

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC
Petitioner

v.

HEADWATER RESEARCH LLC
Patent Owner

Case No. IPR2026-00442
Patent 11,985,155

**PETITION FOR INTER PARTES REVIEW
OF U.S. PATENT NO. 11,985,155**

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. MANDATORY NOTICES PURSUANT TO 37 C.F.R. §42.8(a)(1)	3
A. Real Parties-In-Interest	3
B. Identification of Related Matters Under 37 C.F.R. §42.8(b)(2)	6
C. Lead and Backup Counsel	9
D. Service Information Under 37 C.F.R. §42.8(b)(4)	10
III. FEES	10
IV. REQUIREMENTS UNDER 37 C.F.R. §42.104	10
A. Grounds for Standing	10
B. Identification of Challenges and Precise Relief Requested	10
C. Prior Art Qualification of Asserted References	11
V. BACKGROUND	12
A. The '155 Patent	12
B. Examination History	14
C. Prior Art	15
1. Shah (EX1006)	15
2. Naslund (EX1007)	16
D. Person of Ordinary Skill in the Art (“POSITA”)	17
VI. CLAIM CONSTRUCTION	18
VII. PETITIONER HAS A REASONABLE LIKELIHOOD OF PREVAILING	18

A.	Claims 1, 2, 10, and 11 are Anticipated by and/or Rendered Obvious over Shah (EX1006) alone and/or in view of Naslund (Ground 1)	18
1.	Claim 1 (Preamble): “A communications device comprising:”	19
a.	[1.1]: “a wide area network port configured to connect the communications device to a wide area network;”	19
b.	[1.2]: “a secure memory;”	22
c.	[1.3]: “a secure execution environment configured to be inaccessible to a user application software; and”	23
d.	[1.4]: “a secure data path processing agent configured to:”	30
e.	[1.5]: “execute in the secure execution environment;”	33
f.	[1.6]: “generate a unique identifier for communication to a network element in the wide area network;”	34
g.	[1.7]: “store the unique identifier in the secure memory;”	37
h.	[1.8]: “generate a data record;”	39
i.	[1.9]: “associate the unique identifier with the data record; and”	42
j.	[1.10]: “send the unique identifier to the network element over a trusted communication link between the secure data path processing agent and the network element.”	45
2.	Claim 2: “The communications device of claim 1, wherein the secure data path processing agent includes a device data record mailbox, wherein the device data	

record mailbox is configured to relay the data record to an agent outside of the secure execution environment for transmission to the network element.” 52

3. Claim 10 (Preamble): “A method for use by a communications device” 55
 - a. [10.1]: “including a wide area network port configured to connect the communications device to a wide area network, and” 55
 - b. [10.2]: “further including a secure memory,” 55
 - c. [10.3]: “a secure execution environment configured to be inaccessible to a user application software, and” 55
 - d. [10.4]: “a secure data path processing agent,” 56
 - e. [10.5]: “the method comprising:” 56
 - f. [10.6]: “executing the secure data path processing agent in the secure execution environment;” 56
 - g. [10.7]: “generating, by the secure data path processing agent, a unique identifier for communication to a network element in the wide area network;” 56
 - h. [10.8]: “storing, by the secure data path processing agent, the unique identifier in the secure memory;” 56
 - i. [10.9]: “generating, by the secure data path processing agent, a data record;” 56
 - j. [10.10]: “associating, by the secure data path processing agent, the unique identifier with the data record; and” 57
 - k. [10.11]: “sending, by the secure data path processing agent, the unique identifier to the network element over a trusted communication

link between the secure data path processing agent
and the network element.” 57

4. Claim 11: “The method of claim 10, wherein the secure data path processing agent includes a device data record mailbox, and wherein the method further comprises: relaying, using the device data record mailbox, the data record to an agent outside of the secure execution environment for transmission to the network element.” 57

VIII. OTHER CONSIDERATIONS 57

IX. CONCLUSION.....58

APPENDIX A - LIST OF EXHIBITS

CERTIFICATE OF COMPLIANCE WITH 37 C.F.R. §42.24

CERTIFICATE OF SERVICE

TABLE OF AUTHORITIES

Cases	Page(s)
<i>In re Fulton</i> , 391 F.3d 1195 (Fed. Cir. 2004)	27
<i>Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.</i> , 868 F.3d 1013 (Fed. Cir. 2017)	18
Statutes	
35 U.S.C. §101	18
35 U.S.C. §102	10, 11
35 U.S.C. §102(b)	11, 12
35 U.S.C. §102(e)	11
35 U.S.C. §103	10, 11
35 U.S.C. §112	18
35 U.S.C. §§311-319	1
Rules	
37 C.F.R. §42.8(a)(1)	3
37 C.F.R. §42.8(b)(2)	6
37 C.F.R. §42.8(b)(3)	9
37 C.F.R. §42.8(b)(4)	10
37 C.F.R. §42.10(a)	9
37 C.F.R. §42.10(b)	9
37 C.F.R. §42.15(a)	10

Petition for *Inter Partes* Review of U.S. Patent No. 11,985,155

37 C.F.R. §42.100(b)	18
37 C.F.R. §42.100 <i>et seq.</i>	1
37 C.F.R. §42.104	10
37 C.F.R. §42.104(a).....	10

I. INTRODUCTION

Google LLC respectfully requests *inter partes* review of Claims 1, 2, 10, and 11 (“Challenged Claims”) of U.S. Patent No. 11,985,155 (“’155 Patent”) (EX1001) under 35 U.S.C. §§311-319 and 37 C.F.R. §42.100 *et seq.*

The ’155 Patent relates to a communication device (e.g., mobile device) having a “secure execution environment” for generating and reporting secure “device data records” (DDRs) that are each associated with a unique identifier (e.g., “time stamp”). *See* EX1001, Abs., 1:6-28, 3:54-4:12. The secure DDRs are generated and used for “service usage monitoring” of the communications device during network communication. *See id.*, 2:57-3:4. *See also id.*, Abs. The DDRs and unique identifiers allow network activity to be “securely monitored and reported to a network server” while “device access service policies are being properly enforced.” *Id.*, 4:6-10.

The Challenged Claims recite a communication device/method for generating and associating the “unique identifier” (e.g., the “time stamp” mentioned at EX1001, 5:57) with the device data record in a secure execution environment and sending the unique identifier to a network element over a trusted communication link. *See id.*, 5:41-6:7, 9:23-65. Service usage of the communications device is thereby monitored to identify tampering with the device data records. *Id.* The ’155 Patent states that “securing device based network access (or I/O control) policies” is “helpful in

identifying device software that has been tampered with or any malware that is present on the device.” *Id.*, 4:60-63. *See id.*, 3:54-4:67.

The prior art relied upon in the Grounds of this Petition was not cited in the prosecution of the ’155 Patent, yet this prior art recognized the exact problem/solution described in the ’155 Patent. *See, e.g.*, EX1006, ¶¶[0003], [0017]-[0022]. The ’155 Patent was allowed without *any* prior art rejection. The Examiner therefore erred in a manner material to patentability of the Challenged Claims by not citing and applying the prior art relied upon herein.

The prior art discloses a secure execution environment and secure processing agent for generating a unique identifier (e.g., a “time stamp”) associated with a device data record and communicating the unique identifier to a network element over a trusted communication link. The prior art discloses associating the unique identifier with a device data record for monitoring service usage and preventing tampering exactly as disclosed in the ’155 Patent. *See* EX1006 and EX1007 each in their entirety.

Shah (EX1006) illustrates a Fig. 9 digital rights management (DRM) device 900 including a secure time component (STC) 905 configured to generate a unique identifier as a time stamp (e.g., a current date and time) and a Trusted Platform Module (TPM) 910. *See* EX1006, Abs., ¶¶[0010]-[0013]. A unique identifier is associated with each device data record, such as a message, event, data, or audit log.

Id., ¶¶[0008]-[0013], [0059]. The STC has a tamper detection unit configured to detect tampering and to prevent hardware and software level tampering. *Id.*, ¶¶[0025], [0044]. Each unique identifier is included in a signed time certificate and sent to an “outside source” or “requesting client” of the network that verifies the validity of the signed time certificate. *Id.*, ¶¶[0009]-[0011], [0015]. Shah alone or in combination with Naslund (EX1007) discloses the very basis upon which the ’155 Patent was allowed: i.e., sending a device data record and a unique identifier to a network entity of a communication network. The Challenged Claims are therefore unpatentable. *See* EX1006, EX1007, EX1008 each in their entirety.

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

A. Real Parties-In-Interest

Google LLC¹ is a real party-in-interest.

Out of an abundance of caution, Google identifies Apple Inc. (“Apple”) as a real party-in-interest. Apple and Headwater have recently entered into “a worldwide settlement whereby Headwater licensed its patents to Apple.” Patent Owner’s Request for Discretionary Denial of Institution, *Google LLC v. Headwater Research LLC*, IPR2026-00048, Paper 8, 2 (PTAB Jan. 7, 2026).

¹ Google LLC is a subsidiary of XXVI Holdings Inc., which is a subsidiary of Alphabet Inc.

As identified in the related matters below, the '429 Patent is being asserted against multiple Carriers in E.D. Tex. Case Nos. 2:25-cv-00901, 2:25-cv-00902, 2:25-cv-00903, with Case No. 2:25-cv-00902 serving as the lead consolidated case for all pretrial issues. On December 1, 2025, the Carriers in those cases filed a joint opposed motion to stay the litigations under, among other things, the customer-suit exception. *See* Defendants' Joint Opposed Motion to Stay, *Headwater Res. LLC v. Dish Network Corp. et al.*, Civ. Action No. 2:25-cv-00902 (Dec. 1, 2025), ECF No. 55. On December 8, 2025, a redacted version of that motion was made publicly available. *See id.* ECF No. 64. On December 19, 2025, Headwater filed a sealed response to the motion. *See id.* ECF No. 75. On January 9, 2026, the Carriers filed a sealed reply. *See id.* ECF No. 84. In light of these filings, Google names the following Carriers (the named defendants in these cases) as real parties-in-interest to this proceeding:

- DISH Network Corporation f/k/a EchoStar Communications Corporation
- DISH Network LLC
- Dish Wireless, LLC d/b/a Boost Mobile
- Charter Communications, Inc.
- Charter Communications, LLC
- Charter Communications Operating, LLC
- Comcast Cable Communications, LLC d/b/a Xfinity

- Comcast Cable Communications Management, LLC
- Comcast Corporation
- Comcast of Houston, LLC d/b/a Xfinity
- Spectrum Gulf Coast, LLC
- Spectrum Management Holding Company, LLC

Charter Communications, Inc., Charter Communications, LLC, Charter Communications Operating, LLC, Spectrum Gulf Coast, LLC, Spectrum Management Holding Company, LLC and Headwater Research LLC filed a Joint Motion to Stay All Deadlines and Notice of Settlement on August 5, 2026. *Headwater Res. LLC v. Dish Network Corp. et al.*, Civ. Action No. 2:25-cv-00902 (E.D. Tex.), ECF No. 114 (Aug. 5, 2026).

Comcast Cable Communications, LLC d/b/a Xfinity, Comcast Cable Communications Management, LLC, Comcast of Houston, LLC, and Headwater Research LLC filed a Joint Motion to Stay All Deadlines and Notice of Settlement on August 7, 2026. *See Headwater Res. LLC v. Dish Network Corp. et al.*, Civ. Action No. 2:25-cv-00902 (E.D. Tex.), ECF No. 117 (Aug. 7, 2025).

To be clear, none of these Carriers funded, directed, or controlled the filing or preparation of this Petition, nor did Google prepare or file the Petition at the Carriers' behest. Instead, Google makes this identification out of an abundance of caution and in the interest of over-disclosure.

B. Identification of Related Matters Under 37 C.F.R. §42.8(b)(2)

The following is a list of any judicial or administrative matters that would affect, or be affected by, a decision in this proceeding:

Related District Court Matters

Headwater Research LLC v. Google LLC, Civ. Action No. 5:26-cv-07551 (N.D. Cal.) (“7551 Litigation”) transferred from Civ. Action No. 7:25-cv-00369 (W.D. Tex.) (“369 Litigation”) – Complaint filed Aug. 27, 2025 and ordered related to Civ. Action 5:26-cv-01460 (N.D. Cal.) Aug. 7, 2026;

Headwater Research LLC v. Apple Inc., Civ. Action No. 7:25-cv-00370 (W.D. Tex.) – Complaint filed Aug. 27, 2025, Dismissed Oct. 31, 2025 (“370 Litigation”);

Headwater Research LLC v. Charter Communications, Inc. et al., Civ. Action No. 2:25-cv-00901 (E.D. Tex.) – Complaint filed Aug. 27, 2025, Notice of Settlement and Motion to Stay Aug. 5, 2026, Stay granted Aug. 6 – Consolidated with 25-cv-00902 (E.D. Tex.) for all pre-trial issues;

Headwater Research LLC v. Dish Network Corp. et al., Civ. Action No. 2:25-cv-00902 (E.D. Tex.) – Complaint filed Aug. 27, 2025, Stayed July 6, 2026 due to Defendants’ bankruptcy filings;

Headwater Research LLC v. Comcast Cable Communications, LLC d/b/a Xfinity et al., Civ. Action No. 2:25-cv-00903 (E.D. Tex.) – Complaint filed Aug. 27,

Petition for *Inter Partes* Review of U.S. Patent No. 11,985,155

2025, Notice of Settlement and Motion to Stay Aug. 7, 2026, Stay granted Aug. 11, 2026 – Consolidated with 25-cv-00902 (E.D. Tex.) for all pre-trial issues;

Headwater Research LLC v. AT&T Services, Inc. et al., Civ. Action No. 2:25-cv-00215 (E.D. Tex.) – Complaint filed Feb. 18, 2025 – Consolidated with 25-cv-00156 (E.D. Tex.), Dismissed Sep. 30, 2025;

Headwater Research LLC v. T-Mobile USA, Inc. et al., Civ. Action No. 2:25-cv-00164 (E.D. Tex.) – Complaint filed Feb. 10, 2025 – Consolidated with 25-cv-00156 (E.D. Tex.), Dismissed Sep. 30, 2025; and

Headwater Research LLC v. Cellco Partnership d/b/a Verizon Wireless et al., Civ. Action No. 2:25-cv-00156 (E.D. Tex.) – Complaint filed Feb. 6, 2025 – Dismissed Sep. 30, 2025.

