

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

AMAZON.COM SERVICES LLC,
Petitioner,

v.

HEADWATER RESEARCH LLC,
Patent Owner.

Case No. IPR2026-00361
Patent No. 9,491,564

**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.....	1
A. Real Party-In-Interest	1
B. Related Matters.....	1
1. United States Patent & Trademark Office	1
2. U.S. District Court for the Eastern District of Texas, Marshall Division	1
3. U.S. District Court for the Western District of Texas, Midland/Odessa Division.....	2
4. U.S. District Court for the Northern District of California	2
C. Counsel and Service Information - § 42.8(b)(3) and (4).....	2
I. INTRODUCTION	3
II. GROUNDS FOR STANDING.....	3
III. UNPATENTABILITY GROUNDS.....	4
IV. '564 PATENT.....	5
A. Brief Description	5
B. Prosecution History	6
V. PERSON OF ORDINARY SKILL IN THE ART	6
VI. CLAIM INTERPRETATION.....	6
VII. GROUND 1: TS-23.140 AND RAKIC RENDER OBVIOUS CLAIMS 1-8, 9-14.....	7
A. TS-23.140 (EX-1004)	7
B. Rakic (EX-1007)	9
C. The MMS-Rakic Combination	12
1. Implementing TS-23.140's UE/Device with a Modem.....	12
2. Securing Interface MM1 Using SSL/TLS	13
3. Implementing TS-23.140's Device with an Interprocess Communication Bus	16
4. Applying Rakic's Message Validation Techniques	18
5. MMS-Rakic	21
D. Claim Analysis.....	22

1.	Claim 1	22
a.	[1PRE] A mobile end-user device comprising:.....	22
b.	[1A] a wireless modem configurable to exchange data via a connection to a wireless network;.....	23
c.	[1B1].....	26
i.	“an executing device link agent”	26
ii.	“respective executing processes for a plurality of software components”	27
iii.	“an inter-process software communication bus providing secure communication between...”	29
d.	[1B2] wherein providing secure communication comprises receiving access authorization information from a secure server, and allowing access to the bus only for software components identified by the access authorization information; and	31
e.	[1C] the device link agent, configured to.....	34
f.	[1D1] maintain a secure message link through the wireless network and an Internet network to a message link server,.....	35
g.	[1D2] the message link server operating a message service that receives messages over a network from a plurality of network functions,	40
h.	[1E]	43
i.	receive secure messages from the message link server over the secure message link	43
ii.	the received messages identified for delivery to multiple ones of the software components, and	44
iii.	including message content received by the message link server from multiple ones of the network functions, and.....	45
i.	[1F] for software components identified by the access authorization information, route messages identified for delivery to a given one of those software components via the inter-process software communication bus to a	

	software process corresponding to the given software component.....	49
2.	Claim 2.....	50
3.	Claim 3.....	50
4.	Claim 4.....	51
5.	Claim 5.....	54
6.	Claim 6.....	55
7.	Claim 7.....	56
8.	Claim 8.....	57
9.	Claim 10	58
10.	Claim 12	63
11.	Claim 13	66
12.	Claim 14	66
VIII.	FOUNDATIONS 2A-2C	67
A.	FOUNDATION 2A: MMS-Rakic in View of Cole (EX-1006)	67
B.	FOUNDATION 2B: MMS-Rakic in View of Sathish (EX-1031).....	69
C.	FOUNDATION 2C: MMS-Rakic-Cole-Sathish	70
IX.	FOUNDATIONS 3A-3D.....	70
A.	Ogawa (EX-1005).....	70
B.	FOUNDATION 3A: Implementing Ogawa's Encryption Teachings	72
1.	MMS-Rakic-Ogawa	72
a.	Applying Ogawa's Symmetric Encryption Techniques..	72
b.	Ogawa's Decryption Unit	74
2.	Claim 7.....	76
C.	FOUNDATIONS 3B-3D	76
X.	FOUNDATIONS 4A-4D	77
A.	Ellison (EX-1019).....	77
B.	FOUNDATION 4A: Implementing Ellison's Isolated Execution Environment	79
1.	MMS-Rakic-Ellison	79
2.	Claim 9.....	81

TABLE OF AUTHORITIES

CASES

<i>Headwater Research LLC v. Amazon. Com Services LLC</i> , Case No. 2:26-cv-00304 (filed Apr. 16, 2026).....	2, 54
<i>KSR v. Teleflex</i> , 550 U.S. 398 (2007).....	passim
<i>Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.</i> , 868 F.3d 1013 (Fed. Cir. 2017)	6

STATUTES

35 U.S.C. §282.....	6
---------------------	---

OTHER AUTHORITIES

37 C.F.R. §42.100	6
37 C.F.R. §42.104	4
83 Fed. Reg. 51,340 (Oct. 11, 2018).....	6

APPENDIX LISTING OF EXHIBITS

Exhibit	Description
1001	U.S. Patent No. 9,491,564 (“the ’564 Patent”)
1002	Prosecution History of U.S. Patent No. 9,491,564 (“the ’564 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 (Release 6) (“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. 2009/0282256 (“Rakic”)
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 https://www.openmobilealliance.org/release/MMS/V1_2-20030923-C/OMA-ERELD-MMS-V1_2-20030923-C.pdf
1012	“Open Mobile Alliance; Multimedia Messaging Service Architecture Overview Version 1.2” (MMSARCH) specification, available at https://www.openmobilealliance.org/release/MMS/V1_2-20030923-C/OMA-MMS-ARCH-V1_2-20030920-C.pdf
1013	The Secure Sockets Layer (“SSL”) Protocol, V. 3.0, available at https://web.archive.org/web/19970614041044/http://home.netscape.com/eng/ssl3/ssl-toc.html and https://web.archive.org/web/19970617034012/http://home.netscape.com/eng/ssl3/3-SPEC.HTM#1
1014	The Transport Layer Security (“TLS”) Protocol, V. 1.1, available at https://www.ietf.org/rfc/rfc4346.txt
1015	U.S. Patent App. Pub. No. 2003/0096625 (“Mi-Su Lee”)

1016	RESERVED
1017	RESERVED
1018	Liaison Statement, European Telecommunications Standards Institute AT-F Rapporteur Meeting, 4 to 6 February 2003 (ETSI/ AT-F TD18), available at https://www.3gpp.org/ft2/tsg_sa/TSG_SA/TSGS19/Docs/PDF/SP-030167.pdf
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 www.openmobilealliance.org/release/MMS/V1_2-20050301-A/OMA-MMS-ENC-V1_2-20050301-A.pdf
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), https://www.uspto.gov/sites/default/files/documents/Memo_re_prior_findings_of_fact_and_conclusions_of_law_9_16_25.pdf
1024	Declaration of Friedhelm Rodermund
1025	RESERVED
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, Wireless Communications and Mobile Computing (2007) (“Mostafa”)
1029	Dictionary of Computer Science, Engineering, and Technology, CRC Press LLC, 2001
1030	Needham et al., “Using Encryption for Authentication in Large Networks of Computers” (ACM, 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” (IEEE Proceedings, Vol. 63, No. 9, Sept. 1975) (“Saltzer”)
1033	Li et al., “Symbian OS platform security model,” available at https://www.usenix.org/system/files/login/articles/73507-li.pdf (Login Magazine, Aug. 2010)
1034	RESERVED
1035	RESERVED
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 https://www.cnet.com/reviews/nokia-e71-review/
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. 2006/0077940 (“Ganji”)
1041	U.S. Patent App. Pub. No. 2005/0282531 (“Andreasson”)
1042	U.S. Patent App. Pub. No. 2003/0193967 (“Fenton”)
1043	U.S. Patent App. Pub. No. 2004/0085894 (“Wang”)
1044	U.S. Patent No. 6,094,424 (“Kalmanek”)
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	U.S. Patent App. Pub. No. 2005/0091380 (“Gonen”)
1058	U.S. Patent App. Pub. No. 2004/0258063 (“Raith”)
1059	U.S. Patent App. Pub. No. 2004/0111476 (“Trossen”)
1060	Prosecution History of U.S. Patent No. 9,232,403 (“the ’403 FH”)
1061	U.S. Patent App. Pub. No. 2007/0239898 (“Friend”)
1062	U.S. Patent No. 7,269,433 (“Vargas”)

MANDATORY NOTICES

A. Real Party-In-Interest

Petitioner Amazon.com Services LLC and Amazon.com, Inc. are real parties in interest.

B. Related Matters

To the best of Petitioner's knowledge, the '564 patent has been involved in the following matters:

1. United States Patent & Trademark Office

The application from which U.S. Patent No. 9,491,564 issued is a Continuation of U.S. Patent Application No. 14/979,233 (U.S. Patent No. 9,532,161), is a Continuation of U.S. Patent Application No. 14/667,353 (U.S. Patent No. 9,232,403), which 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. Application No. 12/380,780 (U.S. Patent No. 8,839,388) which claims priority from U.S. Provisional Application Nos. 61/206,354, 61/206,944, 61/207,393, and 61/207,739. Petitioner identifies *Google LLC v. Headwater Research LLC*, IPR2026-00271 as a related matter, which challenges the '564 patent. Petitioner is concurrently seeking joinder to IPR2026-00271.

2. U.S. District Court for the Eastern District of Texas, Marshall Division

i) *Headwater Research LLC v. Amazon. Com Services LLC*, Case No. 2:26-

cv-00304 (filed Apr. 16, 2026); ii) *Headwater Research LLC v. Cellco Partnership, d/b/a Verizon Wireless et al*, Case No. 2-25-cv-00709; iii) *Headwater Research LLC v. T-Mobile USA, Inc. et al*, Case No. 2-25-cv-00710; iv) *Headwater Research LLC v. AT&T Services, Inc. et al*, Case No. 2-25-cv-00711.

3. U.S. District Court for the Western District of Texas, Midland/Odessa Division

i) *Headwater Research LLC v. Apple Inc.*, Case No. 7-25-cv-00407.

4. U.S. District Court for the Northern District of California

i) *Google LLC v. Headwater Research LLC*, Case No. 5:25-cv-07453; ii) *Headwater Research LLC v. Google LLC*, Case No. 3:26-cv-01460; iii) *Apple Inc v. Headwater Research LLC*, Case No. 5-25-cv-07591.

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

LEAD COUNSEL
Jessica Kaiser (Reg. No. 58,937) kaiser-ptab@perkinscoie.com PERKINS COIE LLP 1900 Sixteenth Street, Suite 1400 Denver, CO 80202-5255 Telephone: (303) 291-2300
BACK-UP COUNSEL
Christopher Marando (Reg. No. 67,898) Marando-ptab@perkinscoie.com PERKINS COIE LLP

1900 Sixteenth Street, Suite 1400 Denver, CO 80202-5255 Telephone: (303) 291-2300

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

I. INTRODUCTION

Amazon.com Services LLC (“Amazon” or “Petitioner”) requests *inter partes* review (“IPR”) and cancellation of claims 1-14 of US 9,491,564 (“’564 Patent”) (EX-1001). The patentability analysis of this Petition is substantively equivalent to the petition in IPR2026-00271, and Petitioner conditionally requests joinder to that proceeding. The Board considered substantially similar claims with several identical limitations in IPR2024-00341, which challenged related US 8,406,733 (“’733 Patent”)¹ and cancelled claims 1-17, 19, 21-27, and 29-30 of the ’733 Patent over an obviousness combination based on the TS-23.140 standard (EX-1004). EX-1022, 51. This Petition likewise relies on TS-23.140 as its primary reference, and where applicable, identifies relevant findings of fact and conclusions of law regarding TS-23.140 from the Board’s prior adjudication. EX-1023.

II. GROUNDS FOR STANDING

Petitioner certifies that the ’564 Patent is available for IPR and that Petitioner is not barred or estopped from requesting IPR of claims 1-14. 37 C.F.R. § 42.104(a).

¹ The ’564 and ’733 Patents share a specification.

III. UNPATENTABILITY GROUNDS

Below table identifies each §103 unpatentability ground presented herein.

Grounds, Reference(s)		Claims
1	TS-23.140, Rakic	1-8, 10, 12-14
2A	TS-23.140, Rakic, Cole	1-8, 10, 12-14
2B	TS-23.140, Rakic, Sathish	1-8, 10, 12-14
2C	TS-23.140, Rakic, Cole, Sathish	1-8, 10, 12-14
3A	TS-23.140, Rakic, Ogawa	7
3B	TS-23.140, Rakic, Ogawa, Cole	7
3C	TS-23.140, Rakic, Ogawa, Sathish	7
3D	TS-23.140, Rakic, Ogawa, Cole, Sathish	7
4A	TS-23.140, Rakic, Ellison	9
4B	TS-23.140, Rakic, Ellison, Cole	9
4C	TS-23.140, Rakic, Ellison, Sathish	9
4D	TS-23.140, Rakic, Ellison, Cole, Sathish	9
5A	TS-23.140, Rakic, Shen	11
5B	TS-23.140, Rakic, Shen, Cole	11
5C	TS-23.140, Rakic, Shen, Sathish	11
5D	TS-23.140, Rakic, Shen, Cole, Sathish	11

The '564 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	Prior Art Basis
TS-23.140		March 2005 (EX-1024) ²	102(b)
Rakic	5/12/2008	11/12/2009	102(a)/102(e)
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)
Ellison	9/22/2000	7/25/2006	102(b)
Shen	3/18/2005	9/22/2005	102(b)

IV. '564 PATENT

A. Brief Description

The '564 Patent is directed to a “mobile end-user device” with “an inter-process software communication bus” that provides “secure communication between an executing device link agent” and “software component processes,” where “software processes are allowed to access the bus based on access authorization information from a secure server that identifies those components.” EX-1001, Abstract; EX-1003, ¶¶35-36. The device link agent is configured to “maintain a secure message link” to a “message link server,” over which it “receive[s] secure messages.” EX-1001, Abstract. The device link agent delivers such messages to software component processes over the bus. *Id.*

² Confirming public availability/accessibility on/around March 2005.

B. Prosecution History

The patent issued after no Office Actions. EX-1002, 531-539. The Examiner considered neither TS-23.140 (EX-1004) nor Rakic (EX-1007). EX-1003, ¶¶37-38.

V. PERSON OF ORDINARY SKILL IN THE ART

A person of ordinary skill in the art (“POSA”) relating to the subject matter of the ’564 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

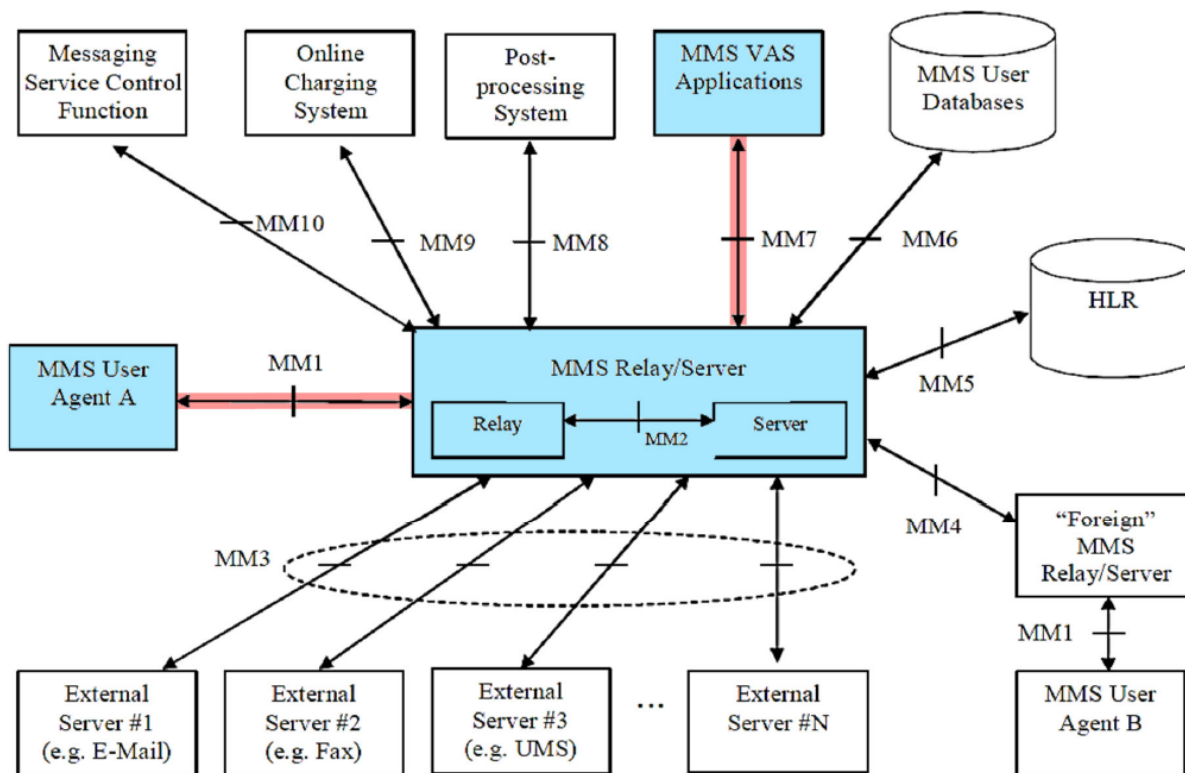
that each challenged claim satisfies all statutory requirements or waive arguments only raisable in District Court.

