” associated with a pre-shared DMK (*i.e.*, “*initiation key*”) to confirm that the terminals have received the same DMK (which may be used to establish direct communication between the terminals). *See supra*, Section X.C.3. And *Kumar* teaches associating a “Preshare Key” (PSK) with an SSID value, which identifies a wireless network with which the PSK is associated. EX1016, Fig. 2, [0057]. A POSITA would have understood that the *Teo-Madoukh*-RFC 4279-*Kumar* combination teaches associating *Teo*’s DMK with a wireless network identity (*e.g.*, SSID, as taught by *Kumar*), and exchanging that associated network identity in place of RFC 4279’s “PSK identity” to verify that the terminals have received the same DMK (*i.e.*, the DMK associated with the exchanged network identity), as taught by RFC 4279. EX1003, ¶ 214. When implemented in such a manner, the network identity (*e.g.*, SSID) teaches “*a virtual network identity*,” which the ’572 Patent describes simply as an identifier that identifies a network with which an initiation key is associated. *Id.*; EX1001, 10:40-

51. Accordingly, *Teo-Madoukh*-RFC 4279-*Kumar* combination renders obvious “*wherein the initiation key is associated with a virtual network identity.*”

As with Claim 6, the *Teo-Madoukh*-RFC 4279 combination teaches that the mobile communication terminals exchange the “PSK identity” to confirm that both terminals have received the same DMK, thereby verifying that the associated DMK is valid for generating a DTEK. *See supra*, Section X.C.3. A POSITA would have recognized that this verification would operate in the same manner when the “PSK identity” is implemented as a network identity (e.g., SSID), as taught by *Kumar* and described above. EX1003, ¶ 215. Thus, the *Teo-Madoukh*-RFC 4279-*Kumar* combination renders obvious “*verifying the validity of the initiation key further comprises determining a match of the virtual network identity on each of the mobile devices via the D2D communication channel*” at least for the same reasons discussed above with reference to Claim [6b]. This combination would have been obvious for the additional reasons discussed above in Sections X.D.1-2.

E. Ground 5: *Teo in view of Madoukh and S3-070234* Renders Obvious Claims 11-12

1. Motivation to Combine

As discussed above in Ground 1, a POSITA would have been motivated to combine *Teo* with *Madoukh*. A POSITA would have been motivated to further combine these references with S3-070234. EX1003, ¶ 123.

Teo describes sending a pre-shared key, DMK, to mobile communication terminals to facilitate their direct communication. EX1005, 7:24-27, 10:19-28. As in Ground 1, the DMK is associated with a lifetime that indicates when the DMK expires. *See supra*, Section X.A.3.ii. The mobile communication terminals use the DMK to generate additional keys, such as the DAK, DCMAC, and DTEK, which are used to ensure the security of direct communications. *Id.*, 37:4-38:25. S3-070234 describes various proposals for increasing the security and integrity of cryptographic keys used in encryption. EX1013, 1. One such proposal is implementing “counters related to limiting key usage, e.g. to limit the number of key derivations from one parent key.” *Id.*, 1-2. In combination, the *Teo-Madoukh-S3-070234* combination teaches a mobile communication terminal that uses a counter to limit the number of times the DMK is derived into other keys, such as the DAK. EX1003, ¶ 124.

A POSITA would have been motivated to combine *Teo*’s system wherein a pre-shared key DMK is used to derive other keys with S3-070234’s usage-based counter for limiting the number of key derivations of a parent key. EX1003, ¶ 125. Such limiting of the DMK’s use would have been a matter of common sense to a POSITA. *Id.* It is a well-known principle in cryptographic key management that the severity of a key being compromised increases the more often the key is used. *Id.* (citing EX1009, 183). While the DMK’s lifetime offers a time-based mechanism

to limit the overuse of the DMK, a POSITA would have recognized that security concerns arise when the DMK is used many times before the lifetime expires. Accordingly, a POSITA would have been motivated to seek out additional methods for limiting a DMK's exposure, such as S3-070234 method for counting key usage. EX1003, ¶ 125.