Related PTAB Matters

None.

Related Applications

The '155 Patent issued from U.S. Patent App. No. 18/088,450 filed December 23, 2022, which is a CON of U.S. Patent App. No. 17/008,031, filed Aug. 31, 2020 (US Pat 11,665,186), which is a CON of U.S. Patent App. No. 15/977,731, filed May 11, 2018 (US Pat 10,771,980), which is a CON of U.S. Patent App. No. 15/158,522, filed May 18, 2016 (US Pat 9,980,146), which is a CON of U.S. Patent App. No. 14/272,274, filed May 7, 2014 (abandoned), which is a DIV of U.S. Patent App. No.

Petition for *Inter Partes* Review of U.S. Patent No. 11,985,155

13/247,998, filed Sep. 28, 2011 (US Pat 8,725,123), which is a CIP of U.S. Patent App. No. 13/134,028, filed May 25, 2011 (US Pat 8,589,541), which is a CIP of U.S. Patent App. No. 12/695,019, filed Jan. 27, 2010 (US Pat 8,275,830), and a CIP of U.S. Patent App. No. 12/695,020, filed Jan. 27, 2010 (US Pat 8,406,748), and a CIP of U.S. Patent App. No. 12/694,455, filed Jan. 27, 2010 (US Pat 8,402,111), and a CIP of U.S. Patent App. No. 13/134,005, filed May 25, 2011 (US Pat 8,635,335), and a CIP of U.S. Patent App. No. 12/695,021, filed Jan. 27, 2010 (US Pat 8,346,225), which is a CIP of U.S. Patent App. No. 12/380,780, filed Mar. 2, 2009 (US Pat 8,839,388).

The '155 Patent claims priority to U.S. Provisional App Nos. 61/472,606, filed Apr. 6, 2011; 61/435,564, filed Jan. 24, 2011; 61/422,574, filed Dec. 13, 2010; 61/422,572, filed Dec. 13, 2010; 61/422,565, filed Dec. 13, 2010; 61/420,727, filed Dec. 7, 2010; 61/418,509, filed Dec. 1, 2010; 61/418,507, filed Dec. 1, 2010; 61/407,358, filed Oct. 27, 2010; 61/389,547, filed Oct. 4, 2010; 61/387,247, filed Sep. 28, 2010; 61/387,243, filed Sep. 28, 2010; 61/385,020, filed Sep. 21, 2010; 61/384,456, filed Sep. 20, 2010; 61/381,159, filed Sep. 9, 2010; 61/381,162, filed Sep. 9, 2010; 61/348,022, filed May 25, 2010; 61/264,126, filed Nov. 24, 2009; 61/264,120, filed Nov. 24, 2009; 61/252,151, filed Oct. 15, 2009; 61/252,153, filed Oct. 15, 2009; 61/237,753, filed Aug. 28, 2009; 61/275,208, filed Aug. 25, 2009;

61/270,353, filed Jul. 6, 2009; 61/207,739, filed Feb. 13, 2009; 61/207,393, filed Feb. 10, 2009; 61/206,944, filed Feb. 4, 2009; and 61/206,354, filed Jan. 28, 2009.

U.S. Patent App. No. 19/089,864 filed Mar. 25, 2025 is a CON of U.S. Patent App. No. 18/630,537 filed Apr. 9, 2024 (US Pat 12,294,602), which is a CON of U.S. Patent App. No. 18/088,450.

C. Lead and Backup Counsel

Pursuant to 37 C.F.R. §42.8(b)(3) and §42.10(a), Petitioner hereby identifies lead and backup counsel as follows:

<u>Lead Counsel</u> Patrick C. Keane (Reg. No. 32,858) BUCHANAN INGERSOLL & ROONEY PC 1700 K Street, N.W., Suite 300 Washington, DC 20006 Telephone (703) 838-6522 Facsimile (202) 452-7989 patrick.keane@bipc.com	<u>Backup Counsel</u> Roger H. Lee (Reg. No. 46,317) BUCHANAN INGERSOLL & ROONEY PC 1700 K Street, N.W., Suite 300 Washington, DC 20006 Telephone (703) 838-6545 Facsimile (202) 452-7989 roger.lee@bipc.com
<u>Backup Counsel</u> Andrew J. Koopman (Reg. No. 65,537) BUCHANAN INGERSOLL & ROONEY PC 2200 Renaissance Blvd., Suite 350 King of Prussia, PA 19406 Telephone (610) 993-4217 Facsimile (610) 407-0701 andrew.koopman@bipc.com	<u>Backup Counsel</u> Samuel Harrod (Reg. No. 79,148) BUCHANAN INGERSOLL & ROONEY PC Union Trust Building 501 Grant Street Suite 200 Pittsburgh, PA 15219 Telephone (412) 562-8805 Facsimile (412) 562-1041 samuel.harrod@bipc.com

A Power of Attorney is being filed concurrently herewith in accordance with 37 C.F.R. §42.10(b).

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

Petitioner consents to electronic service at the email addresses listed above.

III. FEES

The undersigned authorizes the Office to charge Deposit Account 02-4800 for fees required by 37 C.F.R. §42.15(a).

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

A. Grounds for Standing

Petitioner certifies that the '155 Patent is available for IPR and Petitioner is not barred or estopped from requesting an IPR of the Challenged Claims on the grounds identified herein. 37 C.F.R. §42.104(a).

B. Identification of Challenges and Precise Relief Requested

Petitioner challenges Claims 1, 2, 10, and 11 of the '155 Patent and requests that these claims be found unpatentable for the reasons set forth in Petitioner's Grounds as follows:

Ground	Reference(s)	Basis	Claims
1	U.S. Patent Application Publication No. 2007/0266256 to Shah et al. ("Shah") (EX1006) alone and/or in view of U.S. Patent Application Publication No. 2005/0246282 to Naslund et al. ("Naslund") (EX1007)	§102/103	1, 2, 10, 11

Petitioner relies upon evidence listed in the Exhibit List (Appendix A), including the Declaration and *Curriculum Vitae* of David Williams (EX1011, ¶¶1-

218; EX1012) and the Declaration and *Curriculum Vitae* of Friedhelm Rodermund (EX1024, ¶¶1-116; EX1025).

C. Prior Art Qualification of Asserted References

For this Petition, Petitioner assumes the earliest effective filing date of the '155 Patent is January 28, 2009 — the filing date of U.S. Provisional Application No. 61/206,354.² This is the earliest filing date claimed by the '155 Patent. The '155 Patent is subject to pre-AIA 35 U.S.C. §§102/103.

Shah (EX1006), published on November 15, 2007 and filed on May 8, 2007 is prior art at least under §102(b) and §102(e).

Naslund (EX1007), published on November 3, 2005 and filed on April 25, 2003 is prior art at least under §102(b) and §102(e).

UICC-terminal interface; Physical and logical characteristics (3GPP TS 31.101 version 7.01 Release 7) (EX1018) constitutes prior art as of June 20, 2007 and not later than June 21, 2007 at least under §102(b). *See* EX1024, ¶¶66, 72, 81.

Characteristics of the Universal Subscriber Identity Module (USIM) application (3GPP TS 31.102 version 8.0.0 Release 8) (EX1019) constitutes prior art as of December 21, 2007 at least under §102(b). *See* EX1024, ¶¶84, 98.

² Petitioner does not concede that any challenged claim is entitled to an effective filing date of January 28, 2009.

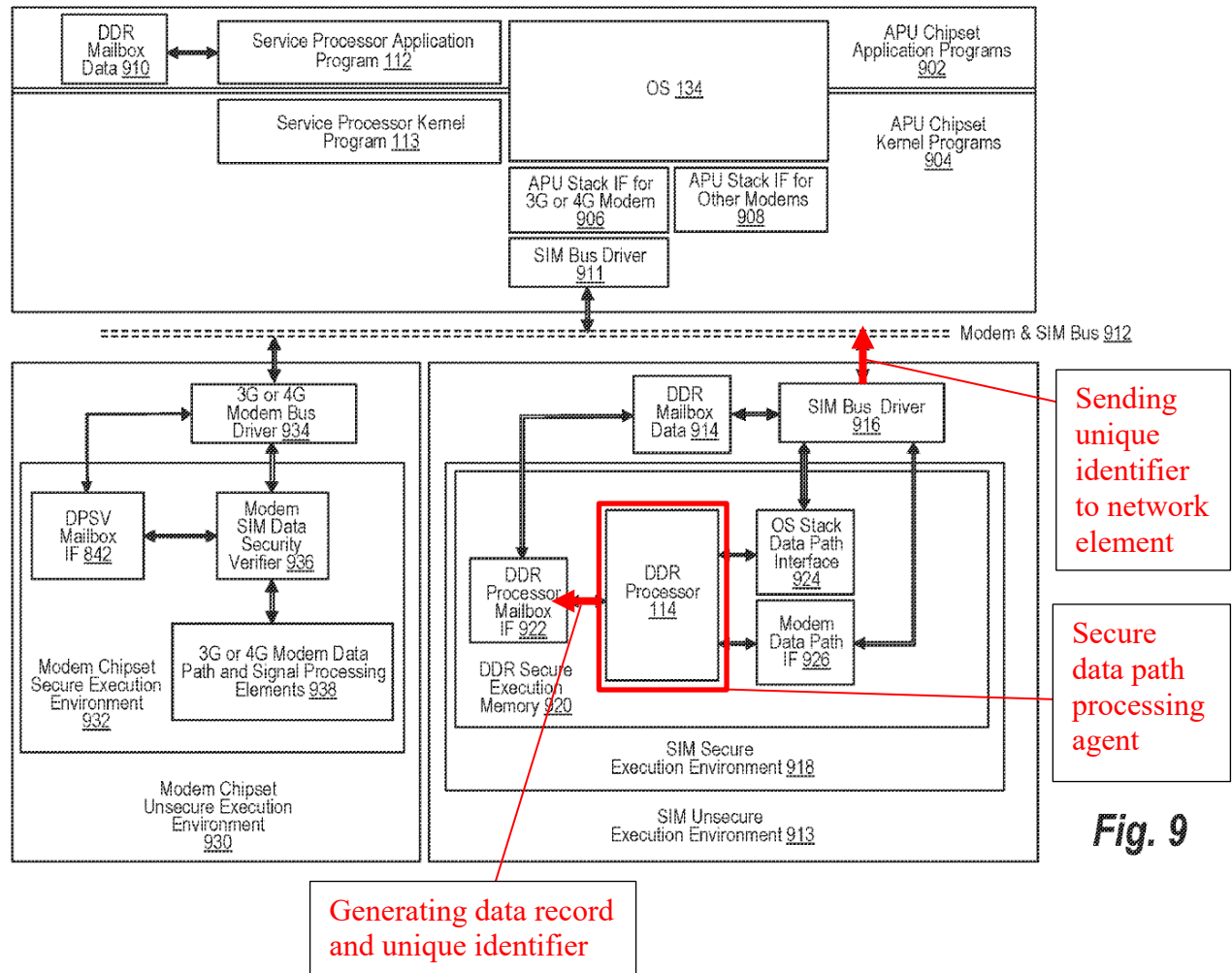
Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface (3GPP TS 51.011 version 4.10.0 Release 4) (EX1020) constitutes prior art as of January 12, 2004 at least under §102(b). *See* EX1024, ¶¶101, 116.

Mobile Execution Environment (MExE); Functional description; Stage 2 (3GPP TS 23.057 version 7.0.0 Release 7) (EX1021) constitutes prior art by June 13, 2007 and not later than June 19, 2007 at least under §102(b). *See* EX1024, ¶¶45, 51, 63.

V. BACKGROUND

A. The '155 Patent

The '155 Patent is directed to a communications device with a secure execution environment for executing a secure data path processing agent configured to generate a unique identifier to secure each device data record (DDR) of monitored service usage. *See* EX1001, Abs., 2:57-3:38. Figure 9 shows an exemplary embodiment of a communications device for generating unique identifiers and DDRs.



EX1001, Fig. 9 (Annotated)

EX1011, ¶¶27-28.

Each “unique identifier” generated by the secure data path processing agent can be used to detect tampering or errors in the monitored service usage. EX1001, 5:41-6:7. Examples of the “unique identifier” include a “time stamp”, “time stamp information”, and/or “sequence count”. *Id.*, 5:55-64. (See also *id.*, 7:62-67; “the unique sequence identifier includes one or more of the following: sequence count, time stamp, start time indicator, stop time indicator, contiguous time interval

identifier, and aggregate usage count at the beginning or end of the record, reference time, or elapsed time at the beginning or end of the record.”). The communications device sends the DDRs with unique identifiers to a network element over a trusted communication link. *Id.*, 9:23-41. For example, a sequence of DDRs in combination with the unique identifiers provide traceability to identify if DDRs have been tampered with or omitted. *Id.*, 7:53-67. The communications device sends the DDRs to a service controller at the network element using a signed or encrypted communication channel so the service controller can determine compliance with a network access policy. *Id.*, 4:17-67. EX1011, ¶¶29-30.