VII. GROUND 1: TS-23.140 AND RAKIC RENDER OBVIOUS CLAIMS 1-8, 9-14

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, ¶¶43-44.

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”³ in the network. *Id.*, 18; EX-1003, ¶45.

“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, ¶¶46-47 (citing EX-1028, 732-733). 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, ¶48.

Before transporting such application-specific data, applications “register with the appropriate MMS User Agent or MMS VAS Application” by “provision[ing]... its application identification value and... negotiat[ing]... details (amount and format) of information to be exchanged...” EX-1004, 54.

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

³ Emphasis is added throughout unless otherwise indicated.

mechanisms based on public/private key cryptography...” EX-1003, ¶¶49-50 (citing EX-1004, 19, 41, 25-26; EX-1011, 11; EX-1012, 11, 21).

B. Rakic (EX-1007)

Rakic discloses a system where a “[client] device may receive” and “validate” “(e.g., authenticate)” “secure push message[s] based on [an] electronic signature.” EX-1007, Abstract, [0039], [0044]-[0045], [0050], FIGS. 2A-2B; EX-1003, ¶¶51-53. “[V]alidat[ing]... secure push message[s] may protect the client device” by, e.g., allowing “the client device” to “authenticate the sender” and/or “verify that an intended recipient of the secure push message is the client device, and that the client device includes a correct component.” EX-1007, [0041].

The client device (e.g., “a portable phone”/“portable digital assistant”) may comprise a “[c]ommunication path” to “provide an interface through which” the device’s “components... communicate with one another[,]” and a “network interface... for communicating with other devices” “via a network,” e.g., “the Internet,” “a WLAN,” and “UMTS [(i.e., 3G)].” EX-1007, [0001], [0013], [0051]-[0052], [0057], [0122], FIGS. 2A-2B. The client device also comprises a “[d]isplay” and “[c]ontrol buttons” for “user... interact[ions].” EX-1007, [0052]. The client device “may include additional functional components, such as... an application (e.g., an instant messenger client...)” and “may perform a specific task” “related to

an application” “in accordance with contents of [a] secure push message.” EX-1007, [0051], [0059].

Rakic further discloses an “administrator device” with “a secure push message server” and “additional functional components,” e.g. “an application (e.g., an email server, a[] file transfer protocol (FTP) server, etc.).” EX-1007, [0045], [0063]. The “[s]ecure push message server... may send secure push messages to client device[s]... via a wireless network[.]” EX-1007, [0065]. The administrator device “may include a database of information about client device[s].” EX-1007, [0047], [0069].

“Given a message or a payload from an application... secure push message server... may generate a key, an electronic signature, and a secure push message.” EX-1007, [0065]. The key may be generated by creating a hash of an administrator code and identifying information for a client device (or component thereof). EX-1007, [0042] (“The format of the secure push message... may be easily modified to accommodate different types of applications/devices that receive/send secure push messages”), [0066]-[0068], [0071]-[0072] (the “record [for a client device (or component thereof)] may include additional... or different fields than those illustrated in FIG. 7”), [0080], [0085] (“push message server... may automatically generate the administrator code.”); EX-1003, ¶54. Administrator and client may exchange the administrator code and identifying information for the client device (or

component thereof) during initial configuration. EX-1007, [0048]. “Once the key is generated, secure push message server... may generate an electronic signature based on the key and the message” by “signing [the] message with [the] key.” EX-1007, [0040], [0049], [0067], [0079], [0105]; EX-1003, ¶55. The “secure push message server... generate[s] the secure push message by appending the electronic signature to the message[.]” EX-1007, [0067].

Figure 8 depicts a secure push message, comprising the push message (blue) and the signature (green):

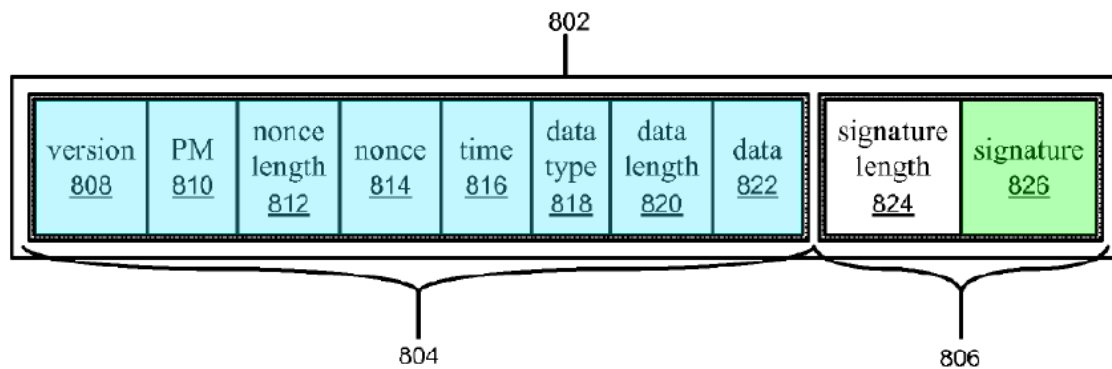


Fig. 8

EX-1007, FIG. 8. The message body further comprises “[d]ata field 822[, which] may include content (e.g., payload)[,]” and “PM field 810[, which] may indicate a particular method that is used to generate a signature, to encrypt the data, or *to perform a combination of generating a signature and encrypting the data.*” EX-1007, [0075], [0078].

Rakic’s secure push server then sends the secure push message to the client device, which is “validate[d]... based on the electronic signature” by the secure push message client of the client device. EX-1007, [0040], [0050], [0065], [0107]. The secure push message client does this by creating a hash of the administrator code and the identifying information for the client device (or component thereof). EX-1007, [0110]-[0111]; EX-1003, ¶¶56-57. The client then signs the data block of the received message with the key and compares the result to the signature of the received message. EX-1007, [0112]. If the signatures match, the client determines that the message is valid. EX-1007, [0112]. If the message is valid and the data block contains data intended for a “component[of the client device], such as... an application[,]” the data is sent to the component. EX-1007, [0112]-[0119], [0122], [0130]-[0131]; EX-1003, ¶57 (explaining that the data can cause a component to perform a task).

C. The MMS-Rakic Combination

As discussed below, “MMS-Rakic” refers to an encrypted MMS system where communications with the MMS User Agent on TS-23.140’s UE/device—either over a network (e.g., with an MMS Relay/Server) or within the device (e.g., with other applications)—are secured using Rakic’s teachings.

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, FIG. 2, 17, 23-24. 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, [0001], [0008], [0022]-[0023], [0027]-[0028], [0044], 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 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 MMS User

Agent and Relay/Server use interface MM1. EX-1003, ¶64; EX-1004, 24, FIG. 4 (below); EX-1018, 6, 9.

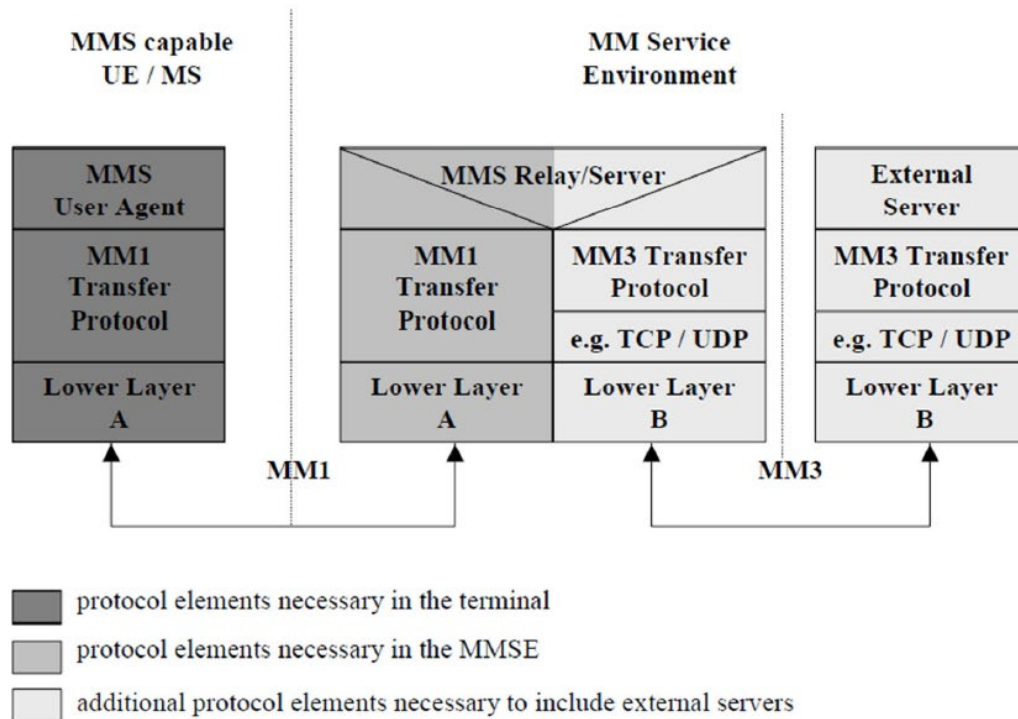


Figure 4: Protocol Framework to provide MMS

EX-1004, 24, FIG. 4

POSAs 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, 21.⁴ In that implementation, the “MMS User Agent is... responsible for sending and receiving MMs by utilizing the message transfer services of the appropriate network protocols” e.g. SSL/TLS for securing MM1. 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. 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.

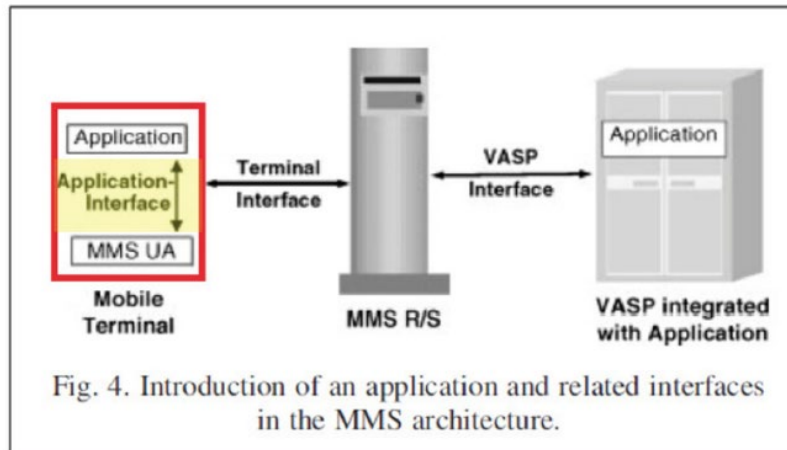
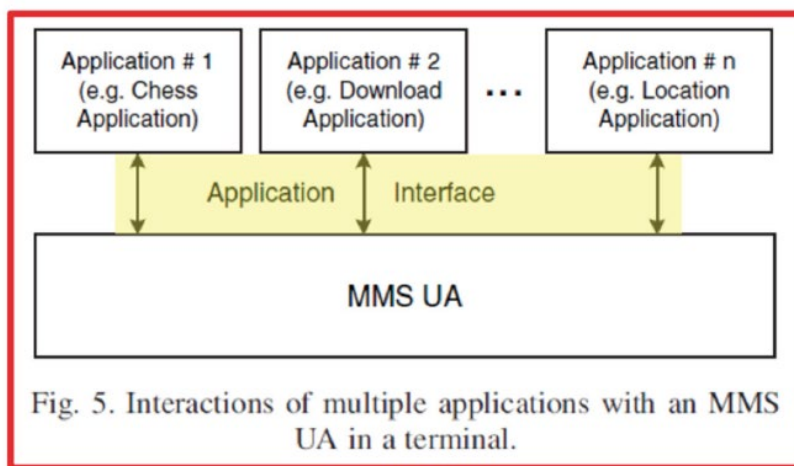
⁴ WAP/OMA is Open Mobile Alliance’s Wireless Application Protocol. EX-1003, ¶66. To describe “[d]etails” for this “implementation of the MM1 transfer protocol,” TS-23.140 incorporates-by-reference EX-1011 (“Enabler Release Definition”). *See* EX-1004, 13, 24-25, 162. EX-1011 incorporates-by-reference 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. 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, ¶71. 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)

Rakic confirms the presence of such “communication path[s]” in the context of devices that receive push messages from servers. EX-1007, [0058]-[0059] (disclosing “[c]ommunication path” that “provide[s]... interface through which [device] components”—e.g., “application[s]”—“communicate with one another”), FIG. 3; *see also* EX-1003, ¶¶72-73 (citing 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, ¶74. 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, ¶75. For these same reasons, POSAs would have reasonably expected success using a bus. EX-1003, ¶¶76-77.

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.

4. Applying Rakic’s Message Validation Techniques

TS 23.140 discloses “[t]he MMS User Agent... provid[ing] additional

application layer functionalities such as... the **signing** of an MM on an end-user to end-user basis[,]” but does not provide details regarding how to implement such signing functionality between network entities, for example for messages containing content sent by an MMS VAS Application to an MMS User Agent. EX-1004, 19, 54-56.

Rakic discloses such details, including how to “validate... secure push message[s] based on [an] electronic signature” to “authenticate the sender” and/or “verify that an intended recipient of the secure push message is the client device, and that the client device includes a correct component.” *Supra* §VII.B; EX-1007, Abstract, [0041], [0044]-[0045], [0050].

POSAs had multiple reasons to implement Rakic’s message signing and validation techniques for messages containing content sent by a VAS Application to a User Agent. EX-1003, ¶¶78-83.

First, TS-23.140 expressly teaches having the MMS User Agent handle MM signing on an end-user to end-user basis, and Rakic provides details regarding how to implement such signing functionality. EX-1003, ¶81; EX-1004, 19.

Second, implementing Rakic’s validation process on TS-23.140’s User Agents for messages containing signed content originating from VAS Applications would enhance the reliability and security of TS-23.140’s MMS system by ensuring that messages routed to destination applications originate from an authorized source,

that routing information has not been tampered with, and that only the intended destination application receives the message. EX-1003, ¶82; EX-1007, Abstract, [0041]-[0042], [0050], [0059], [0070]-[0071].

Third, implementing Rakic's signature-generation and verification process into TS 23.140's MMS system would have been nothing more than applying known message signing/validation techniques (e.g., signature verification) to known components (MMS VAS Application and MMS User Agent) to achieve predictable results (end-user-to-end-user message delivery in which the MMS User Agent verifies that received, signed messages are from a valid source). *KSR*, 550 U.S. at 416; EX-1003, ¶83.

POSAs would have reasonably expected success implementing Rakic's message validation techniques to the TS-23.140 system given (1) TS-23.140 and Rakic share a similar push-message architecture, in which a network server transmits content to a client device; and (2) TS-23.140 contemplates User Agents signing MMs on an end-user-to-end-user basis, and Rakic provided an exemplary, predictable implementation of such message validation using signature-generation/verification. EX-1003, ¶84.

In such an implementation, the secure push message signing functionality of Rakic's secure push message server is incorporated into TS-23.140's VAS Application and the signature validation functionality of Rakic's secure push

message client is incorporated into TS-23.140's User Agent. *Supra* §VII.B. Additionally, during the application registration process described in TS-23.140—where an application “provisions an MMS User Agent or an MMS VAS Application with its application identification value and... negotiates... the details (amount and format) of information to be exchanged...” (EX-1004, 54)—the necessary information used to create keys for signing and signature validation (e.g., the VAS Application's administrator code) are provisioned as needed to facilitate Rakic's message signing and signature validation functionality. EX-1003, ¶¶85-86; EX-1004, 54-56; EX-1007, [0048].

5. MMS-Rakic

“MMS-Rakic” (EX-1003, ¶¶87-91) refers to the above-discussed MMS system that POSAs would have formed based on TS-23.140 and Rakic.

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

MMS-Rakic 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. *Supra* §VII.C.2.

MMS-Rakic implements an interprocess bus for communications that occur within TS-23.140's UE/device. *Supra* §VII.C.3.

In MMS-Rakic, Rakic’s secure push message signing functionality is implemented as part of TS-23.140’s VAS Application, and Rakic’s signature validation functionality is implemented as part of TS-23.140’s User Agent in a UE/device. *Supra* §VII.C.4.

