

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

GOOGLE LLC,  
Petitioner,

v.

HEADWATER RESEARCH LLC,  
Patent Owner.

---

Case No. IPR2026-00203  
Patent No. 9,232,403

---

**PETITION FOR INTER PARTES REVIEW  
UNDER 35 U.S.C. §§ 311-319 AND 37 C.F.R. § 42.1 et seq.**

## TABLE OF CONTENTS

MANDATORY NOTICES.....	x
A. Real Party-In-Interest .....	x
B. Related Matters.....	x
1. United States Patent & Trademark Office .....	x
2. U.S. District Court for the Eastern District of Texas .....	xi
3. U.S. District Court for the Northern District of California.....	xii
C. Counsel and Service Information - § 42.8(b)(3) and (4).....	xii
I. INTRODUCTION .....	1
II. GROUNDS FOR STANDING.....	1
III. UNPATENTABILITY GROUNDS.....	1
IV. '403 PATENT .....	2
A. Brief Description .....	2
B. Prosecution History .....	3
V. PERSON OF ORDINARY SKILL IN THE ART .....	4
VI. CLAIM INTERPRETATION .....	4
VII. <u>GROUND 1: TS-23.140 AND OGAWA RENDER OBVIOUS</u> CLAIMS 1, 3-6, 11-21.....	5
A. TS-23.140 (EX-1004).....	5
B. Ogawa (EX-1005).....	7
C. The MMS-Ogawa Combination.....	8
1. Implementing TS-23.140's UE/Device with a Modem .....	9
2. Securing Interface MM1 Using SSL/TLS.....	10
3. Applying Ogawa's Encryption Techniques for Network Communications.....	12
4. Ogawa's Decryption and Encryption Units .....	14
5. Implementing TS-23.140's Device with an Interprocess Communication Bus .....	16
6. Securing Interprocess Communications Within the Device .....	18
7. MMS-Ogawa.....	20

D. Claim Analysis .....	21
1. Claim 1 .....	21
a. [1PRE] “A mobile end-user-area device comprising:” .....	21
b. [1A] “a wireless wide-area network (WWAN) modem to exchange Internet data via a connection to a first WWAN, when configured for and connected to the first WWAN;” .....	22
c. [1B1] .....	26
i. “a device messaging agent to receive secure Internet data messages” .....	26
ii. “on behalf of a plurality of software applications capable of execution on the device” .....	28
iii. “and over a secure connection to a network message server reachable via the WWAN” .....	30
d. [1B2] .....	33
i. “wherein at least a subset of the secure Internet data messages contain an identifier for a corresponding one of the software applications” .....	33
ii. “and application data from a respective network application server corresponding to that application” .....	35
e. [1C1] “a secure interprocess communication service,” .....	39
f. [1C2] .....	41
i. “wherein the device messaging agent, for each message in the subset of the secure Internet data messages, maps the identifier to the corresponding one of the software applications” .....	41
ii. “in order to forward the application data on the secure interprocess communication service” .....	43
iii. “to a software process corresponding to the identified software application.” .....	43
2. Claim 3 .....	44
3. Claim 4 .....	45
4. Claim 5 .....	45
5. Claim 6 .....	46

6. Claim 11 .....	47
7. Claim 12 .....	51
8. Claim 13 .....	53
9. Claim 14 .....	54
10. Claim 15 .....	54
11. Claim 16 .....	55
12. Claim 17 .....	58
13. Claim 18 .....	59
14. Claim 19 .....	59
15. Claim 20 .....	60
16. Claim 21 .....	62
VIII. <u>GROUND 2A-2C</u> .....	63
A. GROUND 2A: MMS-Ogawa in View of Cole (EX-1006).....	63
1. Implementing a WWAN Modem (Claims 1, 3-6, 11-21).....	63
2. Adding a WLAN Modem (Claim 2) .....	65
B. GROUND 2B: MMS-Ogawa in View of Sathish (EX-1031).....	71
C. GROUND 2C: MMS-Ogawa-Cole-Sathish .....	72
IX. <u>GROUND 3A-3D</u> .....	72
A. Papineau (EX-1017) .....	72
B. GROUND 3A: Implementing Papineau’s JAM Teachings (Claims 7-10).....	74
1. MMS-Ogawa-Papineau .....	74
2. Claim 7 .....	77
3. Claim 8 .....	78
4. Claim 9 .....	79
C. GROUND 3B-3D .....	80
X. <u>GROUND 4A-4D</u> .....	80
A. Ellison (EX-1019) .....	80
B. GROUND 4A: Implementing Ellison’s Isolated Execution Environment (Claim 10).....	82

1. MMS-Ogawa-Ellison .....	82
2. Claim 10 .....	84
C. GROUNDS 4B-4D .....	85
XI. CONCLUSION.....	85
XII. CLAIM LISTING APPENDIX.....	86

**TABLE OF AUTHORITIES**

**CASES**

*KSR International Co. v. Teleflex Inc.*,  
550 U.S. 398 (2007) ..... passim

*Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*,  
868 F.3d 1013 (Fed. Cir. 2017) .....4

**STATUTES**

35 U.S.C. § 102 .....2

35 U.S.C. § 103 .....1

35 U.S.C. § 282(b) .....4

**REGULATIONS**

37 C.F.R. § 42.100(b) .....4

37 C.F.R. § 42.104(a).....1

**OTHER AUTHORITIES**

83 Fed. Reg. 51,340 (Oct. 11, 2018).....4

## APPENDIX LISTING OF EXHIBITS

<b>Exhibit</b>	<b>Description</b>
1001	U.S. Patent No. 9,232,403 (“the ’403 Patent”)
1002	Prosecution History of U.S. Patent No. 9,232,403 (“the ’403 FH”)
1003	Declaration and Curriculum Vitae of Patrick Traynor
1004	3GPP TS 23.140 v6.9.0 (2005-03); 3rd Generation Partnership Project; Technical Specification Group Terminals; Multimedia Messaging Service (MMS); Functional Description; Stage 2 (“TS-23.140”)
1005	U.S. Patent No. 8,195,961 (“Ogawa”)
1006	U.S. Patent App. Pub. No. 2008/0080458 (“Cole”)
1007	U.S. Patent App. Pub. No. 2004/0111476 (“Trossen”)
1008	PCT Pub. No. 2008/048075 (“Lee”)
1009	U.S. Patent No. 7,975,147 (“Qumei”)
1010	U.S. Patent No. 9,032,192 (“Frank”)
1011	Open Mobile Alliance; OMA-ERELD-MMS-v1_2-20030923-C, Enabler Release Definition for MMS Version 1.2,” available at <a href="https://www.openmobilealliance.org/release/MMS/V1_2-20030923-C/OMA-ERELD-MMS-V1_2-20030923-C.pdf">https://www.openmobilealliance.org/release/MMS/V1_2-20030923-C/OMA-ERELD-MMS-V1_2-20030923-C.pdf</a>
1012	“Open Mobile Alliance; Multimedia Messaging Service Architecture Overview” (MMSARCH) specification, available at <a href="https://www.openmobilealliance.org/release/MMS/V1_2-20030923-C/OMA-MMS-ARCH-V1_2-20030920-C.pdf">https://www.openmobilealliance.org/release/MMS/V1_2-20030923-C/OMA-MMS-ARCH-V1_2-20030920-C.pdf</a>
1013	The Secure Sockets Layer (“SSL”) Protocol, V. 3.0, available at <a href="https://web.archive.org/web/19970614041044/http://home.netscape.com/eng/ssl3/ssl-toc.html">https://web.archive.org/web/19970614041044/http://home.netscape.com/eng/ssl3/ssl-toc.html</a> and <a href="https://web.archive.org/web/19970617034012/http://home.netscape.com/eng/ssl3/3-SPEC.HTM#1">https://web.archive.org/web/19970617034012/http://home.netscape.com/eng/ssl3/3-SPEC.HTM#1</a>
1014	The Transport Layer Security (“TLS”) Protocol, V. 1.1, available at <a href="https://datatracker.ietf.org/doc/html/rfc4346.html">https://datatracker.ietf.org/doc/html/rfc4346.html</a>
1015	U.S. Patent App. Pub. No. 2003/0096625 (“Mi-Su Lee”)
1016	3GPP TS-23.234 v8.0.0 (2008-12); 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP system to Wireless Local Area Network (WLAN) interworking; System description (Release 8) (“TS-23.234”)
1017	U.S. Patent No. 7,779,408 (“Papineau”)

1018	Liaison Statement, European Telecommunications Standards Institute AT-F Rapporteur Meeting, 4 to 6 February 2003 (ETSI / AT-F TD18), available at <a href="https://www.3gpp.org/ftp/tsg_sa/TSG_SA/TSGS_19/Docs/PDF/SP-030167.pdf">https://www.3gpp.org/ftp/tsg_sa/TSG_SA/TSGS_19/Docs/PDF/SP-030167.pdf</a>
1019	U.S. Patent No. 7,082,615 (“Ellison”)
1020	3GPP TS-26.140 v6.2.0 (2005-03); 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Multimedia Messaging Service(MMS); Media formats and codecs
1021	Multimedia Messaging Service Encapsulation Protocol, available at <a href="http://www.openmobilealliance.org/release/MMS/V1_2-20050301-A/OMA-MMS-ENC-V1_2-20050301-A.pdf">www.openmobilealliance.org/release/MMS/V1_2-20050301-A/OMA-MMS-ENC-V1_2-20050301-A.pdf</a>
1022	<i>Samsung Elecs. et al. v. Headwater Research LLC</i> , IPR2024-00341, Paper 28 (July 23, 2025)
1023	Stewart, C.M., Memorandum Re: PTAB Consideration of Prior Findings of Fact and Conclusions of Law (September 16, 2025), <a href="https://www.uspto.gov/sites/default/files/documents/Memo_re_prior_findings_of_fact_and_conclusions_of_law_9_16_25.pdf">https://www.uspto.gov/sites/default/files/documents/Memo_re_prior_findings_of_fact_and_conclusions_of_law_9_16_25.pdf</a> .
1024	Declaration of Friedhelm Rodermund
1025	Mobile Information Device Profile for Java™ 2 Micro Edition Version 2.0 (Nov. 5, 2002) (“MIDP-Specification”)
1026	U.S. Patent App. Pub. No. 2005/0108571 (“Lu”)
1027	U.S. Patent App. Pub. No. 2005/0207379 (“Shen”)
1028	Transporting data between wireless applications using a messaging system—MMS, Miraj E Mostafa, <i>Wireless Communications and Mobile Computing</i> (2007) (“Mostafa”)
1029	<i>Dictionary of Computer Science, Engineering, and Technology</i> , CRC Press LLC, 2001
1030	Needham et al., “Using Encryption for Authentication in Large Networks of Computers” ( <i>ACM</i> , Vol. 21, No. 12, Dec. 1978) (“Needham”)
1031	U.S. Patent No. 8,010,669 (“Sathish”)
1032	Saltzer et al., “The Protection of Information in Computer Systems” ( <i>IEEE Proceedings</i> , Vol. 63, No. 9, Sept. 1975) (“Saltzer”)
1033	Li et al., “Symbian OS platform security model,” available at <a href="https://www.usenix.org/system/files/login/articles/73507-li.pdf">https://www.usenix.org/system/files/login/articles/73507-li.pdf</a> ( <i>Login Magazine</i> , Aug. 2010)

1034	Philip Zimmermann, “Pretty Good Privacy: RSA Public Key Cryptography for the Masses” PGP User’s Guide. Version 1.0, June 1991, available at <a href="https://www.techinsider.org/free-software/research/acrobat/910605.pdf">https://www.techinsider.org/free-software/research/acrobat/910605.pdf</a> (“Zimmerman”)
1035	B. Ramsdell, S/MIME Version 3 Message Specification, IETF RFC 2633, June 1999, available at <a href="https://datatracker.ietf.org/doc/html/rfc2633">https://datatracker.ietf.org/doc/html/rfc2633</a> (“Ramsdell”)
1036	Schroeder et al., “A Hardware Architecture for Implementing Protection Rings” (ACM, Vol. 15, No. 3, Mar. 1972) (“Schroeder”)
1037	Nokia E71 review: Nokia E71, available at <a href="https://www.cnet.com/reviews/nokia-e71-review/">https://www.cnet.com/reviews/nokia-e71-review/</a>
1038	<i>Samsung Elecs. et al. v. Headwater Research LLC</i> , IPR2024-00341, Paper 4 (January 23, 2024)
1039	U.S. Patent App. Pub. No. 2007/0283170 (“Yami”)
1040	U.S. Patent App. Pub. No. 2008/0215883 (“Fok”)
1041	U.S. Patent App. Pub. No. 2003/0220835 (“Barnes”)
1042	U.S. Patent App. Pub. No. 2006/0154699 (“Ko”)
1043	U.S. Patent App. Pub. No. 2005/0207379 (“Shen”)
1044	U.S. Patent App. Pub. No. 2006/0025133 (“Shaheen”)
1045	Dictionary of Computing, S.M.H. Collin, Fifth Edition, Bloomsbury (2004)
1046	IEEE 100 The Authoritative Dictionary of IEEE Standards Terms, Seventh Edition (2000)
1047	U.S. Patent No. 7,962,798 (“Locasto”)
1048	U.S. Patent App. Pub. No. 2004/0002974 (“Kravitz”)
1049	Computer Desktop Encyclopedia, Alan Freedman, Ninth Edition, Osborne/McGraw-Hill (2001)
1050	U.S. Patent No. 5,612,866 (“Savanyo”)
1051	3GPP TS 25.321 v6.5.0 (2005-06); 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Medium Access Control (MAC) protocol specification; (“TS-25.321”)
1052	3GPP TS 25.322 v6.4.0 (2005-06); 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Radio Link Control (RLC) protocol specification; (“TS-25.322”)

1053	3GPP TS 25.323 v5.4.0 (2005-06); 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Packet Data Convergence Protocol (PDCP) specification; (“TS-25.323”)
1054	Lu et al., Heading for Multimedia Message Service in 3G, 6th IEE International Conference on 3G and Beyond, Washington, D.C., USA, Nov. 7-9, 2005
1055	RFC 4355, IANA Registration for Enumservices Email, Fax, MMS, EMS, and SMS (Jan. 2006)
1056	Rodermund, A Picture Speaks a Thousand Words – From SMS to MMS, in Business Briefing: Wireless Technology (2003)
1057	RFC 3164, The BSD syslog Protocol (Aug. 2001)

## MANDATORY NOTICES

### **A. Real Party-In-Interest**

Petitioner Google LLC<sup>1</sup> 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).

### **B. Related Matters**

A decision in this proceeding could affect or be affected by the following:

#### **1. United States Patent & Trademark Office**

The application from which U.S. Patent No. 9,232,403 issued is a Continuation of U.S. Patent Application No. 14/263,604 (U.S. Patent No. 9,037,127), which is a Continuation of U.S. Patent Application No. 12/380,780 (U.S. Patent No. 8,839,388), which claims priority from Provisional Application Nos. 61/207,739, 61/207,393, 61/206,944, and 61/206,354.

---

<sup>1</sup> Google LLC is a subsidiary of XXVI Holdings Inc., which is a subsidiary of Alphabet Inc. XXVI Holdings Inc. and Alphabet Inc. are not real parties-in-interest to this proceeding.

The following U.S. patent application claims the benefit of priority to U.S. Patent No. 9,232,403:

U.S. Patent Application 14/959,808, filed December 4, 2015; U.S. Patent Application 14/979,233 (U.S. Patent No. 9,532,161), filed December 22, 2015; U.S. Patent Application 15/211,430 (U.S. Patent No. 9,615,192), filed July 15, 2016; U.S. Patent Application 15/217,538 (U.S. Patent No. 9,491,564), filed July 22, 2016; U.S. Patent Application 15/239,398 (U.S. Patent No. 9,641,957), filed August 17, 2016; U.S. Patent Application 15/427,837 (U.S. Patent No. 10,321,318), filed February 8, 2017; U.S. Patent Application 15/582,350 (U.S. Patent No. 10,321,320), filed April 28, 2017; U.S. Patent Application 16/421,121 (U.S. Patent No. 11,096,055), filed May 23, 2019; U.S. Patent Application 16/436,628 (U.S. Patent No. 11,228,617), filed June 10, 2019; U.S. Patent Application 17/342,136 (U.S. Patent No. 11,757,942), filed June 8, 2021; U.S. Patent Application 17/401,635 (U.S. Patent No. 11,757,943), filed August 13, 2021; U.S. Patent Application 17/577,237 (U.S. Patent No. 11,757,943), filed January 17, 2022; U.S. Patent Application No. 18/946,594, filed November 13, 2024.

## **2. U.S. District Court for the Eastern District of Texas**

*Headwater Research LLC v. Cellco Partnership, d/b/a Verizon Wireless et al.*, Case No. 2:25-cv-00709; *Headwater Research LLC v. T-Mobile USA, Inc. et*

*al.*, Case No. 2:25-cv-00710; *Headwater Research LLC v. AT&T Services, Inc. et al.*, Case No. 2:25-cv-00711.

**3. U.S. District Court for the Northern District of California**

*Google LLC v. Headwater Research LLC*, Case No. 3:25-cv-07453.

**C. Counsel and Service Information - § 42.8(b)(3) and (4)**

Lead Counsel	Anant K. Saraswat, Reg. No. 76,050
Backup Counsel	Turhan F. Sarwar, pending admission <i>pro hac vice</i> George T. Scott, Reg. No. 62,859
Service Information	<u>E-mail</u> : <a href="mailto:ASaraswat-PTAB@wolfgreenfield.com">ASaraswat-PTAB@wolfgreenfield.com</a> <a href="mailto:TSarwar-PTAB@wolfgreenfield.com">TSarwar-PTAB@wolfgreenfield.com</a> <a href="mailto:GScott-PTAB@wolfgreenfield.com">GScott-PTAB@wolfgreenfield.com</a>  <u>Post and hand delivery</u> : Wolf, Greenfield & Sacks, P.C. 600 Atlantic Avenue Boston, MA 02210-2206  <u>Telephone</u> : 617-646-8000 <u>Facsimile</u> : 617-646-8646

A power of attorney is submitted with the Petition. Counsel for Petitioner consents to service of all documents via electronic mail.

## I. INTRODUCTION

Google LLC (“Petitioner”) requests *inter partes* review (“IPR”) and cancellation of claims 1-21 of US 9,232,403 (“’403 Patent”) (EX-1001). The Board considered substantially similar claims with several identical limitations in IPR2024-00341, which challenged related US 8,406,733 (“’733 Patent”)<sup>2</sup> and cancelled claims 1-17, 19, 21-27, and 29-30 over the TS-23.140 standard (EX-1004) and Ogawa (EX-1005). EX-1022, 51. The Grounds herein are based on the same “MMS-Ogawa” combination from IPR2024-00341. Where applicable, Petitioner identifies relevant findings of fact and conclusions of law from the Board’s prior adjudication. EX-1023.

## II. GROUNDS FOR STANDING

Petitioner certifies the ’403 Patent is available for IPR and that Petitioner is not barred or estopped from requesting IPR of claims 1-21. 37 C.F.R. §42.104(a).

## III. UNPATENTABILITY GROUNDS

Below table identifies each §103 unpatentability ground presented herein.

Grounds, Reference(s)		Claims
1	TS-23.140, Ogawa	1, 3-6, 11-21
2A	TS-23.140, Ogawa, Cole	1-6, 11-21
2B	TS-23.140, Ogawa, Sathish	1, 3-6, 11-21
2C	TS-23.140, Ogawa, Cole, Sathish	1-6, 11-21
3A	TS-23.140, Ogawa, Papineau	7-9

---

<sup>2</sup> The ’403 and ’733 Patents share a specification.

3B	TS-23.140, Ogawa, Cole, Papineau	7-9
3C	TS-23.140, Ogawa, Sathish, Papineau	7-9
3D	TS-23.140, Ogawa, Cole, Sathish, Papineau	7-9
4A	TS-23.140, Ogawa, Ellison	10
4B	TS-23.140, Ogawa, Cole, Ellison	10
4C	TS-23.140, Ogawa, Sathish, Ellison	10
4D	TS-23.140, Ogawa, Cole, Sathish, Ellison	10

The '403 Patent claims priority to a provisional application filed January 28, 2009 (“Critical Date”). As shown below, each reference applied herein is prior art even if Patent Owner (“PO”) establishes entitlement to a January 28, 2009 effective filing date:

Reference	Filed	Published	Basis
TS-23.140		March 2005 (EX-1024 <sup>3</sup> )	102(b)
Ogawa	5/19/2008	10/1/2009	102(a)/102(e)
Cole	9/29/2006	4/3/2008	102(a)/102(e)
Sathish	10/15/2008	8/30/2011	102(a)/102(e)
Papineau	1/21/2004	8/17/2010	102(a)/102(e)
Ellison	9/22/2000	7/25/2006	102(b)

#### IV. '403 PATENT

##### A. Brief Description

The '403 Patent is directed to a “device” comprising a “*device messaging agent*” and a plurality of “*application[s] on the device.*” EX-1001, Abstract; EX-

---

<sup>3</sup> Confirming public availability/accessibility on/around March 2005.