2. Reasonable Expectation of Success

As discussed in Ground 1, a POSITA would have a reasonable expectation of success when combining *Teo* with *Madoukh*. A POSITA would also reasonably expect success in combining these references with S3-070234. EX1003, ¶ 126. A POSITA would have understood that S3-070234's method for limiting the number of derivations of a parent key could be implemented in any device that uses a parent key to derive additional keys, such as *Teo*'s mobile communication terminals that use the DMK to derive the DAK, DCMAC, and DTEK. EX1003, ¶ 127. The combination of *Teo* with S3-070234 would have been predictable and foreseeable because the combination merely involves incorporating known features that are explicitly disclosed by S3-070234. The combination is predictable, at least in part because elements of the combined system would each perform similar functions they had been known to perform prior to the combination. *Id.* For example, *Teo*'s terminals would still perform the same functions, including receiving a pre-shared

key, DMK, for generating additional encryption keys and establishing a D2D communication session, as they did prior to the combination with S3-070234. *Id.*

3. Claim 11. Method according to claim 1, wherein the initiation key is associated with a usage count for limiting a number of uses of the initiation key, and wherein the verifying the validity of the initiation key is further based on the usage count.

The *Teo-Madoukh*-S3-070234 combination renders obvious Claim 11. *Teo* describes mobile communication terminals using a pre-shared key DMK to derive additional keys (*e.g.*, DAK). *See supra*, Sections X.A.3.ii, X.A.3.v. S3-070234 describes implementing “counters related to limiting key usage, *e.g.* to limit the number of key derivations from one parent key.” EX1013, 1-2. A POSITA would have found it obvious to implement S3-070234’s usage-based counter in *Teo*’s mobile communication terminal such that the terminal counts the number of times the DMK is used to derive additional keys and limits the usage of the DMK based on that count. EX1003, ¶ 217.

Accordingly, it would have been obvious to a POSITA that before a mobile communication terminal uses a pre-shared DMK, the terminal would check the counter associated with the DMK to confirm that a threshold number of uses has not been exceeded. EX1003, ¶ 218. A POSITA would have understood that this check, along with checking whether the DMK’s lifetime has expired as discussed above with reference to Claim Elements [1a] and [1b], would ensure that the DMK is valid

for use. *Id.* Thus, the *Teo-Madoukh-S3-070234* combination renders obvious Claim 11. This combination would have been obvious for the additional reasons discussed above in Sections X.E.1-2.

4. Claim 12. Method according to claim 11, further comprising adjusting the usage count after use of the initiation key in establishing the D2D communication session.

As with Claim 11, a POSITA would have found it obvious to modify *Teo*'s mobile communication terminal such that it counts the number of times a DMK (*i.e.*, “*initiation key*”) is used to derive additional keys and limits the usage of the DMK based on that count (as taught by S3-070234). *See supra*, Section X.D.3. In accordance with this operation, a POSITA would have considered it an obvious and necessary step adjust the count whenever the DMK is used to establish a direct communication session (*i.e.*, “*D2D communication session*”). EX1003, ¶ 219. Without this updating, the DMK's usage would not be accurately counted and limited in the manner suggested by S3-070234. *Id.*; EX1013, 1-2. Thus, the *Teo-Madoukh-S3-070234* combination renders obvious Claim 12. This combination would have been obvious for the additional reasons discussed above in Sections X.E.1-2.

F. Ground 6: *Teo* in view of *Madoukh* and *Thakare* Render Obvious Claim 13

1. Motivation to Combine

As discussed above in Ground 1, a POSITA would have been motivated to combine *Teo* with *Madoukh*. A POSITA would have motivated to combine those references with *Thakare*. EX1003, ¶ 128.

Teo teaches receiving a pre-shared key DMK from a base station and using the DMK to generate additional keys, such as DAK, DCMAC, and DTEK, that are used during a direct communication session. EX1005, 13:19-15:2, 32:16-21, 33:1-8, 38:24-25. A POSITA implementing such a procedure would have recognized that errors (*e.g.*, transmission errors or message decryption errors) may occur and prevent the additional keys from being generated. EX1003, ¶ 129. A POSITA thus would have been motivated to seek out solutions to correct for such errors. *Id.* A natural and common sense solution would have been to request a new DMK from the base station and to reattempt generating the additional keys with the new DMK, and a POSITA would have searched for and implemented such solutions—like *Thakare*'s concept of requesting a new encryption key for generating encrypted data packets—to address such errors. *Id.*

