IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of:	Gregory G. Raleigh	
U.S. Patent No.:	8,406,733	Attorney Docket No.: 39843-0164IP1
Issue Date:	March 26, 2013	
Appl. Serial No.:	13/461,141	
Filing Date:	May 1, 2012	
Title:	AUTOMATED DEVICE PROVISIONING AND ACTIVATION	

Mail Stop Patent Board
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

PETITION FOR *INTER PARTES* REVIEW OF UNITED STATES PATENT NO. 8,406,733 PURSUANT TO 35 U.S.C. §§ 311–319, 37 C.F.R. § 42

TABLE OF CONTENTS

I. IPR REQUIREMENTS 1
- **A.** Grounds for Standing 1
- **B.** Challenge and Relief Requested 1
- **C.** Claim Construction 1
- **D.** Level of Ordinary Skill in the Art 2

II. THE '733 PATENT 2
- **A.** Brief Description 2
- **B.** Prosecution History 4

III. THE CHALLENGED CLAIMS ARE UNPATENTABLE 5
- **A.** Claims 1-17, 19, 21-27, 29, and 30 Are Obvious Over TS-23.140 and Ogawa 5
  - 1. TS-23.140 (EX-1004) 5
  - 2. Ogawa (EX-1005) 7
  - 3. MMS-Ogawa Combination 9
  - 4. Claim Analysis 20

IV. PTAB DISCRETION SHOULD NOT PRECLUDE INSTITUTION 76
- **A.** 35 U.S.C. §325(d) – *Advanced Bionics* 76
- **B.** 35 U.S.C. §314(a) - *Fintiv* 77

V. CONCLUSION AND FEES 78

VI. MANDATORY NOTICES UNDER 37 C.F.R § 42.8(a)(1) 79
- **A.** Real Party-In-Interest Under 37 C.F.R. § 42.8(b)(1) 79
- **B.** Related Matters Under 37 C.F.R. § 42.8(b)(2) 79
- **C.** Lead and Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3) 79
- **D.** Service Information 80

APPENDIX OF CLAIMS

CLAIM 1	
1pre	***An end-user device comprising:***
1a	***a modem for enabling communication with a network system over a service control link provided by the network system over a wireless access network,***
1a1	***the service control link secured by an encryption protocol***
1a2	***and [the service control link is] configured to support control-plane communications between the network system and a service control device link agent on the end-user device;***
1b	***[the end-user device comprising:] a plurality of device agents communicatively coupled to the service control device link agent through an agent communication bus, each of the plurality of device agents identifiable by an associated device agent identifier; and***
1c	***[the end-user device comprising:] memory configured to store an encryption key,***
1c1	***the encryption key shared between the service control device link agent and a service control server link element of the network system;***
1d1	***wherein the service control device link agent is configured to: receive, over the service control link, an encrypted agent message from the service control server link element,***
1d2	***[wherein the service control device link agent is configured to:] using the encryption key, obtain a decrypted agent message,***
1d3	***the decrypted agent message comprising a particular agent identifier and message content for delivery to a particular device agent of the plurality of device agents, the particular agent identifier identifying the particular device agent,***

1e	***the message content [being] from a particular server of a plurality of servers communicatively coupled to the service control server link element, and***
1f	***[wherein the service control device link agent is configured to:] based on the particular agent identifier, deliver the message content to the particular device agent over the agent communication bus.***
CLAIM 2	
2	***The end-user device recited in claim 1, wherein the particular server comprises a service usage history server, a policy management server, an access control integrity server, a network traffic analysis server, a beta test server, a service download control server, a billing event server, an activation server, a transaction server, an authentication server, or a content management server.***
CLAIM 3	
3	***The end-user device recited in claim 1, wherein the message content comprises information associated with a service usage.***
CLAIM 4	
4	***The end-user device recited in claim 3, wherein the information associated with the service usage comprises information about one or more of a service usage value, a projected service usage value, a service usage plan limit, a projected service usage overage, a projected service cost overage, a service plan period time duration, a service plan time remaining before end of period, and a service overage.***
CLAIM 5	
5	***The end-user device recited in claim 1, wherein the message content is based, at least in part, on a user preference.***
CLAIM 6	
6	***The end-user device recited in claim 1, wherein the message content comprises information associated with a roaming service usage or a roaming service cost.***

CLAIM 7	
7	***The end-user device recited in claim 1, wherein the message content comprises a service offer, an advertisement, or a transaction offer.***
CLAIM 8	
8	***The end-user device recited in claim 1, wherein the message content comprises information from a third party configured to provide control of a service or a billing for a service.***
CLAIM 9	
9	***The end-user device recited in claim 1, wherein the message content comprises an agent instruction, a setting value, an agent configuration, or a software update.***
CLAIM 10	
10	***The end-user device recited in claim 1, wherein the message content comprises software or a media file.***
CLAIM 11	
11	***The end-user device recited in claim 1, wherein the message content comprises information associated with a service policy.***
CLAIM 12	
12	***The end-user device recited in claim 1, wherein the message content comprises service usage accounting information.***
CLAIM 13	
13	***The end-user device recited in claim 1, wherein the service control device link agent is further configured to send a device message to the service control server link element over the service control link.***
CLAIM 14	
14	***The end-user device recited in claim 13, wherein the device message comprises a service usage report or an integrity report.***

CLAIM 15	
15	***The end-user device recited in claim 13, wherein the device message comprises a user response.***
CLAIM 16	
16	***The end-user device recited in claim 15, wherein the user response comprises an acknowledgment of a roaming cost or a roaming usage.***
CLAIM 17	
17	***The end-user device recited in claim 15, wherein the user response comprises an acknowledgment of a service usage, a service cost, or a service overage.***
CLAIM 19	
19	***The end-user device recited in claim 1, further comprising a user interface, and wherein the particular device agent is configured to assist in presenting a notification through the user interface, the notification based on the message content.***
CLAIM 21	
21	***The end-user device recited in claim 1, wherein the service control link supports asynchronous transmissions by the service control server link element.***
CLAIM 22	
22	***The end-user device recited in claim 1, wherein the service control link supports periodic transmissions by the service control server link element.***
CLAIM 23	
23	***The end-user device recited in claim 1, wherein the service control device link agent is further configured to send a device credential to the network system or receive the device credential from the network system during a service authorization sequence.***

CLAIM 24	
24	***The end-user device recited in claim 23, wherein the device credential comprises one or more of a phone number, an identification number, a security signature, a security credential, a subscriber identity module (SIM) identifier, a mobile equipment identifier (MEID), and a device identifier.***
CLAIM 25	
25	***The end-user device recited in claim 1, wherein a transmission over the service control link is within an ambient service.***
CLAIM 26	
26	***The end-user device recited in claim 1, wherein the particular device agent comprises software.***
CLAIM 27	
27	***The end-user device recited in claim 1, wherein the encryption key is a first encryption key, and the service control device link agent is further configured to encrypt the message content using a second encryption key before delivering the message content to the particular agent, the second encryption key shared by the service control device link agent and the particular agent.***
CLAIM 29	
29	***The end-user device recited in claim 1, wherein the service control link is configured to support control-plane communications using an Internet protocol.***
CLAIM 30	
30Pre	***A method performed by an end-user device, the method comprising:***
30d1	***receiving, over a service control link, an encrypted agent message from a network element,***
30a1	***the service control link secured by an encryption protocol,***

30a2	***the service control link supporting control-plane communications between a service control device link agent on the end-user device and the network element;***
30d2	***using an encryption key…, obtaining a decrypted agent message***
30c	***[the] encryption key shared between the service control device link agent and the network element***
30d3	***the decrypted agent message comprising a particular agent identifier and message content for delivery to a particular device agent of a plurality of device agents on the end-user device,***
30b	***each of the plurality of device agents identifiable by an associated device agent identifier and communicatively coupled to the service control device link agent through an agent communication bus,***
30d4	***the particular agent identifier identifying the particular device agent,***
30e	***the message content [being] from a particular server of a plurality of servers communicatively coupled to the network element; and***
30f	***delivering the message content to the particular device agent over the agent communication bus based on the particular agent identifier.***