D. Claim Analysis

1. Claim 1

a. [1PRE]⁵ A mobile end-user device comprising:

The ’564 specification does not describe a “mobile end-user device,” but uses the term “end user device” (EX-1001, 7:53-65, 8:44-67), which is used to include “networked” devices that have “services delivered” to them. EX-1001, 5:41-6:8, 6:30-38; EX-1003, ¶¶92-93. In IPR2024-00341, the Board “[found] that 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 “Value Added Services”—teaches a “*mobile* end-user device.” EX-1004, 14, 18, 54; EX-1003, ¶93.

⁵ Limitations herein are identified using reference labels from the Claim Appendix.

b. [1A] a wireless modem configurable to exchange data via a connection to a wireless network;

MMS-Rakic includes a “*modem*.” *Supra* §VII.C.1. In IPR2024-00341, the Board credited Petitioner’s showing of “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* modem.” MMS-Rakic’s modem is for communications over 2G/3G wireless networks (*supra* §VII.C.1) and is thus “a *wireless* modem,” as claimed. EX-1003, ¶¶94-95.

MMS-Rakic’s modem is also “configurable to exchange data via a connection to a wireless network,” as claimed. EX-1003, ¶96. This is confirmed in TS-23.140’s FIG. 2, showing a Multimedia Messaging Service Environment (MMSE) in which TS-23.140’s UE/device (*supra* §VII.D.1.a) operates, comprising 2G and 3G wireless networks:

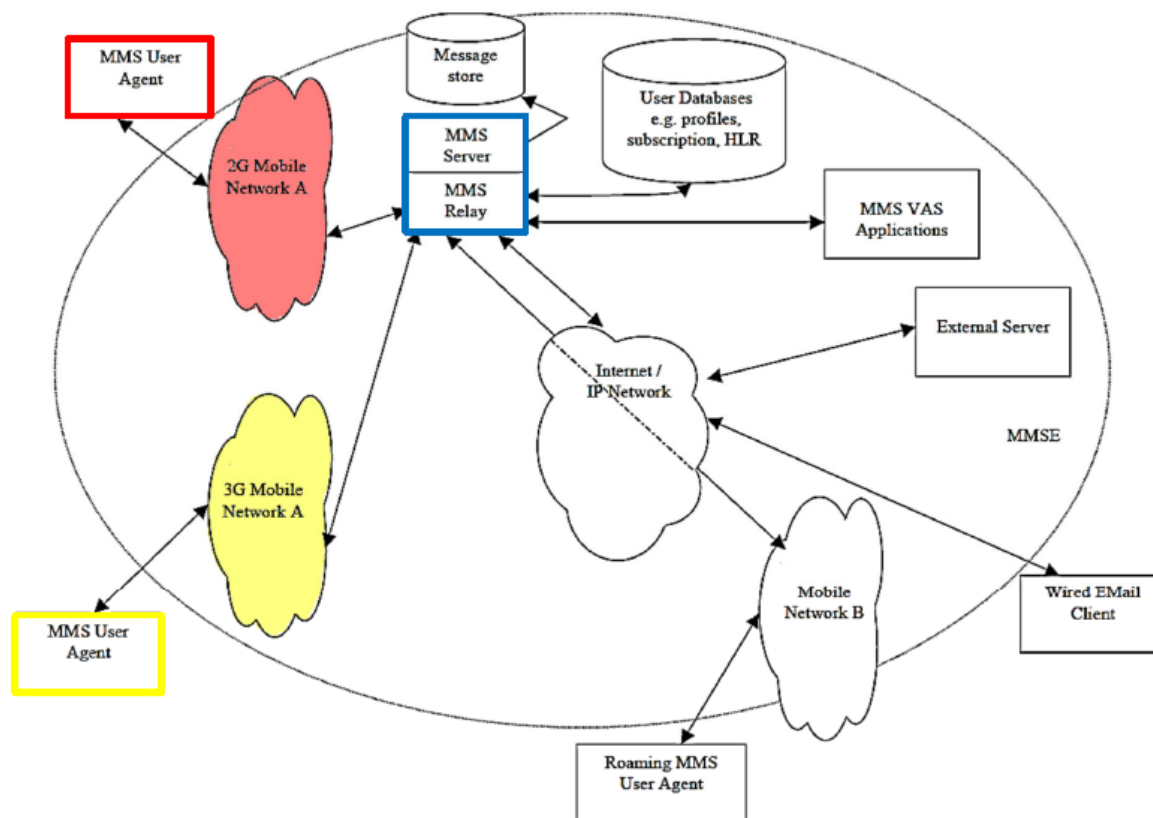
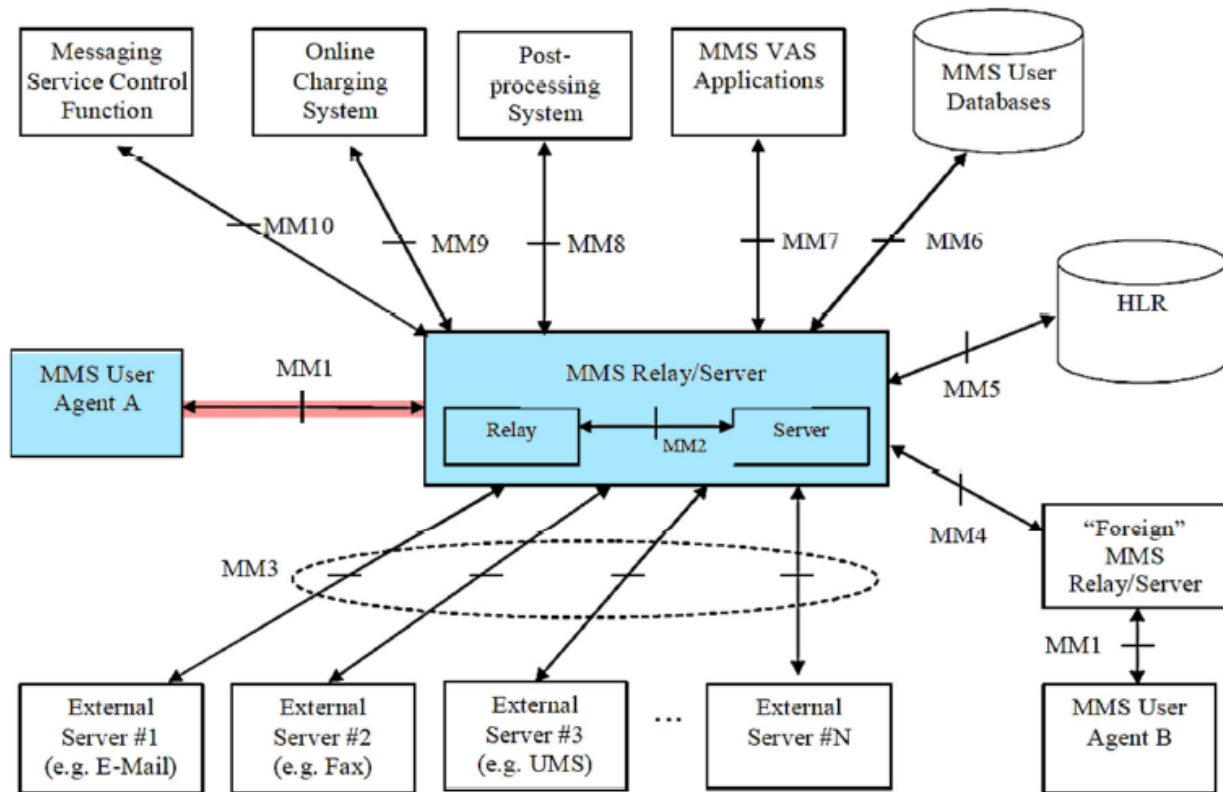


Figure 2: MMS Architectural Elements

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

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 wireless communications between each UE/device’s MMS User Agent and the Relay/Server. EX-1004, 17; EX-1003, ¶97 (citing EX-1004, 17, 23-24, FIG. 4). MM1 is shown below:



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

MMS-Rakic’s DE/device modem also enables MMS-Rakic’s User Agent to exchange messages containing *data* with network elements through interface MM1—including with MMS-Rakic’s Relay/Server, and multiple VAS applications (via the Relay/Server). EX-1004, 14, 18, 23; EX-1003,198. For example, using the modem, MMS-Rakic’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-1003,198.

Thus, MMS-Rakic’s modem (*supra* §VII.C.1) is “configurable to exchange *data* via a connection to” MMS-Rakic’s wireless networks. EX-1003, ¶99.

c. [1B1]

i. “an executing device link agent”

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, 15:53-16:7, 43:21-22; EX-1003, ¶¶100-101; *see also* EX-1029, 12. In IPR2024-00341, the Board agreed. EX-1022, 27; EX-1023. The ’564 specification never uses the term “*executing device link* agent,” but describes a “service control *device link* 1691,” saying it “provides the device side of a system for transmission and reception” of messages. EX-1001, 38:5-8; EX-1003, ¶102.

MMS-Rakic’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 VAS Applications via the Relay/Server. EX-1004, 14, 19, 23-24, 30-31, 35-36, 41-42, 54-56; EX-1003, ¶103. MMS-Rakic’s application-specific data is sent in what TS-23.140 calls “abstract messages.” EX-1004, 14 (“abstract message[s]: 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-Rakic’s User Agent is thus a “device link agent,” as claimed. EX-1003, ¶104. This is consistent with the Board’s IPR2024-00341 finding that TS-23.140’s User Agent is “a service control *device link agent* on the end-user device[.]” EX-1022, 17-18; EX-1023.

Moreover, POSAs understood that MMS-Rakic’s User Agent application is an “*executing*” agent, because it is a software application that runs on TS-23.140’s UE/device to perform various functions (e.g., EX-1004, 19-20) disclosed in TS-23.140. EX-1003, ¶105 (citing EX-1045, 126; EX-1046, 46).

ii. “respective executing processes for a plurality of software components”

MMS-Rakic’s User Agent application (the claimed *device link agent*) “performs MMS-specific operations on a user’s behalf and/or *on another application’s behalf*.” EX-1004, 14; *supra* §VII.D.1.c.i. 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-Rakic’s user device—e.g., 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, ¶106 (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-Rakic’s “other” destination applications are separate from (and in communication with) the user device’s MMS User Agent application. EX-1003, ¶107 (citing EX-1004, 14, 54; EX-1028, 732-733); *supra* §VII.C.3. 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, ¶108. 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 are “a plurality of software components,” as claimed. EX-1003, ¶108 (citing EX-1046, 46).

The ’564 specification does not use the term “executing process” or discuss “respective executing processes for a plurality of software components.” EX-1003, ¶109. However, POSAs understood that TS-23.140’s forwarding of application data to destination applications constitutes communications with “respective executing processes for a plurality of software components,” 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. *Id.*; 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, ¶110. POSAs thus understood that MMS-Rakic’s User Agent, which forwards application-specific data to various destination applications, communicates with “respective” “processes for a plurality of software components.” EX-1003, ¶110. POSAs further understood that each respective process for MMS-Rakic’s destination applications is “executing” on TS-23.140’s device, as claimed, because they are software applications that run on TS-23.140’s UE/device to perform the applications’ respective functions. *Id.* (citing EX-1045, 126; EX-1046, 46).

iii. “an inter-process software communication bus providing secure communication between...”

Element [1B1] requires “an inter-process software communication bus providing secure communication between” the claimed “device link agent” (*supra* §VII.D.1.c.i) and “processes for a plurality of software components” (*supra* §VII.D.1.c.ii). The specification describes an “agent communication bus” implemented “as an *inter-process software communication bus*,” which may 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).”

EX-1001, 43:21-31.

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 UE/device over *some* interface. EX-1004, 14, 54-56; *supra* §VII.C.3. 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 analysis (EX-1022, 18-32; EX-1023)—that POSAs “understood that [TS-23.140’s] destination applications would have been communicatively coupled to the MMS User Agent by ‘an agent communication bus,’ ...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, 43:24-31. Thus, POSAs understood MMS-Rakic includes “an inter-process software communication bus providing... communication between” the MMS User Agent (“device link agent”) and the one or more processes of the destination applications (“respective... processes”). EX-1003, ¶¶111-112. *See also* EX-1001, 42:14-43:44.

Separately, as discussed *supra* §VII.C.3, it also would have been obvious to implement the interface between MMS-Rakic’s User Agent application and the respective processes of the user device’s destination applications using a software *bus* for interprocess communications—e.g. a “D-bus.” EX-1003, ¶113; EX-1031,

10:56-62; *see* EX-1022, 48-49 (agreeing software bus for interprocess communications was obvious); EX-1023. For this alternative reason, MMS-Rakic includes an *inter-process software communication bus*.

MMS-Rakic's "*bus*" provides "*secure*" communication between an "executing device link agent and respective executing processes for a plurality of software components" because access to MMS-Rakic's bus is only allowed for software components identified by access authorization information received from a secure server, as discussed *infra* §VII.D.1.d. EX-1003, ¶114.

- d. **[1B2] wherein providing secure communication comprises receiving access authorization information from a secure server, and allowing access to the bus only for software components identified by the access authorization information; and**

The '564 specification only mentions "access authorization" once, when describing a "message... security framework technique[]... which *only allows access to the agents that are on the secure authorization list* and in which the list is provided by the secure server and *signatures are provided by the secure server[.]*" EX-1001, 42:59-43:8. The specification does not define any requirements for the "secure server." *See* EX-1001, 42:59-43:17; EX-1003, ¶115.

In MMS-Rakic, "providing secure communication comprises receiving access authorization information from a secure server," as claimed. EX-1003, ¶116. MMS-Rakic'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, ¶116 (citing EX-1004, 56, 60, 69, 72-73, 111; describing “MM1-Retrieve.RES”). The “application identifier” is the identifier that allows MMS-Rakic’s User Agent to “immediately route[]” a received application-specific message to the corresponding one of the “executing processes for a plurality of software components.” EX-1004, 56; EX-1003, ¶116.

MMS-Rakic’s VAS Application incorporates the secure push message signing functionality of Rakic’s “*secure* push message server.” *Supra* §VII.C.4. To prepare a message comprising application-specific data for sending to a destination application, MMS-Rakic’s VAS Application generates a key by creating a hash of its administrator code and the destination application’s identifier. EX-1003, ¶117; EX-1007, [0041]-[0042], [0048], [0059], [0066]-[0068], [0070]-[0071], [0080], [0085]. After the key is generated, MMS-Rakic’s VAS Application uses the key to sign the message and generate a signature that is appended to the message. EX-1007, [0040], [0049], [0067], [0079], [0105], Fig. 8; EX-1003, ¶118. As discussed *supra* §VII.A and further *infra* in §§VII.D.1.g-VII.D.1.h, MMS-Rakic’s VAS Application then sends the signed message, via the Relay/Server, to the User Agent of the UE/device on which the destination application resides. EX-1003, ¶118; EX-1007, [0049]-[0050], [0107]; EX-1004, 14, 17-18, 21, 23-25, 41. MMS-Rakic’s VAS

Application is a “secure server” as claimed because it incorporates the functionality of Rakic’s “*secure* push message *server*” and because TS-23.140 discloses that communications with it (over MM7) are secured, e.g., using TLS (EX-1004, 41). EX-1003, ¶118.

The User Agent (“device link agent”) of MMS-Rakic’s UE/device thus receives a message comprising an application identifier and a signature (collectively, “access authorization information”) from the VAS Application (“secure server”) which meets [1B2]’s “receiving access authorization information from a secure server” requirement because the User Agent is an end-point of MMS-Rakic’s inter-process software communication bus, over which application-specific data received from the network is “transported without alteration” (EX-1004, 14) to a destination application on the device. EX-1003, ¶119.

Moreover, in MMS-Rakic, “access to the bus” is “allow[ed]... only for software components identified by the access authorization information,” as claimed. EX-1003, ¶120. MMS-Rakic’s User Agent incorporates the signature validation functionality of Rakic’s secure push message client. *Supra* §VII.C.4. After receiving the signed message, MMS-Rakic’s User Agent generates a key by creating a hash of the administrator code (which was previously provisioned during destination application registration) and the destination application’s identifier. EX-1003, ¶120; EX-1007, [0110]-[0111]. After the key is generated, MMS-Rakic’s User

Agent signs the data block of the message with the key and compares the resulting signature to the signature of the message. EX-1003, ¶120; EX-1007, [0112]. ***If the signatures match***, the message is deemed valid and routed by MMS-Rakic’s User Agent to the identified destination application. EX-1003, ¶120; EX-1007, [0112]-[0119], [0122], [0131]; EX-1004, 54-56.