B. Examination History

The only rejection made during prosecution of the ’155 Patent was a non-statutory double patenting rejection based on U.S. Patent 10,771,980 (the “’980 Patent”, EX1022) and U.S. Patent 11,665,186 (the “’186 Patent”, EX1023). Patent Owner addressed this rejection by filing a terminal disclaimer and the Examiner allowed all claims. EX1002, pp.62-120. The Examiner’s reasons for allowance stated that the prior art generally failed to teach independent Claim 1. *Id.*, p.67.

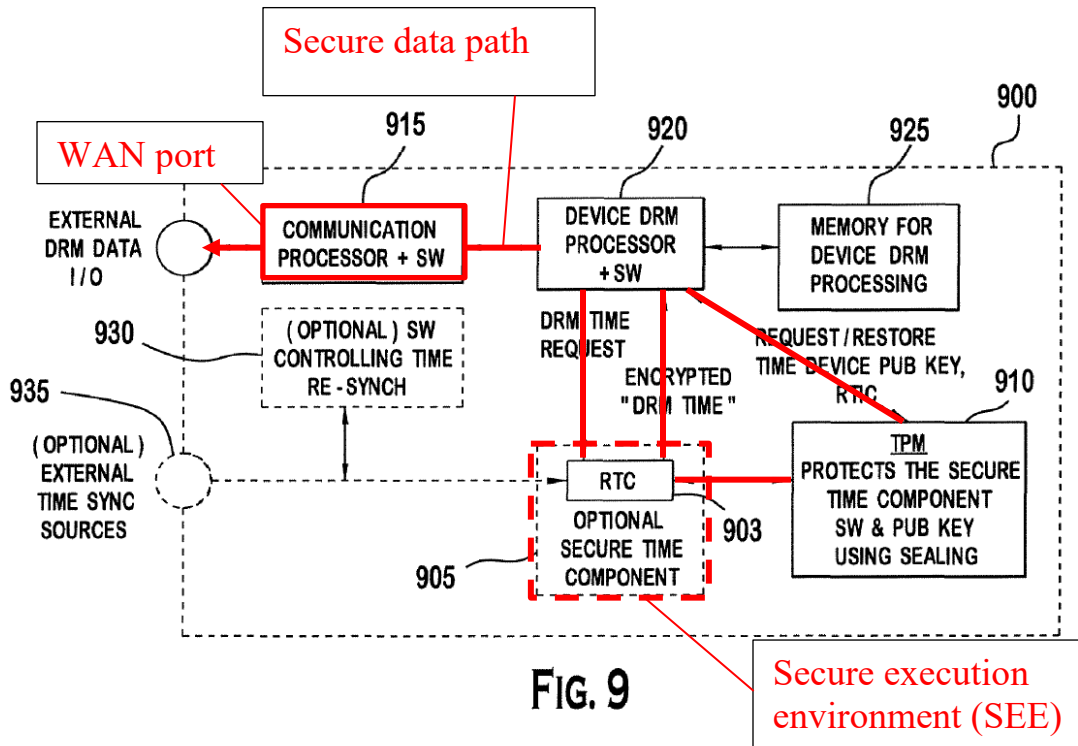
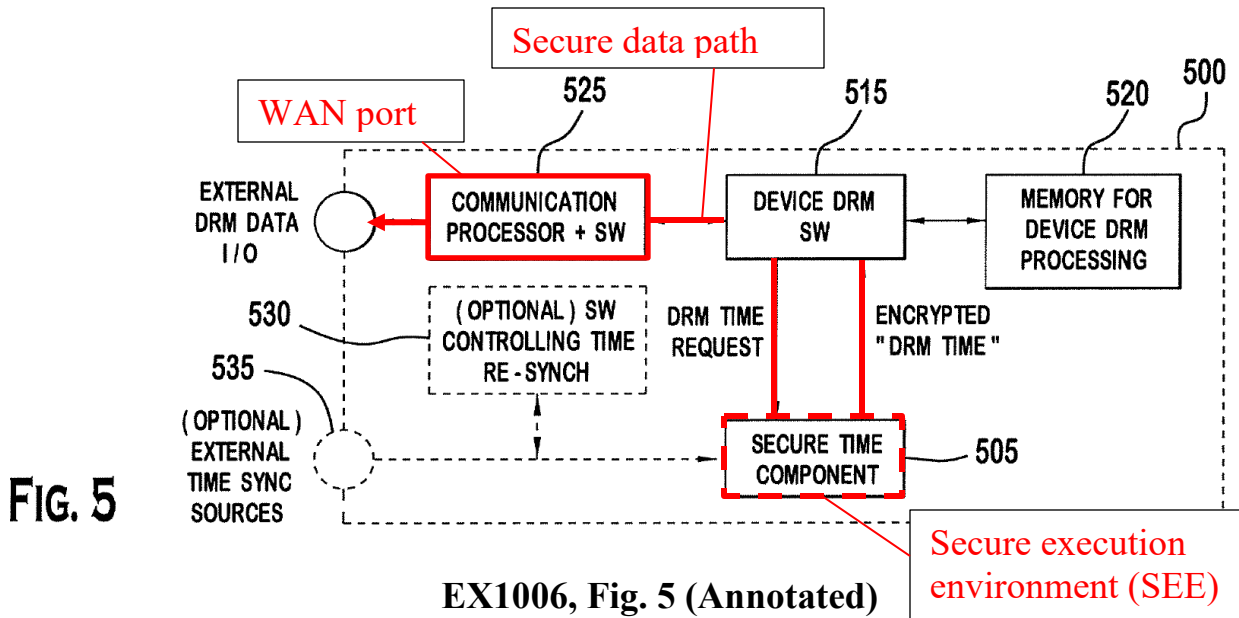
In comparison with the ’980 and ’186 Patent claims, the ’155 Patent adds the claimed concept of associating a “unique identifier” (e.g., “time stamp”) with a device data record. *See* EX1004, EX1005. However, all limitations of the Challenged Claims, including the “unique identifier,” are disclosed in the prior art

cited in this Petition. For example, the prior art cited herein discloses and suggests associating a unique identifier (e.g., time stamp) with a device data record for monitoring service usage and preventing device data record tampering during network communication in exactly the same way as is disclosed in the '155 Patent.

C. Prior Art

1. Shah (EX1006)

Shah illustrates a communications device (e.g., wireless transmit/receive unit (WTRU)) as an exemplary Fig. 9 digital rights management (DRM) device with advanced security functions. EX1006, Abs, ¶¶[0026], Fig. 9. The DRM device includes a secure time component (STC) (i.e., secure execution environment (SEE)) for generating a unique identifier (e.g., secure time certificate) and a trusted platform module (TPM) with secure memory (i.e., protected memory) for executing trusted computing operations. *Id.*, ¶¶[0024], [0041], Figs. 5 and 9. The secure time certificate includes current date and time (i.e., “time stamp”) associated with a device data record (e.g., an audit log). *See id.*, Abs., ¶¶[0008]-[0010], [0013]. The STC communicates the secure time certificate to a requesting network element for verification. *Id.*, ¶¶[0008]-[0011]. *See also id.*, ¶¶[0073]-[0075] (Tables 2, 3, 4). An exemplary STC for generation of a unique identifier (i.e., “Encrypted DRM Time”) is illustrated in Shah’s annotated Figures 5 and 9 below:



EX1006, Fig. 9 (Annotated)

EX1006, Figs. 5, 9; EX1011, ¶¶44-46; *see also* EX1006, Fig. 1 *infra* (§VII.A.1.c.)

2. Naslund (EX1007)

Naslund discloses a communications device as a client device for accessing a

network. The client device has a logging agent for logging information and monitoring usage of received digital content. EX1007, ¶¶[0010], [0052], [0069]. The logging agent is implemented in a secure execution environment for generating secure usage information. *Id.*, ¶¶[0114]-[0115], Figs. 7, 8. The logging agent allows traceability of content usage and provides usage repudiation deterring effects to lower the risk of tampering or violation of usage rules of digital content. *Id.*, ¶[0058]. The client device includes time information (e.g., a time stamp, sequence number, etc.) in the usage information for assessing whether tampering of the usage information occurred. *Id.*, ¶[0097]. The client device transmits the usage information in a secure channel from a secure environment to an external network element for analysis. *Id.*, ¶¶[0074], [0080]. EX1011, ¶¶47-51.

D. Person of Ordinary Skill in the Art (“POSITA”)

A person of ordinary skill in the art (“POSITA”) pertinent to the ’155 Patent at the time of the invention would have at least a bachelor’s degree in computer science, computer engineering, or a similar field, and approximately two years of industry or academic experience in a field related to wireless communications and/or networking. Work experience can substitute for education, and additional education can substitute for work experience. EX1011, ¶36.

VI. CLAIM CONSTRUCTION

Claim terms in an IPR are construed according to their “ordinary and customary meaning” to those of skill in the art. 37 C.F.R. §42.100(b). Petitioner submits that, for the purposes of this proceeding and the grounds presented herein, no claim term requires express construction. *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017).³ Petitioner and Patent Owner have not proposed any express claim construction of any term of the Challenged Claims in the Related Litigation. *See* EX1013, EX1014, EX1015, EX1016, and EX1017. EX1011, ¶¶39-41.

VII. PETITIONER HAS A REASONABLE LIKELIHOOD OF PREVAILING

The Challenged Claims are unpatentable over the prior art. EX1011, ¶50.

A. Claims 1, 2, 10, and 11 are Anticipated by and/or Rendered Obvious over Shah (EX1006) alone and/or in view of Naslund (Ground 1)

The following sections reference where elements of Claims 1, 2, 10, and 11 are anticipated by/obvious over the prior art. EX1011, ¶51.

³ Petitioner does not concede that any term in the Challenged Claims meets the statutory requirements of 35 U.S.C. §112, or that the Challenged Claims recite patentable subject matter under 35 U.S.C. §101.

1. Claim 1 (Preamble): “A communications device comprising:”

To the extent the Preamble is limiting, Shah discloses/suggests the Preamble. The '155 Patent discloses that its communications device encompasses a wireless communications device. EX1001, 2:57-67. Shah “relate[s] to wireless communications systems” and “secured time functionality on a wireless device.” EX1006, ¶[0002]. *See also id.*, ¶[0003] (“wireless communications devices”). Shah discloses a communications device (i.e., a wireless transmit/receive unit (WTRU)) “capable of operating in a wired or wireless connected environment.” *Id.*, ¶[0037]. *See also id.*, ¶[0113]. Shah’s WTRU includes a digital rights management (DRM) device. *See id.*, ¶¶[0003], [0017], [0026], Figs. 5 and 9 (§V.C.1., *supra.*). EX1011, ¶¶52-56.

a. [1.1]: “a wide area network port configured to connect the communications device to a wide area network;”

Shah discloses/suggests Element [1.1]. Shah discloses that the communication device (i.e., DRM device) includes a wide area network (WAN) port configured to connect the communications device to a WAN. *See, e.g.*, EX1006, ¶¶[0003], [0037], [0046], [0113]. Shah’s “DRM device 900” includes a “communication processor 915” that connects to a network and communicates with external data input/output (I/O). *See id.*, Figs. 5, 9, §V.C.1., *supra.* (Fig. 9 DRM device 900 includes “communication processor 915” the functions of which are also discussed in relation

to the Fig. 2 “communication processor 215”). Shah’s WTRU establishes “a secure channel between the WTRU and the network.” EX1006, ¶[0040]. EX1011, ¶¶57-60.

Shah’s WTRU connects to various WANs such as mobile wireless networks and/or the “Internet.” EX1006, ¶[0003] (“connectivity to internet based services”, “content is delivered over a wireless network”), ¶[0037] (device connects to “an access point (AP), or any other type of network”). *See also id.*, ¶¶[0046], [0113]. A WAN includes a mobile network such as a 2G, 3G, or 4G network, and so forth. *See* EX1001, 3:21-25. EX1011, ¶61.

A POSITA would have understood that a cellular or mobile network (e.g., 3G network implementing 3GPP standards) disclosed by Shah is an example “wide area network” because such networks covered wide areas such as cities. *See* EX1006, ¶[0016]. Such networks conforming to the 3GPP standards (a 3G mobile network or other cellular voice/data network, e.g., 1G, 2G) were widely known as WANs, and methods/systems for connecting to such networks were well known in the art prior to the filing date of the ’155 Patent. *See, e.g.*, EX1009, ¶[0012] (“international standards collaboration project for wireless wide area networks, the 3rd Generation Partnership Project (3GPP)”), ¶¶[0038]-[0044]. *See also* EX1007, ¶[0153] (referencing “3GPP”), EX1008, ¶[0004]. EX1011, ¶¶62-63.

Shah’s “communication processor” and communication path thereof for connection with a WAN constitutes the claim 1 “WAN port” because it is

“configured to connect the communications device to a wide area network.” Shah does not explicitly use the term “wide area network port” but discloses a WTRU (i.e., DRM device) having a 3G network connection (i.e., a WAN port) for network connectivity. EX1011, ¶¶64-65.

A POSITA would have recognized that components (such as Shah’s communication processor) providing network connectivity via a “network connection” (e.g., to the Internet or a cellular network such as 3G) for a device (Shah’s DRM device) constitute a WAN port—logical and/or physical. *See* EX1006, ¶[0016] (referencing “3GPP” compliant devices). *See also id.*, ¶[0037] (“network interfacing device capable of operating in a wired or wireless connected environment.”). Shah’s network connection constitutes a WAN port configured to connect the DRM device to a WAN (e.g., a 3GPP compliant network). A POSITA would have understood Shah’s 3G network connection to be a WAN port because documents demonstrating the state-of-the-art prior to the filing date of the ’155 Patent used the term “WAN port” to describe 3G network connections of Shah. *See* EX1010, ¶[0030]. EX1011, ¶¶66-68.