EXHIBITS

EX-1001	U.S. Patent No. 8,406,733 to Raleigh ("the '733 Patent")
EX-1002	Excerpts from the Prosecution History of the '733 Patent ("the Prosecution History")
EX-1003	Declaration and Curriculum Vitae of Dr. Patrick Traynor
EX-1004	3GPP TS 23.140 v6.9.0 (2005-03); 3rd Generation Partnership Project; Technical Specification Group Terminals; Multimedia Messaging Service (MMS); Functional Description; Stage 2 ("TS-23.140")
EX-1005	U.S. Pat. No. 8,195,961B2 ("Ogawa")
EX-1006	**RESERVED**
EX-1007	**RESERVED**
EX-1008	PCT Pat. App. Pub. No. WO 2008/048075A1 ("Lee")
EX-1009	U.S. Pat. No. 7,975,147B1 ("Qumei")
EX-1010	U.S. Pat. No. 9,032,192B2 ("Frank")
EX-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*
EX-1012	"Open Mobile Alliance; Multimedia Messaging Service Architecture Overview" (MMSARCH) specification, available at *https://www.openmobilealliance.org/release/MMS/V1_2-20030923-C/OMA-MMS-ARCH-V1_2-20030920-C.pdf*
EX-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*

EX-1014	The Transport Layer Security ("TLS") Protocol, V. 1.1, available at *https://www.ietf.org/rfc/rfc4346.txt*
EX-1015	U.S. Pat. App. Pub. No. 2003/0096625 ("Mi-Su Lee")
EX-1016	**RESERVED**
EX-1017	**RESERVED**
EX-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/ftp/tsg_sa/TSG_SA/TSGS_19/Docs/PDF/SP-030167.pdf*
EX-1019	**RESERVED**
EX-1020	USPTO Binding Interim Guidance Addressing PTAB's Approach to Discretionary Denials, June 21, 2022, available at *https://www.uspto.gov/sites/default/files/documents/interim_proc_discretionary_denials_aia_parallel_district_court_litigation_memo_20220621_.pdf*
EX-1021	Plaintiff Headwater Research LLC's Disclosure of Asserted Claims And Infringement Contentions, *Headwater Research LLC v. Samsung Electronics Co.*, 6:23-cv-00103-JRG-RSP (WDTX)
EX-1022	Docket Control Order , 2:23-CV-00103-JRG-RSP, [63] December 1, 2023
EX-1023	Samsung Stipulation letter regarding IPR grounds in District Court Litigation
EX-1024	Declaration of Friedhelm Rodermund
EX-1025	**RESERVED**
EX-1026	U.S. Patent No. 7,509,487 to Lu et al. ("Lu")
EX-1027	U.S. Patent Pub. No. 2005/0207379 to Shen et al. ("Shen")

EX-1028	*Transporting data between wireless applications using a messaging system—MMS*, Miraj E Mostafa, Wireless Communications and Mobile Computing (2007) ("Mostafa")
EX-1029	Dictionary of Computer Science, Engineering, and Technology, CRC Press LLC, 2001
EX-1030	**RESERVED**
EX-1031	U.S. Patent No. 8,010,669 to Sathish
EX-1032	U.S. Patent No. 7,689,252 to Nishida
EX-1033	**RESERVED**
EX-1034	**RESERVED**
EX-1035	RDF Primer, W3C Recommendation 10 February, 2004 available at https://www.w3.org/TR/rdf-primer/
EX-1036	Yahoo's RSS Reader goes LIVE on My Yahoo, available at https://www.searchenginejournal.com/yahoos-rss-reader-goes-live-on-my-yahoo/212/
EX-1037	Nokia E71 review: Nokia E71, available at https://www.cnet.com/reviews/nokia-e71-review/
EX-1038	Plaintiff Headwater Research LLC's Amended Infringement Contentions, *Headwater Research LLC v. Samsung Electronics Co.*, 6:23-cv-00103-JRG-RSP (WDTX)
EX-1039	U.S. Patent No. 8,620,988 to Sohm et al. ("Sohm")
EX-1040	U.S. Patent No. 5,581,704 to Barbara et al. ("Barbara")

I. IPR REQUIREMENTS

A. Grounds for Standing

Petitioners Samsung Electronics Co., Ltd. and Google LLC certify that the '733 Patent is available for IPR and that Petitioners are not barred or estopped from this review. 37 C.F.R. §42.104(a).

B. Challenge and Relief Requested

Petitioners request IPR of the Challenged Claims on the grounds below. *See* EX-1003, ¶¶1-238.

Ground	Challenged Claim(s)	35 U.S.C. §103
1	1-17, 19, 21-27, 29, 30	TS-23.140 and Ogawa

Reference	Filing Date	Publication Date	Prior Art basis
TS-23.140	-	March 2005 (EX-1024[1])	102(b)
Ogawa	5/19/2008	10/1/2009	102(a)/102(e)

C. Claim Construction

[1] Confirming public availability/accessibility of TS-23.140 on/around March 2005, and similar for OMA references (EX-1011-to-1012).

Claim terms are construed herein using the standard used in civil actions under 35 U.S.C. §282(b), in accordance with the ordinary and customary meaning as understood by a POSITA and the patent's prosecution history. 37 C.F.R. §42.100(b). The Board need only construe terms to the extent necessary "to resolve [a] controversy." *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 (Nov. 13, 2018). Petitioners are not conceding that each Challenged Claim satisfies all statutory requirements, nor waiving arguments that can only be raised in district court.

D. Level of Ordinary Skill in the Art

A person of ordinary skill in the art ("POSITA") relating to the subject matter of the '733 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, ¶¶21-22, 1-15. Additional graduate education could substitute for professional experience, and vice versa. *Id.*

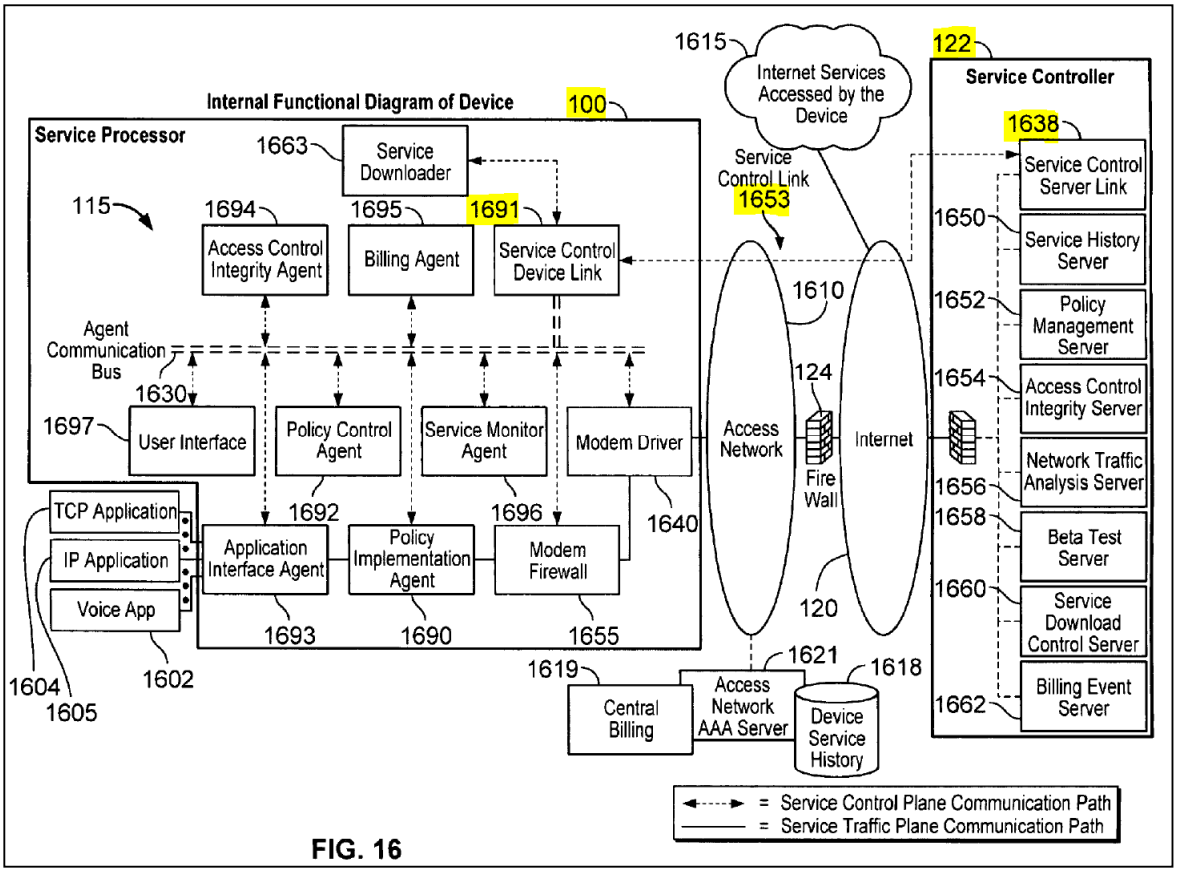
II. THE '733 PATENT

A. Brief Description

The '733 Patent is directed to "devices" "receiving control-plane communications from a network element over a secure service control link." EX-1001, Ab-

stract. Control-plane communications include communications sent over a network "involving supervision" and "control" of "service[s]" being delivered to a device. EX-1001, 37:34-46, 68:19-28.