MMS-Rakic’s User Agent (“device link agent”) thus routes the message to the destination application (“software component”) over MMS-Rakic’s bus (*supra* §VII.D.1.c.iii) ***only if the signature*** (which, as discussed, is generated using the identifier that identifies the destination application) ***is valid***. EX-1003, ¶121. This meets [1B2]’s “allowing access to the bus only for software components identified by the access authorization information” requirement because the User Agent is an end-point of MMS-Rakic’s inter-process software communication bus, over which application-specific data received from the network is “transported without alteration” (EX-1004, 14) to a destination application on the device. EX-1003, ¶121.

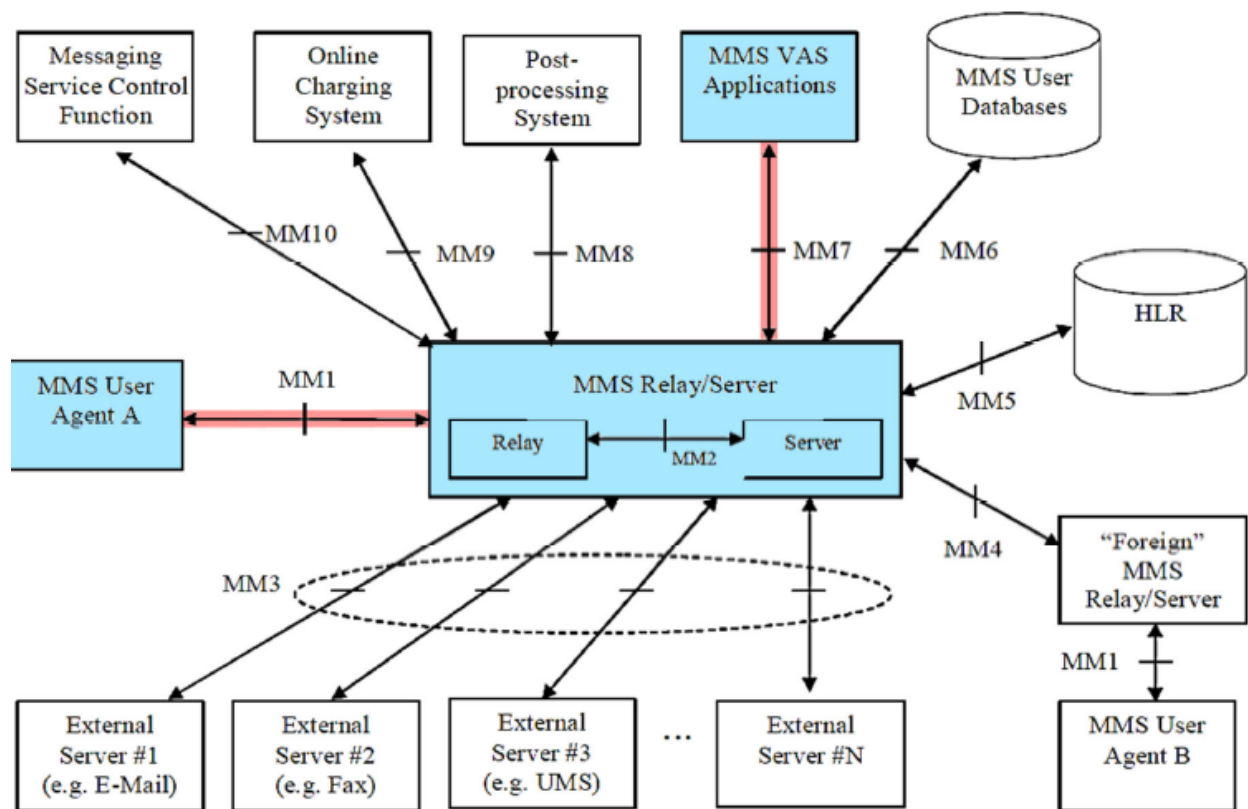
e. [1C] the device link agent, configured to

MMS-Rakic’s User Agent is a “device link agent” implemented to incorporate the signature validation functionality of Rakic’s secure push message client. *Supra* §VII.D.1.c.i. As explained below, MMS-Rakic’s User Agent is configured to perform elements [1D1]-[1F].

f. [1D1] maintain a secure message link through the wireless network and an Internet network to a message link server,

While the specification never describes a “message link server,” it describes “service control *server link* 1638,” which “provides the network side of a system for transmission and reception of service agent” messages and a “*secure* mechanism for transmitting and receiving” “information between the device agents... and other network elements[.]” EX-1001, 69:16-56. Based on the claim’s plain language, “*message link server*” includes a *server* with a *link* to the claimed device link agent, over which *messages* (e.g., between a device and another network element) are relayed. EX-1003, ¶¶122-123; EX-1001, 16:13-16, 69:16-65.

As discussed *supra* §VII.A, TS-23.140’s Relay/Server relays messages between a UE/device’s User Agent and VAS Applications using various communication interfaces between the Relay/Server and other elements in the MMSE—e.g., MM1 (EX-1004, 17-18, 21, 23-25) for communications between a User Agent and Relay/Server (*id.*, 23-24, FIG. 4), and MM7 for communications between the Relay/Server and VAS Applications (*id.*, 14, 18, 23-26, 41). The path of messages between the VAS Applications and User Agent—through the Relay/Server—is annotated red below:



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

Because MMS-Rakic’s Relay/Server is a *server* that relays *messages* (e.g., between a device and another network element) to the User Agent over *link* MMI, it is a “*message link server*,” as claimed. EX-1003, ¶124.

Element [IDI] also requires “a secure message link” between the “device link agent” and the “message link server.” The ’564 specification does not use the term “secure message link,” or require the connection between the “message link server” and the “device link agent” to be secured in any particular way—instead leaving to POSAs precisely how such a link would be secured. EX-1001, 69:25-34; Fig. 16; EX-1003, ¶125. The specification describes, e.g., using “*secure transport protocols*

running over Transmission Control Protocol (TCP),” and notes that “approaches for implementing a secure control channel over the Internet includ[e]... running TCP Transport Layer Security (TLS).” EX-1001, 16:66-17:22; *see also id.*, 89:29-36; EX-1003, ¶125. The specification uses “TLS” and Secure Socket Layer (SSL) interchangeably. *E.g.*, EX-1001, 95:54; EX-1003, ¶125. In MMS-Rakic, the User Agent (the claimed “device link agent”) communicates with the Relay/Server (the claimed “message link server”) over interface MM1. *Supra* §VII.D.1.c.i. And MM1 is secured using SSL/TLS. *Supra* §VII.C.2. MMS-Rakic’s MM1 is thus a “secure message link” between the User Agent and Relay/Server, as claimed. EX-1003, ¶126.

Element [1D1] also requires the claimed “device link agent” (MMS-Rakic’s User Agent) to “*maintain*” the “secure message link.” The ’564 specification leaves to POSAs precisely how a “device link agent” “*maintain[s]* a secure message link,” saying only that the “the service control device link 1691 *provides the device side of a system for transmission and reception of service agent to/from network element functions.*” EX-1001, 38:5-8. MMS-Rakic’s User Agent provides the device side of MMS-Rakic’s system for transmitting/receiving messages on behalf of destination applications to/from VAS Applications—which *includes* MM1 between the User Agent and Relay/Server. EX-1003, ¶127. MMS-Rakic’s User

Agent thus “maintain[s] a secure message link” to the Relay/Server in the same way the specification discloses. *Id.*

Element [1D1] further requires that the “secure message link” be maintained “***through the wireless network and an Internet network.***”

As discussed *supra* §VII.D.1.b, MMS-Rakic’s User Agent communicates with the Relay/Server over the MM1 interface through a “wireless network” (e.g., a 2G or 3G mobile network). In TS-23.140, “multimedia messaging may encompass many different network types[,]” and “***connectivity*** between these different networks shall be 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.***” EX-1004, 17, 18 (“MMS connectivity across different ***networks*** (MMSEs) is provided based on ***Internet*** protocols.”). POSAs thus understood that each of TS-23.140’s wireless ***networks*** (e.g., 3G Mobile Network A), which must be communicated over via the “***Internet protocol*** and its associated set of messaging protocols,” is also “an Internet network.” EX-1003, ¶128. Thus, MMS-Rakic’s “secure” MM1 interface is also “maintain[ed]... through” “an Internet network to” the Relay/Server (“a message link server”). *Id.*

TS-23.140 further teaches a “secure message link” that is “maintain[ed]” “through” “an Internet network” that is ***separate*** from “the wireless network.” EX-

1003, ¶129. TS-23.140 says the “[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 the ways in which communications are facilitated over such networks or what “network types” the MMS “architecture... shall ***combine***.” E.g., EX-1004, 16-17, 23-24. POSAs understood, based on these disclosures, that TS-23.140 discloses scenarios in which a user device’s MM1 interface encompasses multiple different networks that have been combined to communicate with MMS-Rakic’s Relay/Server—e.g., the wireless network of element [1A] ***and*** a separate network that also uses Internet protocol, as TS-23.140 teaches (EX-1004, 16-17). EX-1003, ¶129. For such an implementation of MM1, encompassing a “combine[d] different networks” as TS-23.140 teaches (EX-1004, 16-17), the “secure message link” (MM1) is “maintain[ed]” by the User Agent “through the wireless network” of [1A] and a separate “Internet network.” EX-1003, ¶129.

Moreover, implementing MMS-Rakic’s User Agent device to be able to connect to the Relay/Server through both a wireless network and an Internet network would have been obvious. EX-1003, ¶130. It was well-documented to implement, and POSAs would have reasonably expected success implementing, a mobile user

device to connect to a *wireless* local area network connected to the Internet to allow the device to communicate with a remote server. *E.g.*, Cole (EX- 1006), [0031]-[0035], FIG. 1 (mobile device 110 connects to remote server 195 through public network 170, which may be the “Internet”). POSAs understood that such an implementation of MMS-Rakic—e.g., where a User Agent’s device is implemented to connect to a WLAN which connects to the Internet to allow the device to communicate with the Relay/Server—would have desirably provided an additional access path to the Relay/Server using existing IP-based MMS protocols, thereby improving accessibility to MMS in environments where 2G/3G cellular coverage was weak, unavailable, or costly—resulting in increased user flexibility and connectivity for MMS services. EX-1003, ¶130.

g. [1D2] the message link server operating a message service that receives messages over a network from a plurality of network functions,

The ’564 specification never describes a “message service” or what it means for a “message link server” to “operat[e]” one. EX-1003, ¶131. Based on the claim’s plain language, POSAs understood “operating a message service” to include a service that facilitates receipt and transmission of messages over a network by [1C]’s device link agent. *Id.*; *see also* EX-1001, 69:34-37.

MMS-Rakic’s Relay/Server (“message link server”) operates a message service. As discussed *supra* §§VII.A, VII.D.1.d, and VII.D.1.f, MMS-Rakic’s

Relay/Server relays signed messages between MMS-Rakic's User Agent ("device link agent") and, e.g., VAS Applications. EX-1004, 14, 17-18, 21, 23-26, 41, FIG. 3; EX-1003, ¶132.

As discussed below, MMS-Rakic's VAS Applications comprise "network functions" which send messages to MMS-Rakic's User Agent. EX-1003, ¶¶132-133. The '564 specification uses "network function" to encompass any network element that provides some function (e.g. to another network element or to a user) over the network. EX-1003, ¶133; EX-1001, 80:12-20; *see also id.*, 38:5-8, 69:34-37, 79:44-46. MMS-Rakic's VAS Applications are "network elements" that provide a function over the MMSE network. EX-1003, ¶134.

FIG. 2 (below) shows TS-23.140's MMSE which includes "***a collection of MMS-specific network elements***" communicating with one another:

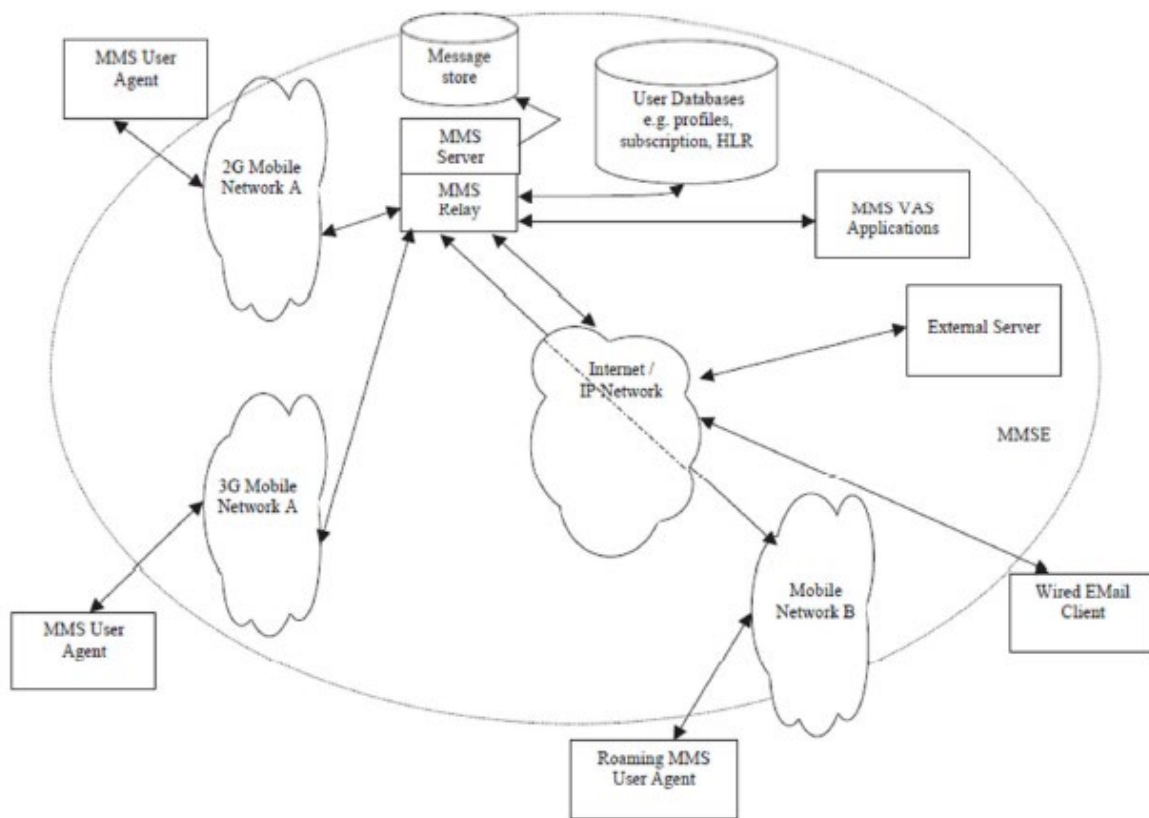


Figure 2: MMS Architectural Elements

EX-1004, 17, FIG. 2

VAS Applications provide various functions “to MMS users” over the MMSE network—e.g., “Value Added Services (e.g. news service or weather forecasts).” EX-1004, 14, 23. As discussed *supra* §VII.D.1.c.i, VAS Applications transport application-specific data sent in “abstract messages” to destination applications on UE/devices via the Relay/Server and each UE/device’s respective User Agent. EX-1004, 14 (describing “abstract messages”), 19, 23-24, 30-31, 35-36, 41, 54-56 (discussing using “abstract messages” to “transport application data”); EX-1003,

¶134. “There could be *several* MMS VAS Applications included in or connected to an MMSE.” EX-1004, 18.

Because MMS-Rakic’s VAS Applications are network elements that provide value added services over the MMSE to destination applications, MMS-Rakic’s VAS Applications constitute “a plurality of network functions.” EX-1003, ¶135. As discussed, MMS-Rakic’s Relay/Server receives messages from the VAS Applications over MM7 within the MMSE network. *Id.* MMS-Rakic’s Relay/Server (“message link server”) thus “operat[es] a message service” that “receives messages over a network” from a “plurality of network functions” (the VAS Applications), as claimed. *Id.*

h. [1E]

i. receive secure messages from the message link server over the secure message link

As discussed *supra* §VII.D.1.f, MMS-Rakic’s User Agent (“device link agent”) maintains interface MM1 (“secure message link”) to the MMS Relay/Server (“message link server”)—over which MMS-Rakic’s User Agent receives messages, as discussed *supra* §VII.D.1.c.i. Such messages received over MM1 are “secure[d]” at least using SSL/TLS, because MMS-Rakic’s MM1 between is secured using SSL/TLS (*supra* §VII.C.2). They are also signed, in view of Rakic’s teachings (*supra* §VII.C.4). MMS-Rakic’s User Agent thus “receive[s] secure messages from the message link server over the secure message link.”