1003, ¶¶35-36. The device messaging agent “securely communicates with a *network message server* over a wireless network.” EX-1001, Abstract. The device messaging agent also communicates with applications on the device using a “*secure interprocess communication service*.” *Id.* In claims 1-21, the device messaging agent receives, from the network message server, “secure Internet data messages” (Element [1B1]<sup>4</sup>) with a “subset” of the messages including “application data” from a “*network application server*” and an “*identifier*” corresponding to one of the device’s applications (Element [1B2]). Using the identifier, the device messaging agent forwards the application data on the secure interprocess communication service to a process corresponding to the identified application on the device (Element [1C1]-[1C2]).

## **B. Prosecution History**

Continuation application 14/667,353 was filed March 24, 2015. PO filed a preliminary amendment to replace the title and abstract and add new claims. EX-1002, 364-370. The examiner rejected the claims as indefinite. EX-1002, 616. Among the terms identified in this rejection was “first WWAN,” “device messaging agent,” “on behalf of a plurality of software applications,” “network message server,” “identifier,” and “secure interprocess communication service.”

---

<sup>4</sup> Limitations herein are identified using reference labels from the Claim Appendix.

EX-1002, 616-619. To traverse this rejection, PO attempted to identify examples (EX-1002, 730-37) for missing terms “to illustrate that those skilled in the art have the material at hand to ascertain what is meant by the various terms....” EX-1002, 730; EX-1003, ¶¶37-39. Where applicable, PO’s prosecution statements are discussed below.

## **V. PERSON OF ORDINARY SKILL IN THE ART**

A person of ordinary skill in the art (“POSA”) relating to the subject matter of the ’403 Patent as of January 28, 2009 would have had (1) at least a bachelor’s degree in computer science, electrical engineering, or a related field, and (2) 3-5 years of experience in services and application implementation in communication networks. EX-1003, ¶¶30-34. Additional graduate education could substitute for professional experience, and vice versa. *Id.*

## **VI. CLAIM INTERPRETATION**

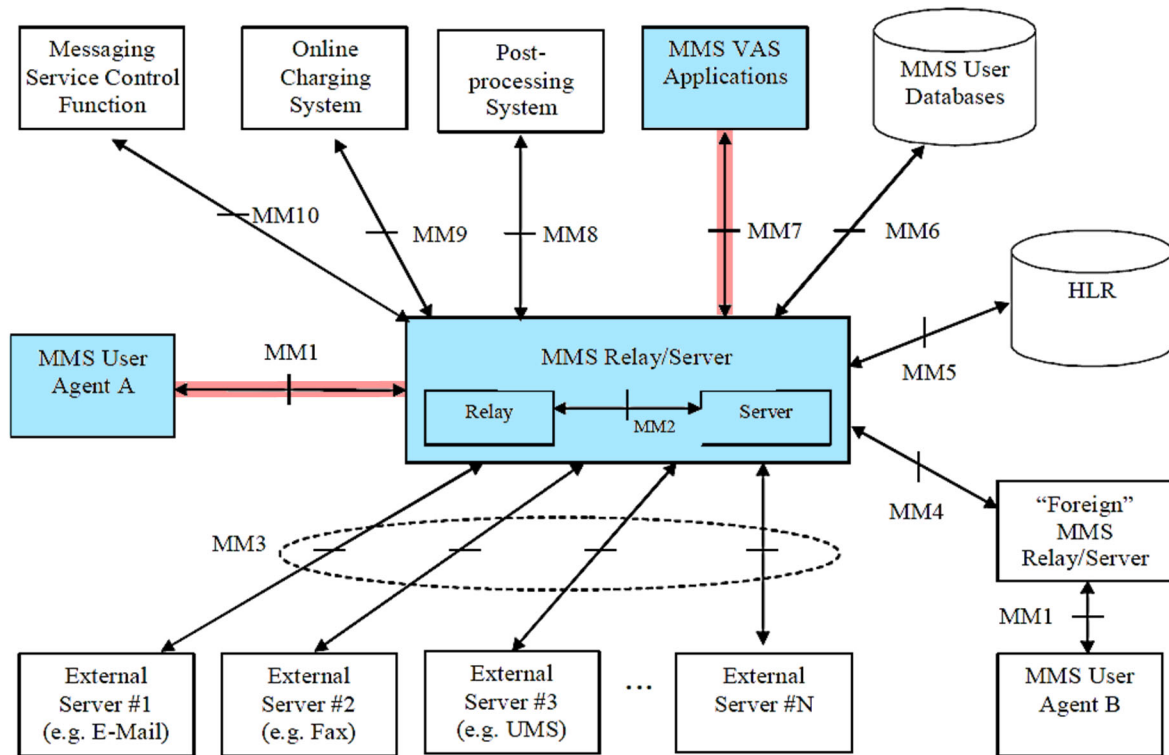
Claim terms are construed herein using the standard used in civil actions under 35 U.S.C. §282(b), in accordance with “ordinary and customary meaning” as understood by a POSA and the prosecution history. 37 C.F.R. §42.100(b). The Board need only construe terms to the extent necessary to resolve disputes between the parties. *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017); 83 Fed. Reg. 51,340, at 51,353 (Oct. 11, 2018). No claim term requires the Board to adopt an exact outer boundary construction

because the prior art meets the claims under any plausible interpretation as detailed below. In describing how terms are interpreted for this Petition, Petitioner does not concede that each challenged claim satisfies all statutory requirements or waive arguments only raisable in District Court.

**VII. GROUND 1: TS-23.140 AND OGAWA RENDER OBVIOUS CLAIMS 1, 3-6, 11-21**

**A. TS-23.140 (EX-1004)**

The TS-23.140 standard describes a “Multimedia Messaging Service, MMS.” EX-1004, 10. One MMS environment is shown below:



**EX-1004, 23, FIG. 3 (annotated)**

“MMS User Agent A” is an “application residing on a UE [user equipment]... or... external device” that “performs MMS-specific operations on a user’s behalf and/or on another application’s behalf.” *Id.*, 14, 18-19; EX-1003, ¶¶44-45.

The “MMS Relay/Server” relays messages from the network to the User Agent using interface MM1. EX-1004, 17-18, 21, 23-25. Messages may include “MMS VAS [Value Added Services]” content from “MMS VAS Applications” “provided... by third-party Value Added Service Providers (VASP)” via interface MM7 and then relayed to the User Agent to “provid[e] Value Added Services (e.g. news service or weather forecasts) to MMS users.” *Id.*, 14, 18, 23, 41. There may be “*several* MMS VAS Applications”<sup>5</sup> in the network. *Id.*, 18; EX-1003, ¶46.

“MMS may... be used to transport data specific to applications” “other than the MMS User Agent...” which also “reside on [the] MMS User Agent [device].” EX-1004, 14, 54-56; EX-1003, ¶¶47-48 (citing EX-1028, 731-733). For such “application data,” “the MMS User Agent... route[s] the received MMS information on to the destination application” using a “destination application identifier” in the received message. EX-1004, 14, 54-56; EX-1003, ¶49.

TS-23.140 discloses message “encryption... on an end-user to end-user basis,” and using, e.g., Transport Layer Security (TLS) and “authentication

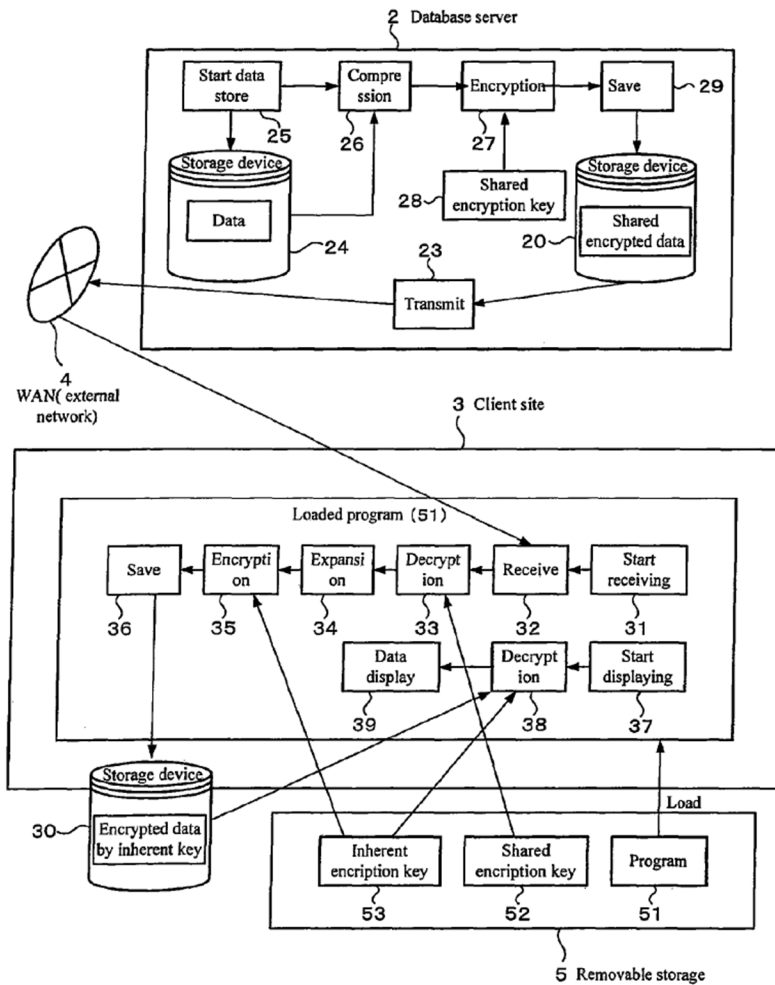
---

<sup>5</sup> Emphasis added throughout unless otherwise indicated.

mechanisms based on public/private key cryptography....” EX-1003, ¶50 (citing EX-1004, 19, 41, 25-26; EX-1011, 11; EX-1012, 21).

**B. Ogawa (EX-1005)**

Ogawa discloses a “data encryption system” facilitating secure network communications between a server and client. EX-1005, 3:18-21, 9:15-38, FIG. 7 (below); *see also id.*, FIG. 1, 3:44-54; EX-1003, ¶¶51-52.



**EX-1005, FIG. 7**

“SSL (Secure Socket Layer) is utilized to prevent some security risks presented during the exchange of data between network terminals.” EX-1005, 3:61-4:4. SSL is a predecessor of TLS. EX-1003, ¶53 (citing EX-1010, 1:38-42).

Ogawa teaches *further* securing data using a “shared encryption key” used by both client and server. EX-1005, 6:42-47, 7:11-21, 9:16-38, 4:48-57, 5:18-23. The key is used to encrypt data transmitted to the client, and decrypt received encrypted data at the client. EX-1005, 9:21-34, 5:60-65. Decryption is conducted by the client’s “decryption unit.” EX-1005, 5:59-6:9, 6:46-47, 7:11-21; EX-1003, ¶¶54-56.

Ogawa also teaches encrypting data transmitted *within* the client using an “encryption unit” and “inherent encryption key.” EX-1005, 5:59-6:26, 5:24-25; EX-1003, ¶57.

### **C. The MMS-Ogawa Combination**

As discussed below, “MMS-Ogawa” refers to an encrypted MMS system where communications with the MMS User Agent on TS-23.140’s UE/device—which may occur over a network (e.g., with an MMS Relay/Server) or within the device (e.g., with other applications)—are secured using Ogawa’s teachings. The Board endorsed this combination in IPR2024-00341 when cancelling claims 1 and 27 of the ’733 Patent. EX-1038, 9-15, 30-31, 69-72; EX-1022, 49-51; EX-1023.

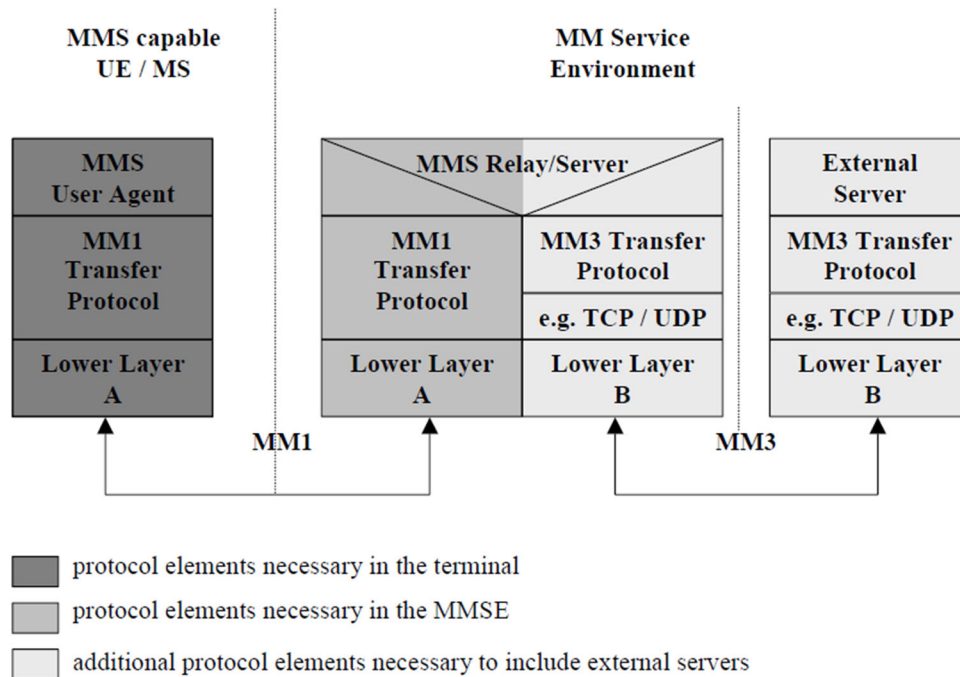
## 1. Implementing TS-23.140's UE/Device with a Modem

TS-23.140's "MMS User Agent" resides on a UE/device. EX-1004, 14, 18-19. TS-23.140 says the MMS User Agent communicates with the MMS Relay/Server using, e.g., "2G and 3G wireless networks," but does not disclose details regarding how the UE/device facilitates communications over such networks. *E.g.*, EX-1004, 17, 23-24, FIG. 2. It was well-documented and desirable to use a *modem* to enable communications over TS-23.140's described networks. EX-1003, ¶¶58-61; EX-1008, Abstract, ¶¶1, 8, 22-23, 27-28, 44, FIGS. 1, 4; EX-1006, Abstract, [0003], [0031]-[0035]. Using a modem to enable TS-23.140's UE/device to communicate over TS-23.140's wireless networks would have been an obvious way to implement what TS-23.140 describes, and is nothing more than utilizing familiar components to achieve a predictable result of facilitating TS-23.140's communications. *KSR v. Teleflex*, 550 U.S. 398, 416 (2007); EX-1003, ¶62. POSAs would have reasonably expected success implementing TS-23.140's UE/device with a modem because this was a well-known way (as noted above) to achieve TS-23.140's described wireless network communications (e.g., EX-1004, 17, 23-24, FIGS. 2-4). EX-1003, ¶¶62-63.

In IPR2024-00341, the Board agreed, finding this implementation supported by the evidentiary record. EX-1022, 40-41 (citing, e.g., EX-1004, 14, 17-19, 23-24; EX-1008, [0027]-[0028], [0044], FIGS. 1, 4); EX-1023.

## 2. Securing Interface MM1 Using SSL/TLS

TS-23.140 explains that network communications between its User Agent and Relay/Server use interface MM1. EX-1003, ¶64; EX-1004, 24, FIG. 4 (below); EX-1018, 6, 9.



**Figure 4: Protocol Framework to provide MMS  
EX-1004, 24, FIG. 4**

POSA had multiple reasons to secure MM1 with an SSL/TLS protocol:

**First**, TS-23.140 contemplates implementations which use “transport layer security mechanisms” (e.g., SSL/TLS) to secure its communication links. EX-1003, ¶¶65-66. For example, for MM1 between the User Agent (on the UE/device) and Relay/Server, TS-23.140 teaches an “WAP/OMA” implementation of MMS (EX-1004, 24-25, 30, 55, 162, 174) where “transport layer security protocol

provides for secure data transmission.” EX-1012, 21.<sup>6</sup> In that implementation, the “MMS User Agent is... responsible for sending and receiving MMs by utilising the message transfer services of the appropriate network protocols” e.g. SSL/TLS for securing MM1 between the User Agent and Relay/Server. EX-1012, 17, 21; EX-1003, ¶66. TS-23.140 includes similar disclosures regarding other links, e.g. MM7 between the Relay/Server and VAS Applications. *E.g.*, EX-1004, 41.

***Second***, it was well-documented to use SSL/TLS to achieve secure communications between network entities, e.g. client and server. EX-1003, ¶67 (citing EX-1012, 21; EX-1010, 1:38-42; EX-1013, 3).

***Third***, such an implementation is nothing more than utilizing familiar protocols to achieve a predictable result of facilitating secure communications over MM1. *KSR*, 550 U.S. at 416; EX-1003, ¶68.

---

<sup>6</sup> WAP/OMA is Open Mobile Alliance’s Wireless Application Protocol. EX-1003, ¶66. To describe “[d]etails” for this “implementation of the MM1 transfer protocol,” TS-23.140 incorporates-by-reference EX-1011 (“Enabler Release Definition”). EX-1004, 13, 24-25, 162. EX-1011 incorporates-by-reference EX-1012 (“Architecture Overview”). EX-1011, 4, 5, 10.

POSAs would have reasonably expected success implementing MM1 to use SSL/TLS, given TS-23.140's teachings and incorporated disclosures (e.g., EX-1012, 21), and the widespread use of such protocols. EX-1003, ¶¶69-70.

In IPR2024-00341, the Board agreed, finding this implementation supported by the evidentiary record. EX-1022, 41-42 (citing, e.g., EX-1004, 24-25, 55, FIG. 4; EX-1010, 1:38-42; EX-1012, 21; EX-1013, 3; EX-1018); EX-1023.

### **3. Applying Ogawa's Encryption Techniques for Network Communications**

TS-23.140 discloses message "encryption... on an end-user to end-user basis." EX-1004, 19. In addition to "transport layer security mechanisms," "authentication mechanisms based on public/private key cryptography... may *also* be used." EX-1003, ¶¶71-72 (citing EX-1004, 17, 25, 30, 41, 62; EX-1012, 21; EX-1005, 8:16-21). TS-23.140 does not provide details regarding how to implement additional end-user-to-end-user encryption beyond SSL/TLS.

Implementing encryption for messages transmitted by a server to a client using shared-key encryption was well-documented in the prior art. EX-1003, ¶73 (citing EX-1005; EX-1027, [0054]-[0060]; EX-1009, 3:25-27, 8:1-5). Ogawa discloses details regarding how to implement such message encryption in a client-server environment like the one described in TS-23.140, where "SSL... is utilized to prevent some security risks presented during the exchange of data between network terminals." EX-1005, 3:44-53, 3:61-4:4, 9:16-34. EX-1003, ¶73.

POSAs had multiple reasons to implement Ogawa's encryption techniques with TS-23.140's MMS system ("MMS-Ogawa Message Encryption"):

**First**, implementing Ogawa's encryption to TS-23.140's MMS system would have achieved "improved security" and provided "an end-user to end-user" security solution for MMS, as TS-23.140 contemplates. EX-1003, ¶¶74-75 (citing EX-1004, 19, 24-25; EX-1012, 21).

**Second**, encrypting MMS communications using Ogawa's additional layer of security beyond SSL/TLS would have been beneficial for "enterprise applications"—a type of value-added service application that POSAs would have been motivated to ensure its MMS system could handle. EX-1003, ¶76 (citing EX-1027, [0002]-[0003], [0017], [0021]-[0022]; EX-1004, 54).

**Third**, implementing Ogawa's encryption in TS-23.140's MMS system would have been nothing more than implementing known methods/techniques (encryption using a shared key as Ogawa teaches) to known systems/devices (TS-23.140's Relay/Server and UE/device) to achieve predictable results (end-user-to-end-user encrypted data). *KSR*, 550 U.S. at 416; EX-1003, ¶77.

POSAs would have reasonably expected success implementing Ogawa's encryption techniques to the TS-23.140 system given (1) the similar client-server architectures in both references (with SSL/TLS-protected network connections) and (2) TS-23.140's contemplation of end-user-to-end-user encryption, of which

Ogawa provides an exemplary, predictable implementation. EX-1003, ¶¶78-82 (citing EX-1005, 3:44-53, 3:60-4:4, 4:48-57, 6:64-7:21, 9:16-34, FIG. 7; EX-1009, 3:25-27, 8:1-5). In IPR2024-00341, the Board agreed this modification was obvious. *Infra* §VII.C.4.