FIG. 16 (below) shows ***service control link 1653*** between service controller 122's ***service control server link 1638*** and device 100's ***service control device link 1691***. *Id.*; EX-1003, ¶43. Service control link 1653 is a "control plane communication link [that] provides for a secure (e.g., encrypted) communications link for providing secure, bidirectional communications between the [device's] service processor 115 and the service controller 122." EX-1001, 68:28-37. FIG. 16's service controller 122 comprises multiple servers. *Id.,* 75:20-77:46.



EX-1001, FIG. 16 (annotated)

The specification describes "two or three layers of encryption in the service control link," with one layer "implemented in the transport services stack." EX-1001, 87:58-63. For "secure control plane communication[s]" received by a device from service controller 122 over link 1653, service control device link 1691 "decode[s]" (*e.g.*, "decrypts"), unpacks, and routes the communications "to the appropriate agent" on the device using "agent route 2416." *Id.*, 87:49-58, 89:21-33, 90:19-53; EX-1003, ¶¶42-45.

B. Prosecution History

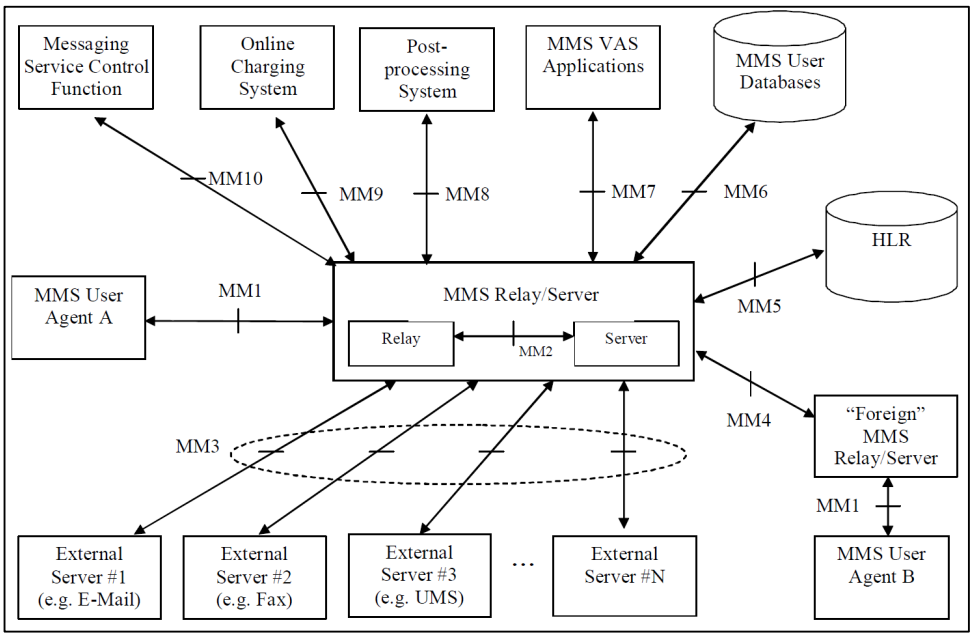
The '733 Patent claims priority to a provisional application filed January 28, 2009 ("Critical Date"). EX-1001, 1. The patent issued after one Office Action that included only §112 rejections. EX-1002, 97-101. The Examiner did not consider TS-23.140 (EX-1004) or Ogawa (EX-1005). EX-1003, ¶¶46-47.

III. THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. Claims 1-17, 19, 21-27, 29, and 30 Are Obvious Over TS-23.140 and Ogawa

1. TS-23.140 (EX-1004)

TS-23.140 is a standard describing a "non-realtime Multimedia Messaging Service, MMS." EX-1004, 10.[2] One MMS implementation environment is shown below:



[2] References to EX-1004 are to page numbers printed at the ***top*** of each page.

EX-1004, 24, Figure 3

Above, "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, ¶¶48-49.

The MMS Relay/Server relays messages from the network to the MMS User Agent using interface MM1. EX-1004, 17-18, 21, 23-25. The messages may include "MMS VAS [Value Added Services]" content, "provided… by third-party Value Added Service Providers (VASP)" via interface MM7 (*id.*, 14, 18, 23), and then relayed to the MMS User Agent to "provid[e] Value Added Services (e.g. news service or weather forecasts) to MMS users." *Id.*, 14, 41. The MMS Relay/Server can relay messages from "***several*** MMS VAS Applications"[3] in the network. *Id.*, 18; EX-1003, ¶50.

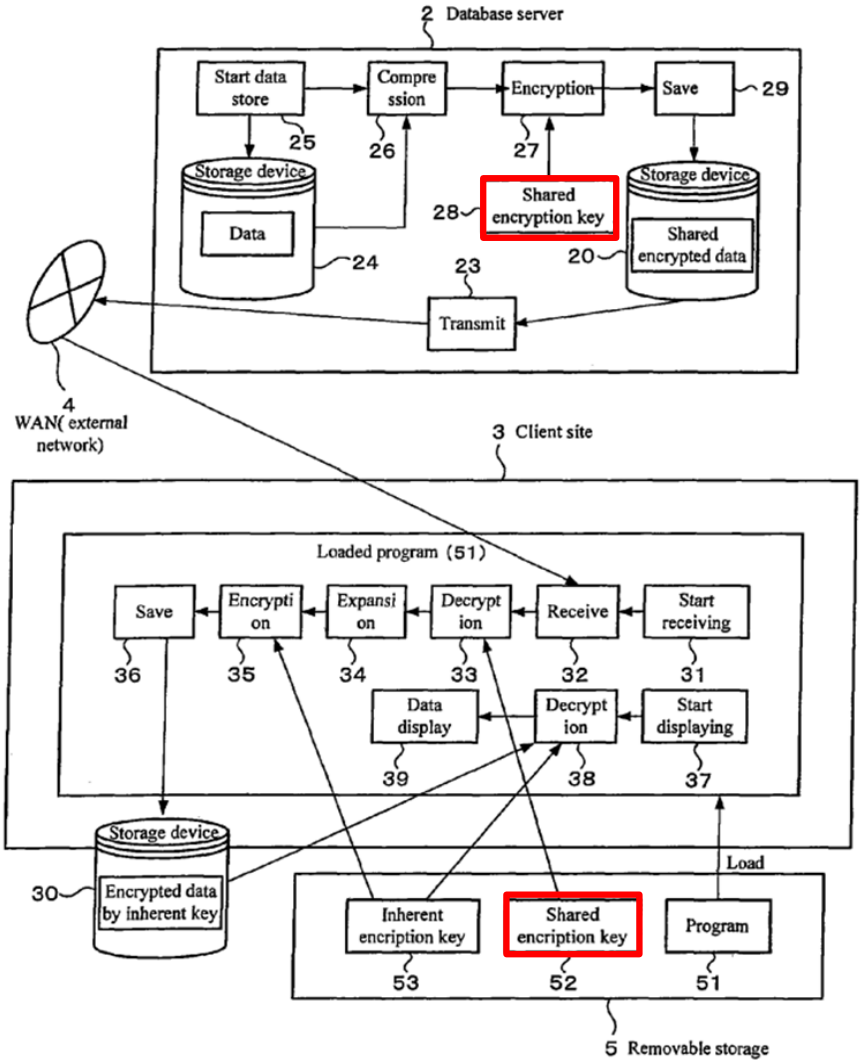
"MMS may be used to transport data specific to applications" "other than the MMS User Agent" which also "reside on [the] MMS User Agent [device]." *Id.,* 14, 54-56; EX-1003, ¶51 (citing EX-1028, 732-733). For such "application data," "the MMS User Agent… route[s] the received MMS information on to the destination application" using a "destination application identifier" included with the received message. EX-1004, 14, 54-56; EX-1003, ¶52.

[3] Emphasis is added throughout unless otherwise indicated.

TS-23.140 discloses both "encryption… on an end-user to end-user basis," and using protocols such as Transport Layer Security (TLS) and "authentication mechanisms based on public/private key cryptography" for securing communications. EX-1003, ¶53 (citing EX-1004, 19, 41, 25-26; EX-1012, 21).

2. Ogawa (EX-1005)

Ogawa discloses a "data encryption system" that facilitates secure communications between database server 2 and client site 3 through network 4, shown below. EX-1005, 3:18-21, 9:15-20, FIG. 7; *see also id.*, FIG. 1, 3:44-54; EX-1003, ¶¶54-56 (explaining that FIG. 7 illustrates a client-server system that performs functions described for FIG. 1).