Rakic also discloses its signed messages—which in MMS-Rakic are received from the Relay/Server over interface MM1 (*supra* §VII.D.1.d, VII.D.1.g)—being encrypted. *Supra* §VII.B; *infra* §VII.D.7; EX-1007, [0075] (disclosing messages secured using “a combination of generating a signature ***and encrypting the data***” in the payload), [0078]; EX-1003, ¶¶136-138. POSAs understood that such messages received “from the message link server over the secure message link” in MMS-Rakic—e.g., those “encrypted” as Rakic contemplates, in addition to being secured by virtue of applying SSL/TLS to MM1 and signed in view of Rakic—were secure for this additional reason. EX-1003, ¶138.

ii. the received messages identified for delivery to multiple ones of the software components, and

In MMS-Rakic, MMS is “used to transport data specific to applicationss” on the user device that are not the MMS User Agent. EX-1004, 54-56; EX-1003, ¶139 (citing EX-1028, 732-733); *supra* §§VII.D.1.c.i, VII.A. MMS-Rakic’s destination “applicationss” are “***multiple***... software components.” *See supra* §VII.D.1.c.ii.

The messages received by MMS-Rakic’s User Agent are “abstract messages” comprising access authorization information including a signature and an “application identifier of the destination application” that allows the User Agent to “immediately route[]” each message to the one “destination application” (of the device’s multiple) “referred to from the destination application identifier.” EX-1004, 56; *supra* §VII.D.1.d; EX-1003, ¶140. Because MMS is used in MMS-Rakic to

transport data specific to applications—and because this routing for each message takes place using an application identifier “present in [each] abstract message” (EX-1004, 55) sent by the Relay/Server to the User Agent—POSAs understood that “the received messages [are] identified for delivery to multiple ones of the software components.” EX-1003, ¶140.

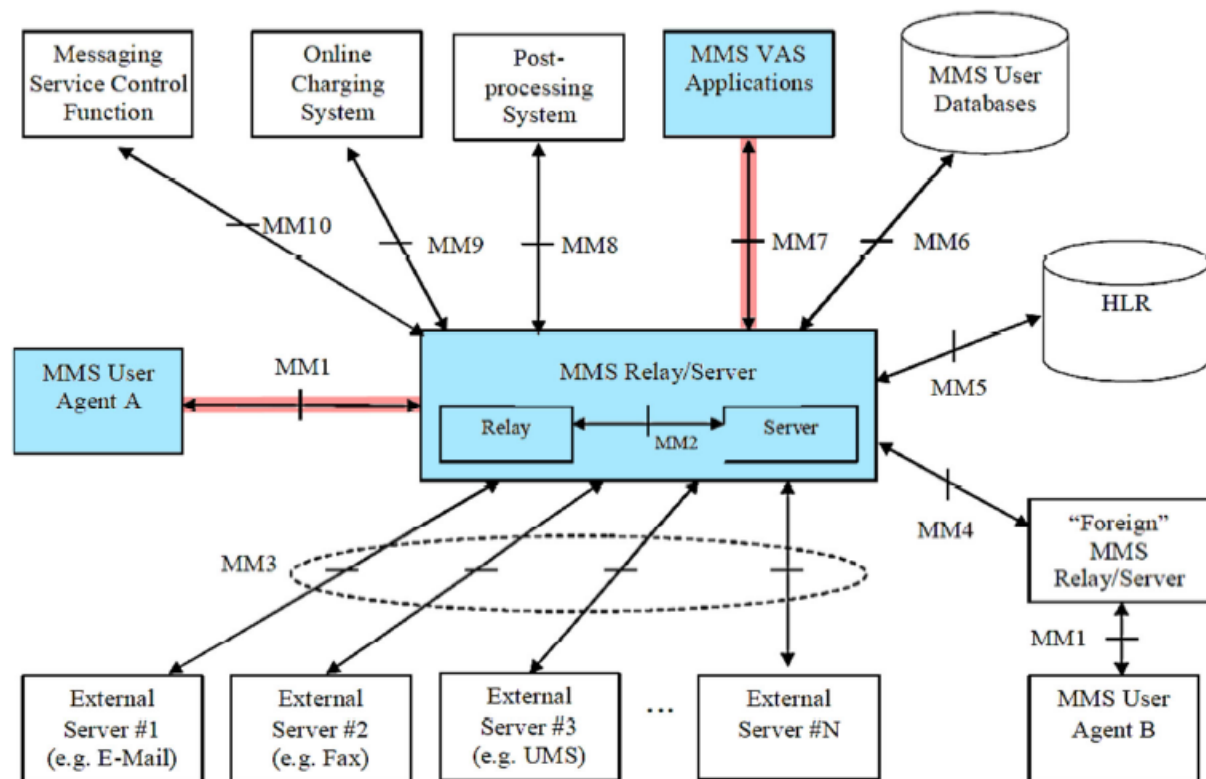
iii. including message content received by the message link server from multiple ones of the network functions, and

As discussed *supra* §§VII.D.1.c.i-VII.D.1.c.ii, MMS-Rakic’s secure messages (including the “abstract messages” discussed *supra* §§VII.D.1.c.i, VII.D.1.d, VII.D.1.g) are “used to transport data specific to applications” other than the MMS User Agent. EX-1004, 54-56; EX-1003, ¶141 (citing EX-1028, 732-733); *supra* §VII.A. TS-23.140 states that such “Application Data may be of any **content** type[.]” EX-1004, 14, 54-56 (disclosing “transporting” such “Application Data” in “abstract messages”).

TS-23.140 also discloses that “abstract messages” sent by VAS Applications for delivery by the Relay/Server to the User Agent include “content.” EX-1003, ¶142 (citing EX-1004, 69-70, 112-113, explaining that MM1_retrieve.RES and MM7_submit.REQ messages include content for delivery to the MMS User Agent). POSAs thus understood that TS-23.140’s application-specific “application data”—transported in MMS-Rakic’s abstract messages to specific applications “without

alteration” (EX-1004, 14, 54-56)—constitute “*message content*” as claimed. EX-1003, ¶142.

POSAs further understood that abstract messages (with “message content”) received by MMS-Rakic’s User Agent (“device link agent”) are “received by the” Relay/Server (“message link server”) “from multiple ones of the” VAS Applications (“network functions”), as claimed. EX-1003, ¶143. In MMS-Rakic, messages containing application data (including the “abstract messages” discussed *supra* §§VII.D.1.c.i, VII.D.1.d, VII.D.1.g) include data from various VAS Applications. EX-1004, 14, 18, 23, 41 (“The MMS Relay/Server may support services... provided... by third-party [VASPs].... Messages originated from the VASP may be targeted to the recipient...”), 54-56; EX-1003, ¶144. These messages contain “application data” used to “provid[e] Value Added Services (e.g. news service or weather forecasts) to MMS users.” EX-1004, 14, 41; EX-1003, ¶144; *supra* §VII.A. The path of such application data is annotated red below:



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

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

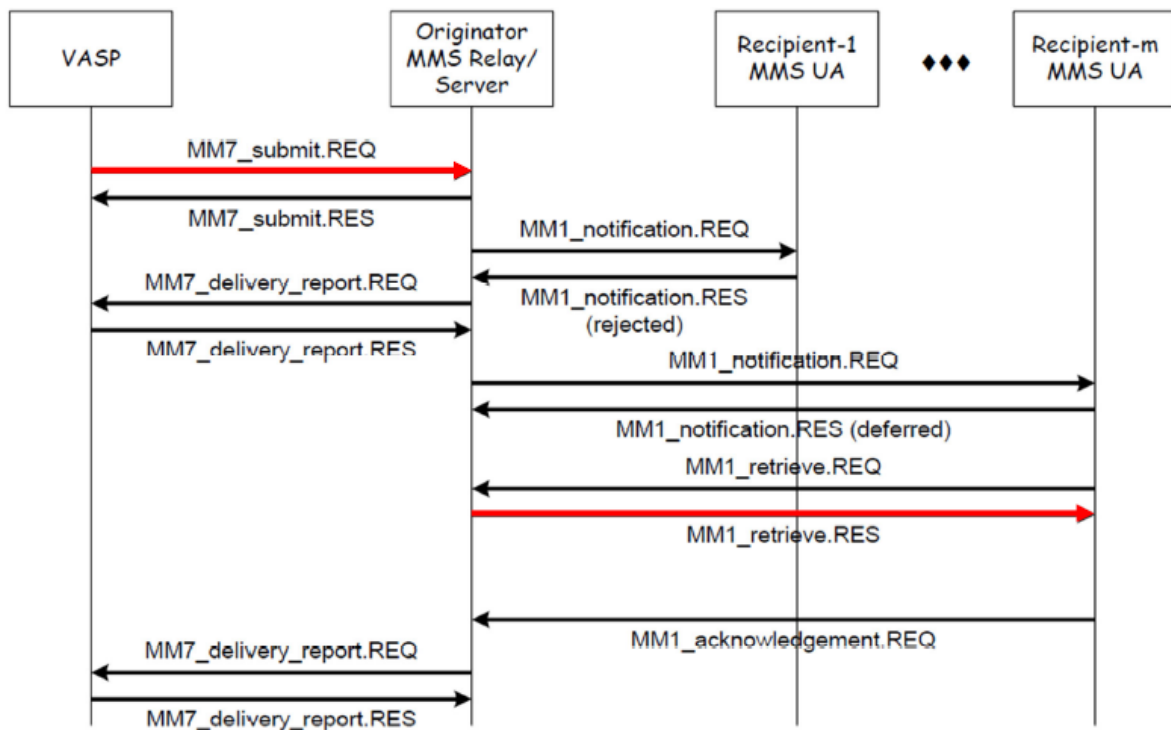


Figure 8. Sample data flow of MM7 message distribution

EX-1004, 111, FIG. 8 (annotated)

See also EX-1004, 111-116 (describing VASP-added “Content” and “Applic-1D... 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-1D” in MM1_retrieve.RES); EX-1003, ¶144. 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.

- i. **[1F] for software components identified by the access authorization information, route messages identified for delivery to a given one of those software components via the inter-process software communication bus to a software process corresponding to the given software component.**

In IPR2024-00341, relying on the teachings of TS 23.140, the Board found that the prior art disclosed substantially the same limitation in the '733 Patent. EX-1022, 39-40, §II.D.3(m); EX-1023; EX-1003, ¶145.

MMS-Rakic's User Agent "transport[s]" application-specific messages (including the "abstract messages" discussed *supra* §VII.D.1.h) by "***routing***"—"without alteration"—"received MMS information on to the destination application that ***is referred to by the destination application identifier***" included in the received messages. EX-1004, 14, 55-56; EX-1003, ¶146. As discussed *supra* §§VII.C.3 and VII.D.1.c.iii, these messages are routed over "an inter-process software communication bus providing secure communication between" MMS-Rakic's User Agent and the one or more processes (discussed *supra* §VII.D.1.c.ii) of the destination applications.

POSAs understood that the "messages [are] identified for delivery to a given one of those" destination applications ("software components"), because MMS-Rakic's User Agent routes each message to the application "***referred to***" (EX-1004, 54) by the application identifier. EX-1003, ¶147. POSAs thus understood that, for "messages identified for delivery to a given one of those software components"

(including each abstract message discussed *supra* §VII.D.1.h), MMS-Rakic’s User Agent (“*device link agent*,” *supra* §VII.D.1.c.i), “*route[s]*” the “messages” to a software process of the identified destination application (“*to a software process corresponding to the given software component*”) “via the inter-process software communication bus.” EX-1003, ¶147.

POSAs also understood MMS-Rakic’s User Agent only “route[s] messages” “for software components identified by the access authorization information.” As discussed *supra* §VII.D.1.d, MMS-Rakic’s User Agent only routes received messages to the identified destination application over MMS-Rakic’s bus if the signature (generated using the identifier that identifies the destination application) is deemed valid. EX-1007, [0112]-[0119], [0122], [0131]; EX-1004, 54-56; EX-1003, ¶148.

2. Claim 2

MMS-Rakic’s “access authorization information” (*supra* §§VII.D.1.d, VII.C.4)—which is “provided by the secure server for a given one of the software components”—“*comprises*” MMS-Rakic’s “*signature*,” meeting claim 2. EX-1003, ¶149.

3. Claim 3

Claim 3 requires claim 1’s “software components” to “include” a “first” and “second” “device component” that respectively “receive[] message content” in

different “format[s.]” TS-23.140 discloses “support[ing]” various data “formats.” EX-1004, 20; EX-1003, ¶150 (citing EX-1020). POSAs understood MMS-Rakic’s applications (“chess,” “weather”) comprise “components” on the “device” and would have implemented MMS-Rakic to desirably receive data in different formats specific to those applications, and reasonably expected success. EX-1003, ¶150 (discussing obviousness).

4. Claim 4

Claim 4 requires that claim 3’s “first format comprises a notification message,” and that the “first device component” is “a user service interface agent configured to display the notification message on” a “user interface.”

TS-23.140’s functional disclosures confirm the presence of a user interface in TS-23.140’s UE/device—e.g., “MM *presentation*” (where the MM is “*displayed* to the end user”) and “*presentation* of notifications to the user,” e.g., in an “manual” “retrieval mode[],” where “the end user” is “*made aware* of the MM notification and... *allowed to make a decision* whether to download the MM[.]” EX-1004, 19-20; EX-1003, ¶¶151-152. Moreover, every depiction of a device comprising a User Agent in TS-23.140 comprises a user interface. EX-1004, 16 (Figure 1, showing displays/keyboards/keypads), 155-160 (Figures A.1-A.8, showing touchscreens/styluses), 173 (Figure E.1).

User interfaces on devices to facilitate content presentation was well-documented. *E.g.*, EX-1007, [0052] (“client device” with display “provid[ing] visual information to the user” and control buttons “permit[ting]... user... interact[ion]”); *supra* §VII.B. POSAs thus understood TS-23.140’s UE/device includes a “user interface.” EX-1003, ¶153. Alternatively, such an implementation would have been an obvious way to implement what TS-23.140 describes, and is nothing more than utilizing familiar, known components (a UE/device with a user interface on, e.g., a display) to achieve a predictable result of facilitating content-presentation to a user. *KSR*, 550 U.S. at 416; EX-1003, ¶153.

TS-23.140 also discloses a destination application receiving “notification” messages, e.g., a MM1_notification.REQ abstract message with a “destination application identifier” that is sent to the User Agent to notify the destination application of an incoming MM (which may later be sent in a MM1_retrieve.RES abstract message). EX-1004, 56, 60, 61, 66-68, 69-71. Upon receiving such a MM1_notification.REQ message with a “destination application identifier,” “the MMS User Agent... *immediately route[s]*” it “to the [identified] destination application... without presentation to the user.” EX-1004, 56; EX-1003, ¶154. TS-23.140 further discloses “manual” “retrieval of MMs,” where the “end user is *made aware* of the MM notification and is allowed to make a decision whether to download the MM or not.” EX-1004, 19-20. TS-23.140 thus contemplates scenarios

where the MMS User Agent routes a notification message intended for presentation to a user to a destination application without presenting it to the user. EX-1003, ¶155 (discussing EX-1004, 56, 66-68 and “MM1_notification.REQ”). POSAs understood that in such a scenario, the destination application that receives the notification message is responsible for presenting the notification message to the user using the user interface of TS-23.140’s UE/device. EX-1003, ¶155.

Such a destination application in MMS-Rakic (which receives a MM1_notification.REQ message and displays the notification to a user, as described above) constitutes a “*user service interface agent* configured to display the notification message on the user interface,” as claimed. EX-1003, ¶156. The ’564 specification uses “user service interface agent” to include an agent that “provide[s] a service [and/or user] interface to users.” EX-1001, Fig 22B (“*User Interface Agent* 1697” “Provide[s] *service interface* to users.”); 66:35-36 (using “service interface” and “user interface” interchangeably); 96:39-42 (“communicates... user input to the user service interface agent”), 97:65-67 (“the user can be notified... via the user service interface agent”); EX-1003, ¶156. And each destination application in MMS-Rakic described above (1) is an *agent* because, as discussed *supra* §§VII.D.1.c.i and VII.D.1.c.ii, it is a component implemented in software that perform some function on behalf of an entity (e.g., client, server), (2) receives “Value Added *Services*” from VAS Applications (*supra* §VII.D.1.g), and (3) as

discussed above, presents the notification using MMS-Rakic's *user interface*, meeting claim 4. EX-1003, ¶156.

5. Claim 5

Claim 5 requires that claim 4's "user service interface agent" be "configured to obtain a user input as a response to [claim 4's] display of the notification message, and deliver the user input to an agent on the device."

For the "manual" MM retrieval mode discussed *supra* §VII.D.4, "the end user is made aware of" a "MM notification" and "***allowed to make a decision whether to download the MM...***" EX-1004, 19-20. TS-23.140 discloses the User Agent retrieving the MM from the Relay/Server by (1) responding to the MM1_notification.REQ message with a MM1_notification.RES message, and (2) requesting download of the MM by sending a MM1_retrieve.REQ message. EX-1004, 60, 66, 69. TS-23.140 also explains that "an application" on TS-23.140's UE/device "may trigger an MMS User Agent... to submit" such "abstract messages," where the User Agent "insert[s]" information "receive[d]... from the application" into an "abstract message" and sends it. EX-1004, 55; EX-1003, ¶¶157-158.