State-of-the-art references such as Lu (EX1009) and Rada (EX1010) make clear that a 3G network is a WAN and that a WAN connection is synonymous with a “WAN port”. *See, e.g.*, EX1009, ¶[0042] (“third generation (3G) wireless wide area networks”), EX1010, ¶¶[0005], [0029]-[0030] (“wireless WAN port”), Fig. 1A.

The only claimed function of the WAN port in claim 1 is “to connect the communications device to a wide area network.” EX1011, ¶¶69-71.

The ’155 patent “port” functions as a wireless network connection and the ’155 Patent describes exemplary embodiments where the port is a wireless network connection. *See* EX1001, 2:66-3:1 (“a wireless connection and other input/output (I/O) connections or ports”), 3:24-29 (“a wide area wireless network (e.g., 2G, 3G, 4G, etc.) ... or another I/O connection or port”). *See also id.*, 3:43-53, 25:43-54, 43:58-61. Shah teaches a WAN port configured to connect the communications device (i.e., DRM device) to a WAN. EX1006, ¶[0113]. *See* EX1001, 4:5-10. To the extent it is argued that Shah does not expressly disclose a “WAN port,” a POSITA would have understood Shah’s network connection to function identically as a WAN port (e.g., a 3GPP compliant device). *See* EX1006, ¶¶[0016], [0037]-[0040]. Use of a WAN port to connect Shah’s DRM device to a WAN would have been an obvious implementation of Shah for the same reasons discussed above. EX1011, ¶¶72-75.

b. [1.2]: “a secure memory;”

Shah discloses/suggests Element [1.2]. Shah discloses that the communication device (“DRM device”) includes a secure memory. The DRM device includes a secure memory (“protected memory”, “RAM under TPM-protection”, or “TPM-controlled memory”) inside of or external to a Trusted Platform Module (TPM)

within the DRM device. EX1006, ¶¶[0045], [0091], [0095], Fig. 9 (including “TPM 910” the functions of which are also discussed in relation to “TPM 250” and “TPM 330” of Figures 2 and 3, respectively). Even in embodiments where the memory is outside of the TPM, it is “protected with encryption by TPM” and therefore still secure. *See id.*, ¶[0095] (“DRM time [is] restored from the TPM-controlled memory”). A POSITA would have further understood Shah’s memory to be secure due to Shah’s techniques and systems providing for “*secure* time functionality for a wireless device” (*see* title) and doing so by use of, *inter alia*, the secure (“protected”) memory. *Id.* at ¶[0045]. *See also id.*, ¶[0041] (STC “is configured to provide a secure record of the time of certain events, or data entries.”). EX1011, ¶¶76-78.

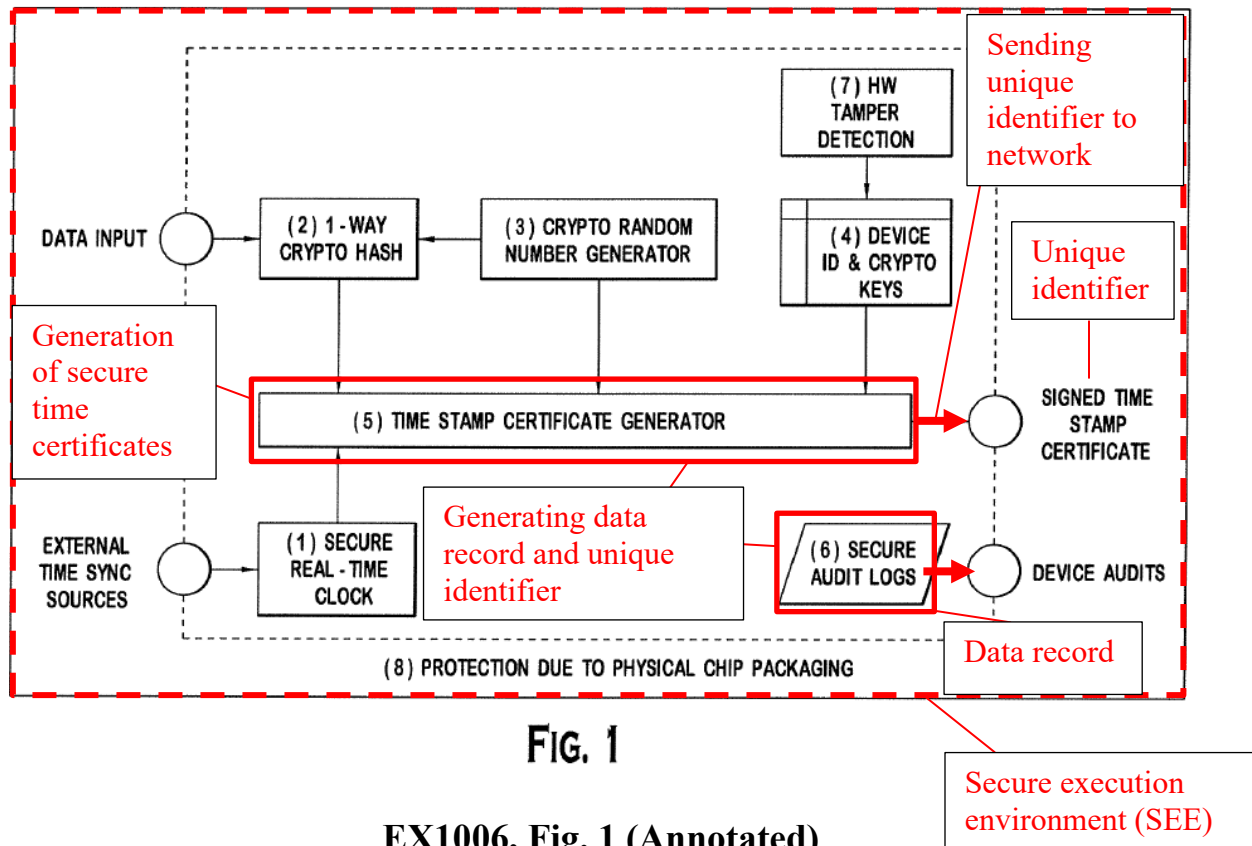
c. [1.3]: “a secure execution environment configured to be inaccessible to a user application software; and”

Shah discloses/suggests Element [1.3]. Shah discloses a secure execution environment (SEE) (e.g., the secure time component (STC) of Fig. 9 that generates time certificates) configured to be inaccessible to “a user application software.” *See*, EX1006, Abs., ll.4-6, ¶¶[0008]-[0010], [0024], [0045], Fig. 1; *see also id.*, Figs. 5, 9 including “STC 505” and “STC 905”, respectively, the functions of which are also discussed in relation to “STC 230” and “STC 340” of Figures 2 and 3, respectively. EX1011, ¶¶79-80.

Shah’s Figure 1 shows a secure execution environment including executable functions of the STC to generate the secure time certificates, including the secure

real-time clock (e.g., the RTC), cryptographic hashing, time stamp certificate generation, and audit logging. EX1006, ¶¶[0008]-[0010], [0012], [0024], [0041], Fig.

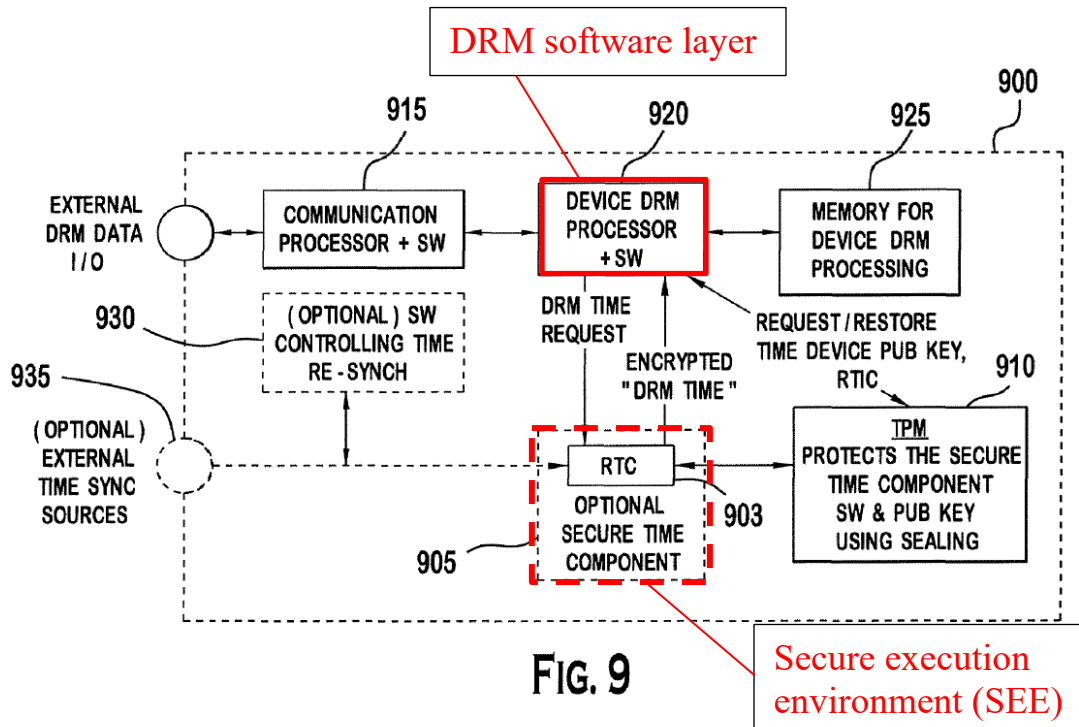
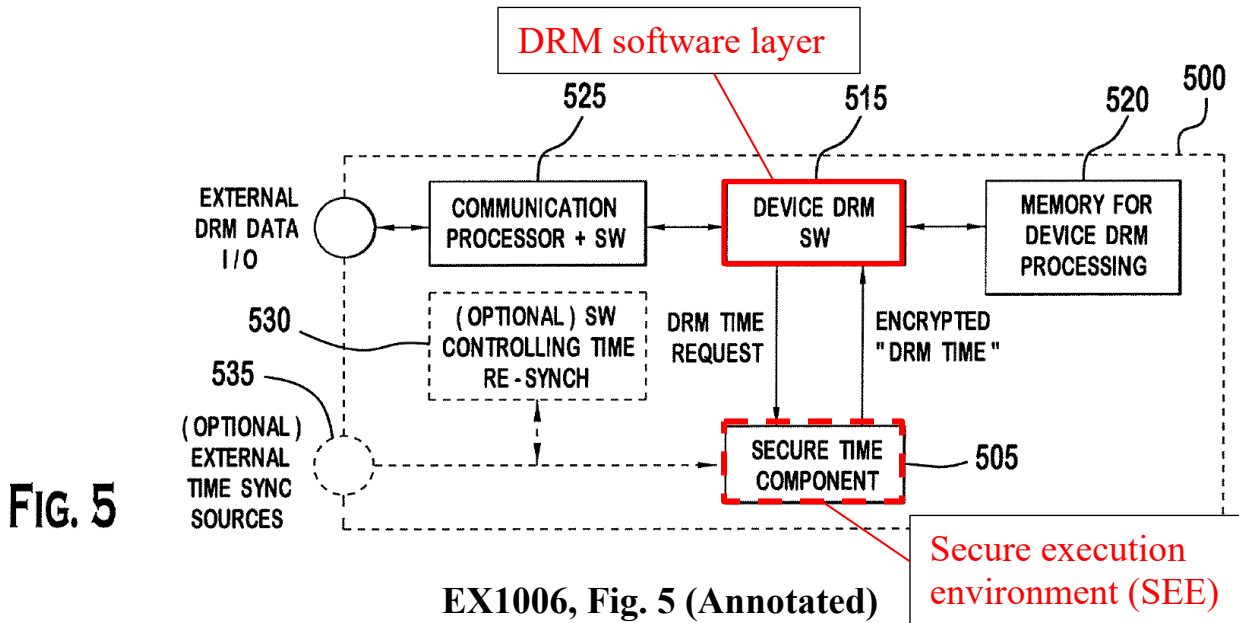
1.



EX1011, ¶81. The SEE of the STC (outlined in red above) used to generate the secure time certificates is included within a secure physical chip (i.e., “PROTECTION DUE TO PHYSICAL CHIP PACKAGING”). *Id.* EX1011, ¶82.

Shah’s Figure 5/9 embodiments include “digital rights management (DRM)” devices implementing secure DRM software. *See* EX1006, ¶¶[[0003], [0017]-[0023], [0026]. DRM “imposes additional requirements ... to ensure that the content stored on the device is accessed by authorized users” and “that the content is being accessed

in a trusted manner.” *Id.*, ¶[0003]. *See also id.*, ¶¶[0026], [0032], [0036]. Shah’s DRM device embodiments are shown in Figures 5 and 9 (annotated below) implementing a DRM software layer.



EX1006, Fig. 9 (Annotated)

EX1006, Figs. 5 and 9; EX1011, ¶83. Shah’s DRM software (i.e., “Device DRM SW 515” and “Device DRM Processor and SW 920”) is a secure component providing an additional layer of security to the SEE (i.e., STC 505/STC 905), making the SEE further inaccessible to all user application software. EX1011, ¶84.