EX-1005, FIG. 7 (annotated).

In Ogawa, "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, 9:16-34. SSL is a well-known predecessor of TLS. EX-1003, ¶57 (citing EX-1010, 1:38-42).

Ogawa teaches ***further*** encrypting data using a "shared encryption key" distributed to (and used by) both client and server. EX-1003 ¶58 (citing EX-1005, 6:42-47, 7:11-21, 9:16-20). The key is used to (1) encrypt data transmitted to the client, and (2) decrypt received encrypted data at the client. EX-1005, 9:21-34, 5:60-65; EX-1003, ¶59. Decryption is conducted by a "decryption unit" on the client. EX-1005, 5:59-6:9; EX-1003, ¶60.

3. MMS-Ogawa Combination

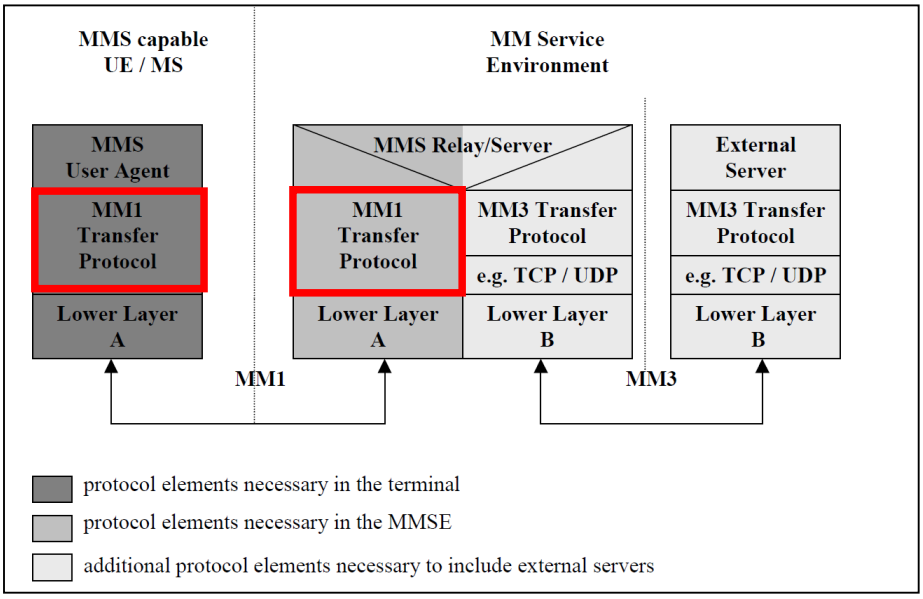
(a) Implementing TS-23.140's User Device with a Modem

TS-23.140 says its "MMS User Agent" "resid[es] on a UE [user equipment]… or… external device." EX-1004, 14, 18-19. TS-23.140 says the User Agent communicates with the MMS Relay/Server using, *e.g.*, "2G and 3G wireless networks," but does not disclose details regarding how the device on which the User Agent resides facilitates communications over such networks. *E.g.,* EX-1004, 17, 23-24. Before the Critical Date, it was well-known to use a ***modem*** to enable communications over the networks described in TS-23.140. EX-1003, ¶¶61-62; EX-1008, ¶¶27-28, 44, FIGS. 1, 4. Using a modem to enable a user device to communicate over the wireless networks in TS-23.140 would have been a conventional and obvious way to implement what TS-23.140 describes, and is nothing more than utilizing familiar, known components to achieve a predictable result of facilitating TS-23.140's communications. *KSR Int'l v. Teleflex*, 550 U.S. 398, 416

(2007); EX-1003, ¶63. A POSITA would have reasonably expected success in implementing TS-23.140's device with a modem because this was a well-known, conventional way of achieving the wireless network communications that TS-23.140 describes. EX-1003, ¶63.

(b) Securing Interface MM1 Using SSL/TLS

TS-23.140 explains that network communications between the MMS User Agent and the MMS Relay/Server use the MM1 Transfer Protocol. EX-1003, ¶¶64-65; EX-1018; EX-1004, 24, FIG. 4 (below).



EX-1004, 24, FIG. 4 (annotated)

A POSITA had multiple reasons to secure MM1 with a SSL/TLS protocol:

First, it was conventional and well-known for client-server communications to use SSL/TLS to achieve secure communications between a client and server. EX-1003, ¶66-67 (citing, *e.g.*, EX-1010, 1:38-42; EX-1013, 3).

Second, TS-23.140 contemplates implementations which use "transport layer security mechanisms" (*e.g.*, SSL/TLS) to secure communication links, including MM1 between the user device (with the MMS User Agent) and the MMS Relay/Server. EX-1003, ¶68 (citing EX-1004, 24-25; EX-1011, 11 (which was incorporated-by-reference into EX-1004, at 13, 162); EX-1012, 21 (which was incorporated-by-reference into EX-1011, at 4, 5, 10).

Third, such an implementation is nothing more than utilizing familiar, known protocols to achieve a predictable result of facilitating TS-23.140's user agent and other applications to securely interface with one another. *KSR*, 550 U.S. at 416; EX-1003, ¶69.

A POSITA would have reasonably expected success implementing MM1 to use SSL/TLS, given TS-23.140's teachings and incorporated disclosures, and the widespread use of such security protocols before the Critical Date. EX-1003, ¶70.

(c) Applying Ogawa's Symmetric Encryption Techniques

TS-23.140 discloses "encryption of an MM [Multimedia Message] on an end-user to end-user basis." EX-1004, 19. In addition to "transport layer security mechanisms," TS-23.140 says "authentication mechanisms based on public/private key

cryptography may ***also*** be used." EX-1003, ¶¶71-72 (citing EX-1004, 25, 42; EX-1012, 21). TS-23.140 does not provide details regarding how to implement additional end-user-to-end-user encryption beyond SSL/TLS.

Before the Critical Date, it was well-known to implement encryption for messages transmitted by a push server (*e.g.*, TS-23.140's MMS Relay/Server) to an end-user device using symmetric encryption, with a key that is shared between the server and the end-user device and stored in their respective memories. EX-1003, ¶72 (citing, *e.g.*, EX-1005; EX-1027, [0054]-[0060]; EX-1009, 3:25-27, 8:1-5). Ogawa discloses details regarding how to implement symmetric encryption on messages 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. EX-1003, ¶73.

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

First, implementing the data encryption taught in Ogawa to TS-23.140's MMS system would have achieved a system "having improved security" and providing "an end-user to end-user" security solution for MMS applications, as contemplated by TS-23.140. EX-1003, ¶74 (citing EX-1004, 19, 24-25; EX-1012, 21).

Second, encrypting MMS communications using an additional layer of security beyond SSL/TLS as taught in Ogawa would have been particularly beneficial for "enterprise applications"—a type of value-added service application that a POSITA would have been motivated to ensure its MMS system could handle. EX-1003, ¶75 (citing EX-1027, [0017], [0021-0022]; EX-1004, 54).

Third, implementing Ogawa's data encryption into TS-23.140's MMS system would have been nothing more than implementing known methods/techniques (symmetric encryption using a shared key as taught in Ogawa) to known systems/devices (the MMS Relay/Server and MMS User Agent device taught in TS-23.140) to achieve predictable results (end-user-to-end-user encrypted data, as contemplated by TS-23.140). *KSR*, 550 U.S. at 416; EX-1003, ¶76.

A POSITA would have reasonably expected success implementing Ogawa's encryption techniques to the TS-23.140 system given (1) the similar client-server communication architectures taught by both references (with connections between network elements protected by, *e.g.*, SSL/TLS) and (2) TS-23.140 contemplates end-user-to-end-user encryption, and Ogawa (and corroborating references) provided an exemplary, predictable implementation of such encryption using a symmetric, shared encryption key. EX-1003, ¶¶77-79.

(d) Ogawa's Decryption and Encryption Units

Ogawa teaches a "decryption unit" for decrypting received encrypted data as

part of its symmetric encryption system. EX-1005, 5:59-6:9 ("[R]eceived shared key encrypted data will be decrypted using the shared encryption key 52 which was supplied to the decryption unit 33 and beforehand stored…"); EX-1003, ¶80. A POSITA would have had reason to implement the decryption unit as part of the MMS User Agent in TS-23.140, because (1) the MMS User Agent is responsible for receiving data from TS-23.140's MMS Relay/Server and distributing the data to the correct applications on the user device, and (2) TS-23.140 expressly identifies the MMS User Agent as "provid[ing]… functionalities such as … ***decryption***." EX-1003, ¶80 (citing EX-1004, 14, 54-56). Such an implementation would have, *e.g.*, beneficially allowed the MMS User Agent to decrypt an encrypted message from the MMS Relay/Server and any information identifying the destination application to which the message should be routed. EX-1003, ¶¶80-81.