#### 4. Ogawa's Decryption and Encryption Units

Ogawa teaches a “decryption unit” for decrypting received encrypted data. EX-1005, 5:59-6:9 (“[R]eceived shared key encrypted data will be decrypted using the shared encryption key 52 which was supplied to the decryption unit 33 and beforehand stored...”); EX-1003, ¶83. POSAs would have been motivated to implement the decryption unit *as part of TS-23.140's MMS User Agent* application, because (1) the MMS User Agent is responsible for receiving data from TS-23.140's MMS Relay/Server and distributing it to the correct applications on the UE/device, and (2) TS-23.140 expressly identifies the MMS User Agent as “provid[ing]... functionalities such as... *decryption*.” EX-1003, ¶83 (citing EX-1004, 19, 54-56). Such an implementation would have, e.g., beneficially allowed the User Agent to decrypt an encrypted message from the Relay/Server and any information identifying where it should be routed. EX-1003, ¶83.

Ogawa also teaches an encryption unit for encrypting (or “re-encrypt[ing]”) data before transmitting within the device, e.g., to storage. EX-1005, 5:59-6:9; EX-1003, ¶84. As with the decryption unit, POSAs would have been motivated to

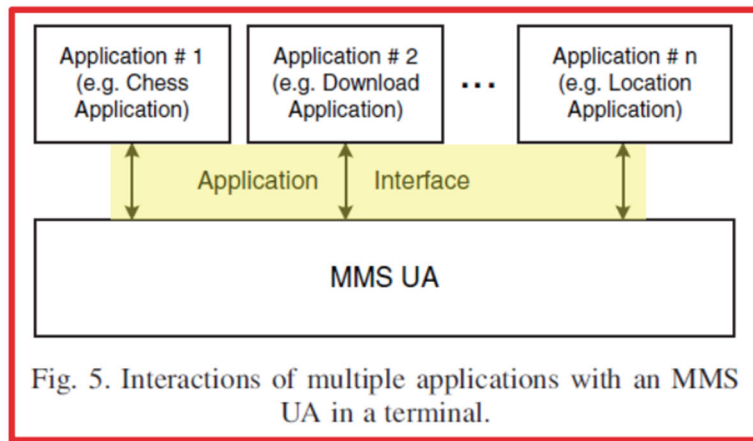
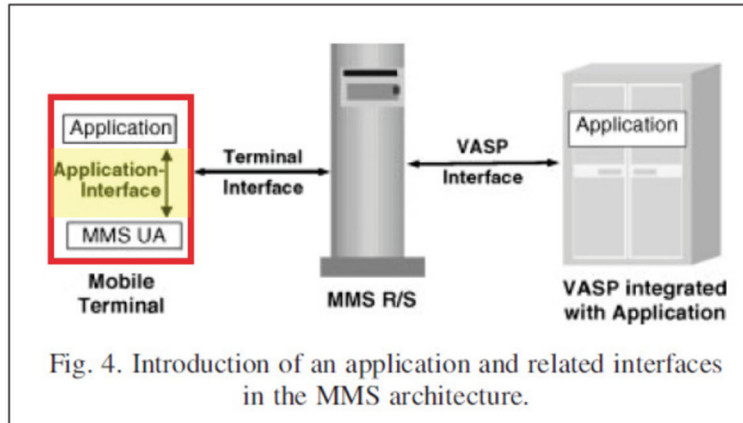
implement the encryption unit *as part of TS-23.140's MMS User Agent application*, because (1) secure transmission and storage of data within a UE/device desirably would have helped prevent, e.g., theft, (2) the MMS User Agent is responsible for “transport of application data” and “all aspects of storing” messages on TS-23.140's UE/device, and (3) TS-23.140 expressly identifies the MMS User Agent as “provid[ing]... functionalities such as... *encryption*.” EX-1003, ¶84 (citing EX-1004, 19; EX-1037).

POAs would have reasonably expected success incorporating Ogawa's encryption and decryption units into TS-23.140's MMS User Agent application, because each prior art component would continue performing functions they performed prior to combining—MMS User Agents and MMS Relay/Server would continue to exchange data using secure communication links, and Ogawa's decryption and encryption units (implemented as part of each User Agent) would decrypt/encrypt data exchanged with the Relay/Server. EX-1003, ¶¶85-86. Such a combination would have been well within a POA's capability to implement. *Id.*

The Board in IPR2024-00341 considered the modifications described in §§VII.C.3-VII.C.4, and found them supported by the evidentiary record. EX-1022, 42-43 (citing, e.g., EX-1004, 14, 17, 19, 24-25, 41, 54-56, 62; EX-1005, 3:60-4:4, 4:34-57, 5:59-6:9, 6:64-7:21, 8:16-19, 9:16-34, FIG. 7; EX-1009, 3:25-27, 8:1-5; EX-1012, 21; EX-1027, [0017], [0021]-[0022], [0054]-[0060]); EX-1023.

## 5. Implementing TS-23.140's Device with an Interprocess Communication Bus

TS-23.140 discloses its MMS User Agent receiving “data specific to an application other than the MMS User Agent” from MMS VAS Applications and “rout[ing]” that “received MMS information” (e.g., application-specific data) “to [a] destination application” on the UE/device—but leaves to POSAs the “[d]etails of... how an MMS User Agent... would *interface* with” such applications. EX-1004, 14, 54-56; EX-1003, ¶87. Contemporaneous references discussing MMS confirm that TS-23.140's UE/device included an interface for communications between the MMS User Agent and other applications. *E.g.*, EX-1028, 729-730, 732-733, FIGS. 4-5 (annotated below).



**EX-1028, FIGS. 4-5 (annotated)**

See also EX-1003, ¶188; EX-1008, [0028], FIG. 4.

POSAs would have been motivated to implement the interface between TS-23.140’s MMS User Agent application and other applications using a software *bus* for interprocess communications (e.g., a D-Bus), which was a well-documented way to enable applications to interface with one another. EX-1031, 10:56-62 (“the D-Bus may be an example of a device inter-process communication channel used to send information between applications.”); see also EX-1048, [0001], [0003], [0004], [0019] (“communication” between “one or more processes” occurring over a “bus”); EX-1049, 907 (“software bus”: “A programming interface that allows

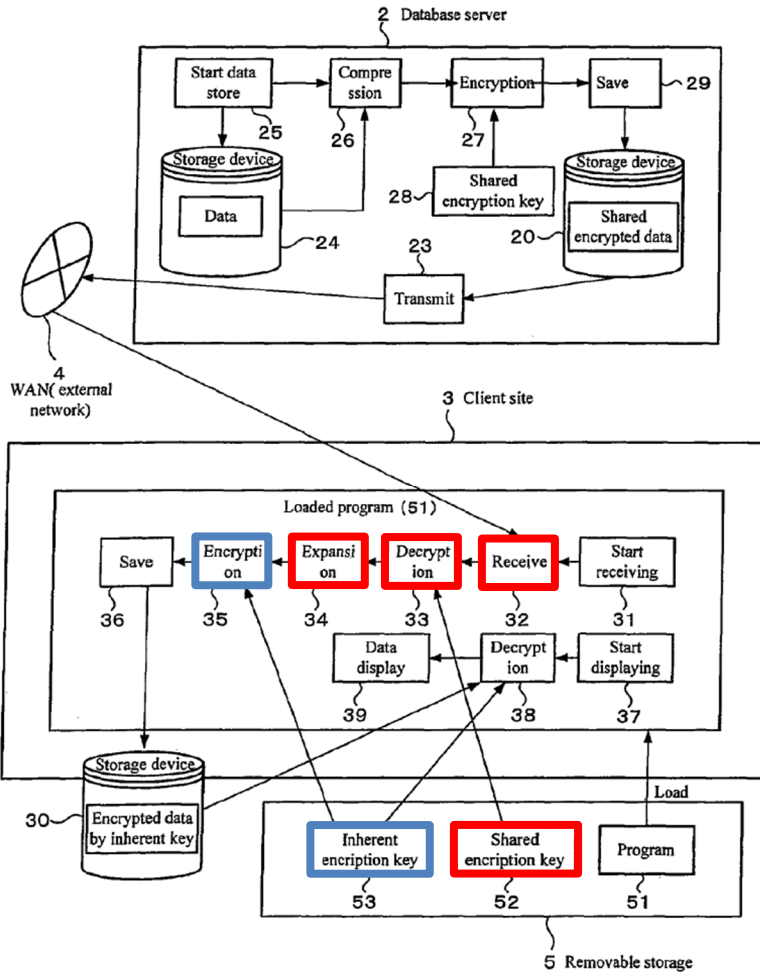
software modules to transfer data to each other...”); EX-1050, 2:64-3:6 (“software bus” that “interconnects” a “control software’s subsystems”), 3:51-67, FIG. 5; EX-1003, ¶89. Using such a bus to enable an MMS User Agent to communicate with other applications on TS-23.140’s UE/device would have been an obvious way to implement what TS-23.140 describes, and is nothing more than utilizing familiar components to achieve a predictable result of facilitating TS-23.140’s intra-device communications. *KSR*, 550 U.S. at 416; EX-1003, ¶90. For these same reasons, POSAs would have reasonably expected success using a bus. EX-1003, ¶¶91-92.

In IPR2024-00341, the Board agreed with Petitioner’s “argu[ment] that [POSAs] would have implemented communications between the MMS User Agent and other applications over a bus, such as a D-bus” (EX-1022, 45), and found this implementation supported by the evidentiary record. EX-1022, 48-49 (citing, e.g., EX-1008, [0028], FIG. 4; EX-1028, 732-733; EX-1031, 10:56-62); EX-1023.

## **6. Securing Interprocess Communications Within the Device**

Ogawa discloses encryption unit 35 for re-encrypting data transmitted within a client. *Supra* §VII.C.4; EX-1005, 6:1-9; EX-1003, ¶¶93-94. In Ogawa, an encrypted message received by the client is decrypted (using decryption unit 33 and shared encryption key 52) and decompressed/expanded (if needed) using unit 34. EX-1005, 5:24-27, 5:59-6:26. It is then re-encrypted by encryption unit 35

using “inherent encryption key 53” before being transmitted within the client. *Id.*; see also *id.*, FIG. 7 (below).



**EX-1005, FIG. 7 (annotated)**

POSAs were motivated to include Ogawa’s re-encryption functionality in MMS-Ogawa’s User Agent—e.g., to secure decrypted application data received over MM1 before transmitting it to any other component on the user device—and would have reasonably expected success doing so. This is because (1) in-device encryption using an inherent key was taught by Ogawa, (2) securing interprocess communications between applications using encryption was well-documented

(e.g., EX-1039, Abstract, [0001]-[0004], [0007]-[0008]), and (3) an implementation where internal communications were protected using an inherent key would have improved data security in MMS-Ogawa’s UE/device and would have helped, e.g., prevent unauthorized data access by, e.g., rogue software. EX-1003, ¶¶95-97. In IPR2024-00341, Petitioner discussed Ogawa’s inherent keys and securing communications *within* MMS-Ogawa’s UE/device (EX-1038, 69-72)—contentions which the Board “determine[d]” were “fully supported by the record” (EX-1022, 50-51; EX-1023).

## 7. MMS-Ogawa

“MMS-Ogawa” (EX-1003, ¶¶97-102) refers to the above-discussed encrypted MMS system that POSAs would have formed based on TS-23.140 and Ogawa.

MMS-Ogawa implements TS-23.140’s UE/device (configured to use MMS) with a modem for wireless network communications. *Supra* §VII.C.1.

MMS-Ogawa implements TS-23.140’s MMS Relay/Server and UE/device such that messages transmitted across the interface between TS-23.140’s MMS User Agent and MMS Relay/Server are secured with SSL/TLS *and* encrypted using MMS-Ogawa Message Encryption. *Supra* §§VII.C.2-VII.C.3.

Ogawa’s encryption and decryption units are implemented as part of the MMS User Agent in TS-23.140’s UE/device. *Supra* §VII.C.4.

MMS-Ogawa implements an interprocess bus for communications between applications within TS-23.140’s UE/device (*supra* §VII.C.5), which are secured using Ogawa’s inherent key (*supra* §VII.C.6).

#### **D. Claim Analysis**

##### **1. Claim 1**

###### **a. [1PRE] “A mobile end-user-area device comprising:”**

The ’403 specification<sup>7</sup> does not describe a “mobile end-user-area<sup>8</sup> device,” but uses the term “end user device”; “end user device” is used to include “networked” devices that have “services delivered” to them. EX-1001, 5:65-6:28, 6:49-56, 8:3-15, 8:60-9:15; EX-1003, ¶¶103-104. In IPR2024-00341, the Board found “the User Equipment of TS-23.140 teaches, suggests, or would have been understood to disclose, to the extent the preamble is limiting, ‘[a]n end-user device.’” EX-1022, 15; EX-1023. POSAs further understood TS-23.140’s “UE”/“MS”/“external *device*”/“*mobile* phone”—with a User Agent “perform[ing]... operations on a user’s behalf,” and through which “users” receive

---

<sup>7</sup> Herein, “specification” refers to EX-1001, 1:1-163:36, and FIGs. 1-64, which reflect the as-filed continuation application disclosure (EX-1002, 10-250), but not the title or abstract, which Applicant later added (*id.*, 365).

<sup>8</sup> “-area” is likely a typographical error. Each dependent claim recites “The mobile end-user device of claim 1.”

“Value Added Services”—teaches a “*mobile* end-user-area device.” EX-1004, 14, 18, 54; EX-1003, ¶104.

- b. [1A] “a wireless wide-area network (WWAN) modem to exchange Internet data via a connection to a first WWAN, when configured for and connected to the first WWAN;”

MMS-Ogawa includes a “*modem*.” *Supra* §VII.C.1. In IPR2024-00341, the Board credited Petitioner’s showing that MMS-Ogawa “had a modem” for network communications based on TS-23.140’s disclosures. EX-1022, 15-16 (citing EX-1004, 14, 18, 23-25, 55-56, FIGs. 2-4); EX-1023.

Element [1A] requires “a *wireless wide-area network (WWAN)* modem.” The specification uses “WWAN modem” to include “a wide area access technology modem” for 2G/3G networks; MMS-Ogawa’s modem for 2G/3G wireless networks (*supra* §VII.C.1) is thus “a wireless wide-area network (WWAN) modem,” as claimed. EX-1001, 29:52-53; *see also id.*, 33:57-63, 2:17-23, 12:63-13:3, 25:29-45, 27:38-44; EX-1003, ¶¶105-106.

POSAs understood MMS-Ogawa’s modem for 2G/3G wireless networks (*supra* §VII.C.1) is “[for] exchang[ing] Internet data via a connection to a first WWAN, when configured for and connected to the first WWAN,” as claimed. EX-1003, ¶107. This is confirmed in TS-23.140 FIG. 2, showing a Multimedia Messaging Service Environment (MMSE) in which TS-23.140’s UE/device operates, comprising 2G and 3G wireless networks:

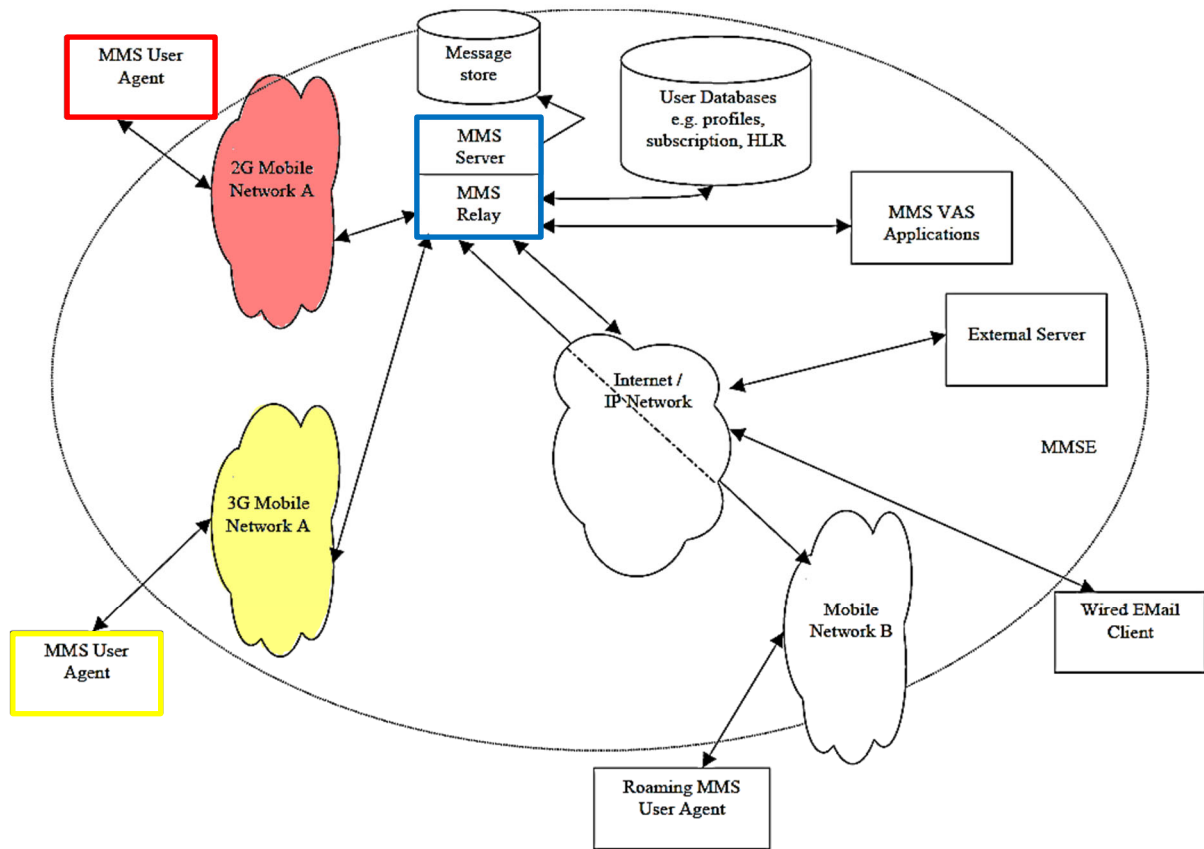
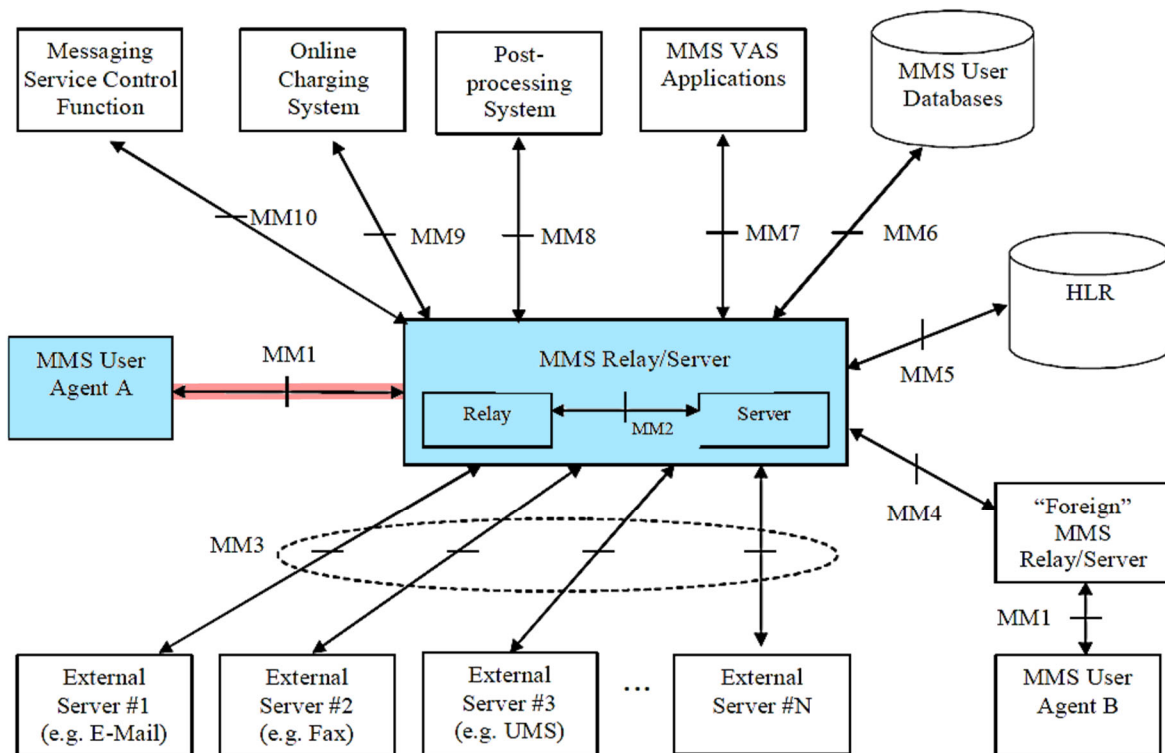


Figure 2: MMS Architectural Elements

**EX-1004, 17, FIG. 2 (annotated)**

“Figure 2 shows... multimedia messaging may encompass many different network types.” EX-1004, 17. “The basis of *connectivity* between these different networks” is “provided by the *Internet* protocol and its associated set of messaging protocols,” which “enables messaging in 2G and 3G wireless networks to be compatible with messaging systems found on the *Internet*.” *Id.*; *see also id.*, 18 (“MMS *connectivity* across different networks (MMSEs) is provided based on *Internet* protocols.”).