In the scenario discussed *supra* §VII.D.4, where the destination application is forwarded the MM1_notification.REQ message without presentation by the MMS User Agent, and is thus itself responsible for presenting the MM notification, POSAs

would have implemented (and reasonably expected success implementing) the destination application to (1) receive the user's decision whether to download the MM, and (2) trigger the User Agent to submit MM1_notification.RES/MM1_retrieve.REQ messages to the Relay/Server. EX-1003, ¶159. This was an efficient way to acquire/handle the user's decision, and consistent with TS-23.140's teachings. *Id.*

MMS-Rakic's User Agent is "an *agent* on the device." *Supra* §VII.D.1.c.i. Thus, the destination application that receives the MM1_notification.REQ message obtains the user's decision ("user input") in response to presenting the MM notification, and delivers it to "an agent on the device." EX-1003, ¶159.

6. Claim 6

The '564 specification says a "policy control agent" may "[t]ake[] policy instructions from the network" and "adapt[] device service policy settings." EX-1001, Fig. 22A, 48:31-38.

TS-23.140 discloses User Agents interfacing (through the Relay/Server) with MMS User Databases "contain[ing] user related information such as subscription and configuration" data, user profiles, access controls, server storage space, delivery rules, and UE/device capabilities. EX-1004, 18, 22-24; EX-1003, ¶¶160-161. Contemporaneous references confirm TS-23.140's UE/device routinely processed device setting/policy updates that were communicated (through push messages) by

the User Databases. EX-1003, ¶162; EX-1041, [0003]; EX-1042, [0032]; EX-1057, [0032]; EX-1058, [0043]; EX-1059, [0037]. POSAs thus understood TS-23.140 teaches a User Agent device comprising a hardware/software element (“policy control agent”) that receives and processes user-subscription/configuration information (“message content” in a “first format that contains service settings and/or configuration information”). EX-1003, ¶163.

TS-23.140 expressly says such user-subscription/configuration processing (e.g., “user profile management”) need not be performed by MMS User Agents. EX-1004, 19. POSAs thus would have recognized that implementing MMS-Rakic’s “policy control agent” as a separate, dedicated element that communicates with MMS-Rakic’s User Agent (“device link agent”) over MMS-Rakic’s “bus” was a reasonable, viable, and desirable option that would have simplified MMS-Rakic’s User Agent functionality, and met claim 6. EX-1003, ¶¶163-164.

7. Claim 7

Claim 7 requires “the received secure messages” to be “encrypted,” and “the device link agent” to be “configured to decrypt the received secure messages prior to delivering those messages to respective software processes.”

As discussed *supra* §VII.D.1.h.i, “received secure messages” are “secure[d]” using SSL/TLS (*supra* §VII.C.2), and signed and encrypted pursuant to Rakic’s teachings. EX-1007, [0075] (disclosing messages secured using “a combination of

generating a signature *and encrypting the data*” in the payload), [0078]; *supra* §VII.B. SSL/TLS is a form of encryption. EX-1003, ¶¶165-166. POSAs therefore understood that “the received secure messages are encrypted,” as claimed.

TS-23.140 discloses the MMS User Agent “provid[ing]... functionalities such as... decryption and encryption of an MM on an end-user to end-user basis.” EX-1004, 19; EX-1003, ¶167 (also citing EX-1004, 54-56). Decrypting received secure messages at the endpoint of MM1 in MMS-Rakic—MMS-Rakic’s User Agent—would have desirably facilitated the functionality discussed *supra* §VII.D.1.i—e.g., by allowing the device to decrypt the necessary information to validate and accurately route, within the device, the application data being transported by MMS-Rakic’s User Agent. EX-1003, ¶167. POSAs thus understood MMS-Rakic’s User Agent as being “configured to decrypt the received secure messages prior to delivering those messages to respective software processes,” as claimed. *Id.*

8. Claim 8

Claim 8 recites alternative transportation options for claim 1’s “messages,” including “encryption on a transport services stack.” As discussed *supra* §VII.D.1.c.i, in the specification, external communication with the component that “provid[es] the device side of a system for transmission and reception” of messages (“service control device link 1691”) occurs over “service control link 1653.” EX-1001, 38:5-8, 69:25-34. The specification describes including 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, 89:14-36. As discussed *supra* §VII.C.2, MMS-Rakic’s MM1 utilizes TLS. POSAs understood that, just as in the ’564 specification, MMS-Rakic’s use of TLS to secure MM1 between the User Agent and the 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, ¶168.

9. Claim 10

Claim 10 recites that the “device link agent” is “configured to receive” “upload messages” “from one or more of the authorized software components.” The “upload messages identify[] a corresponding” “network function[] to which” the “software component has requested delivery.” Claim 10 says the “device link agent transmit[s] the upload messages to the network message server over the secure message link, for delivery by the network message server to the respective identified network elements.”

“Network message server” has no antecedent basis; the only recited server the “device link agent maintain[s] a secure message link” to is claim 1’s “message link server.” EX-1003, ¶¶169-170. Likewise, “network elements” has no antecedent basis; the only element “identified” in the “upload messages” are “network functions.” EX-1003, ¶170. POSAs thus understood that Claim 10 at minimum

encompasses an interpretation where the recited “network message server” is claim 1’s “message link server,” and the recited “respective identified network elements” are the “corresponding... network functions” identified in claim 10’s “upload messages.” *Id.*

As discussed *supra* §§VII.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 User Agent application). EX-1004, 14, 54-55. As discussed *supra* §VII.D.1.d, MMS-Rakic’s User Agent receives, via the Relay/Server, a message from a VAS Application that contains “access authorization information”—comprising a signature and a destination application identifier—which the User Agent validates and uses for routing the message to the identified destination application over a bus. POSAs understood that such destination applications are “authorized software components,” because they are the destination applications identified in validated messages and thereby authorized to receive messages over MMS-Rakic’s bus. EX-1003, ¶171.

As discussed *supra* §§VII.D.1.h-VII.D.1.i, MMS-Rakic’s User Agent (“device link agent”) exchanges “secure messages” containing application-specific data with MMS-Rakic’s Relay/Server over the “secure message link” (MM1). 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, ¶172.

“[A]n application... trigger[s] an MMS User Agent... to submit” “abstract messages.” EX-1004, 55. “Upon” this “triggering,” the User Agent “insert[s]” information “receive[d]... from the application” into an “abstract message” and sends it. *Id.*; EX-1003, ¶173. Because the originating device application⁶ triggers the User Agent to send an abstract message that incorporates information provided by that application, POSAs understood that MMS-Rakic’s User Agent is “configured to receive” “upload messages” containing this information from claim 1’s “software components.” EX-1003, ¶173. POSAs understood that MMS-Rakic’s “upload messages” are then packaged as abstract messages comprising a destination application identifier and content for delivery to the VASP, and sent to the Relay/Server over MM1. EX-1003, ¶173 (citing EX-1004, 55, 62-63, 65, 116-118).

⁶ In the context of claim 1, this application is called the destination application to which application-specific data is transported, as discussed *supra* §VII.D.1.c.ii.

Claim 10 requires that “each of the upload messages identify[] a corresponding one of the network functions to which the device respective software component has requested delivery.” In MMS-Rakic, the “abstract message” sent to the Relay/Server “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, ¶179 (citing EX-1004, 63, 65, 117-118, explaining that both MM1_submit.REQ and MM7_deliver.REQ include the destination application identifier). POSAs therefore understood that the claimed “upload message” that MMS-Rakic’s User Agent receives from a destination application (and packages as an “abstract message” to send to the Relay/Server) includes information “identifying a corresponding one of the network functions” to which delivery of the message is requested—because that information allows the User Agent to include the destination application identifier that the VAS Application uses to route the message to the correct destination application. EX-1003, ¶180; EX-1004, 55-56.

Claim 10 requires that “the device link agent transmit[] the upload messages to the network message server over the secure message link, for delivery by the network message server to the respective identified network elements.” MMS-Rakic does this. TS-23.140 illustrates how information from a device application is transmitted to a VASP (via the MMS Relay/Server) using its MM1_submit.REQ and

MM7_deliver.REQ “abstract message” examples. EX-1004, 62, 116, 58, 189-190; EX-1003, ¶¶174-178. TS-23.140 discloses that after the Relay/Server receives an MM1_submit.REQ message from the User Agent, it sends an MM7_deliver.REQ message to the VAS Application. EX-1003, ¶181; EX-1004, 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[.]”), FIG. 9 (annotated below):

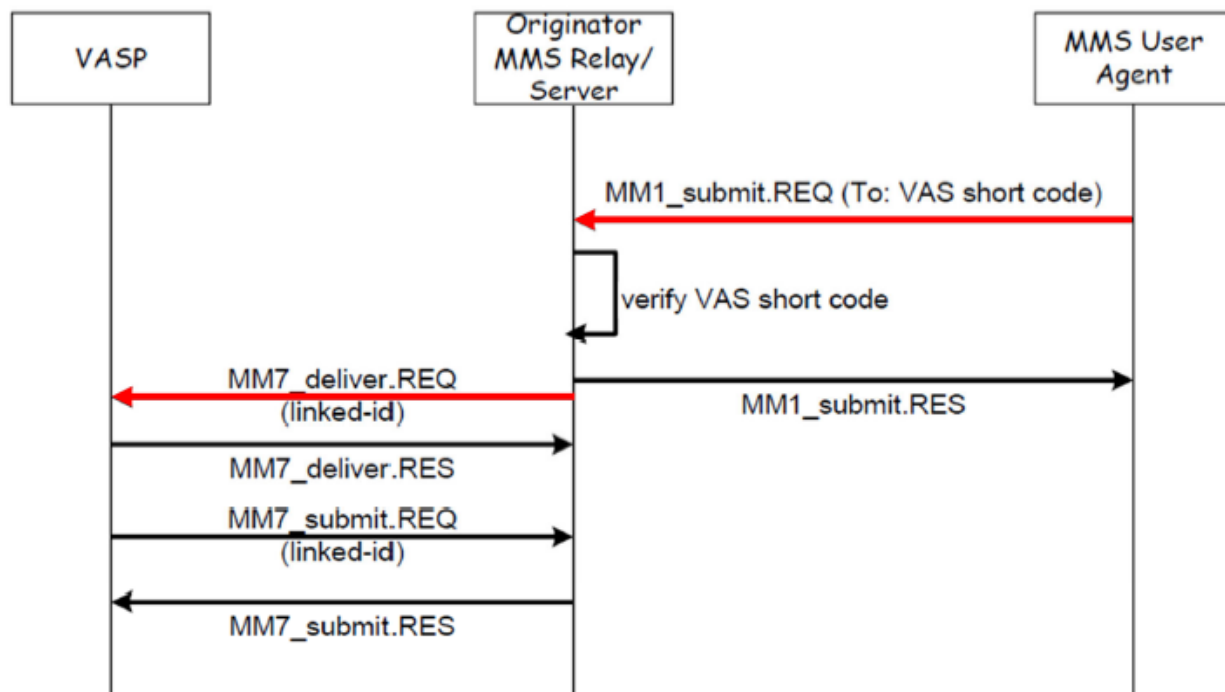


Figure 9: Use of MM7_deliver and subsequent response

EX-1004, 117, FIG. 9 (annotated)

MMS-Rakic's User Agent ("*device link agent*," *supra* §VII.D.1.c.i) thus "*transmit[s] the upload messages to the*" Relay/Server ("message link server," *supra* §VII.D.1.f, which claim 10's "*network message server*" encompasses) "*over the secure message link*" (MMS-Rakic's MM1, discussed *supra* §VII.D.1.f), "*for delivery by the*" Relay/Server "*to the respective identified*" VAS Applications ("network functions," *supra* §VII.D.1.g, which claim 10's "*network elements*" encompass). EX-1003, ¶182.

10. Claim 12

Claim 12 recites "at least one of the secure messages received from the network message server comprises multiple identifier/data pairs." As discussed *supra* §VII.D.9, "network message server" has no antecedent basis and at minimum encompasses claim 1's "message link server." EX-1003, ¶183.

The '564 specification does not describe a "secure message" that "comprises multiple identifier/*data* pairs." During prosecution of related U.S. Patent No.9,232,403, which shares a specification with the '564 Patent, PO identified Figure 25 as disclosing this limitation. EX-1060, 736. FIG. 25 (annotated below) shows a "service controller communication *frame*" comprising multiple identifier/*message* pairs (respectively blue, green). EX-1001, 91:11-63.

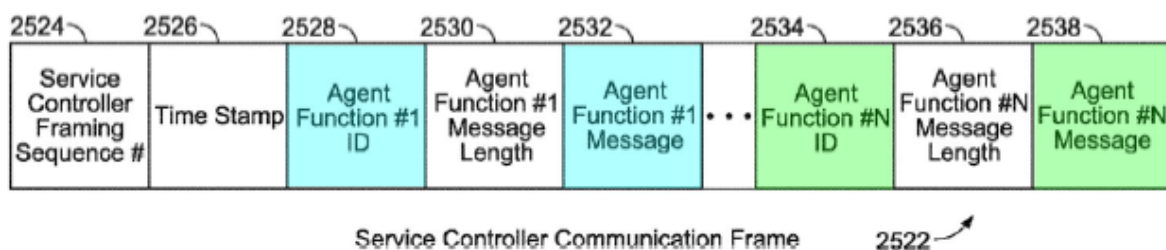


FIG. 25

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, 70:3-16. Claim 12’s “message[] compris[ing] multiple identifier/data pairs” thus encompasses a network message server that collects/buffers messages (each comprising an agent identifier and payload), and sends the collected messages to a “device messaging agent” as a group/frame of messages. EX-1003, ¶¶184-185.

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, ¶186. 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.h, 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 message[] received from the network message server compris[ing] multiple identifier/data pairs,” as claimed. EX-1003, ¶187.

Further, aggregating multiple messages in a single frame would have been obvious. POSAs had reason to implement MMS-Rakic such that its Relay/Server transmits multiple collected MMs to a User Agent in a frame. EX-1003, ¶188. TS-23.140 is part of a suite of well-known 3GPP specifications that define layered architecture and data transport mechanisms for MMS communications. *Id.* 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, ¶189 (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-Rakic’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, ¶190. Thus, implementing MMS-Rakic’s User Agent to receive a message (frame) containing “multiple ID/data pairs” was obvious. EX-1003, ¶191.

11. Claim 13

Claim 13 requires that claim 2’s “given one of the software components is identified by a secure unique identifier.” As discussed *supra* §§VII.D.1.d, VII.C.4, and VII.D.2, claim 2’s “given one of the software components” is “identified by... access authorization information” comprising a signature and a destination application identifier that identifies the destination application. The identifier *uniquely* identifies the destination application. EX-1004, 55 (describing ways to “guarantee... global uniqueness”). And, as discussed *supra* §§VII.C.4, VII.D.1.d, and VII.D.1.h.i, the destination application identifier is part of a secure message that is (1) signed by the signature, (2) encrypted per Rakic’s teachings, and (3) sent over MM1 which is secured using SSL/TLS (*supra* §VII.C.2). MMS-Rakic’s destination application is thus “identified by a *secure* unique identifier,” as claimed. EX-1003, ¶192.

12. Claim 14

Claim 14 recites a “method of operating a mobile end-user device” that recites steps corresponding to system limitations recited in claim 1. MMS-Rakic meets each

element of claim 14 for the same reasons discussed *supra* for the corresponding element in claim 1:

Claim 14 Elements	Corresponding Claim 1 Elements	Section
[14PRE]	[1PRE], [1A]	§§VII.D.1.a-b
[14A]	[1B2]	§VII.D.1.d
[14B1]	[1B1]	§VII.D.1.c
[14B2]	[1B2]	§VII.D.1.d
[14C1]	[1D1]	§VII.D.1.f
[14C2]	[1D2]	§VII.D.1.g
[14D]	[1E]	§VII.D.1.h
[14E]	[1F]	§VII.D.1.i

EX-1003, ¶193.

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.3). EX-1022, 40-41, 45, 48-49; EX-1023. Grounds 2A-2C expressly modify MMS-Rakic 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. EX-1003, ¶¶194-195.

A. GROUND 2A: MMS-Rakic in View of Cole (EX-1006)

It was well-documented to use a *modem* to enable communications over 2G/3G networks. *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).