Ogawa also teaches an encryption unit for encrypting (or "re-encrypt[ing]") data before transmitting it to another part of the device, *e.g.*, storage. EX-1005, 5:59-6:9; EX-1003, ¶¶81-82. As with the decryption unit, a POSITA would have had reason to implement the encryption unit as part of the MMS User Agent in TS-23.140, because (1) being able to securely store data on a user device was a desirable feature that would have helped prevent, *e.g.*, theft, (2) the MMS User Agent is responsible for "all aspects of ***storing***" messages on TS-23.140's user device, and

(3) TS-23.140 expressly identifies the MMS User Agent as "provid[ing]… functionalities such as… ***encryption***." EX-1003, ¶82 (citing EX-1004, 14).

A POSITA would have reasonably expected success in an implementation with Ogawa's encryption and decryption units incorporated into TS-23.140's MMS User Agent, because the prior art components would continue to perform functions they performed prior to the combination—MMS User Agents and the MMS Relay/Server would continue to exchange data using secure communication links, and Ogawa's decryption and encryption units (as implemented as part of the MMS User Agent) would use an encryption key to encrypt/decrypt data received from the MMS Relay/Server. EX-1003, ¶83. Such a combination would have been well within a POSITA's capability to implement. *Id.*

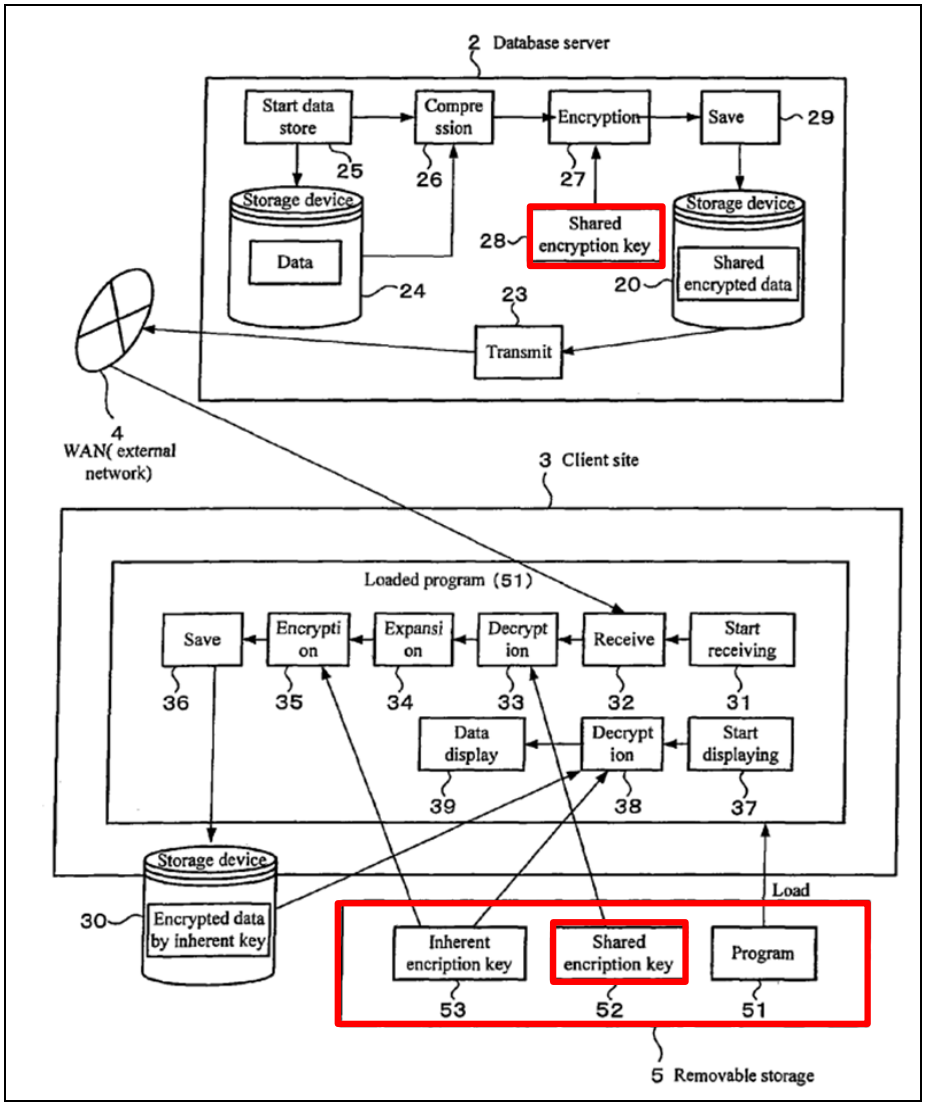
(e) Storing Ogawa's Shared Encryption Key

TS-23.140's user device has "memory." EX-1004, 19-20. Ogawa teaches the well-known technique of ensuring that each device/entity in a network environment that encrypts or decrypts communications using symmetric encryption ***stores*** the encryption key in memory connected to it. EX-1005, 3:18-34, 4:48-57, 5:59-65, 6:64-7:21, FIGS. 1, 7; EX-1003, ¶84 (citing EX-1009, 8:1-5, 3:25-27). For symmetric encryption, there were a limited number of ways to ensure the same key was used by encrypting/decrypting devices, including: (1) storage of the same key at each encrypting/decrypting device in persistent memory, and (2) generation of

the same key at each encrypting/decrypting device prior to performing the encrypting/decrypting operation, and storage of that key temporarily during the operation. EX-1003, ¶85. In both ways, the key was stored during the encryption/decryption. EX-1003, ¶85.

A POSITA would have had multiple reasons to store Ogawa's encryption key in the TS-23.140 user device's memory to facilitate decryption of encrypted messages received from the MMS Relay/Server. EX-1003, ¶86.

First, an implementation in which the encryption key was stored in TS-23.140 user device's memory would have been a way to implement the symmetric encryption teachings of Ogawa, which discloses storing the shared encryption key in removable storage 5 that is connected to client site 3 and functions as a memory for the client site 3, so that the key can be retrieved and used when needed to decrypt a message. EX-1005, 3:61-4:7, 5:41-47, 9:21-34, FIG. 7; EX-1003, ¶87.



EX-1005, FIG. 7 (annotated)

Storing Ogawa's encryption key in memory of the TS-23.140 user device (i.e., the client site, in Ogawa's terminology) would have beneficially enabled the MMS User Agent (modified to include Ogawa's decryption and encryption units, as discussed above) to access the key and perform the decryption/encryption described in Ogawa. EX-1003, ¶88.

Second, such an implementation would have been nothing more than implementing a known method (storage of a symmetric/shared key in memory as taught by Ogawa and background references) to known systems (TS-23.140's user device with memory) to achieve a predictable result of enabling Ogawa's symmetric encryption/decryption of communications between TS-23.140's MMS User Agent and MMS Relay/Server. *KSR*, 550 U.S. at 416; EX-1003, ¶89.

Third, storing the shared key on memory within TS-23.140's user device would have been an obvious, readily-implementable design choice that a POSITA would have known would facilitate storing of Ogawa's shared encryption key in a location accessible to the user device, as was necessary for symmetric encryption. EX-1003, ¶¶90-94. That this design was well-known to POSITAs is corroborated by references like Qumei, which describes storing an "enciphering key" in an end-user device. EX-1009, 3:25-27; EX-1003, ¶¶90-94 (citing EX-1005, 5:42-58).

Storing the encryption key in TS-23.140's device's memory and enabling it to be retrieved from memory when needed would have been well within a POSITA's skill to implement, and a POSITA would reasonably have expected success in doing so, because this would have involved using components to perform the functions they performed prior to the combination. EX-1003, ¶95.

(f) MMS-Ogawa

"MMS-Ogawa" refers to the above-discussed encrypted MMS system that a POSITA would have been led to form based on TS-23.140 and Ogawa.

MMS-Ogawa implements TS-23.140's user device (configured to use the MMS service as described in TS-23.140) with a modem for wireless network communications. *Supra* §III.A.3(a).

MMS-Ogawa also implements TS-23.140's MMS Relay/Server and user device so that messages transmitted across the interface between TS-23.140's user device and the MMS Relay/Server are secured with both SSL/TLS and encrypted using symmetric MMS-Ogawa Message Encryption. *Supra* §§III.A.3(b)-III.A.3(c).