FIG. 2 illustrates multiple “MMS User Agent” UEs/devices—including one (top left) configured for communications with the Relay/Server through a connection to “2G Mobile Network A” and another (bottom left) configured for communications with the Relay/Server through a connection to “3G Mobile Network A.” See also EX-1004, 14, 17-19, 23-24. These connections are part of the respective interface MM1 for each UE/device which facilitates “*Internet* protocol” communications between each UE/device’s MMS User Agent and the Relay/Server. EX-1004, 17; EX-1003, ¶108 (citing EX-1004, 17, 23-24, FIG. 4). MM1 is shown below:



**EX-1004, 23, FIG. 3 (annotated)**

MMS-Ogawa's user device modem also enables MMS-Ogawa's User Agent to exchange messages containing *data* with network elements through interface MM1—including with MMS-Ogawa's Relay/Server, and multiple VAS applications (via the Relay/Server). EX-1004, 14, 18, 23; EX-1003, ¶109. For example, using the modem, MMS-Ogawa's User Agent may “transport *data* specific to applications other than MMS” (e.g., in “abstract messages”) to/from a VAS Application. EX-1004, 17, 54-56; EX-1003, ¶109.

Thus, MMS-Ogawa's modem (*supra* §VII.C.1) is a “WWAN” modem used “to exchange *Internet data* via a connection to” MMS-Ogawa's 2G or 3G WWAN, “when configured for and connected to” each of those networks. EX-1003, ¶110.

Moreover, MMS-Ogawa's WWAN modem is “to exchange Internet data via *a first WWAN, when configured for and connected to the first WWAN,*” as claimed. During prosecution, PO said “[t]he modifier ‘first’ is merely indicative that this is an identifiable WWAN to which the modem can connect....” EX-1002, 730. MMS-Ogawa's 2G and 3G networks are each an identifiable WWAN to which MMS-Ogawa's user device can connect, when configured for and connected to it. EX-1003, ¶111.

c. [1B1]

MMS-Ogawa meets each limitation in Element [1B1], discussed below. In IPR2024-00341, the Board found MMS-Ogawa met substantially the same limitation in the '733 Patent. EX-1022, 36, §II.D.3(i); EX-1023; EX-1003, ¶112.

i. “a device messaging agent to receive secure Internet data messages”

The specification uses “agent” to include a component—e.g., one “implemented... entirely in software”—that performs some function on behalf of e.g., a client or server. EX-1001, 15:58-16:12, 42:48-55; EX-1003, ¶113; *see also* EX-1029, 12. In IPR2024-00341, the Board agreed. EX-1022, 27; EX-1023.

Element [1B1] requires a “*device messaging* agent.” The '403 specification never uses that term. PO stated during prosecution that “service control device link 1691”—which may perform a “central agent communication hub function” (EX-1001, 42:9-15, 44:62-45:5) and “provides the device side of a system for transmission and reception” of messages (*id.*, 37:40-43)—is an “embodiment” of the “device messaging agent.” EX-1002, 731; EX-1003, ¶114. PO’s prosecution statements indicate a “*device messaging* agent” includes an agent (on a *device*) that is used for *messaging*—e.g., to/from a network element. EX-1003, ¶114; EX-1002, 731.

MMS-Ogawa’s “MMS User Agent” is a device-side “application” (i.e., implemented in software) on TS-23.140’s UE/device that receives and transmits

messages to/from the MMS Relay/Server over MM1 and “*performs MMS-specific operations on a user’s behalf and/or on another application’s behalf*” (*supra* §VII.A)—e.g., transportation of application-specific data to/from third-party MMS VAS Applications via the MMS Relay/Server. EX-1004, 14, 19, 23-24, 30-31, 35-36, 41-42, 54-56; EX-1003, ¶115. MMS-Ogawa’s application-specific data is sent in what TS-23.140 calls “abstract *messages.*” EX-1004, 14 (“abstract messages: information which is transferred between two MMS entities used to convey an MM and/or associated control information between these two entities.”), 54-56 (discussing using “abstract messages” to “transport application data”). MMS-Ogawa’s User Agent is thus a “device messaging agent,” as claimed. EX-1003, ¶116. This is consistent with the Board’s finding in IPR2024-00341 that MMS-Ogawa’s User Agent is “a service control device link agent on the end-user device” (EX-1022, 17-18) which is what PO identified as the “device messaging agent” during prosecution (EX-1002, 731). EX-1023.

MMS-Ogawa’s device messaging agent is used “*to receive secure Internet data messages,*” as explained below.

The ’403 specification does not describe “secure Internet data messages,” or require “Internet data messages” to be secured in any specific way; instead, it leaves to POSAs how communications are “secur[ed], sign[ed], encrypt[ed] and/or otherwise protect[ed]” when sent. EX-1001, 69:22-25; EX-1003, ¶117.

MMS-Ogawa's modem enables MMS-Ogawa's User Agent to exchange "**Internet** protocol" communications via interface MM1, including "abstract **messages**" with "**data** specific to applications other than MMS." *Supra* §VII.D.1.b; EX-1004, 14, 17-18, 23-24, 54-56, FIGS. 3-4; EX-1003, ¶118. MMS-Ogawa's device messaging agent is thus used to **receive Internet data messages**.

Such messages received over MM1 are "**secure[d]**" using: (1) SSL/TLS, because MM1 between the User Agent on the user device and the Relay/Server (over which the messages are sent) is secured using SSL/TLS (*supra* §VII.C.2), and (2) MMS-Ogawa Message Encryption (*supra* §§VII.C.3-VII.C.4).

MMS-Ogawa's User Agent is thus "**a device messaging agent to receive secure Internet data messages**," as claimed. EX-1003, ¶119.

**ii. "on behalf of a plurality of software applications capable of execution on the device"**

During prosecution, PO stated that "'on behalf of'... indicat[es] operation in a proxy capacity," and that "on behalf of a plurality of software applications capable of execution on the device" "merely indicates that the secure Internet data messages are directed to the device messaging agent, with the expectation that the device messaging agent will deliver the internal contents of the messages to the appropriate processes on the device based on the application ID(s) in each message." EX-1002, 732.

As discussed *supra* §VII.D.1.c.i, MMS-Ogawa’s User Agent application (the claimed *device messaging agent*) “performs MMS-specific operations on a user’s behalf and/or *on another application’s behalf*.” EX-1004, 14. Among these operations is the “transport [of] data specific to *applications*” (i.e., a *plurality*) “other than the MMS User Agent,” that are also on MMS-Ogawa’s user device—for example, a “chess *application*” that “initially need[s] to register with the appropriate MMS User Agent” in order to send/receive such data. EX-1004, 14, 54-56; EX-1003, ¶¶120-121 (citing EX-1028, 732-733). TS-23.140 discloses, e.g., “received MMS information” (from, e.g., an MMS VAS Application) “immediately route[d]” by the User Agent “to the destination application... without presentation to the user.” EX-1004, 56.

MMS-Ogawa’s “other” destination applications are separate from (and in communication with) the user device’s MMS User Agent application. EX-1003, ¶122 (citing EX-1004, 14, 54; EX-1028, 732-733); *supra* §VII.C.5. The Board in IPR2024-00341 agreed. EX-1022, 30-31; EX-1023. Confirming this is TS-23.140’s disclosure of destination applications “downloadable... to a mobile phone” or “integrat[ed] into a mobile phone” through an “application registration process.” EX-1004, 54; EX-1003, ¶122.

Based on TS-23.140’s disclosures regarding destination applications—e.g., what they do and how they are added to TS-23.140’s UE/device—POSAs

understood that these applications run on TS-23.140's UE/device and are a plurality of *software* applications *capable of execution on the device*. EX-1003, ¶123 (citing EX-1045, 126; EX-1046, 46). Thus, MMS-Ogawa's User Agent is a "*device messaging agent*" that "*receive[s] secure Internet data messages*" (*supra* §VII.D.1.c.i) "*on behalf of a plurality of software applications capable of execution on the device*," as claimed. EX-1003, ¶124.

**iii. "and over a secure connection to a network message server reachable via the WWAN"**

The '403 specification never describes a "network message server." PO stated during prosecution that "service control server link 1638"—which may "provide[] the network side of a system for transmission and reception" of messages<sup>9</sup> (EX-1001, 68:9-48)—is an embodiment of the claimed "network message server." EX-1002, 732-733. PO's statements indicate a "*network message server*" includes a *server* (on a *network*) that is used to relay *messages* to/from a device. EX-1003, ¶¶125-126; EX-1001, 16:13-16, 68:9-48; EX-1002, 732-733.

As discussed *supra* §VII.D.1.b, MMS-Ogawa's "MMS Relay/*Server*" is part of the MMSE (which TS-23.140 describes as a "*network*") and can be reached by the MMS User Agent over the WWAN (e.g., 2G/3G wireless network). EX-1004,

---

<sup>9</sup> PO characterized the specification's omission of "messages" as a "typographical error." EX-1002, 732-733.

17-18, FIG. 2. Moreover, as discussed *supra* §VII.A, the Relay/Server relays messages between the User Agent and VAS Applications using various communication interfaces between the Relay/Server and other MMSE elements—e.g., MM1 (EX-1004, 17-18, 21, 23-25) between a User Agent and the Relay/Server (*id.*, 23-24, FIG. 4) and MM7 between the Relay/Server and VAS Applications (*id.*, 14, 18, 23-26, 41). POSAs thus understood that MMS-Ogawa’s Relay/Server is a ***network message server reachable via the WWAN***. EX-1003, ¶127. This is consistent with the Board’s finding in IPR2024-00341 that MMS-Ogawa’s Relay/Server is “a service control server link element of the network system” (EX-1022, 34-36) which is what PO identified as the “network message server” during prosecution (EX-1002, 732-33). EX-1023.

POSAs likewise understood that communications between MMS-Ogawa’s User Agent and Relay/Server occur “***over a secure connection***,” as claimed. EX-1003, ¶128. While the ’403 specification does not describe a “secure connection,” or require the connection between the network message server and device messaging agent to be secured in any particular way, the specification describes a “service control link 1653” as the connection between what PO identified as a network message server (service control server link 1638) and what PO identified as a device messaging agent (service control device link 1691) as “provid[ing] for

a *secure (e.g., encrypted)* communications link for providing secure, bidirectional communications...” EX-1001, 68:18-27, FIG. 16; EX-1003, ¶129.

The specification leaves to POSAs precisely how “the service control server link 1638 provides for *securing, signing, encrypting and/or otherwise protecting* the communications before sending such communications over the service control link 1653.” EX-1001, 69:22-25; *supra* §VII.D.1.c.i; EX-1003, ¶130. The specification, e.g., describes use of “secure transport protocols running over Transmission Control Protocol (TCP),” e.g., “Transport Layer Security (TLS).” EX-1001, 17:2-24; *see also id.*, 69:25-30, 87:55-62; EX-1003, ¶130. TLS and Secure Socket Layer (SSL) are used interchangeably. *E.g.*, EX-1001, 94:3; EX-1003, ¶130.

As discussed *supra* §VII.D.1.c.i, MMS-Ogawa’s User Agent (“device messaging agent”) communicates with the Relay/Server (“network message server”) over interface MM1. MMS-Ogawa’s MM1 interface is secured using SSL/TLS. *Supra* §VII.C.2. MMS-Ogawa’s messages are also encrypted using MMS-Ogawa Message Encryption (*supra* §VII.C.3) when sent using MMS, including when transmitted over MM1. EX-1003, ¶131. MMS-Ogawa’s MM1 is thus a “secure connection,” and the secure Internet data messages received from MMS-Ogawa’s Relay/Server over MM1 (*supra* §VII.D.1.c.i) are received “*over a secure connection to*” the “*network message server reachable via a WWAN,*” as

claimed. EX-1003, ¶132. This is consistent with the Board’s finding in IPR2024-00341 that MM1 between MMS-Ogawa’s User Agent and Relay/Server is a “service control link,” i.e., connection, “*secured* by an encryption protocol.” EX-1022, 16-17; EX-1023.

**d. [1B2]**

MMS-Ogawa meets each limitation in Element [1B2], discussed below. In IPR2024-00341, the Board found MMS-Ogawa met substantially the same limitation in the ’733 Patent. EX-1022, 37-39, §§II.D.3(k)-II.D.3(l); EX-1023; EX-1003, ¶133.

**i. “wherein at least a subset of the secure Internet data messages contain an identifier for a corresponding one of the software applications”**

In MMS-Ogawa, MMS is “used to transport data specific to applications” on the user device that are not the MMS User Agent. EX-1004, 54-56; EX-1003, ¶134 (citing EX-1028, 732-733); *supra* §§VII.D.1.c.i, VII.A. MMS-Ogawa’s destination applications are *software applications*. *Supra* §VII.D.1.c.ii.

MMS-Ogawa’s User Agent receives application data from the Relay/Server via MM1, in “abstract messages” that each include an “application identifier of the destination application”—e.g., a “chess” application. EX-1004, 54-56; EX-1003, ¶¶135-136 (citing EX-1004, 54-56, 60, 69, 72-73, 111; describing “MM1-Retrieve.RES”). The “application *identifier*” is the *identifier* that allows MMS-

Ogawa’s User Agent to “immediately route” a received application-specific message to the “destination application that is referred to from the destination application identifier” (EX-1004, 56)—i.e., to the *corresponding one of the software applications*. EX-1003, ¶135.

During prosecution, PO stated that “*at least a subset*” “is intended to indicate that the secure Internet data messages sent to the device messaging agent can be sent for multiple purposes, only one of which is to provide data to applications.” EX-1002, 733. PO also said the claimed “*identifier* is a value that the device messaging agent and network message server both associate with an agent/function/process/application on the device.” EX-1002, 733.

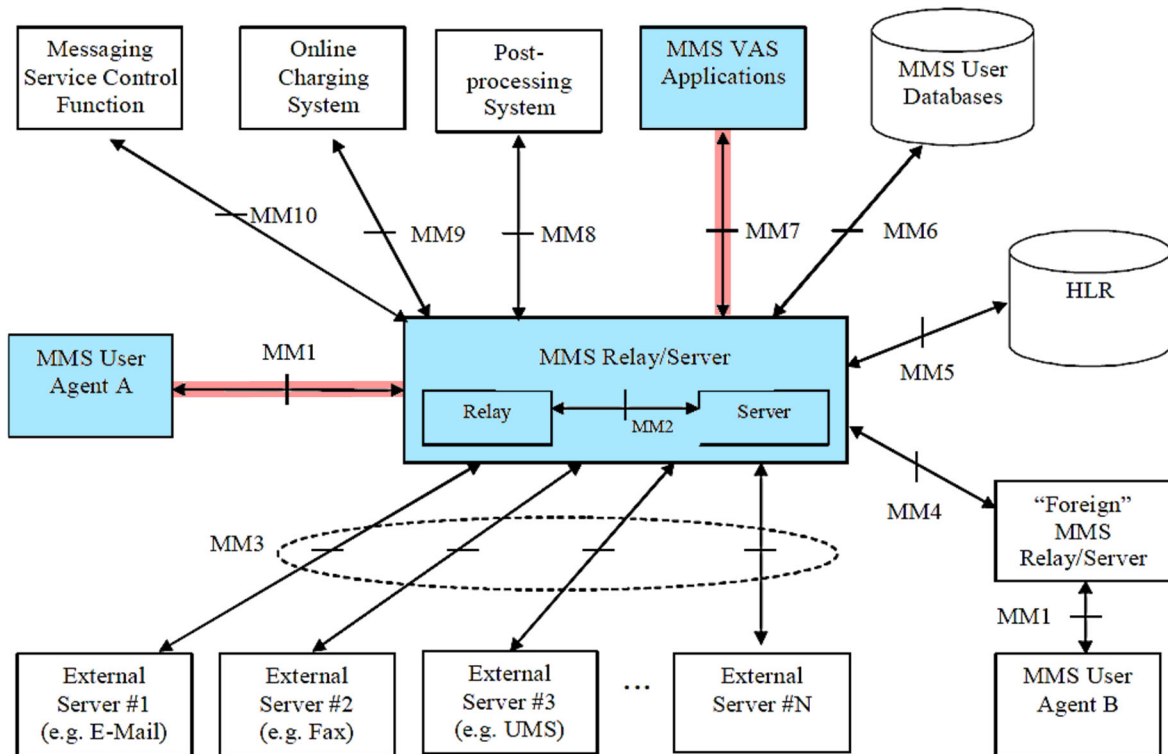
In MMS-Ogawa, one of MMS’s uses is to transport application-specific data to applications (*see supra* §§VII.D.1.c.i, VII.A), which is routed using an application identifier “present in an abstract message” (EX-1004, 55) that is sent by MMS-Ogawa’s Relay/Server to the User Agent; POSAs thus understood “*at least a subset of*” MMS-Ogawa’s “*secure Internet data messages*” (*supra* §VII.D.1.c.i) “*contain an identifier for a corresponding one of the software applications*,” as claimed. EX-1003, ¶137.

**ii. “and application data from a respective network application server corresponding to that application”**

As discussed *supra* §§VII.D.1.c.i-VII.D.1.c.ii, MMS-Ogawa’s secure Internet data messages (including the “abstract messages” subset discussed *supra* §VII.D.1.d.i) are “used to transport data specific to applications” other than the MMS User Agent. EX-1004, 54-56; EX-1003, ¶138 (citing EX-1028, 732-733); *see also supra* §VII.A. TS-23.140 expressly calls such data “application data.” EX-1004, 14, 54-56 (disclosing “transporting” “Application Data” in “abstract messages”). POSAs thus understood TS-23.140’s application-specific data—which is transported in MMS-Ogawa’s messages (e.g., abstract messages) to specific applications “without alteration” (EX-1004, 14, 54-56)—constitute ***application data***. EX-1003, ¶138.

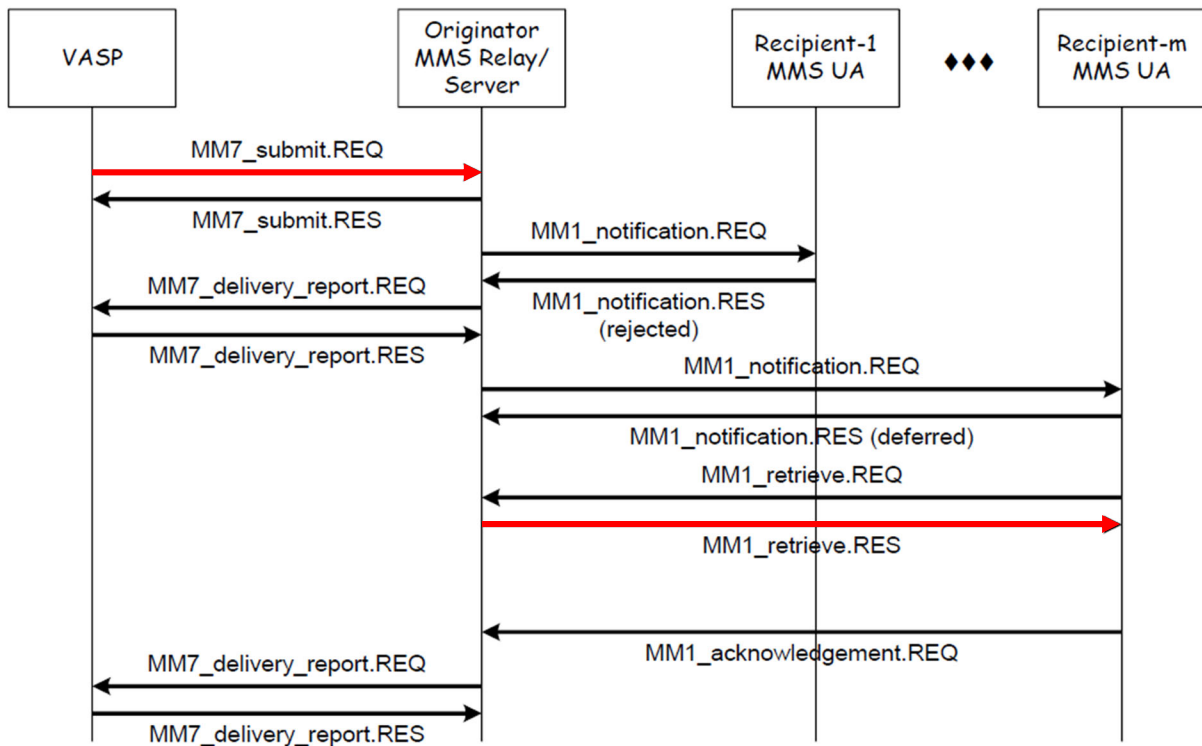
Further, as discussed below, POSAs understood that the “at least a subset of” MMS-Ogawa’s secure Internet data messages (discussed *supra* §VII.D.1.d.i) “contain... application data from a respective network application server corresponding to that application.” EX-1003, ¶139. The ’403 specification never uses the term “network application server.” Based on its plain language, the term includes a server that interacts with an application on a user device to deliver some service to a user. EX-1003, ¶139; *cf.* EX-1001, 86:59-87:5.