2. Reasonable Expectation of Success

A POSITA would have had a reasonable expectation of success in combining *Teo* with *Madoukh* as described above in Ground 1. A POSITA would have had a

reasonable expectation of success in combining *Thakare* with those references. EX1003, ¶ 130. A POSITA would have recognized that *Thakare*'s process of requesting a new key upon encountering errors in the using the key was a complementary process to the concepts relied upon in *Teo*. *Id.*, ¶ 131. That modification—requesting a new DMK from the base station upon determining that the DMK has failed in generating additional keys—would have involved basic design skill and would not have required any undue experimentation, as such tasks were well-known at the time of invention. *Id.*

3. Claim 13. Method according to claim 1, further comprising requesting a further initiation key via the mobile network if the key agreement procedure fails in providing the session key.

The *Teo-Madoukh-Thakare* combination renders obvious Claim 13. *Teo* teaches mobile communication terminals receiving, from a base station (*i.e.*, a component of a “*mobile network*”), a pre-shared key DMK (*i.e.*, “*initiation key*”), which is used in a pre-shared key approach (*i.e.*, “*key agreement procedure*”) to generate a DTEK (*i.e.*, “*session key*”). *See supra*, Section X.A.3. *Thakare* teaches requesting a new encryption key upon determining that data packets encrypted with the encryption key are not successfully authenticated. EX1018, [0009]. A POSITA would have found it obvious to implement *Thakare*'s process—requesting a new key upon encountering errors when using the key—into *Teo*'s system such that *Teo*'s

terminals request a new DMK upon determining that pre-shared key approach fails in generating the DTEK. EX1003, ¶ 221. A POSITA would have considered this a common-sense response when encountering such a failure. *Id.* (citing EX1011, [0007] (discussing requesting new keys upon expiration of old keys). The *Teo-Madoukh-Thakare* combination therefore renders obvious Claim 13. This combination would have been obvious for the additional reasons discussed above in Sections X.F.1-2.

XI. CONCLUSION

Petitioner respectfully requests institution of IPR and cancelation of Claims 1-17 as unpatentable.

Respectfully submitted,

BAKER BOTTS L.L.P.



Chad C. Walters (Reg. No. 48,022)
Lead Attorney for Petitioner

Date: May 17, 2023

2001 Ross Ave., Suite 900
Dallas, TX 75201-2980
Phone: (214) 953-6511
Fax: (214) 661-4511
chad.walters@bakerbotts.com

CERTIFICATE OF SERVICE

The undersigned hereby certifies on this May 17, 2023, that true and correct copies of the foregoing PETITION FOR INTER PARTES REVIEW OF U.S. PATENT NO. 9,438,572, Exhibits 1001-1009, 1011, 1013-1020, and Petitioner's power of attorney were served in their entirety on the following parties via FedEx Express® or Express Mail:

Correspondence Address:

Hamilton, Brook, Smith & Reynolds,
P.C.
530 Virginia Road
P.O. Box 9133
Concord, MA 01742-9133
United States

BAKER BOTTS L.L.P.



Chad C. Walters (Reg. No. 48,022)
Lead Attorney for Petitioner

Date: May 17, 2023

2001 Ross Ave., Suite 900
Dallas, TX 75201-2980
Phone: (214) 953-6511
Fax: (214) 661-4511
chad.walters@bakerbotts.com

**CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME
LIMITATION, TYPEFACE REQUIREMENTS, AND TYPE STYLE
REQUIREMENTS**

1. This Petition complies with the type-volume limitation of 14,000 words, comprising 13,981 words, excluding the parts exempted by 37 C.F.R. § 42.24(a).

2. This Petition complies with the general format requirements of 37 C.F.R. § 42.6(a) and has been prepared using Microsoft® Word in 14-point Times New Roman.

Respectfully submitted,

BAKER BOTTS L.L.P.



Chad C. Walters (Reg. No. 48,022)
Lead Attorney for Petitioner

Date: May 17, 2023

2001 Ross Ave., Suite 900
Dallas, TX 75201-2980
Phone: (214) 953-6511
Fax: (214) 661-4511
chad.walters@bakerbotts.com