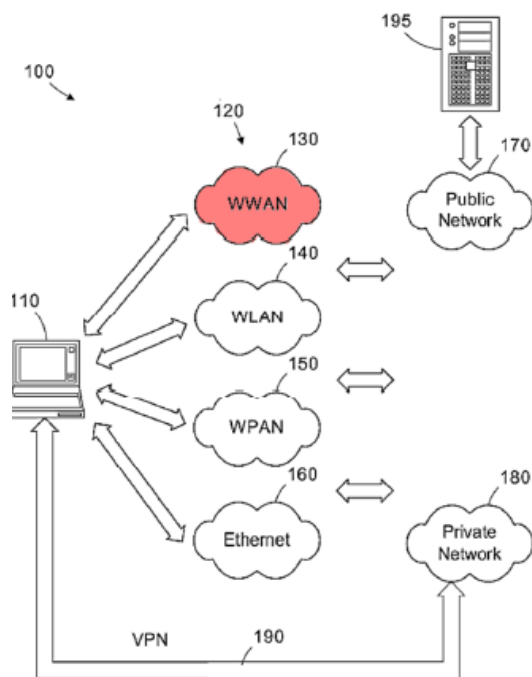


Figure 1

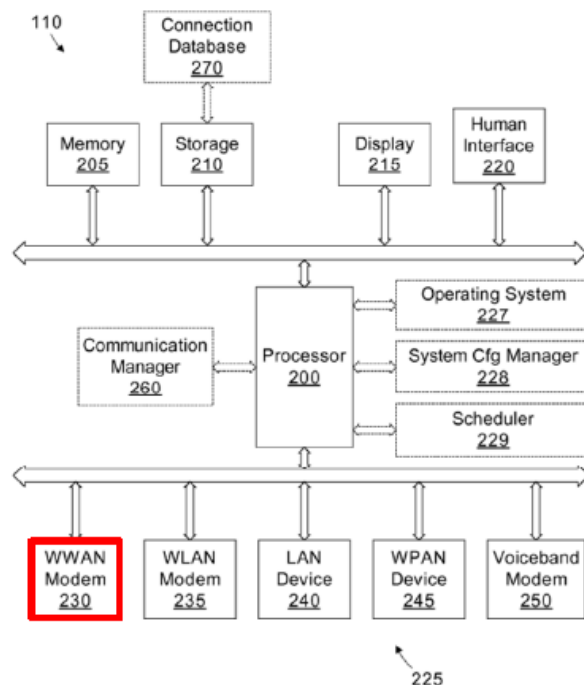


Figure 2

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, ¶¶196-198. This renders obvious claims 1-8, 10, and 12-14 for the same reasons respectively discussed *supra* §VII for MMS-Rakic.

B. GROUND 2B: MMS-Rakic 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.3; 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, ¶¶199-200. 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, ¶¶200-201 (citing EX-1048, [0001], [0003]-[0004], [0019]; EX-1049, 907; EX-1050, 2:64-3:6, 3:51-67, FIG. 5). This combination (“MMS-Rakic-Sathish”), with bus communications

secured as discussed *supra* §VII.C.4, renders obvious claims 1-8, 10, and 12-14 for the corresponding reasons discussed *supra* §VII for MMS-Rakic.

C. GROUND 2C: MMS-Rakic-Cole-Sathish

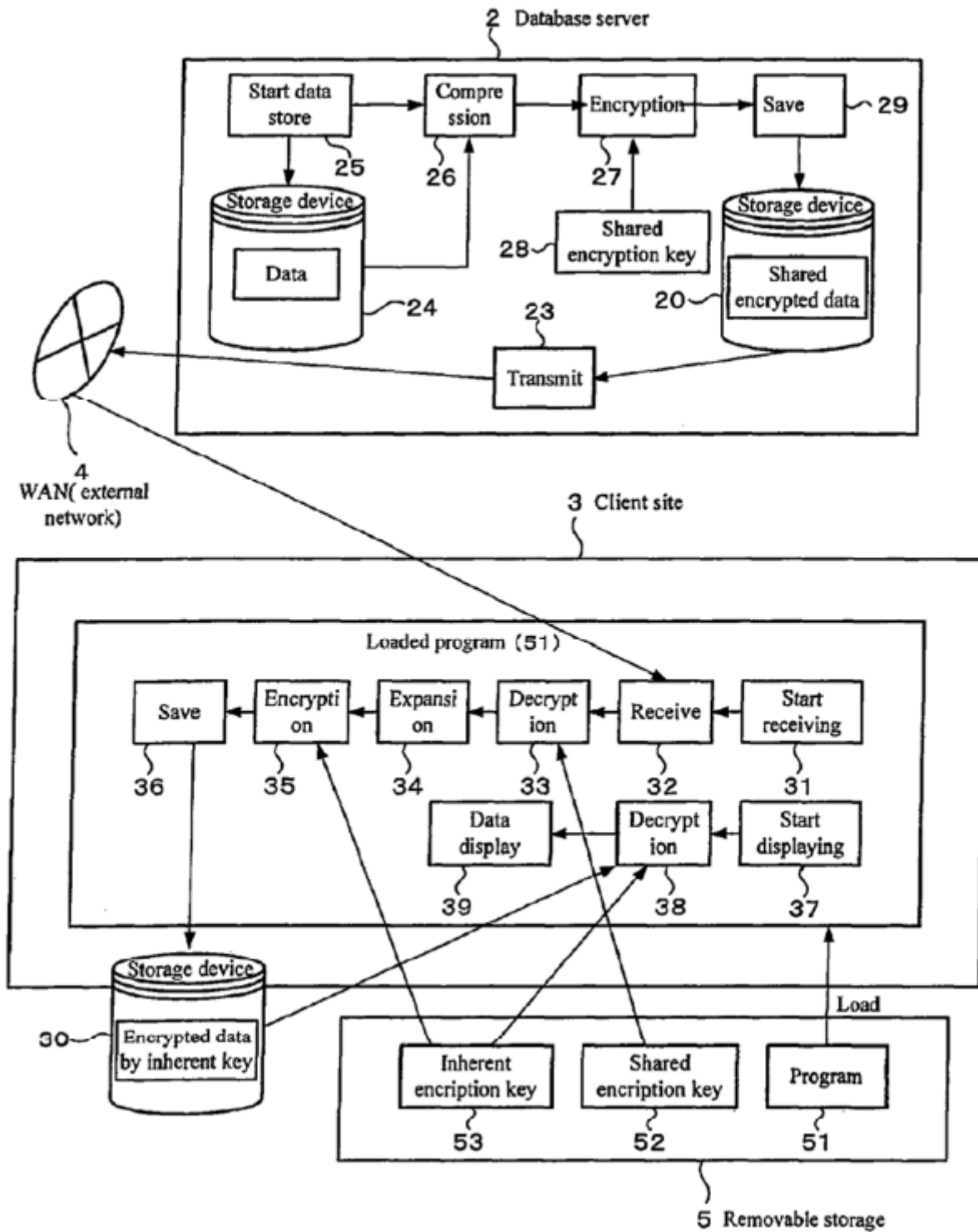
POSAs understood the modifications described *supra* §§VIII.A-VIII.B were compatible, and that it was feasible and desirable to implement MMS-Rakic’s device to incorporate the WWAN modem in view of Cole (for the reasons discussed *supra* §VIII.A) *and* a software interprocess communications bus in view of Sathish (for the reasons discussed *supra* §VIII.B). Such a combination (MMS-Rakic-Cole-Sathish) renders obvious claims 1-8, 10, and 12-14 for the corresponding reasons discussed *supra* §VII. EX-1003, ¶202.

IX. GROUNDS 3A-3D

To the extent claim 7’s “encrypt[ion]”-related requirements are not considered rendered obvious over MMS-Rakic, they are rendered obvious by incorporating Ogawa’s (EX-1005) teachings.

A. 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, ¶¶203-204.



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, ¶¶205-206 (citing EX-1010, 1:38-42).

Ogawa teaches *further* securing data using a “shared encryption key” used by client and server. EX-1005, 6:42-47, 7:11-21, 9:16-38. 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, 5:59-67; EX-1003, ¶¶207-209.

B. GROUND 3A: Implementing Ogawa’s Encryption Teachings

1. MMS-Rakic-Ogawa

a. Applying Ogawa’s Symmetric Encryption Techniques

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, ¶¶210-211 (citing EX-1004, 17, 25, 30, 41, 62; EX-1012, 21; EX-1005, 8:16-21). Moreover, Rakic discloses “perform[ing] a combination of generating a signature *and encrypting the data*” when securing messages. *Supra* §VII.B; EX-1007, [0075], [0078]. Neither TS-23.140 nor Rakic provides details regarding how to implement such encryption.

Implementing encryption for messages transmitted by a server to a client using shared-key encryption was well-documented in the prior art. EX-1003, ¶212 (citing EX-1005; EX-1007; 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, 3:61-4:4, 9:16-34, 3:44-53. EX-1003, ¶212.

POSAs had multiple reasons to implement Ogawa’s encryption techniques with MMS-Rakic’s system (“MMS-Rakic-Ogawa Message Encryption”):

First, implementing Ogawa’s encryption to MMS-Rakic’s system would have achieved “improved security” and “an end-user to end-user” security solution for MMS as TS-23.140 contemplates, and “a combination of generating a signature and encrypting the data” as Rakic contemplates. EX-1003, ¶¶213-214 (citing EX-1004, 19, 24-25; EX-1012, 21; EX-1007, [0075], [0078]).

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, ¶215 (citing EX-1027, [0002]-[0003], [0017], [0021]-[0022]; EX-1004, 54).

Third, implementing Ogawa’s encryption in MMS-Rakic’s system would have been nothing more than implementing known methods/techniques (encryption using a shared key as Ogawa teaches) to known systems/devices (the MMS Relay/Server and UE/device) to achieve predictable results (end-user-to-end-user encrypted data). *KSR*, 550 U.S. at 416; EX-1003, ¶216.

POSAs would have reasonably expected success implementing Ogawa’s encryption techniques to the TS-23.140 system given (1) the similar client-server architectures taught by the combined references and (2) TS-23.140’s and Rakic’s contemplation of end-user-to-end-user data encryption, of which Ogawa provides an exemplary, predictable implementation. EX-1003, ¶¶217-221. In IPR2024-00341, the Board agreed that implementing Ogawa’s encryption techniques “in message transmissions like those in TS-23.140” was obvious. *See infra* §IX.B.1.b.; EX-1003, ¶221.

b. Ogawa’s Decryption Unit

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...”); EX-1003, ¶222. POSAs would have been motivated to implement the decryption unit *as part of MMS-Rakic’s User Agent* application, because (1) the User Agent is responsible for receiving data from MMS-Rakic’s Relay/Server and distributing it

to the correct applications on the UE/device, and (2) TS-23.140 expressly identifies the User Agent as “provid[ing]... functionalities such as... *decryption*.” EX-1003, ¶222 (citing EX-1004, 19, 54-56). Such an implementation would have, e.g., beneficially allowed MMS-Rakic’s User Agent to decrypt an encrypted message from MMS-Rakic’s Relay/Server and any information identifying where it should be routed. EX-1003, ¶222.

POSAs would have reasonably expected success incorporating Ogawa’s decryption unit into MMS-Rakic’s User Agent application, because each prior art component would continue performing functions they performed prior to combining—User Agents and Relay/Server would continue to exchange data using secure communication links, including Rakic’s signed messages that must be validated before being routed to identified destination applications, and Ogawa’s decryption unit (implemented as part of each User Agent) would use a shared encryption key to decrypt data received from the Relay/Server. EX-1003, ¶223. Such a combination would have been well within a POSA’s capability to implement. *Id.*

The Board in IPR2024-00341 considered Ogawa-based modifications of TS-23.140, e.g., as described in §§IX.B.1.a-IX.B.1.b, 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]), 50-51; EX-1023; EX-1003, ¶224.

2. Claim 7

MMS-Rakic-Ogawa's User Agent ("device link agent," *supra* §VII.D.1.c.i) receives messages from the Relay/Server over secure interface MM1. *Supra* §VII.D.1.h. POSAs understood that "the received secure messages are encrypted," as claimed, using both MMS-Rakic-Ogawa Message Encryption (*supra* §IX.B.1.a) and SSL/TLS (*supra* §VII.C.2). EX-1003, ¶¶225-226.

In MMS-Rakic-Ogawa, such received messages are decrypted by the User Agent ("device link agent," *supra* §VII.D.1.c.i)—which provides MMS-Rakic-Ogawa's "decryption" functionalities for encrypted MMS messages (EX-1004, 19)—using Ogawa's decryption unit. *Supra* §§IX.B.1.a-IX.B.1.b; EX-1003, ¶227. As discussed *supra* §§VII.D.1.h-VII.D.1.i, the received messages each contain an "identifier" and "application data," which, as discussed *supra* §VII.D.7, the User Agent obtains for routing purposes by decrypting received encrypted messages. EX-1003, ¶228. Thus, MMS-Rakic-Ogawa's "device link agent" is "configured to decrypt the received secure messages prior to delivering those messages to respective software processes."

C. GROUNDS 3B-3D

The reasons described *supra* §IX.B for incorporating Ogawa's teachings into

MMS-Rakic apply to MMS-Rakic-Cole, MMS-Rakic-Sathish, and MMS-Rakic-Cole-Sathish (*supra* §§VIII.A-VIII.C), because Ogawa’s teachings do not affect how/why POSAs would have combined those references. EX-1003, ¶¶229-230. Incorporating Ogawa’s teachings into those combinations renders obvious the claims identified *supra* §§VIII.A-VIII.C (for the reasons respectively discussed there) and claim 7 (for the reasons discussed *supra* §IX.B.2).

X. GROUNDS 4A-4D

Claim 9, 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, ¶¶231-233. 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, ¶233. Ellison allows “normal” execution for applications (green) outside the device’s secure platform, 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.

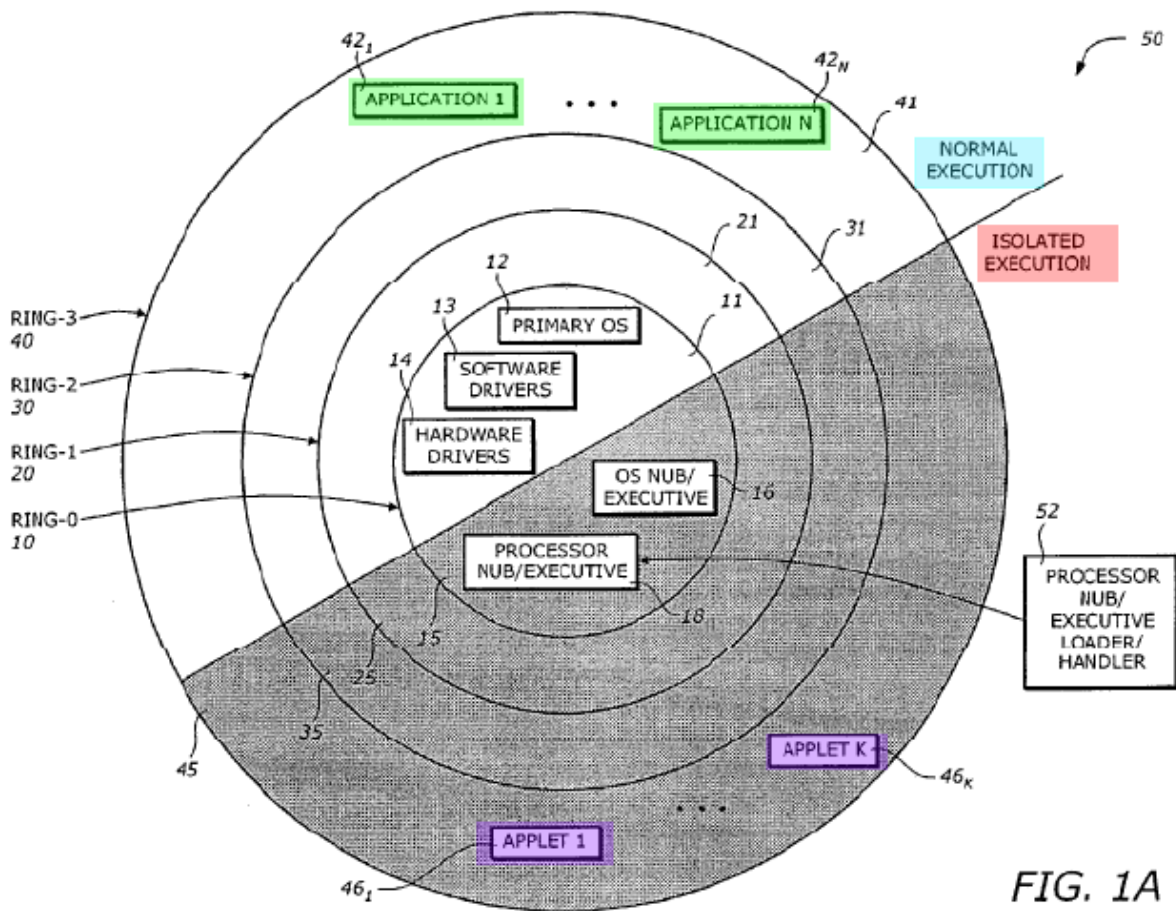


FIG. 1A

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, ¶234.