STC 505/905 (of Shah’s Figures 5/9) can “optionally” use “External Time Sync Sources 535/935” to “re-synchronize its internal clock.” EX1006, ¶¶[0062], [0085]. External Time Sync Sources 535/935 of Shah are not required to interact with STC 505/905 in order to generate the secure time certificate (i.e., unique identifier). Even in embodiments where External Time Sync Sources 535/935 do interact with STC 505/905 for time re-synchronization, External Time Sync Sources 535/935 are “dependable and unalterable external source[s]” such as “secure time server[s]” that do not include user applications. *Id.*, ¶[0090]; *see also id.*, ¶[0015] (“A secure time server is defined herein as a network based server that, upon request by a client on the network, securely provides a reference time to the requesting client over the network”). These secure time servers perform secure re-synchronization of the STC’s internal clock which is then used to generate the secure time certificates upon request from a separate requesting entity (e.g., rights issuer (RI) of Figs. 7 and 8). *Id.*, ¶[0041] (“The STC 230 is configured to provide a secure record of the time of certain events, or data entries, in the form of a time certificate or signatures of

time related data, as outputs to a requesting entity.”), Figs. 7 and 8. A POSITA would have understood that secure time servers do not include user applications as they are reference points for the generation of secure time certificates (i.e., unique identifiers), as opposed to requesting entities using the certificates for authentication of user applications. EX1011, ¶¶85-87.

“Software (SW) Controlling Time Re-Synch 530/930” is also optional and does not include user applications as it is secure software (i.e., instructions) solely for controlling time re-synchronization. *See* EX1006, ¶[0062] (“SW controlling the time re-synch function 530 may be used to control the re-synchronizing process so long as it is secure and isolated from the device DRM SW 515.”). A POSITA would have understood that secure software used solely for re-synching an internal clock to generate a secure time certificate would not include user applications. EX1011, ¶¶88-89.

Because both Software (SW) Controlling Time Re-Synch 530/930 and External Time Sync Sources 535/935 are “optional,” to the extent that Patent Owner contends that these components somehow demonstrate that the STC is accessible to a user application software, Petitioner relies on Shah without these “optional” components. Disclosure of an alternative embodiment (i.e., one with optional components) in a prior art reference does not preclude reliance upon other embodiments (i.e., ones without optional components). *See In re Fulton*, 391 F.3d

1195, 1201 (Fed. Cir. 2004) (“The prior art’s mere disclosure of more than one alternative does not constitute a teaching away from any of these alternatives because such disclosure does not criticize, discredit, or otherwise discourage the solution claimed”). EX1011, ¶90.

The ’155 Patent specification does not expressly recite the phrase “inaccessible to a user application software” outside of the express claim language. In exemplary embodiments, the ’155 Patent specification refers to “user application software”, “user application programs 130”, and “application programs 130.” EX1001, 26:55-56. Fig. 1 (“application programs 130”), Fig. 3 (“user application programs 130”). The ’155 Patent’s “user application programs 130” do not directly access the SEE and are shown to reside outside of the SEE. *See id.*, Figs. 3, 16. The ’155 Patent does not describe the “user application programs 130” or “application programs” as having access to the SEE. *See* EX1006, ¶¶[0008]-[0014], [0044]. EX1011, ¶¶91-92.

Shah’s SEE is similarly “inaccessible to a user application software” because: (1) the STC is inaccessible to all “external attempts” for access; i.e., the STC is “configured to resist external attempts to compromise the device’s internal operations, internal records, or the signed time certificate outputs” (EX1006, ¶[0008]); (2) Shah’s SEE of the STC is “tamper-resistant” (*id.*, ¶[0010]); i.e., it prevents “hardware and software level tampering” (*id.*, ¶[0044]); (3) the STC

presents “an unequivocal, non-alterable and non-repudiable certificate of the current time—also known as a signed time certificate” (*id.*, ¶[0008]; *see also id.*, ¶¶[0012]-[0014]); and (4) any communication to/from the SEE is via a secure channel (*id.*, ¶[0061]). EX1011, ¶93.

The STC of Shah receives “a request for a signed time certificate” as “data input”. EX1006, ¶[0010], Fig. 1. The STC then reads the current date and time from the RTC (“(1) secure real-time clock”) (*id.*, Fig. 1) “securely (i.e., In a tamper-evident and/or tamper-resistant way)” and “a certificate is generated” (“(5) time stamp certificate generator”) (*id.*, Fig. 1) containing the “current date and time ... and any other audit logs” (“(6) secure audit logs”). *Id.*, ¶[0010], Fig. 1. The STC appends a signature to the certificate and presents the time certificate “as combined output.” *Id.* EX1011, ¶94.

The '155 Patent describes that the SEE can receive secure messages from network elements outside of the SEE and generate data records that are then sent outside the SEE. The '155 Patent's “DDR processor located in the secure execution environment is configured to send the device data records to a network element (e.g., storage function located in the network).” EX1001, 9:23-26. *See id.*, 9:23-65. The network elements (e.g., storage functions) that receive the device data records from the SEE have a “secure communication channel” established with the SEE. *Id.*, 9:42-45. The '155 Patent does not describe any secure communication channels between

the SEE and “user application programs 130”. Thus, the SEE is inaccessible to “user application software.” EX1011, ¶¶95-96.

Shah’s unique time certificates are similarly transmitted from the SEE (e.g., components of the STC 505 or STC 905) to external elements (e.g., Device DRM Software (SW) 515 or Device DRM Processor and SW 920) via a secure communication channel. *See* EX1006, ¶¶[0061] (“Reports containing the DRM time may be sent in UTC format and may include a digital signature signed by a private key of a public key pair.”). The STC 505 exclusively sends its unique time certificates to the DRM software (i.e., no user application software access) along this secure communication channel. Similarly, the STC 905 only sends the time certificates to the DRM processor and software and to the TPM to “further strengthen the time-information security provided”. EX1006, ¶¶[0097]. Shah’s SEE is therefore inaccessible to user application software to the same extent as the SEE of the ‘155 Patent. EX1011, ¶¶97-99.

d. [1.4]: “a secure data path processing agent configured to:”

Shah discloses/suggests Element [1.4]. Shah’s communication device (i.e., DRM device) includes a secure data path processing agent (i.e., STC and TPM). *See* Element [1.3], *supra*. EX1006, ¶¶[0039], [0045]; *see also id.*, Fig. 9 including “TPM 910” the functions of which are also discussed in relation to “TPM 250” and “TPM 330” of Figures 2 and 3, respectively. *See id.*, ¶¶[0039]-[0047]. EX1011, ¶¶100-101.

Shah's STC and TPM are "configured to provide a secure record of the time of certain events, or data entries" (i.e., device data records) for monitoring and reporting to a requesting entity. EX1006, ¶[0041]. The STC is a secure agent for monitoring and reporting secure time components of the DRM device's communication activity (e.g., data, messages, events). *Id.*, ¶[0059]. *See id.*, ¶¶[0086]-[0087]. Shah's STC processes data with secure time records as the data traverses the DRM device's data path (e.g., inputs/outputs), constituting a secure "data path" processing agent. *See id.*, ¶¶[0006]-[0011], Figs. 5, 9. EX1011, ¶¶102-104.

Shah's TPM secures the data path by providing protected memory for securing time records from tampering. *See* EX1006, ¶¶[0005]-[0010]. For example, the TPM can "perform privacy-protected authentication and attestation of the platform" and "secure binding, sealing and signing of data to secure keys protected by the TPM itself." *Id.*, ¶[0006]. The TPM is "used to provide many useful 'secure' applications." *Id.*, ¶[0007]. *See also id.*, ¶[0005]. EX1011, ¶¶105-106.

Shah's STC and TPM constitute a secure data path processing agent because together these components "provide many useful 'secure' applications" that "resist external attempts to compromise the device's internal operations, internal records, or the signed time certificate outputs." *Id.*, ¶¶[0007]-[0008]. "The STC and the TPM are integrated to provide accurate trusted time information for applications internal

and external to the WTRU” (i.e., DRM device). *Id.*, ¶[0024]. Because the protected memory on the DRM device is “protected with encryption” by the STC and TPM regardless of where the protected memory is located (*see id.*, ¶[0045]), the data path traversed by the time records from storage in the protected memory to an external network is secured by the STC and TPM. Shah’s STC and TPM further secure the data path traversed by time records by cryptographically protecting “the public key that can decrypt the DRM [t]ime information,” such that the time records are secure from malicious processes/actors. *Id.*, ¶[0100]. The TPM provides an additional layer of security by performing “time-requester authentication and [an] integrity-check of the STC on a DRM device 900.” *Id.*, ¶[0098]; *see also id.* (“The security of an STC 905 as described above can be further strengthened, in the context of a device DRM application, by using the functionality that a TPM 910 can provide.”). EX1011, ¶¶107-110.

The ’155 Patent explains that a “data path” is secure where, for example, the data path “cannot be accessed by device user application software.” EX1001, 56:63-66. The data path “is secured by signing or encrypting with a shared key.” *Id.*, 58:66-67. Shah’s “data path” traversing the TPM is secure because it is “protected with encryption” using a public key and is “under cryptographic protection by the TPM 910 using a TPM Sealing command”. EX1006, ¶¶[0045], [0100]. *See id.*, ¶[0005] (“local protection of data are thereby made much more secure with the TPM.”),

¶[0007] (“A platform that has a TPM bound on it can be used to provide many useful ‘secure’ applications.”), Figs. 5 and 9 (“Encrypted ‘DRM Time’”). Processing the “data path” with the STC and TPM allows the DRM device to process and monitor user data transmitted over the network. *See id.*, ¶¶[0007], [0020]-[0024], [0041] (“The STC 230 is configured to provide a secure record of the time of certain events, or data entries, in the form of a time certificate or signatures of time related data, as outputs to a requesting entity”), [0048]. EX1011, ¶¶111-112.

Shah’s Fig. 9 shows an exemplary secure data path through which time records are transmitted with protection from the STC and TPM. *See* EX1006, Fig. 9, §V.C.1., *supra*. Shah’s STC and TPM are configured to perform secure data path processing for the DRM device by monitoring and reporting communication activity within the DRM device with a secure source of time. EX1006, ¶[0054]. *See also id.*, ¶[0059]. TPM security prevents external software, such as user application software, from accessing the TPM and the STC (the secure source of time) of the SEE. *Id.*, ¶¶[0005], [0040], [0100]. EX1011, ¶¶113-115.

e. [1.5]: “execute in the secure execution environment;”

Shah discloses/suggests Element [1.5]. Shah’s secure data path processing agent (STC and TPM) is configured to execute in the secure execution environment (i.e., SEE, within the STC). Shah’s STC and TPM execute secure operations within the SEE of the STC to monitor usage and generate secure time certificates. EX1006,

¶¶[0008], [0025], [0039]-[0042], [0045], [0091], [0095], Figs. 1, 5, and 9. *See* Elements [1.6]-[1.10]. *See also* Element [1.3], *supra*. Shah's STC components are configured to execute functions in the SEE of the STC to generate secure time certificates. *Id.*, ¶¶[0008], [0010], [0012], [0013], [0024]. *See* Element [1.3], *supra*. EX1011, ¶¶116-118.

f. [1.6]: “generate a unique identifier for communication to a network element in the wide area network;”

Shah discloses/suggests Element [1.6]. Shah discloses that the secure data path processing agent (i.e., STC and TPM) is configured to generate a unique identifier as a secure time stamp for data (including a current date and time). *See, e.g.*, EX1006, ¶¶[0008]-[0010], [0025], [0041], [0048], [0059]. This time stamp forms a unique identifier in the same manner as the “sequence count and/or time stamp information” constituting unique identifiers in the '155 Patent. EX1001, 5:55-59. EX1011, ¶¶119-120.

The secure time stamp is part of a signed time certificate for communication to a network element in the WAN. Shah's STC (e.g., via a time report and sync controller as a component of the STC, *see* EX1006, ¶[0041]) is configured to generate the signed time certificate including a “hash, current date and time [*time stamp*] ... and any other audit logs”. *Id.*, ¶¶[0008]-[0010], [0025], Fig. 1 ((5) time stamp certificate generator), Fig. 9 (DRM device 900 including STC 905 and TPM 910). Each of the time stamp and/or hash are used for non-repudiation and

identification of a secure time for the signed time certificate. *Id.*, ¶[0008] (The STC presents “an unequivocal, non-alterable and non-repudiable certificate of the current time—also known as a signed time certificate”), ¶[0013]. EX1011, ¶¶121-122.

Shah discloses that the STC generates the signed time certificate including the secure time stamp. EX1006, ¶¶[0009]-[0010] (“The generation of a valid signed time certificate *by* an STC is a two step process.”) (emphasis added). *See id.*, Fig. 1 ((5) time stamp certificate generator). The unique identifier (i.e., secure time stamp) of the signed time certificate is for communication to a network element (e.g., a “Rights Issuer” (RI) platform, or verifier) in a wide area network for verification. *See id.*, ¶[0009] (“an outside source must verify the validity of the signed certificate”), ¶[0011] (verification by an “outside ‘verifier’”), ¶[0016] (“It would be desirable to improve the 3GPP authentication protocols to include time information and hence provide an opportunity for the local time to be verified or synchronized with the network time.”). *See e.g.*, Fig. 7 (DRM device transmitting “request time”), Fig. 8, (DRM device transmitting “ROLE (rights object last examined) parameter”), Tables 5-8, ¶¶[0078]-[0080]. EX1011, ¶¶123-124.

Shah’s DRM device is a WTRU implementing an STC and TPM for Digital Rights Management (DRM). EX1006, ¶[0026]. *See id.*, ¶¶[0003], [0017]-[0018]. Shah’s WTRU (i.e., DRM device) sends a unique identifier (i.e., time stamp) as a

Time an RO (rights object) was last examined (T-ROLE) as part of the RO last examined (ROLE) parameter to the network element (e.g., rights issuer or “RI”) in a Rights Object Acquisition Protocol (ROAP) request messages to provide a secure record of the time. *See id.*, ¶¶[0078]-[0079], Fig. 8. The STC and TPM generate a unique identifier for communication to a network element (e.g., rights issuer (RI) in Shah’s DRM device) in the wide area network. EX1011, ¶¶125-126.