In MMS-Ogawa, Ogawa's encryption and decryption units are implemented as part of the MMS User Agent in TS-23.140's user device (*supra* §III.A.3(d)), and a common key is distributed to (and stored in the respective memories of) TS-23.140's user device and MMS Relay/Server (*supra* §III.A.3(e)). EX-1003, ¶¶96-98.

4. Claim Analysis

(a) Claims 1 and 30

[1pre]/[30pre][4]

The '733 specification does not define requirements for an "end-user device" (*see* EX-1001, 8:3-15, 8:60-9:15), using the term to include "networked" devices that have "services delivered" to them. EX-1001, 5:65-6:28, 6:49-56; EX-1003, ¶99. If the preambles are limiting, a POSITA understood MMS-Ogawa's "UE [***user*** equipment]"/"external ***device***"—with a MMS User Agent that "performs… operations on a ***user's*** behalf," and through which "Value Added Services" are "provided" (delivered) to "***users***"—is an "end-user device." EX-1004, 14; EX-1003, ¶99. As explained below, MMS-Ogawa's end-user device performs the method of claim 30.

[1a]

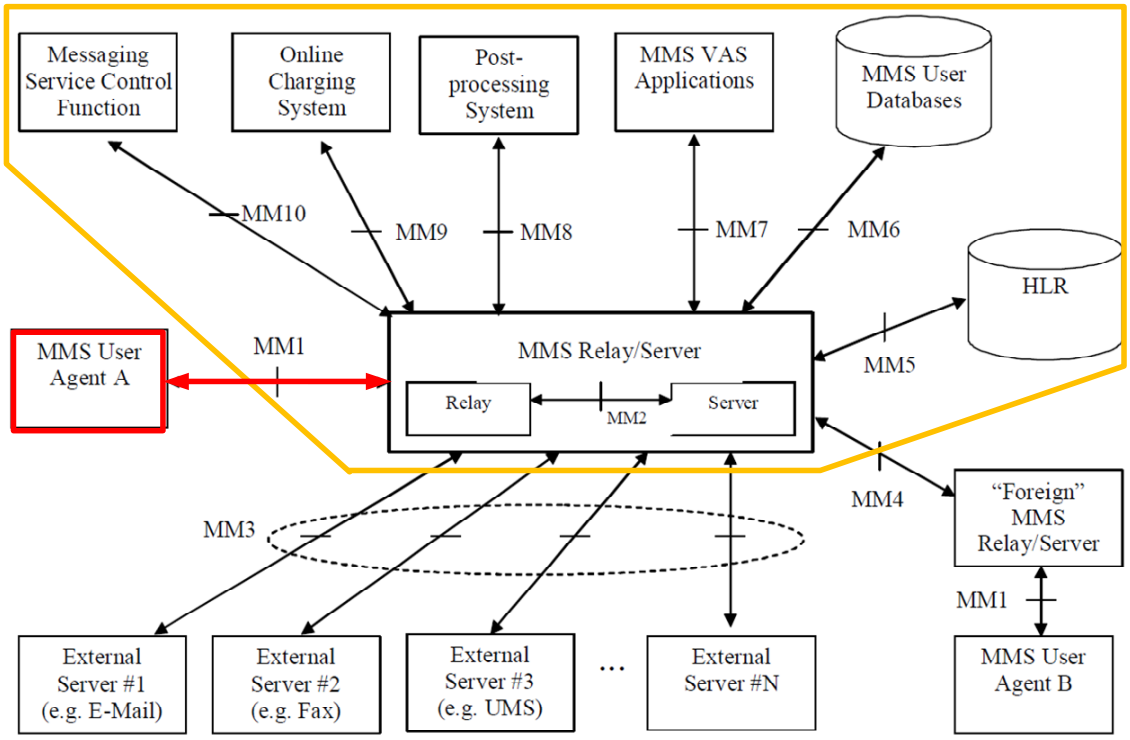
Element [1a] requires "a ***modem*** for enabling communication" that takes place "over a wireless access network." EX-1003, ¶100. The '733 specification uses "modem" to include those that enable communication over "2G" and "3G" "wireless access networks." EX-1001, 12:61-13:32, 25:29-45, 27:38-44, 29:52-53,

[4] Limitations herein are identified using reference labels from the Claim Appendix.

33:59-65, 34:24-27; EX-1003, ¶100. MMS-Ogawa's modem for 2G and 3G wireless networks (*supra* §III.A.3(a)) is thus a "modem for enabling communication" taking place "over a wireless access network" as claimed. EX-1003, ¶100.

Element [1a] also requires that the modem enable communication "with a ***network system*** over a service control link." The '733 specification never describes a "***network system***" in the context of a "service control link." EX-1003, ¶101. According to the specification, a "service control link" is a "communication link" "between a device and ***the network***"—which, in the specification's embodiments, is represented by "service controller 122." EX-1001, 17:8-11, 68:20-37, FIGs. 16-20; EX-1003, ¶101. The specification says service controller 122 may "include[] one or more server functions," and may be "implemented on multiple servers… or…. on a single server." EX-1001, 16:13-26. A POSITA thus understood that one or more servers performing one or more server functions would meet the claimed "network system." EX-1003, ¶101.

The modem in MMS-Ogawa's end-user device enables a MMS User Agent to communicate with various network elements (orange below) through interface MM1—including MMS-Ogawa's Relay/Server and multiple VAS applications (via the Relay/Server). EX-1004, 14, 18, 23; EX-1003, ¶102.



EX-1004, Figure 3 (annotated)

A POSITA understood that the outlined network elements above are a "network system" as claimed, because (1) the specification only ever describes a "service control link" as connecting a device to a "network" that comprises one or more servers performing one or more server functions and thus the claimed "network system" encompasses at least that, and (2) the Relay/Server and multiple VAS Applications in TS-23.140's MMS environment (MMSE) comprise servers that perform server functions. EX-1003, ¶¶103-106 (citing EX-1001, 16:13-26, FIGs. 16-20; EX-1004, 14, 25-26); *see* discussion *infra* regarding [1e].

Regarding "service control link," the '733 specification does not set forth any requirements but says it "can provide an efficient and flexible control plane communication link" used for "controlling" some aspect of a "service" (*e.g.,* "data traffic, application usage, communication with… network end points"). EX-1003, ¶107 (citing EX-1001, 7:23-33, 19:67-20:4, 25:46-53, 37:36-61, 68:19-58). MMS-Ogawa's interface MM1 is a "service control link" because it facilitates transmission of, *e.g.*, multimedia message service "associated ***control*** information" and "application/implementation specific ***control*** information" between MMS-Ogawa's network system (which includes the MMS Relay/Server) and the end-user device. EX-1003, ¶107; EX-1004, 14, 55-56.

Element [1a] also requires that the "service control link" be "provided by the network system." The '733 specification never describes how a "network system" "***provide[s]***" a "service control link." EX-1003, ¶108. During prosecution, the examiner rejected this limitation as indefinite. *See* EX-1002, 99-100. In response, Applicant argued this limitation "is supported at least by FIG. 16[,] illustrating service control link 1653 communicatively coupling service processor 115 and service controller 122," and the disclosures that "service processor 115…provides for device side of [the] communications with network elements" and "service controller 122…provides for network side of [the] communications with device 100." EX-1002, 76.

Based on the Applicant's argument, a POSITA would have understood that the "service control link is provided by the network system" in MMS-Ogawa because (1) the MMS Relay/Server and MMS User Agent device are implemented to "communicate[] with" each other through (and thus are communicatively coupled by) MM1, and (2) both entities are implemented to provide for communications with one another. EX-1003, ¶109 (citing EX-1004, 24, FIG. 4, describing the MM1 Transfer Protocol; EX-1018).

MMS-Ogawa's modem is thus "a modem for enabling communication with a network system over a service control link provided by the network system over a wireless access network," as claimed. EX-1003, ¶110.

[1a1]/[30a1]

The claimed service control link must be "secured by an encryption protocol." Regarding communication links, the '733 specification says "traffic… can be provided… with ***secure transport protocols running over Transmission Control Protocol (TCP)***," and that "approaches for implementing a secure control channel over the Internet including… ***running TCP Transport Layer Security (TLS)***." EX-1001, 17:2-26; *see also id.*, 87:62-88:7 (describing use of "standard secure or open Internet networking protocols, such as TLS or TCP."); EX-1003, ¶111. The specification uses "TLS" and Secure Socket Layer (SSL) interchangeably. *E.g.*, EX-1001, 98:42-44; 99:26-29; 101:65-67; EX-1003, ¶111.