“[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.

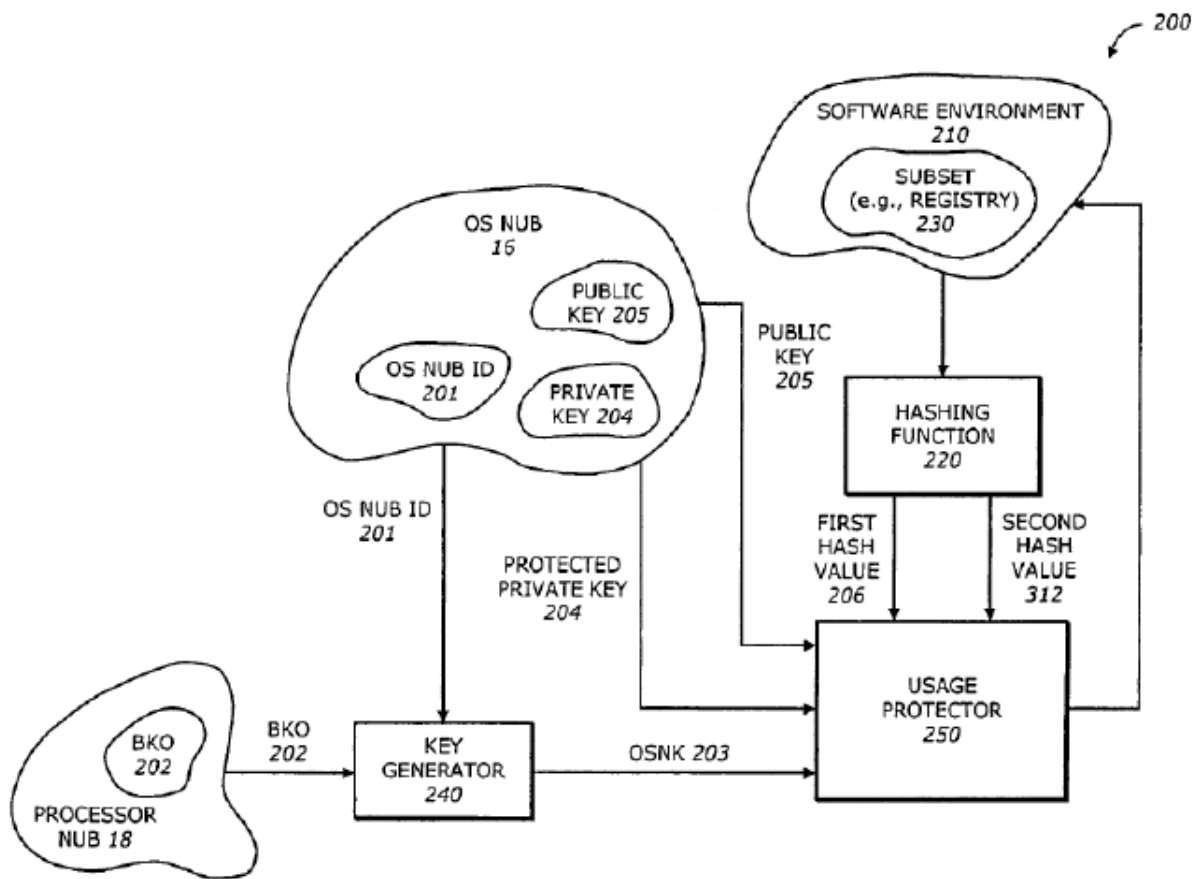


FIG. 2

Above, “usage protector 250” protects “subset 230” against “unauthorized reads” and detecting “intrusion, tampering or unauthorized modification.” *Id.*, 8:66-9:62, FIG. 2; EX-1003, ¶¶235-237.

B. GROUND 4A: Implementing Ellison’s Isolated Execution Environment

1. MMS-Rakic-Ellison

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

First, implementing Ellison’s secure platform (EX-1019, 8:25-9:62, FIG. 2) would have desirably improved MMS-Rakic’s device security, which transports data

for, 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, ¶¶238-239 (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 malicious/unauthorized activity. EX-1019, 8:25-9:62, FIG. 2; EX-1003, ¶239.

Second, combining TS-23.140 and Ellison involved combining known prior art elements (Ellison’s isolated software environment in MMS-Rakic’s device) according to known methods to yield predictable results. *KSR*, 550 U.S. at 416; EX-1003, ¶240.

POSAs would have reasonably expected success incorporating Ellison’s techniques into MMS-Rakic’s user devices because Ellison describes its techniques implemented in “computer system[s]” (like MMS-Rakic’s devices) with “processor[s].” EX-1019, 5:11-16; EX-1003, ¶¶241-242. 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, ¶242 (citing EX-1033, 25-26, FIG. 1). Given (1) TS-23.140’s contemplation 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-Rakic’s User Agent is organized as part of the secure environment and communicates with destination applications residing outside this secure environment. EX-1003, ¶243; EX-1019, 4:30-37. In such an implementation (“MMS-Rakic-Ellison”), the MMS User Agent runs in “isolated execution mode,” while at least one device application runs in “normal execution mode.” EX-1019, 3:4-6; EX-1003, ¶244.

2. Claim 9

Claim 9 requires that the “device link agent executes in a secure execution environment,” while “at least one of the software components executes outside of the secure execution environment.” MMS-Rakic-Ellison meets claim 9. MMS-Rakic-Ellison’s secure, isolated area is the claimed “*secure execution environment*.” EX-1003, ¶¶245-246. MMS-Rakic-Ellison’s User Agent “*executes in a secure execution environment*,” while at least one un-trusted third-party device application “*executes outside of the secure execution environment on the*” device (*supra* §X.B). EX-1003, ¶246. As required by [1F], MMS-Rakic-Ellison’s “device link agent” still has authorized communications with the “software components[]

execut[ing] outside of the secure execution environment” over the “inter-process software communication bus” as claimed. EX-1003, ¶247.

C. GROUNDS 4B-4D

The reasons described *supra* §X.B.1 for incorporating Ellison’s teachings into MMS-Rakic apply to MMS-Rakic-Cole, MMS-Rakic-Sathish, and MMS-Rakic-Cole-Sathish (*supra* §§VIII.A-VIII.C), for claims 1-8 and 12-14, because Ellison’s teachings do not affect how/why POSAs would have combined those references as discussed for those claims. EX-1003, ¶¶248-249. Incorporating Ellison’s teachings into those combinations render obvious claims 1-8 and 12-14 (for the reasons discussed *supra* §§VIII.A-VIII.C) and claim 9 (for the reasons discussed *supra* §X.B.2).

XI. GROUNDS 5A-5D

Claim 11 requires claim 10’s “device link agent” to be “configured to buffer” claim 10’s “upload messages for transmission to the network message server at a time selected by a heartbeat mechanism,” and is rendered obvious by incorporating Shen’s (EX-1027) teachings.

A. Shen (EX-1027)

Shen discloses a “[MMS] system” in which a “[MMS] user device communicates with [a MMS] gateway via [a] wireless LAN... to send and receive multimedia messages.” EX-1027, Abstract. Shen’s user device “sends heartbeat

signals periodically” to the gateway to determine whether the device “is located in the coverage of the wireless LAN.” EX-1027, [0018], [0033]-[0034]. If the gateway receives the heartbeat signal, the client is available, and the gateway, e.g., informs the user of pending messages. EX-1027, [0033]-[0034]. Otherwise, the user is unavailable (e.g., offline), “and the gateway does not send any notification to the user even if there is a MMS message to be sent to that user.” *Id.*; EX-1003, ¶¶250-252.

B. GROUND 5A: Implementing Shen’s Heartbeat Teachings

1. MMS-Rakic-Shen

TS-23.140 identifies the MMS User Agent as responsible for “all aspects of storing MMs on the terminal” (EX-1004, 19) and discloses storing data that it intends to submit to an MMS Relay/Server that is unreachable “*in the UE* until the recipient MMS Relay/Server becomes reachable.” *Id.*, 35-36 (discussing read-reply reports). EX-1003, ¶253; EX-1004, 29.

TS-23.140 does not disclose details regarding (1) how an MMS User Agent determines when an unreachable MMS Relay/Server “*becomes reachable*,” or (2) how an MMS User Agent handles messages it receives from device applications (for relaying to a VAS Application) while waiting for *an unavailable MMS Relay/Server* to “*become[] reachable*.” EX-1004, 29.

One well-known solution for handling such scenarios (unavailable message recipient) was by using heartbeat signals to periodically check for availability and buffering pending messages until the recipient became available. EX-1003, ¶¶254-255 (citing EX-1027, [0018], [0033]-[0034]; EX-1040, [0011]; EX-1061, [0088], [0042], [0094]; EX-1062, 1:54-2:3, 13:33-36, 16:37-53, FIGS. 11-12A). Shen discloses details regarding how to implement such heartbeat signals in an MMS system like TS-23.140's.

POSAs had multiple reasons to implement MMS-Rakic in view of Shen's heartbeat signal teachings.

First, it was well-known that heartbeat messages typically encompassed far less data than MMs. EX-1003, ¶256 (citing EX-1043, [0062]). To conserve network bandwidth, POSAs would have been motivated to implement UE/devices to send a heartbeat message to confirm that a connection to a previously unreachable message recipient—e.g., an MMS Relay/Server—was alive again before attempting transmission of MMs. EX-1027, [0033]-[0034]; EX-1044, cl. 14; EX-1061, [0091], [0094]; EX-1062, 1:54-2:3.

Second, combining TS-23.140 and Shen's teachings involved combining known prior art elements (Shen's heartbeat mechanism in MMS-Rakic's device) according to known methods to yield predictable results. *KSR*, 550 U.S. at 416; EX-1003, ¶257.

POSAs would have reasonably expected success incorporating Shen's techniques into MMS-Rakic's user devices because Shen describes its techniques implemented in a "MMS system." EX-1027, [0018], [0033]-[0034]. EX-1003, ¶258.

In such an implementation, MMS-Rakic's user device would be implemented to store ("buffer") messages until they are able to be sent to an unreachable MMS Relay/Server (EX-1004, 19, 35-36) and Shen's "heartbeat sender" would be used "to determine whether [the MMS Relay/Server] is available." EX-1027, [0033]-[0034]; EX-1003, ¶259.

2. Claim 11

Claim 11 recites that the "device link agent" is "configured to buffer one or more of" claim 10's "upload messages for transmission to the network message server at a time selected by a heartbeat mechanism." As discussed *supra* §VII.D.9, "network message server" has no antecedent basis and at minimum encompasses claim 1's "message link server." EX-1003, ¶¶260-261. As discussed *supra* §§XI.B and VII.D.9, MMS-Rakic-Shen's User Agent stores upload messages received from device applications until it is able to transmit the messages to the MMS Relay/Server—which occurs once the heartbeat mechanism confirms that MMS Relay/Server is available. EX-1003, ¶261.

C. GROUNDS 5B-5D

The reasons described *supra* §XI.B for incorporating Shen's teachings into

MMS-Rakic apply to MMS-Rakic-Cole, MMS-Rakic-Sathish, and MMS-Rakic-Cole-Sathish (*supra* §§VIII.A-VIII.C), because Shen's teachings do not affect how/why POSAs would have combined those references. EX-1003, ¶¶262-263. Incorporating Shen's teachings into those combinations renders obvious the claims identified *supra* §§VIII.A-VIII.C (for the reasons respectively discussed there) and claim 11 (for the reasons discussed *supra* §XI.B.2).

XII. CONCLUSION

The Board should cancel claims 1-14.

Respectfully submitted,
/ Jessica Kaiser /

Jessica Kaiser
Reg. No. 58,937
Attorney for Petitioner

Dated: May 26, 2026

XIII. CLAIM LISTING APPENDIX

Claim 1
[IPRE] A mobile end-user device comprising:
[1A] a wireless modem configurable to exchange data via a connection to a wireless network;
[1B1] an inter-process software communication bus providing secure communication between an executing device link agent and respective executing processes for a plurality of software components,
[1B2] wherein providing secure communication comprises receiving access authorization information from a secure server, and allowing access to the bus only for software components identified by the access authorization information; and
[1C] the device link agent, configured to
[1D1] maintain a secure message link through the wireless network and an Internet network to a message link server,
[1D2] the message link server operating a message service that receives messages over a network from a plurality of network functions,
[1E] receive secure messages from the message link server over the secure message link, the received messages identified for delivery to multiple ones of the software components, and including message content received by the message link server from multiple ones of the network functions, and
[1F] for software components identified by the access authorization information, route messages identified for delivery to a given one of those software components via the inter-process software communication bus to a software process corresponding to the given software component.
Claim 2
The mobile end-user device of claim 1, wherein the access authorization information provided by the secure server for a given one of the software components comprises a signature.
Claim 3
The mobile end-user device of claim 1, wherein the software components include a first device component that receives message content in a first format, and a second device component that receives message content in a second format different than the first format.

Claim 4
The mobile end-user device of claim 3, further comprising a user interface, wherein the first device component is a user service interface agent, and the first format comprises a notification message, the user service interface agent configured to display the notification message on the user interface.
Claim 5
The mobile end-user device of claim 4, the user service interface agent further configured to obtain a user input as a response to the display of the notification message, and deliver the user input to an agent on the device.
Claim 6
The mobile end-user device of claim 3, wherein the first device component is a policy control agent, and the first format contains service settings and/or configuration information.
Claim 7
The mobile end-user device of claim 1, wherein the received secure messages are encrypted, the device link agent further configured to decrypt the received secure messages prior to delivering those messages to respective software processes.
Claim 8
The mobile end-user device of claim 7, wherein the encrypted messages are transported to the device link agent using one or more of encryption on a transport services stack, IP (Internet Protocol) layer encryption, and tunneling.
Claim 9
The mobile end-user device of claim 1, wherein the device link agent executes in a secure execution environment, and at least one of the software components executes outside of the secure execution environment.
Claim 10
The mobile end-user device of claim 1, wherein the device link agent is further configured to receive, from one or more of the authorized software components, upload messages, each of the upload messages identifying a corresponding one of the network functions to which the device respective software component has requested delivery, the device link agent transmitting the upload messages to the network message server over the secure message link, for delivery by the network message server to the respective identified network elements.
Claim 11

The mobile end-user device of claim 10, the device link agent further configured to buffer one or more of the upload messages for transmission to the network message server at a time selected by a heartbeat mechanism.
Claim 12
The mobile end-user device of claim 1, wherein at least one of the secure messages received from the network message server comprises multiple identifier/data pairs.
Claim 13
The mobile end-user device of claim 2, wherein the given one of the software components is identified by a secure unique identifier.
Claim 14
[14PRE] A method of operating a mobile end-user device having a wireless modem to connect to a wireless network, the method comprising:
[14A] receiving access authorization information from a secure server;
[14B] operating an inter-process software communication bus to provide secure communication between an executing device link agent and respective executing processes for a plurality of software components, the secure communication comprising allowing access to the bus only for software components identified by the access authorization information;
[14C] maintaining a secure message link from the device link agent through the wireless network and an Internet network to a message link server, the message link server operating a message service that receives messages over a network from a plurality of network functions;
[14D] receiving secure messages at the device link agent from the message link server over the secure message link, the received messages identified for delivery to multiple ones of the software components, and including message content received by the message link server from multiple ones of the network functions; and
[14E] for software components identified by the access authorization information, routing messages identified for delivery to a given one of those software components via the inter-process software communication bus from the device link agent to a software process corresponding to the given software component.

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

The undersigned hereby certifies that a true copy of the foregoing Petition and supporting materials (Exhibits and Power of Attorney) have been served this 26th day of May 2026, by Federal Express delivery service on Patent Owner at the correspondence address for the attorney of record for the '564 Patent shown in USPTO PAIR:

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

and via electronic mail to the attorneys of record for Plaintiff in the concurrent litigation matter:

mfenster@raklaw.com
rmirzaie@raklaw.com
bledahl@raklaw.com
dchang@raklaw.com
kdavis@raklaw.com
jpickens@raklaw.com
jtsuei@raklaw.com
jwietholter@raklaw.com

Respectfully submitted,
/ Jessica Kaiser /

Jessica Kaiser
Reg. No. 58,937
Attorney for Petitioner

Dated: May 26, 2026

CERTIFICATE OF WORD COUNT

Pursuant to 37 C.F.R. § 42.24, the undersigned certifies that the foregoing Petition for *Inter Partes* Review contains 13,989 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.

Respectfully submitted,

/ Jessica Kaiser /

Jessica Kaiser
Reg. No. 58,937
Attorney for Petitioner

Dated: May 26, 2026