Shah’s DRM device is connected to a WAN (*see* Element [1.1], *supra*) and communicates with an “outside” (i.e., network) element that verifies the certificate, which Shah refers to as an “outside source” (EX1006, ¶[0009]), “outside verifier” (*id.*, ¶[0011]), “requesting entity” (*id.*, ¶[0041]), and rights issuer (“RI”) (*id.*, Fig. 8). Shah seeks to improve “network” protocols for trusted monitoring of service and/or content usage of content provided over the “network.” *Id.*, ¶¶[0003], [0016]-[0019]. A POSITA would have therefore understood that Shah discloses and teaches that the verifier/RI is in the “network” (WAN). Alternately such a configuration would have been an obvious implementation given Shah’s teachings that the verifier/RI is “outside” the DRM device and the DRM device is connected to the network/WAN. *Id.*, ¶¶[0009], [0011], [0016], [0040]-[0041], Fig. 8. *See also id.*, ¶[0072] (Table 1, RI sends server-specific info); Element [1.10], *infra*. EX1011, ¶¶127-129.

A POSITA would have understood that Shah’s “rights issuer” (“RI”) is a separate entity in the network (WAN) outside of the user device. *See* EX1007,

¶¶[0056] (“In a typical implementation, a network operator often fills the roll of the rights issuer.”), [0048] (“DRM functionalities are implemented ... in a server of the network operator...”), [0055]. EX1011, ¶130.

g. [1.7]: “store the unique identifier in the secure memory;”

Shah discloses/suggests Element [1.7]. Shah discloses that the secure data path processing agent is configured to store the unique identifier in the secure memory. Shah’s TPM (of the secure data path processing agent—in combination with the STC) stores secure time stamps (i.e., the “unique identifier” in the signed time certificates) in the secure memory (i.e., protected memory) through interaction with the STC (i.e., SEE). EX1006, ¶¶[0039], [0045] (“the time records produced by the RTC 240 and associated time reporting and re-synch controller 235 are stored in protected memory.”), [0091] (“DRM device 903 is first configured to store a protected value T-Period pre-stored either in secured ROM or in the RAM under TPM-protection... DRM device runs an RTIC (run-time integrity check) of the RTC 903, then measures the current time from the RTC 903, and stores that time value under a TPM Bind or Seal command.”), [0095], [0096] (“DRM time [is] restored from the TPM-controlled memory”). In the DRM device embodiment of Fig. 9, for example, Shah’s TPM “securely store[s] a current DRM time” produced by and received “*from the RTC*” included in the STC. *Id.*, [0095] (emphasis added). Because Shah’s time certificate is stored in the “TPM-controlled memory”, the

“current date and time” and/or “secure time stamps” included in the signed time certificate are therefore also stored in the “TPM-controlled memory.” *Id.*, ¶[0095], Fig. 1. *See* Element [1.6], *supra*. EX1011, ¶¶131-133.

A POSITA would have understood Shah’s signed time certificate to include the unique identifier. *See* EX1006, ¶[0041] (“STC 230 is configured to provide a secure record of the time of certain events, or data entries, in the form of a time certificate”), ¶[0045] (“The presence of a TPM 250 also can ensure that the time records produced by the RTC 240 and associated time reporting and re-synch controller 235 are stored in protected memory.”), ¶[0053]. EX1011, ¶134.

The TPM of Shah’s DRM device stores the unique identifiers (i.e., time stamps of signed time certificates) in protected memory to also maintain the disclosed integrity and non-repudiation features. *Id.*, ¶¶[0008]-[0014], [0040]. *See also id.*, ¶¶[0055], [0057]-[0058], [0091], [0095]-[0096]. Shah’s protected memory “may be located either inside the non-volatile memory in the TPM itself, or in memory external to the TPM but protected with encryption by TPM.” *Id.*, ¶[0045]. Shah’s TPM therefore manages and protects secure time stamps stored in the protected memory by “performing trusted computing operations”. *Id.*, ¶[0024]. EX1011, ¶¶135-137.

h. [1.8]: “generate a data record;”

Shah alone and/or in view of Naslund disclose(s)/suggest(s) Element [1.8]. Shah discloses that the secure data path processing agent is configured to generate a data record, because Shah’s certificate includes an “audit log” which is a data record. EX1006, ¶[0010] (“any other audit logs”), Fig. 1 (“device audits”, (6) secure audit logs), ¶[0006] (“stored memory logs (SMLs)”). Shah discloses that “[t]he STC is also configured to resist external attempts to compromise ... internal records, or the signed time certificate” including the audit log. *Id.*, ¶[0008]. Shah’s audit log is generated by the STC as part of the time certificate within the secure environment. *See id.*, ¶[0025] (Shah’s STC will “save information relating to the RTC ... in an audit log.”); *Id.*, ¶[0010]. *See also id.*, Fig. 1 (the audit log is “secure”). Shah discloses that the STC “produce[s]” the signed time certificate which includes the “secure time stamp”. *Id.* EX1011, ¶¶138-142.

Shah’s STC is also configured to provide a secure time stamp of “***certain events, or data entries***, in the form of a time certificate or signatures of time related data, as outputs to a requesting entity.” EX1006, ¶[0041]. Examples of data records include “phone book applications and data, mobile payment or ticketing applications and related data, authentication and key management functions, or data related to mobile communication protocol stacks.” *Id.*, ¶[0048]. *See also id.*, ¶¶[0011] (describing a “data file”), [0013] (“A signed time certificate is understood to be an

undeniable proof of the date and time that the data was notarized”). EX1011, ¶¶143-144.

Shah discloses that its “secure time stamping” is for data records including “messages, events, or data ... and other related log data”, *id.*, ¶[0059]. *See also id.*, ¶[0012] (STC outputs “the time of the event”), ¶[0041] (STC provides “a secure record of the time of certain events, or data entries, in the form of a time certificate or signatures of time related data”). Shah’s notarized events or data entries constitute an “audit log.” Where the WTRU is a DRM device (*see* Element [1.6], *supra*), the “data record” is an event with a time record (e.g., a log) associated with usage of ROs. EX1006, ¶¶[0078]-[0079]. *See also id.*, ¶¶[0041], [0096]. Shah’s signed time certificates (including the secure time stamps, i.e., unique identifiers) are used to notarize data records generated by the STC. *See id.*, ¶¶[0008]-[0013]. EX1011, ¶¶145-147.

To the extent it is argued that Shah’s audit log is not expressly disclosed as being a data record, a POSITA would have understood an audit log to constitute a data record, as disclosed by Naslund. EX1011, ¶148.

Naslund

Naslund (EX1007) demonstrates that generating data records was well known in the art. Naslund discloses a logging agent on a client device (e.g., a wireless device) that “generates and logs usage information” where usage information “can

be found in a log entry 172.” EX1007, ¶¶[0069], [0087]. Usage information includes “a representation 172-1 or description of the used digital content, e.g. a fingerprint identifying the content or the file name associated with the content.” *Id.*, ¶[0088]. *See id.*, Fig. 6 (logged data record including “representation of digital content”). *See also id.*, ¶¶[0105], [0107]. Naslund discloses embodiments including “a DRM agent 330 incorporating a logging agent” to generate usage information for logging. *Id.*, ¶¶[0127]-[0128]. EX1011, ¶¶149-151.

Naslund demonstrates that it would have been obvious to implement a “logging agent” or similar component in Shah’s STC to generate usage information for Shah’s “audit logs”, including at least a representation or description of digital content used. EX1007, ¶[0088]. A POSITA would have recognized that Naslund’s logging agent would have been useful for a DRM agent as disclosed in Shah because Naslund expressly includes a logging agent in a DRM agent. *See* EX1007, Figs. 2, 7, 8 (on a SIM). Shah expressly recognizes the need for secure time and TPM capabilities on DRM devices to enable more reliable and secure DRM processing. EX1006, ¶[0017]. *See id.*, ¶¶[0017]-[0020], [0109]-[0110]. Implementing Naslund’s logging agent would have improved Shah’s audit log by generating data records (e.g., usage information for audit logs) in Shah’s SEE (e.g., within its DRM device) to provide additional information such as content descriptions, usage quality, and/or

content tags as disclosed by Naslund. *See* EX1007, ¶¶[0087]-[0093], Fig. 6. EX1011, ¶¶152-155.

Including Naslund's logging agent on Shah's STC would have been a straightforward implementation since Naslund expressly discloses use of its logging agent in a DRM agent and Shah expressly contemplates use of an "audit log" (EX1006, ¶¶[0010], [0025]). A POSITA would have had a reasonable expectation of success in using Naslund's logging agent in combination with Shah's secure time certificate generation and audit logging given their closely related technical subject matter. A POSITA would have been motivated to use Shah's secure time certificate in place of or as a supplement to Naslund's "usage time" in the usage information to promote more secure time stamping of usage information for purposes of monitoring usage of content in a DRM context. Shah's time certificate with Naslund's logging agent in the WTRU would have improved content delivery and/or content monitoring in the DRM context, for example, for purposes of accurate billing for content usage or improved tamper detection. *See* EX1006, ¶¶[0007], [0044], [0048], [0109]. *See* EX1007, ¶¶[0003], [0019], [0126], [0140]. EX1011, ¶¶156-158.

i. [1.9]: "associate the unique identifier with the data record; and"

Shah alone and/or in view of Naslund discloses/suggests Element [1.9]. Shah discloses that the secure data path processing agent is configured to associate the unique identifier (i.e., the "secure time stamp" of Shah's signed time certificate) with

the data record (i.e., the “audit log”). Shah’s “secure time stamp” and “audit log” are contained in the same signed time certificate and thus are associated with each other. EX1006, ¶[0010]. *See id.*, Fig. 1 (“signed time stamp certificates” and “device audits”). Shah discloses that the STC is configured to associate the unique identifier with the data record to the same extent as described in exemplary embodiments of the ’155 Patent. EX1011, ¶¶159-161.

Shah’s STC generates the signed time certificate and associates the secure time stamp (unique identifier) with data (data record, e.g., audit logs, messages, and so forth) to associate the unique identifier with the data record when the signed time certificate is generated. *Id.*, ¶[0010]. Shah discloses that the certificate constitutes “an unequivocal, non-alterable and non-repudiatable certificate of the current time—also known as a signed time certificate” of a logged event. EX1006, ¶[0008]. *See also id.*, ¶¶[0013], [0041], [0059]. EX1011, ¶¶162-163.

Shah’s STC generates a data record (i.e. data entry, audit log) that is associated with a time certificate containing a secure time stamp. EX1006, ¶[0010]. The time stamp is associated with and unique to each individual time certificate. *See id.*, ¶¶[0010]-[0013]. Shah’s time certificates are associated with data entries (e.g., for Shah’s audit log) and generated by the STC to provide time records of logged events on the DRM device. EX1006, ¶[0041]. *See also id.*, ¶¶[0008]-[0013], [0048]. EX1011, ¶¶164-166.

To the extent it is argued that Shah lacks express disclosure of associating the unique identifier with the data record, Naslund teaches that it was well known in the art to generate a data record and a unique identifier and associate the data record and unique identifier to track and monitor data usage on a mobile device (e.g., a DRM device, as a disclosed embodiment in Shah). *See, e.g.*, EX1007, ¶¶[0069], [0097], Fig. 6 (showing “representation of digital content 172-1” associated with “usage time 172-N” in log entry 172). EX1011, ¶167.

It would have been obvious to implement Naslund’s technique of capturing and associating data records (i.e., usage information) with time stamps (i.e., unique identifiers) in Shah’s audit logs to similarly associate usage information with Shah’s secure time stamp. In Shah’s system incorporating Naslund’s logging agent (*see* Element [1.8], *supra*), it would have been obvious to associate usage information with Shah’s secure time stamp and/or time certificate to produce log information expressly disclosed by Naslund for Shah’s audit log. *See* EX1007, Fig. 6 (showing log entry 172 including “representation of digital content 172-1” and “usage quality 172-2” associated with “usage time 172-N”). EX1011, ¶¶168-169.