As discussed *supra* §VII.D.1.c.i, MMS-Ogawa’s messages containing application data (including the “abstract messages” subset discussed *supra* §VII.D.1.d.i) include data from VAS Applications. EX-1004, 14, 18, 23, 41 (“The MMS Relay/Server may support services... provided... by third-party [VASPs]. ... Messages that originate from the VASP may be targeted to the recipient....”), 54-56; EX-1003, ¶¶140-141. These messages contain application data “of any content type and format,” and are used to “provid[e] Value Added *Services* (e.g. news service or weather forecasts) to MMS users.” EX-1004, 14, 41; EX-1003, ¶140; *supra* §VII.A. The path of application data between the VAS Applications and User Agent is annotated red below:



**EX-1004, 23, FIG. 3 (annotated)**

Above, application data is transmitted by VAS applications to the Relay/Server via interface MM7, then relayed “without alteration” (EX-1004, 14) to the User Agent via interface MM1, and then routed internally to a specific destination application. EX-1004, 14, 18, 23-25, 41, 54-56, FIG. 8 (below, illustrating exemplary message transmission); EX-1003, ¶¶141-142.



**Figure 8. Sample data flow of MM7 message distribution  
EX-1004, 111, FIG. 8 (annotated)**

See also EX-1004, 111-116 (describing VASP-added “Content” and “Applic-ID... indicat[ing] that... abstract message shall be provided to an application residing on an MMS User Agent” in MM7\_submit.REQ), 69-73 (describing “Content” from

originator and “Applic-ID” in MM1\_retrieve.RES); EX-1003, ¶¶142-143. The Board in IPR2024-00341 agreed, finding that “application-specific data from VAS applications” is “provided” to user agents “by VAS providers communicating through the MMS Relay/Server.” EX-1022, 38 (citing EX-1004, 23-24, 25-26, 41, 112, FIG. 3); EX-1023.

Because MMS-Ogawa’s “MMS VAS Applications” serve messages to the Relay/Server that contain application-specific data that is then transported to specific applications on MMS-Ogawa’s user device by the User Agent (EX-1004, 14, 18, 23-25, 41, 54-56, 69-73, 111-116), MMS-Ogawa’s VAS Applications are *network application servers*. EX-1003, ¶144.

MMS-Ogawa’s VAS Application sends targeted messages to a specific destination application on the user device to provide a specific “Value Added *Service[]*” e.g., “weather forecasts.” EX-1004, 14, 18, 23, 41; EX-1003, ¶145. Per TS-23.140, “applications that intend to transport application specific data using MMS” “initially need to register with the appropriate MMS User Agent or MMS VAS Application” and “negotiate... the details... of information to be exchanged between the two entities.” EX-1004, 54. This, e.g., “may... be the initial step after the download of a downloadable application to a mobile phone.” *Id.* TS-23.140 thus teaches a scenario in which a specific destination application (e.g., a downloaded weather application) receives targeted data from a specific network-

side (e.g., weather VASP) application registered with an MMS VAS Application. *Id.*; EX-1003, ¶145. Based on this, POSAs understood that the “abstract messages” subset of MMS-Ogawa’s secure Internet data messages discussed *supra* §VII.D.1.d.i contain “application data *from a respective network application server corresponding to that application,*” as claimed, because the specific network-side application registered with the MMS VAS Application *corresponds to* the destination application on the device. EX-1003, ¶145.

e. [1C1] “a secure interprocess communication service,”

The ’403 specification never describes an “interprocess communication service.” PO stated during prosecution that “agent communication bus 1630” is an example of the “secure interprocess communication service,” which may be “embodied as ‘an inter-process software communication bus,’ which can be ‘*a variant of D-bus* (e.g., a message bus system for inter-process software communication that, for example, helps applications/agents to talk to one another),’ or ‘another inter-process communication protocol or system, running a session bus in which all communications over the session bus can be *secured*, signed, encrypted or otherwise protected.’” EX-1002, 734; *see also* EX-1001, 41:42-43:4.

As discussed *supra* §VII.C.5, TS-23.140 discloses its MMS User Agent receiving “data specific to an application other than the MMS User Agent” and

“rout[ing]” it “to [a] destination application” on the user device over *some* interface. EX-1004, 14, 54-56. In IPR2024-00341, PO was unable to “dispute that a destination application is in communication with an MMS User Agent,” and the Board found—after extensive briefing and analysis (EX-1022, 18-32; EX-1023)—that POSAs “would have... understood that [TS-23.140’s] destination applications would have been communicatively coupled to the MMS User Agent by ‘an agent communication bus,’ as that term is used in the ’733 patent, because they are, in the words of the ’733 patent, ‘talk[ing] to one another.’” EX-1022, 28-29; *see also id.*, 18-32; EX-1001, 42:51-58. Thus, based on the specification and PO’s prosecution statements—stating that the claimed “interprocess communication service” may be “embodied as ‘an inter-process software communication bus,’” (EX-1002, 734)—POSAs understood MMS-Ogawa includes an *interprocess communication service*. EX-1001, 41:42-43:4; EX-1002, 734; EX-1003, ¶¶146-147.

Separately, as discussed *supra* §VII.C.5, it also would have been obvious to implement the user device’s interface between MMS-Ogawa’s User Agent application and other destination applications using a software *bus* for interprocess communications—e.g. a “D-bus.” EX-1003, ¶148; EX-1031, 10:56-62. The Board in IPR2024-00341 agreed. EX-1022, 48-49; EX-1023. For this alternative reason, MMS-Ogawa includes an *interprocess communication service*. EX-1002, 734.

MMS-Ogawa’s *interprocess communication service* is also *secure*. When describing “agent communication bus 1630”—which PO cited when identifying support for the “inter-process software communication bus” term (EX-1002, 733-734)—the specification cites “point[-]to[-]point” or “bus-level” “message exchange encryption using one or more keys that are partially shared or shared” on the device-side. EX-1001, 41:59-42:18, FIG. 16. POSAs thus understood an “*interprocess communication service*” secured by shared or partially shared encryption keys was “*secure*,” as claimed. EX-1003, ¶149.

As discussed *supra* §VII.C.6, MMS-Ogawa’s interprocess communications are secured using Ogawa’s inherent key when data is routed by the User Agent over TS-23.140’s software *bus* for interprocess communications (*supra* §VII.C.5) to a destination application. EX-1003, ¶150; EX-1005, 5:59-6:26, 5:24-27, FIG. 7. MMS-Ogawa thus includes “a *secure* interprocess communication service,” as claimed. EX-1003, ¶151.

**f. [1C2]**

MMS-Ogawa meets each limitation in Element [1C2], discussed below. In IPR2024-00341, the Board found that MMS-Ogawa met substantially the same limitation in the ’733 Patent. EX-1022, 39-40, §II.D.3(m); EX-1023; EX-1003, ¶¶152-153.

**i. “wherein the device messaging agent, for each message in the subset of the secure Internet**

**data messages, maps the identifier to the corresponding one of the software applications”**

The specification uses “mapping” to describe an “association.” EX-1001, 79:1. Thus, “map” in [1C2] encompasses the device messaging agent *associating* the correct software application with the received “identifier” (recited in [1B2]) when forwarding application data to the destination application. EX-1003, ¶154.

MMS-Ogawa’s User Agent does this: it “transport[s] *data* specific to *applications*” contained in application-specific messages (including the “abstract messages” subset discussed *supra* §VII.D.1.d.i) by “rout[ing]... received MMS information... to the” correct “destination application” based on a “destination application identifier” in the received message. EX-1004, 14, 55-56; EX-1003, ¶154.

TS-23.140 describes the correct “destination application” as being “*referred to from* the destination application identifier.” EX-1004, 56. POSAs understood that the determination of which application is “referred to” by the identifier constituted *associating* the correct destination application with the received identifier. EX-1003, ¶155. POSAs thus understood that MMS-Ogawa’s User Agent (“*device messaging agent*,” *supra* §VII.D.1.c.i), “*for each message in the subset of the secure Internet data messages*” (including each abstract message discussed *supra* §VII.D.1.d.i), “*maps*” the destination application identifier of the destination application (“*the identifier to the corresponding one of the software*

*applications*”) to the application “referred to from” the identifier (“*to the corresponding one of the software applications*” *supra* §VII.D.1.d.ii), as claimed. EX-1003, ¶155; EX-1004, 55-56.

**ii. “in order to forward the application data on the secure interprocess communication service”**

In MMS-Ogawa, MMS is used to “transport data specific to applications,” including “*application data*” from third-party VAS Applications (sent in the abstract messages discussed *supra* §VII.D.1.d.ii) to provide a specific “Value Added *Service*” e.g., “weather forecasts.” EX-1004, 14, 18, 23-25, 41, 54-56, 69, 111-116; EX-1003, ¶156. As discussed in §VII.D.1.e, application data in such application-specific messages are encrypted using Ogawa’s inherent key (*supra* §VII.C.6) and “transported without alteration” of the underlying data (EX-1004, 14)—i.e., forwarded (EX-1003, ¶157)—by MMS-Ogawa’s User Agent to the correct destination application over a “secure interprocess communication service” (i.e., over a bus). POSAs thus understood MMS-Ogawa’s “*map[ping]*” (*supra* §VII.D.1.f.i) is done “*in order to forward*” the “*application data on the secure interprocess communication service*,” as claimed.

**iii. “to a software process corresponding to the identified software application.”**

The ’403 specification does not use the term “software process” or discuss a “software process corresponding to the identified software application.” EX-1004,

¶158. TS-23.140’s forwarding of application data to destination applications constitutes forwarding data “to a software process corresponding to the identified software application,” because POSAs understood that TS-23.140’s destination applications consisted of one or more processes in which specific functions of the application (e.g., receiving data) are executed. EX-1003, ¶158; EX-1046, 46 (defining application: “a software program consisting of one or more processes and supporting functions”); EX-1047, 5:41-61 (“A software application can include multiple processes....”); EX-1048, [0003]-[0004] (describing “[d]ifferent processes within an application”). For example, given a “chess” application, an abstract message’s application data may be forwarded to a specific process for moving opponent chess pieces, or a specific “instance[]” of the application (e.g., “chess application #02”). EX-1004, 55-56; EX-1003, ¶158. POSAs thus understood that “*a software process corresponding to the destination application identified by the destination application identifier*” receives the application data forwarded by MMS-Ogawa’s User Agent, as claimed. EX-1003, ¶¶158-159.

## 2. Claim 3

MMS-Ogawa’s device includes “a plurality of software applications capable of execution on the device” (TS-23.140’s destination applications) to which application-specific data is “transport[ed]”—e.g. “news service” (EX-1004, 14), “weather” (*id.*), “chess” (*id.*, 54), or “messaging” (*id.*) applications. *Supra*

§VII.D.1.c.ii. MMS-Ogawa’s user device thus “*comprises the plurality of software applications*,” as claim 3 requires. EX-1003, ¶160.

### 3. Claim 4

Claim 4 requires claim 3’s “the plurality of applications” to “include” a “first” and “second” application that respectively “receive[] application data” in different “format[s.]” During prosecution, PO said “the use of ‘first’ and ‘second’ applications merely indicates two... elements that receive different types of formatted data in the messages from their respective network application servers.” EX-1002, 734. TS-23.140 discloses “supported [data] formats,” e.g., “Plain Text,” “Audio,” “Still Image,” “Video.” EX-1004, 20; EX-1003, ¶161 (citing EX-1020). POSAs understood MMS-Ogawa’s different applications (e.g., “chess,” “weather”) receive application data in different formats specific to the respective applications, meeting claim 4. EX-1003, ¶161; EX-1004, 14, 55.

### 4. Claim 5

As explained *supra* §VII.D.1.c.iii, MMS-Ogawa’s User Agent (“device messaging agent,” *supra* §VII.D.1.c.i) receives Internet data messages (including the “abstract messages” subset discussed *supra* §VII.D.1.d.i) from the Relay/Server over secure interface MM1. POSAs understood that such messages are “*received encrypted*,” as claim 5 requires, using MMS-Ogawa Message Encryption and SSL/TLS. EX-1003, ¶¶162-163; *supra* §§VII.C.2-VII.C.4.

MMS-Ogawa's received messages are decrypted by the MMS User Agent, which provides "decryption" functionalities (EX-1004, 19) using Ogawa's decryption unit. *Supra* §§VII.C.3-VII.C.4; EX-1004, 19; EX-1003, ¶164. As discussed *supra* §VII.D.1.d.i-VII.D.1.d.ii, each received message in the abstract messages subset contains an "identifier" and "application data." POSAs understood that MMS-Ogawa's User Agent "*decrypt[s] each*" encrypted "*message in the subset*" it receives "*to obtain corresponding identifier and application data,*" as claimed—which facilitates accurate routing for application data transport. EX-1003, ¶165.

## 5. Claim 6

Claim 6 recites alternative transportation options for claim 1's "messages," including "encryption on a transport services stack." *See* EX-1002, 734. As discussed *supra* §VII.D.1.c.iii, in the specification, external communication with what PO identified as a "device message agent" (EX-1002, 731) occurs over "service control link 1653." EX-1001, 68:18-27. The specification describes a "layer[] of encryption in the service control link" that is "implemented in the transport services stack" using "standard secure or open Internet networking protocols, such as TLS or TCP." EX-1001, 87:40-62. As discussed *supra* §VII.C.2, MMS-Ogawa's MM1 utilizes TLS. POSAs understood that, just as in the '403 specification, MMS-Ogawa's use of TLS to secure MM1 between the User Agent

and Relay/Server is implemented in a transport services stack (*see* EX-1012, 21), and is “*encryption on a transport services stack*,” as claimed. EX-1003, ¶166.

## 6. Claim 11

Claim 11 requires “the device messaging agent” to “send secure *upload* Internet data messages *to the network message server over the secure connection*” in “respons[e] to a corresponding request received on the secure interprocess communication channel from a corresponding one of the software applications[.]” While “secure interprocess communication *channel*”<sup>10</sup> has no antecedent basis, POSAs understood that it at least encompasses claim 1’s “secure interprocess communication *service*.” During prosecution, PO said “[c]laim 11 is intended to cover the reverse or upload channel that allows various device applications to send data to a respective corresponding application server.” EX-1002, 735.

As discussed *supra* §§IV.A, VII.D.1.c.i-VII.D.1.c.ii, MMS is used to transport application-specific data between VAS Applications and applications on a user device (other than the MMS User Agent application). EX-1004, 14, 54-55. As discussed *supra* §VII.D.1.c.iii, MMS-Ogawa’s User Agent (“device messaging agent”) exchanges “secure Internet data messages” containing such application-

---

<sup>10</sup> Claims 14-15 and 17 recite same.

specific data with MMS-Ogawa’s Relay/Server (“network message server”) over MM1 (“secure connection”).

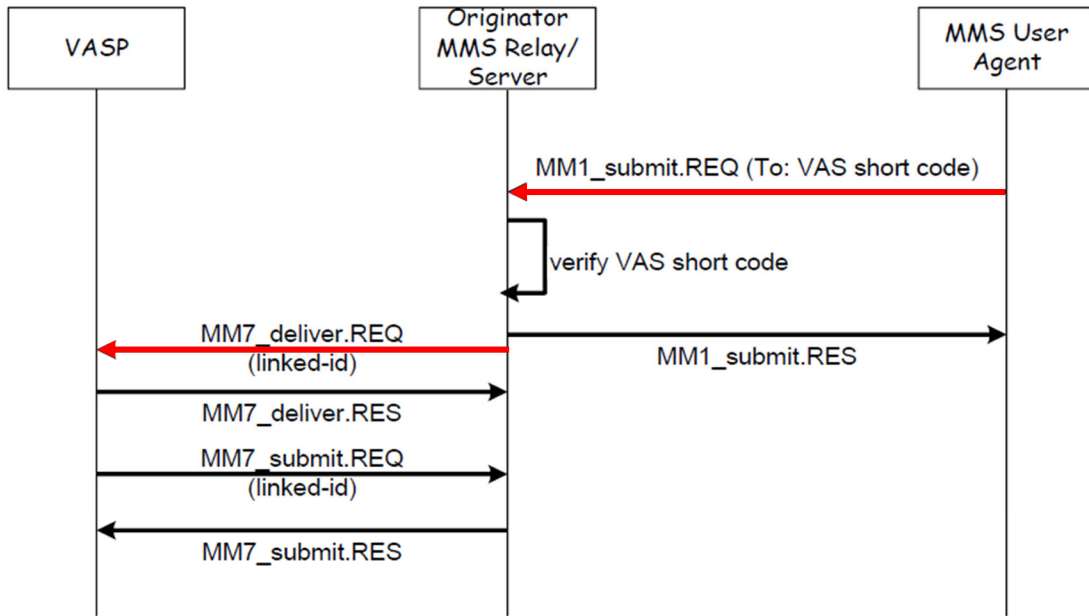
These messages go *both ways*: MMS is also used to *upload* messages from the UE/device to a VASP (via the MMS Relay/Server). TS-23.140 discloses MMS being “used to transport data specific to applications between... an MMS User Agent and an MMS VAS Application (*or vice versa*)” (EX-1004, 55)—e.g., an “abstract message[]... sent *by an MMS User Agent... on behalf of an originating application*” on the user device (*id.*) that is “passed by the MMS Relay/Server *to a VASP*” (EX-1004, 116-117, FIG. 9); EX-1003, ¶¶166-169.

“[A]n application... trigger[s] an MMS User Agent... to submit” “abstract messages.” EX-1004, 55. “Upon” this “triggering”—i.e., *in response to* the application’s *request*—the MMS User Agent “insert[s]” information “receive[d]... from the application” into an “abstract message” and sends it. *Id.*; EX-1003, ¶170.

TS-23.140 illustrates how such information is transmitted to the VASP (via the Relay/Server) using its MM1\_submit.REQ and MM7\_deliver.REQ “abstract message” examples. EX-1004, 62, 116, 58, 189-190; EX-1003, ¶¶170-174.

Specifically, TS-23.140 discloses that the Relay/Server sends MM1\_submit.REQ message information received from the User Agent in an MM7\_deliver.REQ message to the VAS Application. EX-1003, ¶¶171-174; EX-1004, 58, 62, 116-117 (“The MMS Relay/Server will deliver messages” that “originate[]... from a MMS

User Agent” “to the VASP by supplying the MM as the payload of the MM7\_deliver.REQ[.]”), 189-190, FIG. 9 (annotated below):



**Figure 9: Use of MM7\_deliver and subsequent response  
EX-1004, 117, FIG. 9 (annotated)**

As discussed *supra* §VII.D.1.e, communication between MMS-Ogawa’s User Agent application and other applications on the user device occur over MMS-Ogawa’s bus (“secure interprocess communication service”).

MMS-Ogawa’s User Agent (“device messaging agent,” *supra* §VII.D.1.c.i) thus “send[s] secure upload Internet data messages to the” MMS Relay/Server (“network message server,” *supra* §VII.D.1.c.iii) “over” MM1 (“the secure connection,” *supra* §VII.D.1.c.iii) in “respons[e] to” receiving a “corresponding

request received on the secure interprocess communication channel” from one of the downloaded applications on the UE/device (“a corresponding one of the software applications,” *supra* §VII.D.1.d.i). EX-1003, ¶175. MMS-Ogawa’s abstract messages (e.g., MM1\_submit.REQ) are “*secure upload Internet data messages*” because the UE/device *uploads* them to the Relay/Server to deliver information to the VAS Application (“*application server*,” *supra* §VII.D.1.d.ii). EX-1003, ¶175.

Claim 11 further requires that “the device messaging agent” “construct[] from [the] request” “a secure upload Internet data message containing an identifier for a respective network application server corresponding to the requesting software application; and content received with the request.”

MMS-Ogawa’s User Agent does this. “Upon triggering an MMS User Agent... to send an abstract message[,], the MMS User Agent... receive[s] information from the application” that the User Agent “insert[s]... in both the information elements and/or payload... of the abstract message[.]” EX-1004, 55. The message “shall contain a destination application identifier” for use by the VAS Application to “immediately route the received MMS information on to the destination application that is referred to by the destination application identifier.” EX-1004, 55-56; EX-1003, ¶¶176-178 (citing EX-1004, 63, 65, 117-118, explaining that MM1\_submit.REQ and MM7\_deliver.REQ include the destination

application identifier). POSAs therefore understood that MMS-Ogawa’s User Agent “*constructs from [the] request*” a message containing the “identifier *for*” the “*respective network application server corresponding to the requesting software application*”—because the identifier is *for* use by the VAS Application to route the message to the correct destination application. EX-1003, ¶179; EX-1004, 55-56.

TS-23.140 also discloses the MMS User Agent sending *content* from the originating application for delivery by the MMS Relay/Server to the VASP. EX-1003, ¶180 (citing EX-1004, 63, 118, explaining that MM1\_submit.REQ and MM7\_deliver.REQ messages include content for delivery to the VASP). POSAs therefore understood that the message MMS-Ogawa’s User Agent “*constructs from [the] request*” also contains the “*content*,” as claimed. EX-1003, ¶180.

## 7. Claim 12

Claim 12 recites “at least one of” claim 11’s “upload Internet data messages comprises a key for the network application server corresponding to the requesting software application.” No specific “key” type is required, and the specification says “various known security encryption techniques can be implemented... with *public/private or completely private keys*...” EX-1001, 87:55-58. During prosecution, PO did not narrow the key type claim 12 covers. EX-1002, 735.