In MMS-Ogawa, SSL/TLS is used to secure interface MM1, between the user device (with the MMS User Agent) and the MMS Relay/Server. *Supra* §III.A.3(b); EX-1003, ¶112. MMS-Ogawa's MM1 is thus "secured by an encryption protocol," as claimed. EX-1003, ¶112.

[1a2]/[30a2]

Element [1a2] requires that the service control link be "configured to support control-plane communications between the network system and a service control device link agent on the end-user device." Element [30a2] recites that the service control link "support[s] control-plane communications" between the "service control device link agent" and a "***network element***."

The "network element" recited in [30a2] is recited in [30c] and [30d1]. EX-1003, ¶113. The '733 Patent uses "network element" to encompass any element that is part of a network, *e.g.*, a server. EX-1003, ¶113; EX-1001, 23:46-54, FIGs. 1-8. A POSITA understood that MMS-Ogawa's MMS Relay/Server 401/801—which is a server in claim 1's "network system" (as discussed above for [1a])—is also a "network element" as that term is used in the '733 Patent. EX-1003, ¶113.

As discussed for [1a], MMS-Ogawa's interface MM1 (the claimed "***service control link***") is how the MMS Relay/Server—which is part of the claimed "***network system***" in [1a2] and is the "***network element***" in [30a2]—communicates with the MMS User Agent on MMS-Ogawa's "***end-user device***." EX-1003, ¶114.

A POSITA would have understood that MM1 is "configured to support control-plane communications" as claimed. EX-1003, ¶115. The '733 Patent says a "control plane communication link" manages "various aspects of device[-]based network service policy implementation," including "policy settings for the device for network services, …such as access control settings, … user notification settings, user privacy settings, user preference settings, [etc.]" EX-1001, 8:60-9:15, 9:23-24. A POSITA would have understood control-plane communications to encompass communications "across a network" that involve "supervision" and "device-based" "control" of "service[s]" delivered to a device, *e.g.*, by "communicating…, controlling, monitoring, or verifying service policy." *Id.*, 37:36-43, 68:19-28; EX-1003, ¶116.

As discussed for [1a], MMS-Ogawa's MM1 facilitates transmission of, *e.g.*, MMS-"associated ***control*** information" and "application/implementation specific ***control*** information." EX-1003, ¶117; EX-1004, 14, 55-56. TS-23.140 also expressly discusses use of MM1 to communicate information that affects how a service is delivered based on a user device's "capabilities." EX-1004, 19, 21, 30 ("[T]he specific mechanism for terminal capability negotiation shall be defined by the MM1 implementation"); EX-1003, ¶¶117. The MMS Relay/Server "use[s]… information about the capabilities of the recipient MMS User Agent in preparation of MMs to be delivered to the recipient MMS User Agent" and "adjust[s] an MM

to be delivered" based on those capabilities. EX-1004, 30-31; *see also id.*, 35-36 ("MMS Relay/Server decides whether to use ***streaming based on*** the media type and the media format of the subjected MM contents, capability negotiation ***and/or user settings/preferences***."). These are the same types of control-plane communications (affecting a service being delivered) disclosed in the '733 Patent. EX-1003, ¶117; EX-1001, 8:60-9:15. Thus, a POSITA understood MM1 is "configured to support control-plane communications" as claimed. EX-1003, ¶117.

A POSITA would likewise have understood these communications are "***between***" MMS-Ogawa's Relay/Server (which is part of the claimed "network system" ([1a]) and is the "network element" ([30a2])) and "***a service control device link agent*** on the end-user device," as claimed. EX-1003, ¶118.

While the '733 specification does not describe any "service control device link agent" (*id.*), the specification describes a "service control device ***link*** 1691," saying it is a "device side" component that may "provide an efficient and secure solution for transmitting and receiving service policy implementation, control, monitoring and verification information with other network elements." EX-1001, 37:43-62.

And the specification uses the term "agent" to refer to any component—which may, *e.g.*, be "implemented entirely in software"—that performs some function (*e.g.*, transmitting information for, *e.g.*, "control plane communication"). *Id.*,

15:58-16:2, 42:51-52, claim 26; EX-1003, ¶118. The specification does not set forth any required function. EX-1001, 16:2-12. Moreover, it was well-known that an agent performed function(s) on behalf of an entity (*e.g.*, user, client, server). EX-1003, ¶118 (citing EX-1029, 12). This use of "agent" is consistent with Patent Owner's interpretation in litigation. EX-1003, ¶118 (citing EX-1021, 13-23; EX-1038, 17, mapping "agents" to "client app[s]" on an alleged device).

MMS-Ogawa's "MMS User Agent" is a device-side "application" (implemented in software) that communicates with the MMS Relay/Server and "perform[s] [service]-specific operations on a user's behalf and/or on another application's behalf" (*supra* §III.A.1) and, as discussed above, enables the transmission and receipt of communications that control the services the device receives via (and on behalf of) the MMS Relay/Server. EX-1004, 14, 19, 23-24, 30-31, 35-36; EX-1003, ¶119. MMS-Ogawa's User Agent is thus a "service control device link agent," as claimed. EX-1003, ¶119.

[1b]/[30b]

The claimed end-user device must have "a plurality of device agents communicatively coupled to the service control device link agent through an agent communication bus," with "each of the plurality of device agents identifiable by an associated device agent identifier."

As discussed for [1a2], the '733 Patent uses "agent" to include a "software" "component" that performs some function (e.g., transmitting information) on behalf of a client or server. EX-1003, ¶120; EX-1001, 15:58-16:2, 42:51-52; EX-1029, 12; EX-1021, 13-23; EX-1038, 17. A "***device*** agent" is an agent on a device. EX-1003, ¶120.

In MMS-Ogawa, MMS is "used to transport data specific to applications" residing on the end-user device that are not the MMS User Agent. *Supra* §§III.A.3(a), III.A.3(f); EX-1004, 54-55; EX-1003, ¶121 (citing EX-1028, 732-733). TS-23.140 discloses transporting data that include the "application identifier of the destination application" and "application/implementation specific control information." EX-1004, 54-55. This "received MMS information" is "immediately routed" by the MMS User Agent "on to the destination application that is referred to from the destination application identifier (based on the negotiated details upon application registration process) without presentation to the user." EX-1004, 56.

A POSITA understood that this information is used by the destination application to perform functions on behalf of, *e.g.*, a server for a VAS application or an application on another terminal. EX-1003, ¶122 (citing EX-1028, 732-733). Because TS-23.140's destination applications are implemented "in software" on the user device and receive information specific to their associated services to perform

functions on behalf of another entity, a POSITA would have understood these applications to be "a plurality of device agents," as claimed. EX-1003, ¶122.

A POSITA would likewise have understood that in MMS-Ogawa, the MMS User Agent is communicatively coupled to the device's other applications "through an agent communication bus," as claimed. EX-1003, ¶123.

TS-23.140 discloses that its multiple additional "[a]pplications" on the user device "transport application specific data using MMS," but does not describe "[d]etails of these applications or how an MMS User Agent… would interface with them[.]" EX-1004, 54. A POSITA would have understood that the MMS User Agent and other applications would interface "through an agent communication bus" as that term is used in the '733 patent. EX-1003, ¶124 (explaining that the specification uses the term "agent communication bus" to include a communication link that facilitates communications); EX-1001, 42:48-61; EX-1038, 24.

Alternatively, a POSITA would have had reason to implement communications between the MMS User Agent and the device's other applications to occur over a bus. EX-1003, ¶125. Before the Critical Date, it was well-known to use a communications bus (*e.g.,* a "D-bus") for inter-process communications that enable applications to interface with one another, as TS-23.140 describes. EX-1003, ¶125 (citing EX-1031, 10:56-62; EX-1008, ¶28, FIG. 4). Using such a bus on the TS-23.140 device would have been a conventional, obvious way to implement

what TS-23.140 describes, and is nothing more than utilizing familiar, known components to achieve a predictable result of facilitating TS-23.140's user agent and other applications to interface with one another. *KSR*, 550 U.S. at 416; EX-1003, ¶125. A POSITA would have reasonably expected success doing so. EX-1003, ¶¶125-126. The end-user device in MMS-Ogawa thus has "a plurality of device agents communicatively coupled to the service control device link agent through an agent communication bus," as claimed. EX-1003, ¶¶125-126 (citing EX-1008, ¶28, FIG. 4; EX-1028, 732-733).