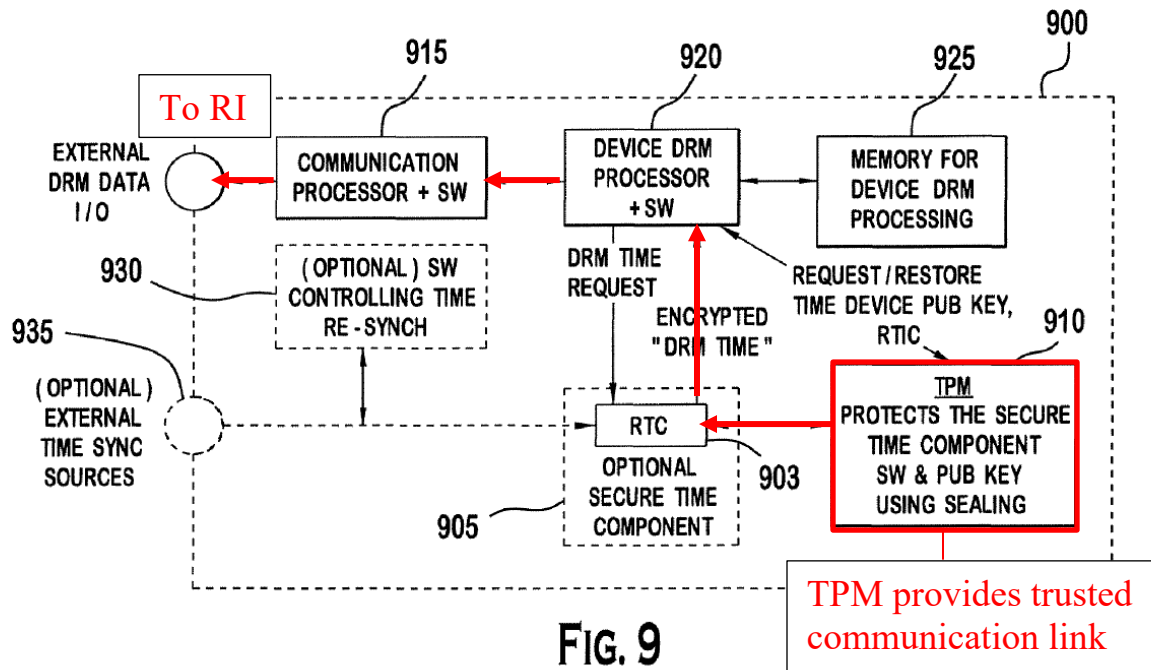
A POSITA would have had a reasonable expectation of success in associating usage information disclosed by Naslund with Shah’s secure time stamp (either by associating the usage information with the secure time certificate or with the time stamp within the secure time certificate) given that Naslund expressly discloses

associating usage information (data records) with a usage time. Associating the usage information with Shah's secure time stamp in Shah's STC would have been a predictable extension of using Naslund's logging agent to log usage information to generate audit logs using Shah's secure time stamp. *See* Element [1.8], *supra*. Shah and Naslund disclose associating the unique identifier with the data record to the same extent as described in exemplary embodiments of the '155 Patent. EX1011, ¶¶170-171.

j. [1.10]: “send the unique identifier to the network element over a trusted communication link between the secure data path processing agent and the network element.”

Shah alone and/or in view of Naslund discloses/suggests Element [1.10]. Shah discloses that the secure data path processing agent (i.e., STC and TPM) is configured to send the unique identifier (time stamp included in the signed time certificate) to the network element (i.e., the same network element referenced in Element [1.6]) over a trusted communication link (e.g., Shah's secure channel) between the secure data path processing agent (i.e., STC and TPM) and the network element (e.g., requesting entity/application, rights issuer (RI)). EX1011, ¶¶172-173.

Figure 9 of Shah shows the data path from the STC to the communications processor (i.e., for transmitting the secure time certificate to the network element, or RI). *See id.*, Fig. 9. The data path is secured by the TPM. EX1006, ¶¶[0090-91], [0095-0105].



EX1006, Fig. 9 (Annotated)

EX1011, ¶174.

The trusted communication link can include intermediate components between the secure data path processing agent (i.e., Shah’s STC) and the network element (i.e., Shah’s RI). *See, e.g., Claim 2, infra.* The ’155 Patent similarly describes exemplary embodiments that can include intermediate components between the secure data path processing agent and the network element. EX1001, 27:30-36. For example, the ’155 Patent discloses a “Service Processor Application Program 112” between the “Secure DDR Processor Programs 326” of the SEE and the network. *See* EX1001, 33-36 (“In some embodiments, the service processor application program 112 communicates the secure DDRs to a network

element/function, such as the service controller 122.”). *See id.*, 27:23-34:56. EX1011, ¶¶175-176.

The ’155 Patent describes in exemplary embodiments that a “trusted” communication link “is trusted because data sent over it is signed.” EX1001, 54:11-12. The trusted communication link can be “configured to secure communications by encryption.” *Id.*, 54:12-15. The ’155 Patent indicates that a “secure communication channel” functions to provide a security protocol to “avoid tampering” with the data records using “an authentication sequence or process with a network element”. *Id.*, 9:28-36. *See id.*, 9:23-65. EX1011, ¶¶177-179.

Shah uses authentication services and/or encryption in the same way to secure the communication channel for transmission of signed time certificates. *See* EX1006, ¶¶[0012], [0014], [0066] (“the time could be sent in encrypted format), [0100] (“Additionally, the public key that can decrypt the DRM Time information encrypted by the STC 905 is under cryptographic protection by the TPM 910 using a TPM Sealing command.” *See also id.*, ¶¶[0041], [0047]. EX1011, ¶180.

Shah’s DRM device and its STC and TPM (i.e., the secure data path processing agent) are configured for “supporting the establishment of a secure channel between the WTRU [(i.e., DRM device)] and the network.” EX1006, ¶[0040]; *see also id.*, ¶[0090] wherein the DRM device “obtains the *secure time update* from the network” (emphasis added). Shah forms the secure channel and

binds communication for transmitting the secure time certificates with the TPM (of the secure data path processing agent). *Id.*, ¶¶[0040], [0045], [0058]. Thus, Shah uses the secure data path processing agent (i.e., STC and TPM combination) to secure the communication link over which secure time certificates are sent to the network. EX1011, ¶¶181-182.

Shah teaches the DRM device transmitting the secure time certificates (including the unique identifiers) over the secure channel between the STC and the network element, supported by “authentication services” of the TPM. *Id.*, ¶[0040]. *See id.*, ¶¶[0046] (DRM “provide[s] a measure of the current time to an external requesting application” and “an external network”), [0050], [0058]. Shah’s time certificate (which contains the unique identifiers) is sent as an output to a requesting entity on the network for verification. *Id.*, ¶¶[0010] (“re-synching signals can be distributed and processed over an IP-based network”), [0011] (“Verification... by an outside ‘verifier’”), [0041], [0046]. *See id.*, ¶¶[0095]-[0096]. EX1011, ¶¶183-184.

Shah discloses communicating the unique identifier (i.e., secure time stamp discussed with regard to Fig. 9) of the signed time certificate to a network element (e.g., a separate RI platform, *see* annotated Fig. 9, *supra.* and annotated Fig. 8 below), i.e., a verifier in a wide area network for verification. *See id.*, ¶¶[0009] (“an outside source must verify the validity of the signed certificate”), [0011], [0016]. *See also id.*, Fig. 7 (DRM device transmitting “updated DRM time” such as that of Fig. 9),

Fig. 8, (DRM device transmitting “ROLE parameter”), Tables 5-8, ¶¶[0078]-[0080]. For example, Shah transmits a ROLE parameter to the RI platform where the ROLE parameter includes a secure time certificate (as generated in Fig. 9) associated with when the device examined an RO (i.e., “DRM time” RO last examined “T-ROLE”). *Id.*, ¶¶[0078]-[0080] (“The DRM device 810 stores these values as elements of a newly proposed parameter ROLE (RO Last Examined)”), (“The DRM device 810 also reports the newly proposed ROLE parameter to the RI”). Shah’s Figure 8 shows the DRM device communicating the secure time certificate in the ROLE parameter over a secure channel to the RI entity on the network for verification.

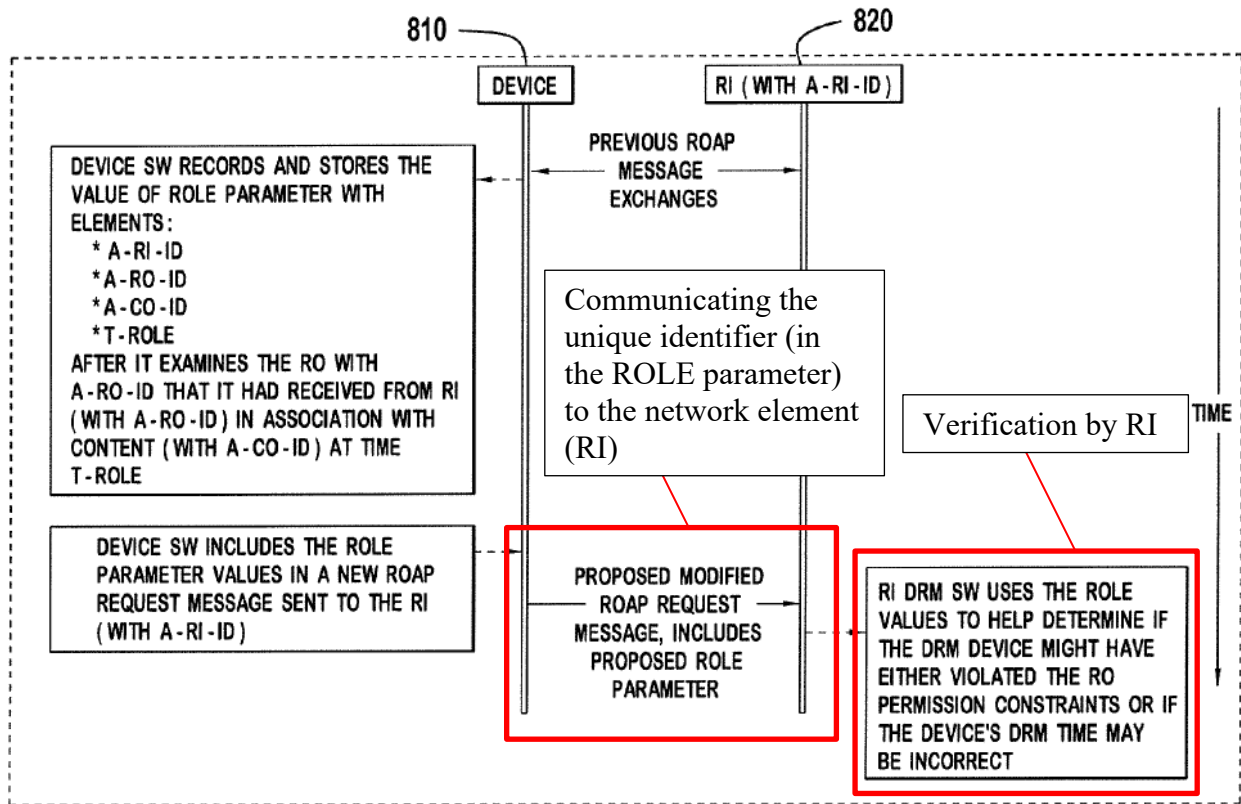


FIG. 8

EX1006, Fig. 8 (Annotated)

EX1011, ¶185.

The unique identifiers (i.e., secure time stamps) are sent to the RI (“Rights Issuer”, i.e., the same network element for which the unique identifiers were generated in Element [1.6])) in the ROLE parameter included in a rights object acquisition protocol (ROAP) request message for verification. *See id.*, ¶¶[0078]-[0084] (“ROLE information may be used by the RI 820 that receives it in the proposed modified ROAP Request messages to help determine if a DRM device’s

time is incorrect, as well as to determine if a DRM device 810 might have violated usage rights”), Tables 6-8. EX1011, ¶186.

To the extent it is argued that Shah lacks express disclosure of a trusted communication link between the secure data path processing agent and the network element, Naslund teaches that it was well known in the art to send a unique identifier over a trusted communication link. Naslund discloses sending usage information (including a unique identifier, *see* Element [1.9], *supra*) “in a secure manner, e.g., by using encryption/authentication or a secure channel” to an external log at a trusted party. EX1007, ¶¶[0080], [0085]. *See id.*, ¶¶[0015], [0017], [0069]-[0070]. Naslund teaches that the usage information (including a unique identifier) is transmitted over a secure and/or trusted channel. Naslund also teaches that the logging agent includes a security operation unit for encryption/authentication and securely transmitting the usage information. *Id.*, ¶[0086]. EX1011, ¶¶187-189.

It would have been obvious to apply Naslund’s secure channel to Shah’s transmission of the secure time certificate to the RI to connect or associate the time certificate and audit log information to a particular account or individual (e.g., an owner or user of the DRM device) to provide secure identification of the time certificate information. *Id.*, ¶[0080]. A POSITA would have had a reasonable expectation of success given that Naslund expressly discloses transmitting usage information over a secure channel. Applying Naslund’s secure channel for sending

Shah's time certificates would have been use of a known technique (secure communication) to improve similar devices (e.g., mobile devices, such as DRM devices) in the same way. EX1011, ¶¶190-191.