MMS-Ogawa’s messages are encrypted using MMS-Ogawa Message Encryption before being transmitted to the User Agent or VAS Applications. *Supra* §§VII.C.3-VII.C.4. POSAs understood that when MMS-Ogawa is used as claim 11 describes—where application-specific data is sent “*by an MMS User Agent... on behalf of an originating application*” on the user device “*to a VASP*”—the recipient VAS Application (which includes the destination application) needs to have the shared encryption key used to encrypt the message to enable decryption. *E.g.*, EX-1005, 5:62-65; EX-1003, ¶¶181-182.

Ogawa teaches a method for sharing encryption keys between entities. EX-1005, 6:64-7:24, FIG. 2; EX-1003, ¶183. Specifically, Ogawa teaches a “key exchange algorithm” where *both* the encrypting entity (in MMS-Ogawa, the MMS User Agent application which sends the upload Internet data message) and the decrypting entity (in MMS-Ogawa, the MMS VAS application that receives the upload Internet data message) generate keys—which are then “exchange[d] in accordance with Diffie-Hellman protocol,” and used to generate the shared encryption key. EX-1005, 6:64-7:24 (steps S9-S10), FIG. 2 (same). POSAs understood this exchange of keys between the MMS User Agent (“*device messaging agent*”) and MMS VAS Application (“*network application server*”)—so that both can generate the shared key needed for MMS-Ogawa Message Encryption—meets claim 12’s requirement that “*at least one of*” claim 11’s

*“upload Internet data messages comprises a key for the network application server corresponding to the requesting software application.”* EX-1003, ¶183.

POSAs understood that such an *“upload Internet data message”* would still be *“secure,”* as claim 11 requires—even though the communications are not yet secured using MMS-Ogawa Message Encryption—because MM1 and MM7 are secured using TLS/SSL. *Supra* §VII.C.2; EX-1004, 41; EX-1003, ¶184.

### **8. Claim 13**

During prosecution, PO indicated claim 13’s “log for... received Secure Internet data messages” encompasses a “communication trace log for... service controller 122 to agent communications.” EX-1002, 735. The specification says “service controller 122 to agent communications” are “logged so that a trace log of some... agent communications can be maintained[,]” and that “the agents can maintain their own communications or attempted communications log, which can then be reported to the service controller 122.” EX-1001, 44:42-47, 45:12-15; EX-1002, 735. PO’s prosecution statements indicate the claimed “log” encompasses a record of at least some communications received by the “device messaging agent” that is sent to a “network application server.” EX-1003, ¶¶185-186 (citing EX-1057).

TS-23.140 discloses a VASP requesting a “read-reply report” for a MM received by the User Agent. EX-1004, 34-35, 59. The read-reply report “shall

[contain/provide]” the sender’s and recipient’s addresses, message ID, read status, and time stamp. EX-1003, ¶187 (citing EX-1004, 34-35). The MMS User Agent stores each read-reply report until it can reach the MMS Relay/Server, at which time it sends the Relay/Server all stored read-reply reports, which are then sent to the VASP; POSAs understood MMS-Ogawa’s User Agent (“device messaging agent”) thus creates a “*log*” that meets claim 13. EX-1003, ¶187 (citing EX-1004, 35).

#### **9. Claim 14**

MMS-Ogawa’s User Agent receives messages from the Relay/Server that are secured using SSL/TLS and MMS-Ogawa Message Encryption, which are decrypted by MMS-Ogawa’s User Agent. *Supra* §§VII.C.2-VII.C.4, VII.D.1.c.iii. Such messages are re-encrypted by the User Agent using an inherent key before being communicated over MMS-Ogawa’s “secure interprocess communication service.” *Supra* §§VII.D.1.e, VII.C.5-VII.C.6. Thus, MMS-Ogawa’s external secure connection between the User Agent and Relay/Server is “*separately secured*” from MMS-Ogawa’s internal secure interprocess communication channel, meeting claim 14. EX-1003, ¶¶188-189.

#### **10. Claim 15**

The specification never uses “security policy” to describe access to an “interprocess communication channel.” EX-1003, ¶190; EX-1001, 36:52. The

specification says its agent communication bus can be “secured” using “point[-]to[-]point” or “bus-level” “message exchange encryption using one or more keys that are partially shared or shared” (EX-1001, 41:62-42:4) and says that, by encrypting the bus, it “can only be accessed... as... permitted by *agent communication policies*” (EX-1001, 88:9-22). *Supra* §VII.D.1.e. Using shared key encryption to restrict access is thus an example of “*subjecting access... to a security policy*,” as claimed. EX-1003, ¶190. MMS-Ogawa’s interprocess communication service is encrypted using Ogawa’s inherent key. *Supra* §§VII.C.6, VII.D.1.e. “Access” by MMS-Ogawa’s applications (“software applications”) to MMS-Ogawa’s bus (“interprocess communication channel”) is thus “*subject to a security policy*” requiring a specific encryption key, meeting claim 15. EX-1003, ¶191.

## 11. Claim 16

Claim 16 recites “at least one of the secure Internet data messages comprises multiple identifier/data pairs.” During prosecution, PO identified Figure 25 as disclosing this limitation. EX-1002, 736. FIG. 25 (annotated below) shows a “service controller communication *frame*” comprising multiple identifier/*message* pairs (respectively blue, green). EX-1001, 90:11-18.

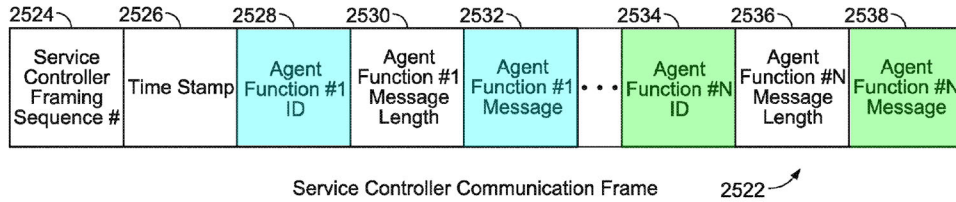


FIG. 25

**EX-1001, FIG. 25 (annotated)**

The specification says “service control server link 1638 can perform collection or buffering of server messages between transmissions[, and] once a transmission trigger has occurred, ...take all buffered agent communications and frame the communications.” EX-1001, 68:62-69:8. PO’s prosecution statements indicate claim 16’s “message[] compris[ing] multiple identifier/data pairs” encompasses a network message server that collects/buffers messages (each comprising an identifier and payload), and sends the collected messages to a “device messaging agent” as a group/frame of messages. EX-1003, ¶192.

TS-23.140 describes the MMS Relay/Server “stor[ing]” a received “MM... until: the associated time of expiry is reached, the MM is delivered, [or] the recipient MMS User Agent requests the MM to be routed forward or the MM is rejected.” EX-1004, 26-28. Messages may be “persistent[ly] stored” in a “MMBox.” EX-1004, 21-22; EX-1003, ¶193. When an unavailable recipient User Agent becomes available, e.g., by moving into coverage, the Relay/Server delivers the group of collected messages to the User Agent. EX-1004, §7.1.3. As explained *supra* §§VII.D.1.d.i-VII.D.1.d.ii, each message in a group of abstract messages

comprises a destination application identifier and application data. That group delivered to the User Agent is a “*secure Internet data message[] compris[ing] multiple identifier/data pairs,*” as claimed. EX-1003, ¶194.

If claim 16 is read to require aggregating multiple messages in a frame, this would have been obvious. POSAs had reason to implement MMS-Ogawa such that its Relay/Server transmits multiple collected MMs to a User Agent in a frame. TS-23.140 is part of a suite of well-known 3GPP specifications that define layered architecture and data transport mechanisms for MMS communications. EX-1003, ¶195. TS-23.140 contemplates each MM conveyed in an HTTP message over TCP/IP, delivered through the 3G packet-switched bearer service. EX-1021, 11, 13, 48 (incorporated into EX-1004 at 12, 174-175). Moreover, POSAs understood that higher-layer data units—e.g., multiple HTTP messages, each carrying an MM—would be aggregated within a single lower-layer frame for transmission to a User Agent; this was desirable because encapsulating multiple identifier/data pairs, or multiple MMs, within a single frame would improve radio-interface efficiency and reduce protocol overhead. EX-1003, ¶196 (citing EX-1051, 12, 15, 28-29, 46-47; EX-1052, 11, 16, 22-23; EX-1053, 8-9, 23). Moreover, POSAs would have reasonably expected success implementing MMS-Ogawa’s Relay/Server to transmit multiple messages using such a frame, given relevant 3GPP specifications expressly supporting encapsulation of multiple higher-layer data units into a single

transport block for the efficiency reasons described above. EX-1003, ¶¶197-198. Thus, implementing MMS-Ogawa's User Agent to receive a message (frame) containing "multiple ID/data pairs" was obvious.

## 12. Claim 17

Claim 17 requires that the claimed "device messaging agent compris[e] an agent router" that "forward[s] the application data" "to the [claimed] software process" over "the secure interprocess communication channel." The '403 specification does not describe an "agent router." During prosecution, PO asserted the term is met by FIG. 24's "agent route' function 2416." EX-1002, 736. The specification does not describe any structural requirements for "agent route 2416," which is shown as part of service control device link 1691. EX-1001, FIG. 24, 89:15-21; *see also*, 42:10-11 (link 1691 is "equivalent to an agent"). Thus "agent router" encompasses a portion of the device messaging agent (either software or hardware) that routes received messages to a destination. EX-1003, ¶199.

MMS-Ogawa's "MMS User Agent... immediately route[s] the received MMS information on to the destination application... referred to by the destination application identifier[.]" EX-1004, 54-56; *supra* §§VII.D.1.c-VII.D.1.d. MMS-Ogawa's User Agent forwards the message's application-specific data content ("*application data*") on the secure interprocess communication service to a software process corresponding to the destination application. *Supra* §§VII.D.1.e-

VII.D.1.f. MMS-Ogawa's User Agent (“*device messaging agent*”) thus comprises an “*agent router*” meeting claim 17. EX-1003, ¶¶200-201.

### **13. Claim 18**

When MMS-Ogawa's User Agent receives a message comprising application-specific data over MM1, the message is decrypted by the User Agent's decryption unit, re-encrypted by the User Agent's encryption unit, and routed “to the destination application that is referred to by the destination application identifier” (EX-1004, 56) over MMS-Ogawa's “secure interprocess communication service” (MMS-Ogawa's bus). *Supra* §§VII.C.3-VII.C.6, VII.D.1.c.iii, VII.D.1.e, VII.D.9. Thus, the message is forwarded by the bus to a process of the destination application (“*at least one of the software processes*”) in an encrypted format, meeting claim 18. EX-1003, ¶202.

### **14. Claim 19**

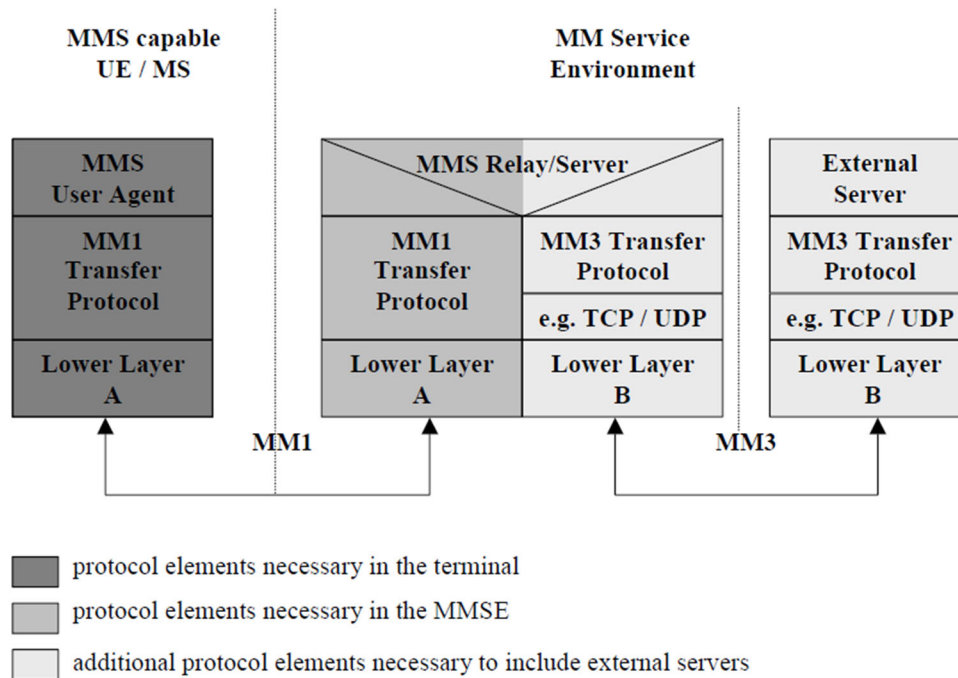
As discussed for Claim 11, TS-23.140 teaches the MMS User Agent sending an MM1\_submit.REQ message to the Relay/Server when another application on the user device wants to send a message to a VAS Application. POSAs understood that if the SSL/TLS-secured connection between MMS-Ogawa's User Agent and Relay/Server (MM1) is not already established—e.g., because the connection timed out, or the UE/device restarted—MMS-Ogawa's User Agent (“*device messaging agent*”) would “initiate the secure connection to” the Relay/Server

(“network message server”) as claim 19 requires—e.g., by sending a TLS “Client Hello” message to establish the connection. EX-1003, ¶203 (citing EX-1014, §7.4.1.2; EX-1026, [0275]-[0293], FIGs. 17-18).

### **15. Claim 20**

Claim 20 requires that claim 1’s “device” “compris[e] a network stack in communication with the device messaging agent and the WWAN modem[,]” and that the claimed “secure connection” be “terminated within the network stack.” The specification uses “networking stack” and “device communications stack” to include a layered set of software components that implement communication protocols. EX-1001, 92:62-94:9; EX-1003, ¶204. PO stated, based on the specification’s alleged disclosure of a “network stack” that uses “basic IP” and “TCP layer security,” that POSAs understood the claimed secure connection “can include security terminated in the network stack.” EX-1002, 736; EX-1003, ¶203.

MMS-Ogawa’s MM1 is secured using SSL/TLS. *Supra* §§VII.C.2, VII.D.1.c.iii; EX-1004, 24-25, FIG. 4 (below); EX-1003, ¶205.



**Figure 4: Protocol Framework to provide MMS  
EX-1004, 24, FIG. 4**

TS-23.140 discloses MM1 implementing OMA MMS. *Supra* §VII.C.2. TS.23-140’s incorporated references disclose a “device implementing OMA MMS” with a “*HTTP/TCP/IP stack*”; MM1 thus comprises a claimed “*network stack.*” EX-1011, 11; *see also* EX-1012, 21 (“HTTP based protocol *stacks...*”); EX-1003, ¶206.

Because MM1 utilizes the TCP/IP stack to provide the “lower layer” connection between MMS-Ogawa’s User Agent and Relay-Server and is secured via the TLS/SSL security layer of the TCP/IP stack, POSAs understood MM1 (“secure connection,” *supra* §VII.D.1.c.iii) terminates within the TCP/IP stack in

the way PO says the claim includes—by using “basic IP” and “TCP layer security.” EX-1002, 736; EX-1004, 24; EX-1012, 21; EX-1003, ¶207.

MMS-Ogawa’s device comprises a WWAN modem for communications via MMS-Ogawa’s User Agent, over TS-23.140’s 3G mobile networks. *Supra* §§VII.D.1.b, VII.C.1. POSAs understood MMS-Ogawa’s User Agent (“device messaging agent”) communicated with MMS-Ogawa’s Relay/Server via the WWAN modem over the MM1 interface, using the TCP/IP stack. EX-1003, ¶208; EX-1004, 17, 24-25, FIG. 4. POSAs also understood MMS-Ogawa’s User Agent sits at the application layer, while MMS-Ogawa’s WWAN modem sits below the TCP/IP stack. EX-1003, ¶208 (citing EX-1004, 19, 24). POSAs thus understood the TCP/IP stack used by MM1 is “*in communication with*” the user device’s MMS User Agent and WWAN modem, as claimed. EX-1003, ¶208.

## 16. Claim 21

Applications on a User Agent device or VAS Application server must “register” before exchanging messages using MMS—e.g., by providing “application identification value[s]” and “negotiat[ing]... details... of information to be exchanged.” EX-1004, 54-55. Only then may the “application... trigger... submi[ssion]” of “abstract messages” to the Relay/Server. EX-1004, 55. POSAs understood MMS-Ogawa’s required registration process with identifiers constitutes an “application[] and... network application server” “authenticat[ing] with each

other prior to passing application data” to one another via the Relay/Server, as claimed. EX-1003, ¶¶209-210; *see also* EX-1004, 41.

### **VIII. GROUNDS 2A-2C**

The Board previously found it would have been obvious to implement TS-23.140 with a modem for network communications (*supra* §VII.C.1) and a software bus for interprocess communications (*supra* §VII.C.5). EX-1022, 40-41, 45, 48-49; EX-1023. Grounds 2A-2C expressly modify MMS-Ogawa in view of Cole (teaching a modem, Ground 2A), Sathish (teaching an interprocess communication bus, Ground 2B), and *both* (Ground 2C) if the Board disagrees with its prior adjudications. Grounds 2A and 2C also address claim 2. EX-1003, ¶¶211-213.

#### **A. GROUND 2A: MMS-Ogawa in View of Cole (EX-1006)**

##### **1. Implementing a WWAN Modem (Claims 1, 3-6, 11-21)**

It was well-documented to use a *modem* to enable communications over 2G/3G WWANs. *Supra* §VII.C.1. Cole, e.g., discloses implementing a mobile device’s “communication interfaces” with “*a WWAN modem*” for connecting to a “2G”/“3G” “wireless wide area network (WWAN)” —which “may interface directly or indirectly with... e.g., the Internet.” EX-1006, [0031]-[0035], [0003], FIGS. 1-2 (below).

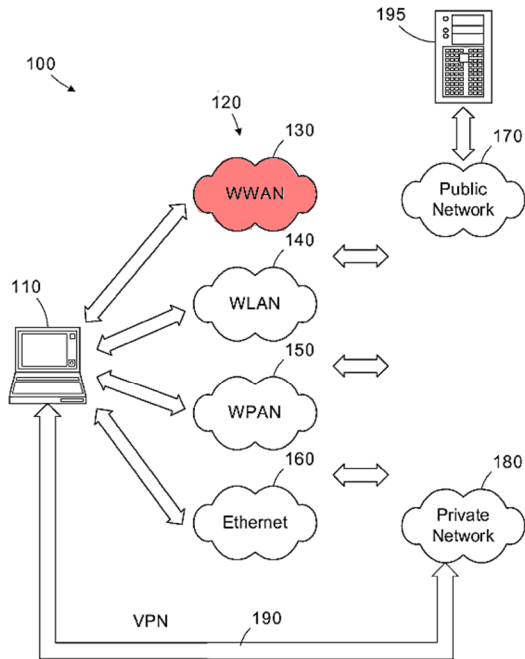


Figure 1

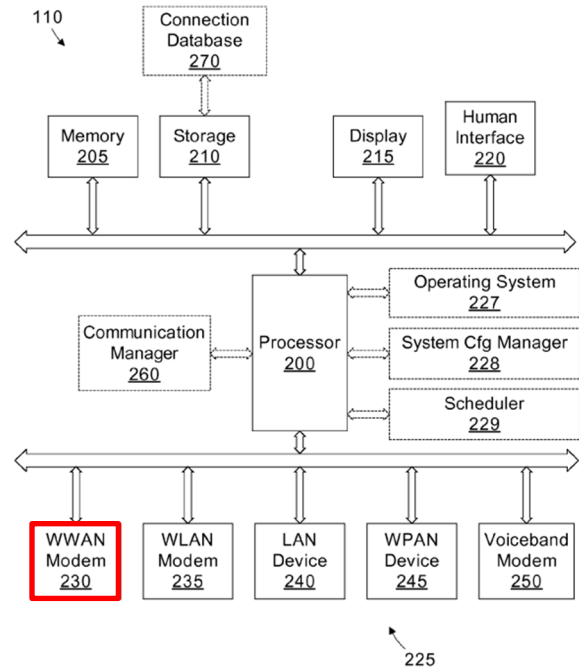


Figure 2

**EX-1006, FIGS. 1-2 (annotated)**

Cole confirms “protocols required to implement connections over [such] communication interfaces... to [such]... communication networks” were “*known to those [of] ordinary skill.*” EX-1006, [0035].

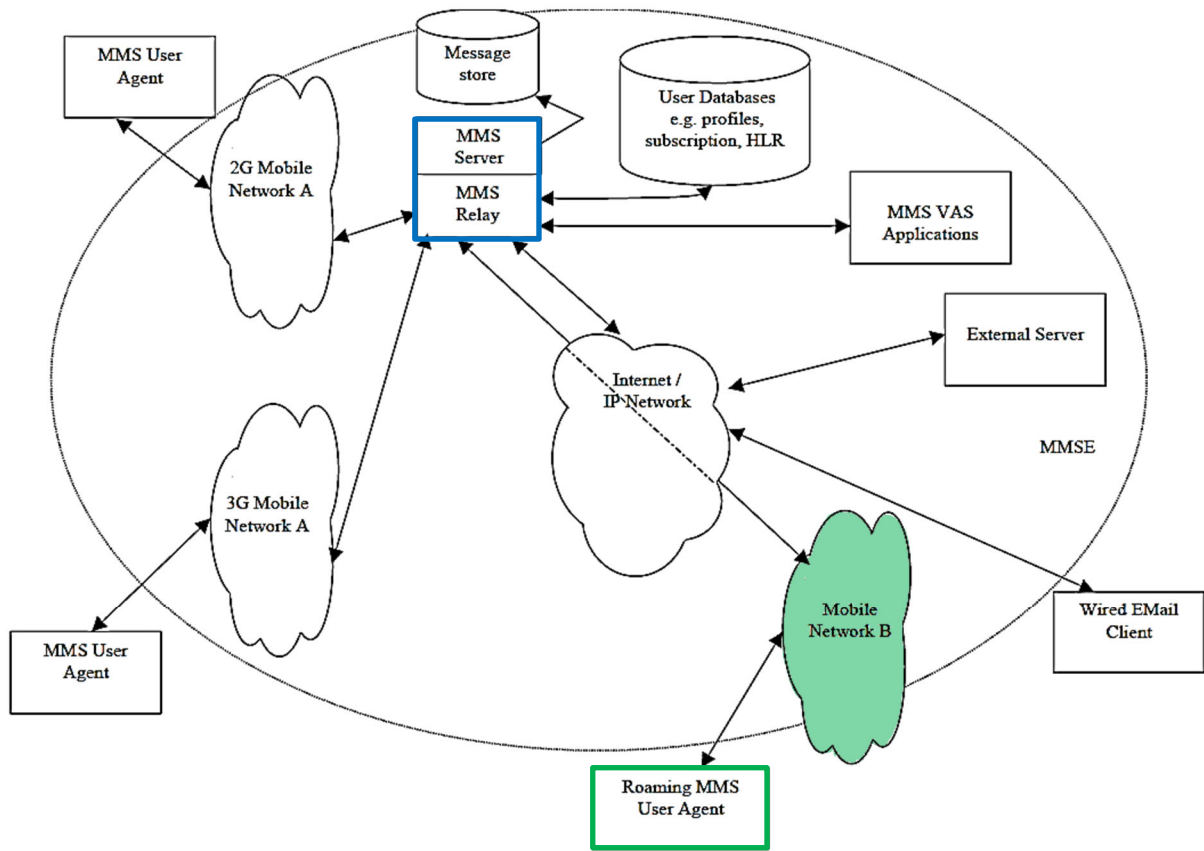
In view of Cole, POSAs would have been motivated to use a “WWAN modem” to enable TS-23.140’s UE/device to communicate over TS-23.140’s disclosed 2G/3G wireless networks, and would have reasonably expected success; such an implementation would have been nothing more than utilizing familiar components (Cole’s WWAN modem in TS-23.140’s UE/device) to achieve a predictable result of facilitating TS-23.140’s disclosed 2G/3G communications. *KSR*, 550 U.S. at 416; EX-1003, ¶¶214-216. This renders obvious claims 1, 3-6,

and 11-21 for the same reasons respectively discussed *supra* §VII for MMS-Ogawa.

## **2. Adding a WLAN Modem (Claim 2)**

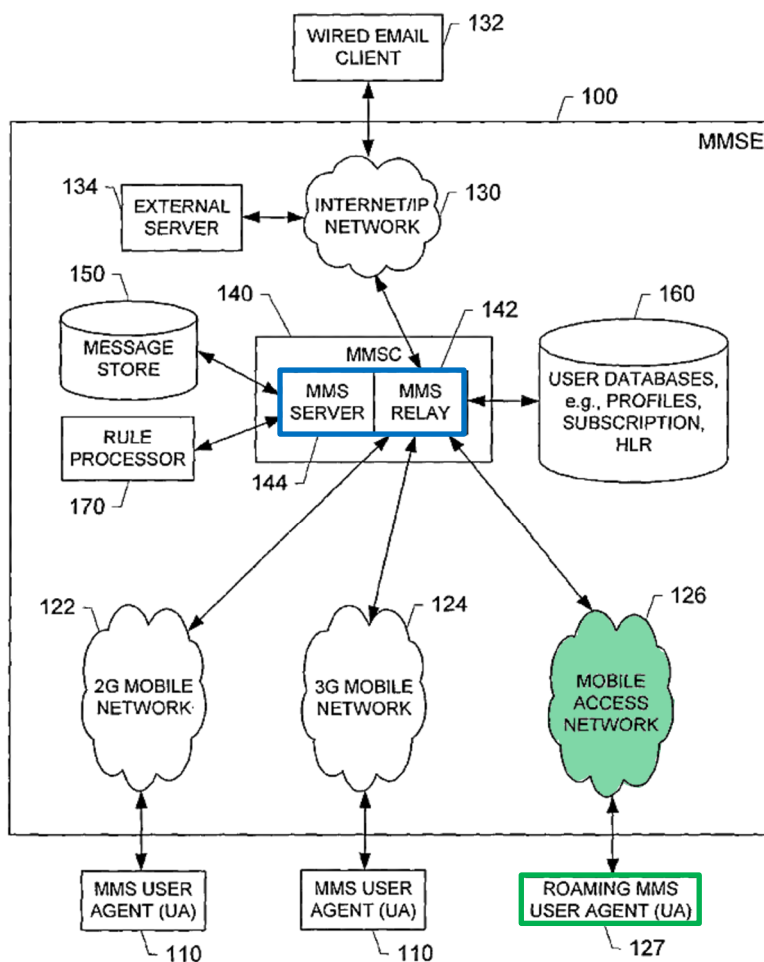
TS-23.140 says “[MMS] architecture... shall combine different networks and network types and shall integrate messaging systems already existent within these networks[,]” and that “connectivity between these different networks shall be provided by the Internet protocol and its... messaging protocols.” EX-1004, 16-17. TS-23.140 does not limit how communications are facilitated over such networks or what “network types” are “combine[d].” EX-1004, 16-17, 23-24.

TS-23.140’s FIG. 2 (below) shows “Roaming MMS User Agent” connecting to the Relay/Server through “Mobile Network B.”



**Figure 2: MMS Architectural Elements**  
**EX-1004, 17, FIG. 2 (annotated)**

Contemporaneous references confirm a “WLAN” was one way to implement this “mobile network” and that it was known to implement User Agents to be “capable of transmitting and receiving multimedia messages” to/from a server (e.g., TS-23.140’s Relay/Server) over “a mobile access network... such as a... WLAN...” while roaming. EX-1007, [0022], FIG. 1 (below); EX-1016, 8, 14, 26-28; EX-1003, ¶¶217-219.



**FIG. 1.**

**EX-1007, FIG. 1 (annotated)**

It was well-documented to implement such WLAN connectivity using a modem. EX-1006, [0003], [0031], [0035], FIG. 2; EX-1003, ¶220 (citing EX-1042, [0050], FIG. 2). In addition to the “WWAN modem” discussed *supra* §VIII.A.1, Cole teaches including a “*WLAN* modem” among a mobile device’s “communication interfaces.” EX-1006, [0031], [0034]-[0035], FIGS. 1-2 (below).

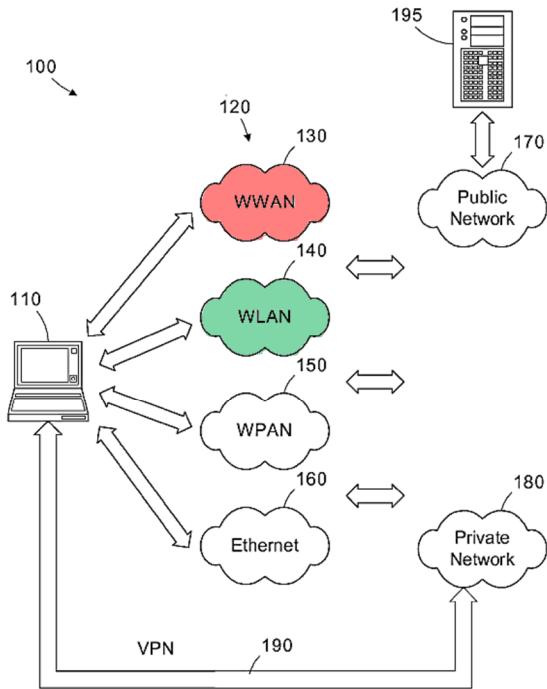


Figure 1

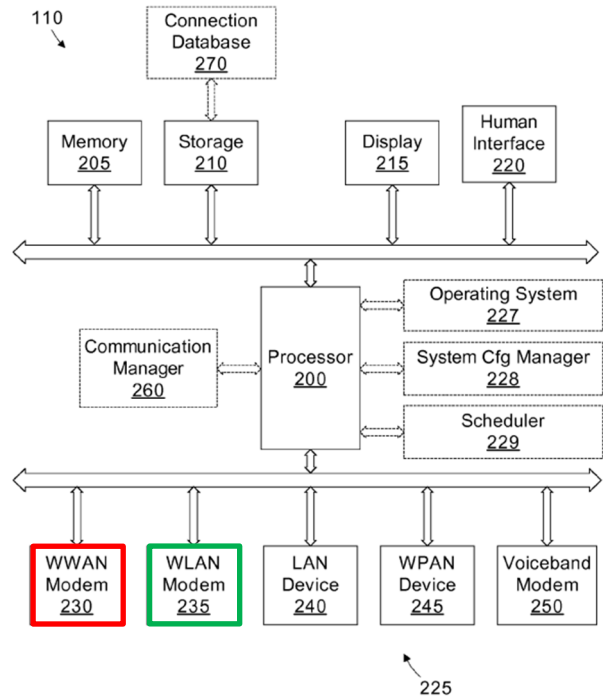


Figure 2

**EX-1006, FIGS. 1-2 (annotated)**

Cole teaches “evaluat[ing] availability, bandwidth, user preferences, application requirements, mobile device resources, etc. to select a particular communication interface 225” connection. EX-1006, [0035]-[0040], [0003]; EX-1003, ¶¶220-222.

POSAs had multiple reasons to implement Cole’s WLAN modem into MMS-Ogawa’s UE/device:

*First*, TS-23.140 contemplates Internet-protocol-based “multimedia messaging... encompass[ing] **many different network types**[,]” and “provid[ing] implementation flexibility... with interoperability across different networks...”).

EX-1004, 17, 24. POSAs thus would have appreciated the desirability of using

MMS over various “different networks types” including WLANs. EX-1003, ¶¶223-224.

**Second**, MMS-related references teach implementing WLAN-enabled devices to access MMS. *E.g.*, EX-1007, [0001], [0022], FIG. 1; EX-1043, [0001]; EX-1044, Abstract. TS-23.234, *e.g.*, teaches “extend[ing] 3GPP services and functionality to the WLAN access environment” and using “WLAN to access 3GPP PS based [e.g., MMS] services.” EX-1016, 8, 14, 26-28, FIG. 6.1; EX-1003, ¶225.

**Third**, Cole teaches that a “wide variety of connection options provides the user with flexibility and the ability to connect to a network in virtually any location.” EX-1006, [0003]-[0004]. Incorporating Cole’s WLAN modem into MMS-Ogawa’s user device would have desirably provided an additional access path to the Relay/Server, improving MMS accessibility where 2G/3G coverage was weak/unavailable/costly. EX-1003, ¶226.

**Fourth**, implementing Cole’s WLAN modem would have been nothing more than implementing known components/techniques (Cole’s WLAN modem) into known systems/devices (TS-23.140’s UE/device, implemented to use SSL/TLS and MMS-Ogawa Message Encryption for MM1 communications with the Relay/Server) to achieve predictable results (secure MMS communications over a non-2G/3G mobile access network). *KSR*, 550 U.S. at 416; EX-1003, ¶227.

POSAs would have reasonably expected success with such an implementation given Cole's confirmation that "protocols required to implement [WLAN] connections... *are known to*" POSAs (EX-1006, [0035]), the above-cited teachings regarding implementing MMS over WLAN networks, and the widespread use of WLAN for mobile device communications. EX-1003, ¶228. POSAs understood nothing in TS-23.140's or Ogawa's teachings require communication over a specific network type (e.g. WWANs). EX-1003, ¶228.

In such an implementation ("MMS-Ogawa-Cole"), the User Agent receives secure messages over a secure connection with the Relay/Server in the same manner described *supra* §VII.D.1 for WWAN connections, because the WLAN is part of interface MM1 facilitating "Internet protocol" communications with the Relay/Server; such messages are secured using both MMS-Ogawa Message Encryption and SSL/TLS. EX-1003, ¶229; *supra* §§VII.C.2-VII.C.4, VII.D.1.c.iii.

MMS-Ogawa-Cole meets claim 2. POSAs understood Cole's WLAN modem to be for "exchang[ing] Internet data via a connection to a first WLAN, when configured for and connected to the first WLAN," as claimed, because during prosecution, PO stated "the term 'first' merely indicates one of several potential WLAN connections" (EX-1002, 737), and MMS-Ogawa-Cole's WLAN modem allows the device to connect to whatever WLAN connection the modem was "configured for and connected to." EX-1003, ¶230. Moreover, MMS-Ogawa-

Cole works the same way MMS-Ogawa works, except that MMS-Ogawa-Cole also includes a WLAN modem, over which the device can connect to a WLAN, via which it can transmit/receive messages to/from the Relay/Server. MMS-Ogawa-Cole's "device messaging agent" thus "further... receive[s] secure Internet data messages over a secure connection via the first WLAN to the network message server," as claimed, for the reasons discussed *supra* §VII.D.1.c. EX-1003, ¶231.

**B. GROUND 2B: MMS-Ogawa in View of Sathish (EX-1031)**

It was well-documented to use a software *bus* to enable the interprocess communications described in TS-23.140. *Supra* §VII.C.5; EX-1004, 14, 54-56; EX-1028, 729-730, 732-733, FIGS. 4-5. Sathish, e.g., describes a "D-Bus" as "an example of a device inter-process communication channel used to send information between applications." EX-1031, 10:56-62. In view of Sathish, POSAs would have been motivated to implement the disclosed interface between TS-23.140's MMS User Agent and the UE/device's other applications using a software bus and would have reasonably expected success doing so. EX-1003, ¶¶232-233. Using such a bus to enable TS-23.140's applications to interface would have been nothing more than utilizing familiar components to achieve a predictable result of facilitating TS-23.140's communications. *KSR*, 550 U.S. at 416; EX-1003, ¶¶233-234 (citing EX-1048, [0001], [0003]-[0004], [0019]; EX-1049, 907; EX-1050, 2:64-3:6, 3:51-67, FIG. 5). This combination ("MMS-Ogawa-Sathish"),

with the bus secured as discussed *supra* §VII.C.6, renders obvious claims 1, 3-6, and 11-21 for the corresponding reasons discussed *supra* §VII for MMS-Ogawa.

**C. GROUND 2C: MMS-Ogawa-Cole-Sathish**

POSAs understood the modifications described *supra* §§VIII.A-VIII.B were compatible, and that it was feasible and desirable to implement MMS-Ogawa’s device to incorporate WWAN/WLAN modems in view of Cole (for the reasons discussed *supra* §VIII.A) **and** a software interprocess communications bus in view of Sathish (for the reasons discussed *supra* §VIII.B, secured as discussed *supra* §VII.C.6). Such a combination (MMS-Ogawa-Cole-Sathish) renders obvious claims 1-6 and 11-21 for the corresponding reasons discussed *supra* §§VII.D.1-VII.D.16, VIII.A.2. EX-1003, ¶¶235-236.

**IX. FOUNDATIONS 3A-3D**

Claims 7-9, which recite a “service downloader” for downloading, e.g., “updated version[s]” of claim 1’s “software applications,” are rendered obvious by incorporating Papineau’s teachings.

**A. Papineau (EX-1017)**

Papineau discloses “a... system for downloading and managing portable applications on a mobile device” that includes a “Java Application Manager (“JAM”)” responsible for “download[ing] electronic content to the... device... from a information network[.]” EX-1017, 1:33-35, 9:36-39. An application manager may, e.g., upgrade existing applications. EX-1017, 10:7-34, 25:39-50;

EX-1003, ¶¶237-238. Downloaded applications may be “protected.” EX-1017, 22:32-47.

Papineau cites the Java 2 Micro Edition (J2ME) Mobile Information Device Profile (“MIDP”), “a set of Java Application Programming Interfaces (API) that provides the runtime environment for J2ME applications[.]” EX-1017, 2:53-56.<sup>11</sup> “J2ME applications that conform to the MIDP are called ‘MIDlets[.]’” EX-1017, 2:57-59, 8:22-23. MIDlets may be grouped into a MIDlet Suite using “a Java Archive (“JAR”) file.” EX-1017, 8:25-27.

Papineau discloses downloading a “Java Application Descriptor (‘JAD’) file” that “provides information to an application manager [e.g., the JAM] about the contents of a JAR file[.]” with which “decisions can be made” regarding whether “a MIDlet is suitable for... the device.” EX-1017, 8:40-9:17, 20:41-48; EX-1003, ¶¶239-240.

If the JAM determines (from the JAD file) that the MIDlet is “suitable,” the JAR (with the MIDlet) is downloaded from the location specified in the JAD’s “MIDlet-Jar-URL” attribute. EX-1017, 23:14-15, 10:7-26. The JAR may be

---

<sup>11</sup> Papineau incorporates-by-reference “version 1.0” of the MIDP specification. EX-1017, 7:58-59. This Petition references Version 2.0 (EX-1025), which is the version POSAs would have considered on the Critical Date. EX-1003, ¶239.

downloaded from a different server than where the JAD was downloaded by using an “absolute” URL. EX-1003, ¶241; EX-1017, 8:40-9:8; EX-1025, 434.

Papineau leaves to POSAs details of how to ensure the correct JAR was downloaded. One known option was to have the JAM check the JAR for indicia verifying the downloaded JAR’s source. It was, e.g., known to “protect[]” a “MIDlet suite” “by *signing* the JAR” file containing the MIDlet. EX-1025, 29. For “trusted” MIDlet suites, “[t]he signature and certificates are added to the application descriptor”—the JAD—“as attributes,” which “[t]he device uses... to verify the signature” in the JAR, after it is downloaded, as part of an “authentication” process. *Id.*; *see also* EX-1017, 8:27-29; EX-1003, ¶242. “The signer... may be the developer or some [distribution/support/billing] entity.” EX-1025, 30. The “signer” has a “public key,” which “is used to verify the signature.” EX-1025, 30-31.

**B. GROUND 3A: Implementing Papineau’s JAM Teachings (Claims 7-10)**

**1. MMS-Ogawa-Papineau**

TS-23.140 discloses “downloadable” applications, but does not disclose details regarding how downloaded applications, or their updates, are managed. EX-1004, 54-56; EX-1003, ¶243. Papineau describes such details. *Supra* §IX.A.

Papineau teaches using a JAM to manage download and installation of applications/updates (MIDlets) on a mobile device. EX-1017, 1:33-35, 9:11-17,

9:36-39, 20:41-48, 22:32-47. POSAs would have been motivated to implement Papineau’s JAM in MMS-Ogawa’s UE/device because TS-23.140 discloses “download of... downloadable application[s] to a mobile phone[,]” and Papineau’s JAM was an established, well-documented way of managing such downloads. EX-1003, ¶244; EX-1004, 54.

Papineau teaches its JAM using a descriptor file (JAD) to verify the suitability of an application/update for a device prior to downloading the corresponding larger JAR file needed to install the application/update. EX-1017, 9:11-14, 10:7-26. POSAs would have been motivated to use JADs because this would have helped avoid wasting device resources and network bandwidth on installation files for unsuitable applications. EX-1003, ¶245.

POSAs would have been motivated to use MMS-Ogawa’s existing MM1 interface between the Relay/Server and User Agent (EX-1004, 23-24; *supra* §VII.C.2) for transporting such JADs—and using MMS-Ogawa’s User Agent to route the files to the JAM—as this would have leveraged MMS-Ogawa’s existing infrastructure to facilitate TS-23.140’s disclosed application downloads. EX-1003, ¶246. Papineau itself teaches such an implementation, noting that “the ability to invoke content, applications, services, downloads, etc. on the device from a push message is... supported,” and “[t]he handling of these messages is the

responsibility of the messaging client, which will invoke the JAM”—or otherwise “pass[]” the message to “the JAM... for handling.” EX-1017, 22:19-21.

Papineau also teaches downloading larger applications/updates (JARs) from a separate server, over a communication channel separate from the channel used to download smaller JADs. EX-1017, 23:14-15; EX-1025, 434. POSAs would have been motivated to do so because this would have helped avoid over-burdening the Relay/Server and MMSE with transportation of *all* application data over MM1. EX-1003, ¶247.