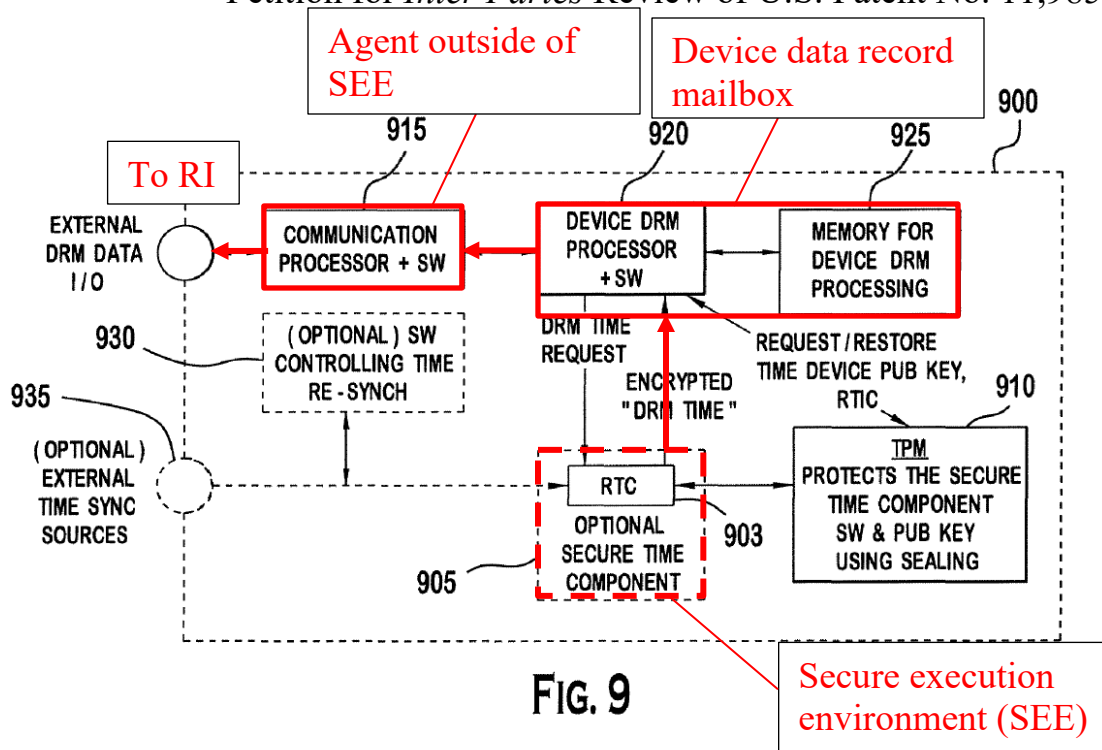
2. **Claim 2: “The communications device of claim 1, wherein the secure data path processing agent includes a device data record mailbox, wherein the device data record mailbox is configured to relay the data record to an agent outside of the secure execution environment for transmission to the network element.”**

Shah discloses/suggests Claim 2. *See* Claim 1, *supra*. Shah discloses that the secure data path processing agent (i.e., the STC and TPM) includes a device data record mailbox (e.g., Fig. 9 “Device DRM processor and SW 920” and “Memory for Device DRM Processing 925”, *see* annotated Fig. 9, §V.C.1., *supra*.). Shah's device data record mailbox is configured to relay the data record (signed time certificate including the audit log) to an agent (e.g., communication processor and SW 915) outside of the SEE (components of Shah's STC) for transmission to the network element (e.g., requesting entity, RI 820). EX1011, ¶¶192-193.

Shah's STC executes functions to generate and output the secure time certificate. EX1006, ¶[0010]. *See id.*, ¶¶[0041], [0046]. *See* Element [1.3], *supra*. According to the '155 Patent, “the DDR mailbox function can be implemented in a variety of ways.” EX1001, 28:35-36. Shah implements a device data record mailbox as a “Device DRM Processor and SW 920” (i.e., “Device DRM SW 515” in Figure 5) and a “Memory for Device DRM Processing 925” (i.e., “Memory for Device

DRM Processing 520” in Figure 5), which receives secure time certificates from the STC 905 and TPM 910 for protected storage. EX1011, ¶¶194-196.

Device DRM processor and SW 920 and the memory for device DRM processing 925 store and relay encrypted DRM time (i.e., secure time certificates) generated in the STC to the communication processor and SW 915. *See id.*, ¶[0024], Fig. 9. EX1011, ¶197. The communication processor and SW 915 (i.e., agent outside the SEE) can then transmit the data record (i.e., signed time certificate including the audit log) to a network element (i.e., requesting entity/application, RI). *See id.*, ¶[0041] (Shah’s STC 905, via the communication processor and SW 915, sends “time certificate or signatures of time related data, as outputs to a requesting entity” on the network), Fig. 7 (DRM device transmitting “updated DRM time”), Fig. 8, (DRM device transmitting “ROLE parameter”), Fig. 9, Tables 5-8, ¶¶[0078]-[0080].).



EX1006, Fig. 9 (Annotated)

EX1011, ¶198.

Shah’s DRM processor and SW 920 and memory for device DRM processing 925 relay the signed time certificates to an agent outside of the SEE to the same extent as described in exemplary embodiments of the ’155 Patent. EX1001, 23:53-63 (“Example techniques for providing the DDR mailbox include shared memory”), 27:31-35 (“DDR mailbox function is used to communicate secure DDRs ... to the service processor application program 112 [which] ... communicates the secure DDRs to a network element/function”). Figure 4 of the ’155 Patent shows an exemplary embodiment of the device data record mailbox for “passing DDR mailbox data 320 between secure DDR SEE 420 and unsecure Service Processor application 112. EX1001, 2:7-10. *See id.*, 28:30-33. Shah’s DRM processor and SW

920 and memory for device DRM processing 925 likewise communicate encrypted DRM time between the STC and the unsecure communication processor 915 interfacing with external, unauthenticated network elements. EX1011, ¶¶199-200.

3. Claim 10 (Preamble): “A method for use by a communications device”

To the extent “A method for use by a communications device” is limiting, Shah discloses/suggests such subject matter. *See* Claim 1 (Preamble), *supra*. Shah discloses a method for use by a communication device for providing secured time functionality to the WTRU. EX1006, ¶[0023]. EX1011, ¶¶201-202.

a. [10.1]: “including a wide area network port configured to connect the communications device to a wide area network, and”

Shah discloses/suggests Element [10.1]. *See* Element [1.1], *supra*. EX1011, ¶203.

b. [10.2]: “further including a secure memory,”

Shah discloses/suggests Element [10.2]. *See* Element [1.2], *supra*. EX1011, ¶204.

c. [10.3]: “a secure execution environment configured to be inaccessible to a user application software, and”

Shah discloses/suggests Element [10.3]. *See* Element [1.3], *supra*. EX1011, ¶205.

d. [10.4]: “a secure data path processing agent,”

Shah discloses/suggests Element [10.4]. *See* Element [1.4], *supra*. EX1011, ¶206.

e. [10.5]: “the method comprising:”

Shah discloses/suggests Element [10.5]. *See* Elements [10.1] and [1.4], *supra*. EX1011, ¶207.

f. [10.6]: “executing the secure data path processing agent in the secure execution environment;”

Shah discloses/suggests Element [10.6]. *See* Elements [1.3]-[1.5], *supra*. EX1011, ¶208.

g. [10.7]: “generating, by the secure data path processing agent, a unique identifier for communication to a network element in the wide area network;”

Shah discloses/suggests Element [10.7]. *See* Element [1.6], *supra*. EX1011, ¶209.

h. [10.8]: “storing, by the secure data path processing agent, the unique identifier in the secure memory;”

Shah discloses/suggests Element [10.8]. *See* Element [1.7], *supra*. EX1011, ¶210.

i. [10.9]: “generating, by the secure data path processing agent, a data record;”

Shah alone and/or in view of Naslund disclose(s)/suggest(s) Element [10.9]. *See* Element [1.8], *supra*. EX1011, ¶211.

- j. [10.10]: “associating, by the secure data path processing agent, the unique identifier with the data record; and”**

Shah alone and/or in view of Naslund discloses/suggests Element [10.10]. *See* Element [1.9], *supra*. EX1011, ¶212.

- k. [10.11]: “sending, by the secure data path processing agent, the unique identifier to the network element over a trusted communication link between the secure data path processing agent and the network element.”**

Shah alone and/or in view of Naslund discloses/suggests Element [10.10]. *See* Element [1.10], *supra*. EX1011, ¶213.

- 4. Claim 11: “The method of claim 10, wherein the secure data path processing agent includes a device data record mailbox, and wherein the method further comprises: relaying, using the device data record mailbox, the data record to an agent outside of the secure execution environment for transmission to the network element.”**

Shah discloses/suggests Claim 11. *See* Claims 10, 2, *supra*. EX1011, ¶214.

VIII. OTHER CONSIDERATIONS

Petitioner is not aware of any secondary considerations evidence bearing any nexus to the purported claimed invention. Any purported evidence of secondary considerations that Patent Owner may present in this proceeding would be insufficient to overcome the strong evidence of obviousness of the Challenged Claims. EX1011, ¶¶215-217.

IX. CONCLUSION

Petitioner has shown a reasonable likelihood of success. Therefore, this Petition should be granted and the Board should institute trial.

Date: August 27, 2026

Respectfully submitted,

/Patrick C. Keane/

Patrick C. Keane, Esq.

Registration No. 32,858

BUCHANAN INGERSOLL & ROONEY PC

1700 K Street, N.W., Suite 300

Washington, DC 20006

Telephone (703) 838-6522

Facsimile (202) 452-7989

patrick.keane@bipc.com

Counsel for Petitioner

APPENDIX A - LIST OF EXHIBITS

Exhibit No.	Description
1001	U.S. Patent No. 11,985,155, issued May 14, 2024 to G. Raleigh et al. (“’155 Patent”)
1002	File History of U.S. Patent Application No. 18/088,450 through September 22, 2025
1003	U.S. Provisional Application No. 61/206,354, filed January 28, 2009
1004	Redline Comparison of ’155 Independent Claim to ’186 Independent Claims
1005	Redline Comparison of ’155 Independent Claim to ’980 Independent Claims
1006	U.S. Patent Application Publication No. 2007/0266256, published November 15, 2007 to Y. Shah et al. (“Shah”)
1007	U.S. Patent Application Publication No. 2005/0246282, published November 3, 2005 to M. Naslund et al. (“Naslund”)
1008	U.S. Patent Application Publication No. 2006/0129848, published June 15, 2006 to E. Paksoy et al. (“Paksoy”)
1009	U.S. Patent Application Publication No. 2005/0259673, published November 24, 2005 to H. Lu et al. (“Lu”)
1010	U.S. Patent Application Publication No. 2007/0002846, published January 4, 2007, to P. Rada et al. (“Rada”)
1011	Declaration of David Williams
1012	<i>Curriculum Vitae</i> of David Williams
1013	Defendant Google LLC’s Opening Claim Construction Brief, filed May 13, 2026 in <i>Headwater Research LLC v. Google LLC</i> , Civ. Action No. 7:25-cv-00369 (W.D. Tex.)

Exhibit No.	Description
1014	Plaintiff Headwater Research LLC's Responsive Claim Construction Brief, filed June 8, 2026 in <i>Headwater Research LLC v. Google LLC</i> , Civ. Action No. 7:25-cv-00369 (W.D. Tex.)
1015	Defendant Google LLC's Reply to Plaintiff's Responsive Claim Construction Brief, filed June 22, 2026 in <i>Headwater Research LLC v. Google LLC</i> , Civ. Action No. 7:25-cv-00369 (W.D. Tex.)
1016	Plaintiff Headwater Research LLC's Sur-Reply to Defendant's Reply to Plaintiff's Responsive Claim Construction Brief, filed July 7, 2026 in <i>Headwater Research LLC v. Google LLC</i> , Civ. Action No. 7:25-cv-00369 (W.D. Tex.)
1017	Joint Claim Construction Statement, filed July 10, 2026 in <i>Headwater Research LLC v. Google LLC</i> , Civ. Action No. 7:25-cv-00369 (W.D. Tex.)
1018	UICC-terminal interface; Physical and logical characteristics (3GPP TS 31.101 version 7.0.1 Release 7)
1019	Characteristics of the Universal Subscriber Identity Module (USIM) application (3GPP TS 31.102 version 8.0.0 Release 8)
1020	Specification of the Subscriber Identity Module – Mobile Equipment (SIM – ME) interface (3GPP TS 51.011 version 4.10.0 Release 4)
1021	Mobile Execution Environment (MExE); Functional description; Stage 2 (3GPP TS 23.057 version 7.0.0 Release 7)
1022	U.S. Patent No. 10,771,980, issued September 8, 2020 to G. Raleigh et al.
1023	U.S. Patent No. 11,665,186, issued May 30, 2023 to G. Raleigh et al.
1024	Declaration of Friedhelm Rodermund

Petition for *Inter Partes* Review of U.S. Patent No. 11,985,155

Exhibit No.	Description
1025	<i>Curriculum Vitae</i> of Friedhelm Rodermund

CERTIFICATE OF COMPLIANCE WITH 37 C.F.R. §42.24

The undersigned hereby certifies that the foregoing Petition totals 10,803 words, excluding the parts which are exempted by 37 C.F.R. §42.24(a)(1).

Date: August 27, 2026

/Patrick C. Keane/

Patrick C. Keane, Esq.

Registration No. 32,858

BUCHANAN INGERSOLL & ROONEY PC

1700 K Street, N.W., Suite 300

Washington, DC 20006

Telephone (703) 838-6522

Facsimile (202) 452-7989

patrick.keane@bipc.com

Counsel for Petitioner

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on this 27th day of August, 2026, a true and correct copy of the foregoing **PETITION FOR *INTER PARTES* REVIEW FOR U.S. PATENT NO. 11,985,155 and EXHIBITS 1001-1025 and Petitioner's Power of Attorney** are being served upon the Patent Owner at the following correspondence address of record via FedEx:

Headwater Research LLC
C/O Farjami & Farjami LLP
26522 La Alameda Ave., Suite 360
Mission Viejo, CA 92691

and courtesy copies are being served on litigation counsel for Patent Owner via electronic mail to:

RUSS AUGUST & KABAT
Marc Fenster (mfenster@raklaw.com)
Reza Mirzaie (rmirzaie@raklaw.com)
Brian Ledahl (bledahl@raklaw.com)
Ben Wang (bwang@raklaw.com)
Dale Chang (dchang@raklaw.com)
Kristopher Davis (kdavis@raklaw.com)
Paul Kroeger (pkroeger@raklaw.com)
James S. Tsuei (jtsuei@raklaw.com)
Philip Wang (pwang@raklaw.com)
James Pickens (jpickens@raklaw.com)
Jason Wietholter (jwietholter@raklaw.com)
Qi (Peter) Tong (ptong@raklaw.com)
Minna Jay (mjay@raklaw.com)

Date: August 27, 2026

/Patrick C. Keane/
Patrick C. Keane, Esq.
Registration No. 32,858
BUCHANAN INGERSOLL & ROONEY PC
1700 K Street, N.W., Suite 300
Washington, DC 20006
Telephone (703) 838-6522
Facsimile (202) 452-7989
patrick.keane@bipc.com
Counsel for Petitioner