Additionally, in view of the relevant specification governing MIDlets (*supra* n.11) and Papineau’s disclosure of protected MIDlets (EX-1017, 22:32-47), POSAs would have been motivated to implement the JAM to verify the signature/certificates of a downloaded application/update before installation, e.g., for trusted MIDlets (*supra* §IX.A; EX-1025, 29-31). Ensuring that a downloaded MIDlet—e.g., a JAR that arrived over a non-MM1 connection—is the correct file from a trusted server would have beneficially helped prevent malicious/tampered software from being installed on the device. EX-1003, ¶248.

Implementing MMS-Ogawa to include Papineau’s JAM that uses JADs and protected/trusted JARs (“MMS-Ogawa-Papineau”) would have been nothing more than implementing known components/techniques (a JAM and associated application/update verification/authentication techniques) into known

systems/devices (MMS-Ogawa's UE/device using MMS to transport application data) to achieve predictable results (securely downloading/updating applications). *KSR*, 550 U.S. at 416; EX-1003, ¶249. POSAs would have reasonably expected success with such an implementation given TS-23.140's disclosure of transporting application data for downloadable applications (EX-1004, 54-56) and because the prior art components (User Agent, Relay/Server, JAM) continue to perform functions they performed prior to combining. EX-1003, ¶250. MMS-Ogawa-Papineau was well within a POSA's capability to implement. EX-1003, ¶¶250-251.

MMS-Ogawa-Papineau renders obvious the claims respectively identified *supra* §VII.D, in addition to claims 7-9 as discussed *infra* §§IX.B.2-IX.B.4.

## 2. Claim 7

Claim 7 requires that "at least one of the applications comprises a service downloader" that "authenticat[es] a downloaded software application based on application data from at least one of the secure Internet data messages."

The specification says "[i]n some embodiments," a "service downloader... provides a download function to install or update service software elements on the device." EX-1001, 66:46-48; EX-1003, ¶¶252-253. The specification never describes "authenticating a downloaded software application ***based on application data from at least one of the secure Internet data messages[,]***" leaving to POSAs the details of how to implement such authentication. EX-1001, 66:55-58.

MMS-Ogawa-Papineau’s JAM “is an application that includes... functionality that downloads” other applications “to the mobile information device” (EX-1017, 9:36-39) and is thus a *service downloader*. EX-1003, ¶254. MMS-Ogawa-Papineau’s JAM receives a message comprising a JAD for a MIDlet (“*downloaded software application*”) over MM1. *Supra* §IX.B.1; EX-1003, ¶255. Using the JAD, the JAM verifies the MIDlet is suitable for installation on MMS-Ogawa-Papineau’s device. EX-1003, ¶255; EX-1017, 9:11-14, 10:7-26. If the MIDlet is suitable, the JAM downloads a JAR and *authenticates* it using the certificates and signature in the JAD (“application data”). EX-1003, ¶255. MMS-Ogawa-Papineau’s JAM thus “*authenticat[es]*” the MIDlet “*based on application data from at least one of the secure Internet data messages*” (i.e., based on information contained in the JAD received over MM1), as claimed.

### 3. Claim 8

Claim 8 requires that claim 7’s “service downloader” be for “download[ing] the downloaded software application using an Internet data connection other than the secure connection....” In MMS-Ogawa-Papineau, the JAD (“application data” in “secure Internet data messages” for authenticating the JAR) is received over MM1 (“*the secure connection*”), and the JAR (“*downloaded software application*”) is received from a separate server, over a separate Internet data

connection; MMS-Ogawa-Papineau thus meets claim 8. *Supra* §IX.B.1; EX-1003, ¶¶256-257.

#### 4. Claim 9

Claim 9 depends from claim 7, further requiring that “the downloaded software application comprises an updated version of the device messaging agent.”

MMS-Ogawa-Papineau’s JAM may upgrade existing applications by downloading newer versions of those applications. EX-1017, 25:39-50, 10:20-34; EX-1003, ¶¶258-259. TS-23.140’s “MMS User Agent *[is an] application*” (EX-1004, 14) and Papineau discloses implementing its JAM teachings in conjunction with such “messaging client[s]” (EX-1017, 22:19-31). Because MMS-Ogawa-Papineau’s JAM is used to update applications on MMS-Ogawa-Papineau’s device, and because the User Agent is an application on the device, an obvious implementation of MMS-Ogawa-Papineau with which POSAs would have reasonably expected success was to implement updates to the User Agent using the JAM, such that the User Agent delivers to the JAM a JAD file (received over MM1) that results in the JAM downloading a JAR file (“downloaded software application”) for updating the User Agent (“updated version of the device messaging agent”). EX-1003, ¶¶259-261 (MMS User Agent could be implemented using JAVA).

### **C. GROUND 3B-3D**

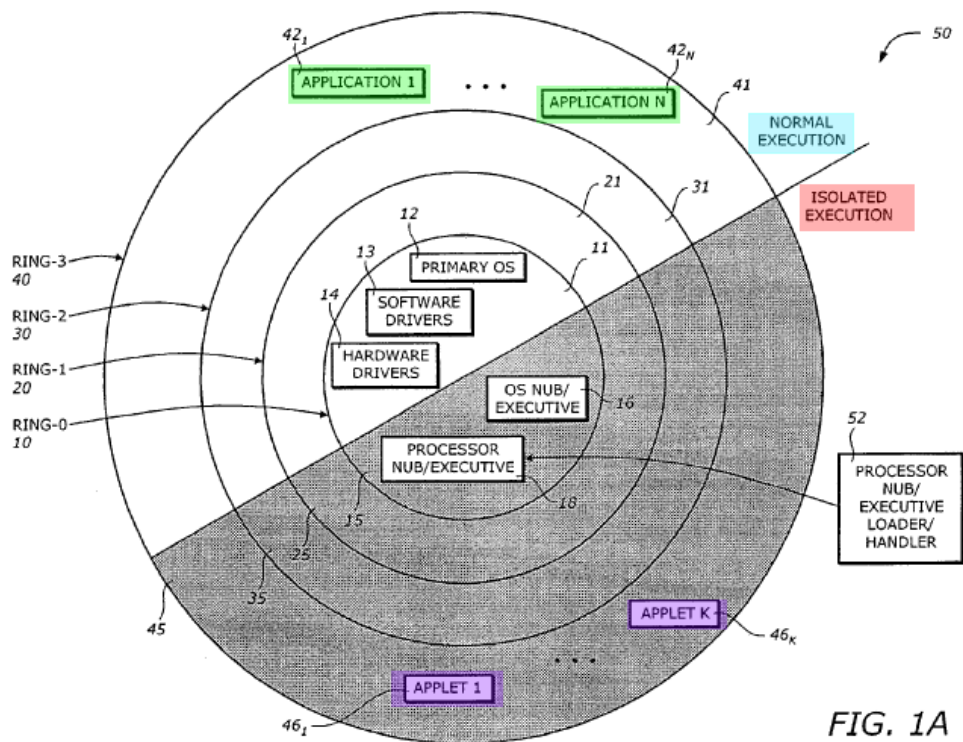
The reasons described *supra* §IX.B.1 for incorporating Papineau’s teachings into MMS-Ogawa apply to MMS-Ogawa-Cole, MMS-Ogawa-Sathish, and MMS-Ogawa-Cole-Sathish (*supra* §§VIII.A-VIII.C), because Papineau’s teachings do not affect how/why POSAs would have combined those references. EX-1003, ¶¶262-263. Incorporating Papineau’s teachings into those combinations renders obvious the claims identified *supra* §§VIII.A-VIII.C (for the reasons respectively discussed there) and claims 7-9 (for the reasons discussed *supra* §§IX.B.2-IX.B.4).

### **X. GROUND 4A-4D**

Claim 10, which recites a “secure execution environment” on claim 1’s device, is rendered obvious by incorporating Ellison’s (EX-1019) teachings.

#### **A. Ellison (EX-1019)**

Ellison discloses “protect[ing] a subset of a software environment.” EX-1019, Abstract; EX-1003, ¶¶264-265. FIG. 1A (below) “illustrat[es] a logical operating architecture” with an “isolated execution mode” (red) where access “is restricted” and a “normal execution mode” (blue) that “operates in a non-secure... or normal environment.” EX-1019, 1:58-59, 3:4-6; 4:65-5:1, 6:1-26, 8:25-32, FIG. 1A-1C; EX-1003, ¶266-267. Ellison allows “normal” execution for applications (green) outside the secure environment, while “[t]he isolated mode applets” (purple) “are tamper-resistant and monitor-resistant from all software attacks from... non-isolated space applications[.]” EX-1019, 4:1-3, 4:65-5:1.



**EX-1019, FIG. 1A (annotated)**

While elements outside Ellison’s isolated area “cannot access the isolated area,” elements within the isolated area “*can* access”—e.g., transport data to/from—the “non-isolated area.” EX-1019, 4:30-37; EX-1003, ¶267.

“[W]hen operating in isolated execution mode,” Ellison’s processor defines an “isolated area 70” in memory. EX-1019, 6:1-26, 8:25-32, FIGS. 1A-1C, 2. FIG. 2 illustrates Ellison’s “secure platform” “within the isolated execution environment[.]” EX-1019, 8:25-32.

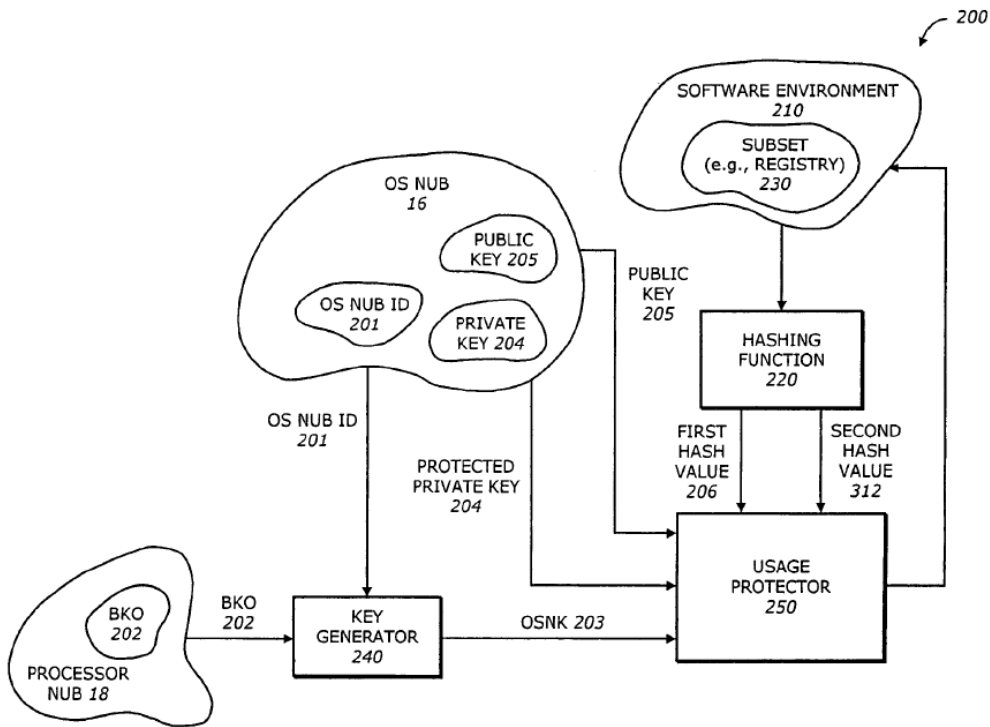


FIG. 2

Above, “usage protector 250” protects “subset 230” against “unauthorized reads” and detects “intrusion, tampering or unauthorized modification.” *Id.*, 8:66-9:62, FIG. 2; EX-1003, ¶¶268-270.

**B. GROUND 4A: Implementing Ellison’s Isolated Execution Environment (Claim 10)**

**1. MMS-Ogawa-Ellison**

POSAs had multiple reasons to implement MMS-Ogawa in view of Ellison.

*First*, implementing Ellison’s secure platform (EX-1019, 8:25-9:62, FIG. 2) would have desirably improved MMS-Ogawa’s device security, which transports data on behalf of, e.g., downloaded third-party VASP applications that should not be trusted with access to sensitive device data/functions. EX-1004, 41, 54-56; EX-

1003, ¶¶271-272 (citing EX-1030, EX-1036, EX-1032, EX-1033). POSAs would have been motivated to incorporate Ellison’s teachings to enable intra-device message transmission with increased security and help guard against malware/unauthorized activity. EX-1019, 8:25-9:62, FIG. 2; EX-1003, ¶272.

*Second*, combining TS-23.140 and Ellison involved combining known prior art elements (Ellison’s isolated software environment in MMS-Ogawa’s device) according to known methods to yield predictable results. *KSR*, 550 U.S. at 416; EX-1003, ¶273.

POSAs would have reasonably expected success incorporating Ellison’s techniques into MMS-Ogawa’s user devices because Ellison describes its techniques implemented in “computer system[s]” (like MMS-Ogawa’s devices) with “processor[s].” EX-1019, 5:11-16; EX-1003, ¶274. Moreover, it was well-known for computing systems to include clients/agents responsible for providing messaging services *within* a trusted/secure computing environment, and for applications (e.g., downloaded third-party applications where messages are directed) to be tiered/organized outside this environment. EX-1003, ¶275 (citing EX-1033, 25-26, FIG. 1). Given (1) TS-23.140’s contemplation of the User Agent communicating with downloaded applications, (2) the well-known need to protect computing environments (including message-providing services) from potentially-malicious downloaded applications/components, and (3) Ellison’s disclosures

confirming same, POSAs would have been motivated to implement Ellison's teaching of a secure execution environment such that MMS-Ogawa's User Agent is organized as part of the secure environment and communicates with destination applications residing outside this secure environment. EX-1003, ¶276; EX-1019, 4:30-37. In such an implementation ("MMS-Ogawa-Ellison"), the MMS User Agent runs in "isolated execution mode," while at least one device application runs in "normal execution mode." EX-1003, ¶277; EX-1019, 3:4-6, 8:25-32, 8:66-9:2, FIG. 2.

## 2. Claim 10

Claim 10 requires that the "device messaging agent" runs in a "secure execution environment on the device," while "at least one of the applications runs outside of the secure execution environment on the device." MMS-Ogawa-Ellison meets claim 10. MMS-Ogawa-Ellison's secure, isolated area is the claimed "*secure execution environment.*" EX-1003, ¶¶278-279. MMS-Ogawa-Ellison's User Agent runs in a "*secure execution environment on the*" device, while at least one un-trusted third-party device application "*runs outside of the secure execution environment on the*" device (*supra* §X.B.1). EX-1003, ¶279. As required by [1C1], MMS-Ogawa-Ellison's "device messaging agent" still has authorized communications with the "application[] run[ning] outside of the secure execution

environment” over the “secure interprocess communication service” as claimed.  
EX-1003, ¶280.

### **C. GROUNDS 4B-4D**

The reasons described *supra* §X.B.1 for incorporating Ellison’s teachings into MMS-Ogawa apply to MMS-Ogawa-Cole, MMS-Ogawa-Sathish, and MMS-Ogawa-Cole-Sathish (*supra* §§VIII.A-VIII.C) for claims 1-6 and 13-21, because Ellison’s teachings do not affect how/why POSAs would have combined those references for those claims. EX-1003, ¶¶281-282. Incorporating Ellison’s teachings into those combinations render obvious claims 1-6 and 13-21 (for the reasons discussed *supra* §§VIII.A-VIII.C) and claim 10 (for the reasons discussed *supra* §X.B.2).

## **XI. CONCLUSION**

The Board should cancel claims 1-21.

Dated: January 23, 2026

Respectfully submitted,  
*Google LLC*

/Anant Saraswat/  
Anant Saraswat, Reg. No. 76,050  
WOLF, GREENFIELD & SACKS, P.C.

## XII. CLAIM LISTING APPENDIX

<b>Claim 1</b>
[1PRE] A mobile end-user-area device comprising:
[1A] a wireless wide-area network (WWAN) modem to exchange Internet data via a connection to a first WWAN, when configured for and connected to the first WWAN;
[1B1] a device messaging agent to receive secure Internet data messages, on behalf of a plurality of software applications capable of execution on the device, and over a secure connection to a network message server reachable via the WWAN,
[1B2] wherein at least a subset of the secure Internet data messages contain an identifier for a corresponding one of the software applications and application data from a respective network application server corresponding to that application; and
[1C1] a secure interprocess communication service,
[1C2] wherein the device messaging agent, for each message in the subset of the secure Internet data messages, maps the identifier to the corresponding one of the software applications in order to forward the application data on the secure interprocess communication service to a software process corresponding to the identified software application.
<b>Claim 2</b>
The mobile end-user device of claim 1, further comprising a wireless local area network (WLAN) modem to exchange Internet data via a connection to a first WLAN, when configured for and connected to the first WLAN, the device messaging agent further to receive secure Internet data messages over a secure connection via the first WLAN to the network message server.
<b>Claim 3</b>
The mobile end-user device of claim 1, further comprising the plurality of software applications.

**Claim 4**

The mobile end-user device of claim 3, wherein the plurality of applications include a first application that receives the application data in a first format, and a second application that receives the application data in a second format different than the first format.

**Claim 5**

The mobile end-user device of claim 1, wherein the secure Internet data messages are received encrypted, the device messaging agent decrypting each message in the subset to obtain the corresponding identifier and application data.

**Claim 6**

The mobile end-user device of claim 5, wherein the secure Internet data messages are transported to the device messaging agent using one or more of encryption on a transport services stack, IP (Internet Protocol) layer encryption, and transport via a tunnel.

**Claim 7**

The mobile end-user device of claim 1, wherein at least one of the applications comprises a service downloader, the service downloader authenticating a downloaded software application based on application data from at least one of the secure Internet data messages.

**Claim 8**

The mobile end-user device of claim 7, wherein the service downloader is to download the downloaded software application using an Internet data connection other than the secure connection used for the secure Internet data messages.

**Claim 9**

The mobile end-user device of claim 7, wherein the downloaded software application comprises an updated version of the device messaging agent.

**Claim 10**

The mobile end-user device of claim 1, wherein the device messaging agent runs in a secure execution environment on the device, and at least one of the applications runs outside of the secure execution environment on the device.

**Claim 11**

[11A] The mobile end-user device of claim 1, wherein the device messaging agent is further to send secure upload Internet data messages to the network message server over the secure connection, wherein at least a subset of the secure upload Internet data messages are sent responsive to a corresponding request received on the secure interprocess communication channel from a corresponding one of the software applications, the device messaging agent constructing from each such request a secure upload Internet data message containing

[11B] an identifier for a respective network application server corresponding to the requesting software application; and

[11C] content received with the request.

**Claim 12**

The mobile end-user device of claim 11, wherein at least one of the upload Internet data messages comprises a key for the network application server corresponding to the requesting software application.

**Claim 13**

The mobile end-user device of claim 1, wherein the device messaging agent creates a log for the received secure Internet data messages.

**Claim 14**

The mobile end-user device of claim 1, wherein the secure interprocess communication channel and the secure connection to the network message server are separately secured.

**Claim 15**

The mobile end-user device of claim 1, wherein access by the software applications to the interprocess communication channel is subject to a security policy.

**Claim 16**

The mobile end-user device of claim 1, wherein at least one of the secure Internet data messages comprises multiple identifier/data pairs.

**Claim 17**

The mobile end-user device of claim 1, the device messaging agent comprising an agent router to forward the application data on the secure interprocess communication channel to the software process corresponding to the identified software application.

**Claim 18**

The mobile end-user device of claim 1, wherein the secure interprocess communication service forwards the application data to at least one of the software processes in an encrypted format.

**Claim 19**

The mobile end-user device of claim 1, the device messaging agent further to initiate the secure connection to the network message server.

**Claim 20**

The mobile end-user device of claim 1, further comprising a network stack in communication with the device messaging agent and the WWAN modem, the secure connection terminated within the network stack.

**Claim 21**

The mobile end-user device of claim 1, wherein at least one of the applications and the network application server corresponding to that application authenticate with each other prior to passing application data via the device messaging agent and network message server.

**CERTIFICATE OF SERVICE UNDER 37 C.F.R. § 42.6 (E)(4)**

I certify that on January 23, 2026, a copy of the foregoing document, including any exhibits or appendices filed therewith, is being served via Overnight FedEx at the following correspondence address of record for the patent:

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

Date: January 23, 2026

/MacAulay Rush/  
MacAulay Rush  
Paralegal  
WOLF, GREENFIELD & SACKS, P.C.

## **CERTIFICATE OF WORD COUNT**

Pursuant to 37 C.F.R. § 42.24, the undersigned certifies that the foregoing Petition for *Inter Partes* Review contains 13,998 words excluding a table of contents, a table of authorities, Mandatory Notices under § 42.8, a certificate of service or word count, or appendix of exhibits or claim listing. Petitioner has relied on the word count feature of the word processing system used to create this paper in making this certification.

Date: January 23, 2026

/MacAulay Rush/  
MacAulay Rush  
Paralegal  
WOLF, GREENFIELD & SACKS, P.C.