In MMS-Ogawa, "each of the plurality of device agents" are also "identifiable by an associated device agent identifier," as claimed. The '733 specification does not describe any requirements for the claimed "associated device agent identifier." EX-1003, ¶127. TS-23.140 says that applications need to register with MMS User Agent after being loaded on the end-user device. EX-1004, 54-55; EX-1003, ¶127. The MMS User Agent delivers application-specific messages to the correct destination application based on a "destination application identifier" included in the message that is associated with the destination application. EX-1003, ¶127; EX-1004, 55-56. A POSITA understood that use of a "destination application identifier" for accurately routing messages to specific destination applications, as TS-23.140 teaches, meant that each of MMS-Ogawa "device agents" was "identifiable by" an "associated device agent identifier," as claimed. EX-1003, ¶127.

[1c]

MMS-Ogawa's end-user device includes memory that stores Ogawa's shared encryption key (*supra* §III.A.3(e)), which as discussed *supra* §III.A.3(f), is used to secure interface MM1 with MMS-Ogawa Message Encryption. EX-1003, ¶¶128-129; *cf.* EX-1001, 87:57-88:7 (describing "two or three layers of encryption"). MMS-Ogawa's end-user device thus includes "memory configured to store an encryption key," as claimed. EX-1003, ¶¶128-129.

Additionally, ***<u>under Patent Owner's claim interpretation</u>*** in litigation, the "encryption key" limitations recited in [1c], [1c1]/[30c], and [1d2]/[30d2] may be ***part of*** the "encryption protocol" that secures limitation [1a1]'s service control link. EX-1021, 3-12 and 25-32 (mapping the ***same*** "security protocol[]" features in the alleged product to the "encryption protocol" in [1a1] and "encryption key" in [1c]); EX-1038, 8, 29. In other words, Patent Owner asserts these "encryption key" limitations are satisfied by systems where encryption is performed using SSL (or similar) "encryption protocol" without an additional layer of encryption. *Id.* As discussed below, MMS-Ogawa also separately meets the claims even if the limitations recited in [1c], [1c1]/[30c], and [1d2]/[30d2] are interpreted to encompass encryption performed ***as part of*** a SSL/TLS-enabled encryption protocol that also meets limitation [1a1] (*i.e.*, single-layer encryption). *See Nidec*, 868 F.3d at 1017; 83 Fed. Reg. 51,340, at 51,353.

Under Patent Owner's interpretation, MMS-Ogawa's memory meets [1c] because MMS-Ogawa's MM1 interface is secured using SSL/TLS. EX-1003, ¶¶130-131; *supra* §§III.A.3(b); III.A.3(f). While TS-23.140 does not describe the details of how SSL/TLS is implemented, such details were well-known to a POSITA before the Critical Date. EX-1003, ¶132 (citing EX-1013, EX-1014, EX-1026). For example, it was well-known that SSL/TLS use ***symmetric*** encryption that involves using the ***same*** key at the source and destination of a message for encryption and decryption. EX-1003, ¶132 (citing EX-1013, EX-1014, EX-1026, 29:31-30:24). A POSITA likewise understood that such keys were conventionally stored (at least temporarily) in the respective memories of the encrypting and decrypting entities. EX-1003, ¶132. Thus, under Patent Owner's claim interpretation—which reads the claims onto systems that ***only*** secure client-server communications based on the symmetric encryption used in SSL/TLS—MMS-Ogawa, which uses SSL/TLS (*supra* §§III.A.3(b); III.A.3(f)), includes "memory configured to store an encryption key," as required by [1c] (under Patent Owner's interpretation). EX-1003, ¶132.

[1c1]/[30c]

Element [1c1] requires that the encryption key be "shared between the service control device link agent"—MMS-Ogawa's ***MMS User Agent***, as discussed

for [1a2]—"and a service control server link element of the network system." Element [30c] recites that the encryption key be "shared between the service control device link agent" and "the network element" (which is mapped to MMS-Ogawa's MMS Relay/Server, as discussed for [30a2]).

While the '733 specification never describes element [1c1]'s "service control server link element of the network system," it refers to a "service control server link 1638," and says it is a "network side" component that may "provide[] an efficient and secure mechanism for transmitting and receiving service policy implementation, control, monitoring and verification information between the device agents… and other network elements…" EX-1001, 68:19-40; EX-1003, ¶133.

As discussed for [1a], the MMS Relay/Server is part of MMS-Ogawa's "network system." A POSITA would have understood that MMS-Ogawa's MMS Relay/Server "provides a mechanism for transmitting and receiving" "service policy… information" to and from "device agents" and the "network elements," because (1) TS-23.140 discloses various communication interfaces between the MMS Relay/Server and other elements in TS-23.140's MMS environment (*e.g.,* MM1, MM7), and (2) TS-23.140 specifically discloses an interface (MM1) which facilitates, as discussed above for [1a2], control-plane communications (affecting a service being delivered) between a MMS User Agent and the MMS Relay/Server.

EX-1003, ¶134 (citing EX-1004, 23-24, FIG. 4). A POSITA thus understood that the MMS Relay/Server—which communicates with a MMS User Agent over MM1—was a "service control server link element of the network system," as claimed. EX-1003, ¶134 (citing EX-1001, 68:19-40).

In MMS-Ogawa, Ogawa's encryption key is stored on the end-user device to enable the MMS User Agent to decrypt data received from the MMS Relay/Server, on which the same encryption key is also stored. *Supra* §III.A.3(e). As discussed *supra* §III.A.3(e), before the Critical Date, this was well-known for symmetric encryption. EX-1003, ¶135 (citing EX-1009, 3:25-27, 8:3-5).

First, a POSITA would have understood that the same key stored at MMS-Ogawa's end user device and MMS Relay/Server for MMS-Ogawa Message Encryption—which is used by both the MMS User Agent (the claimed "***service control device link agent***," as discussed for [1a2]) and the MMS Relay/Server ([1c1]'s "***service control server link element of the network system***" and [30c]'s "***network element***") for encryption/decryption—was "***shared between***" those claimed components, as required. EX-1003, ¶136.

Additionally and alternatively, a POSITA would have understood that ***under Patent Owner's claim interpretation***—which covers systems that only secure client-server communications using the single layer of symmetric encryption used in SSL/TLS—the key for MMS-Ogawa's symmetric SSL/TLS encryption (*supra*

§§III.A.3(b), III.A.3(f)), by being stored temporarily at both the end-user device (with the MMS User Agent) and the MMS Relay/Server, was likewise "***shared between***" the components (under Patent Owner's interpretation). EX-1003, ¶137 (citing EX-1013, 3).

[1d1]/[30d1]

Element [1d1] requires the "service control device link agent" to be "configured to: receive, over the service control link, an encrypted agent message from the service control server link element." Element [30d1] recites "receiving" an encrypted agent message from claim 30's "network element."

In MMS-Ogawa, the MMS User Agent (the claimed "***service control device link agent***," as discussed for [1a2]) receives, over interface MM1 (the claimed "***service control link***," as discussed for [1a]), encrypted data from the MMS Relay/Server (the claimed "***service control server link element***," as discussed for [1c1], and "***network element***" in claim 30, as discussed for [30a2]). EX-1003, ¶138. The data the MMS User Agent receives includes messages from "MMS VAS applications" provided by third-party VASPs to "provid[e] Value Added Services (e.g. news service or weather forecasts) to MMS users." EX-1003, ¶138 (citing EX-1004, 14, 18, 25, 41); *see supra* §III.A.1.

The '733 specification never uses the term "encrypted agent message." Based on the plain language of the claims, a POSITA would have understood the

term to encompass an encrypted message sent to an agent. EX-1003, ¶139. In MMS-Ogawa, messages are encrypted both using MMS-Ogawa Message Encryption and an SSL/TLS encryption protocol before they are transmitted to the MMS User Agent. *Supra* §§III.A.3(b), III.A.3(f).

First, because the messages are encrypted using MMS-Ogawa Message Encryption, a POSITA would have understood that, in MMS-Ogawa, the service control device link agent is thus "configured to" "receive, over the service control link, an encrypted agent message from the service control server link element," as claimed in claim 1 and that the message is received "from a network element," as claimed in claim 30. EX-1003, ¶140.

Additionally and alternatively, ***under Patent Owner's claim interpretation***—which covers systems with only the single layer of symmetric encryption used in SSL/TLS—MMS-Ogawa's symmetric SSL/TLS encryption (*supra* §§III.A.3(b), III.A.3(f)) alone also meets limitations [1d1] and [30d1], because SSL/TLS is a protocol for encrypting messages sent to MMS-Ogawa's MMS User Agent. EX-1003, ¶141.

[1d2]/[30d2]

The claims require the service control device link agent to (or be configured to) "us[e]" the "encryption key" to "obtain[]" a "decrypted agent message." EX-

1003, ¶142. The '733 specification never uses the term "decrypted agent message." Based on the plain language of the claims, a POSITA would have understood the term to encompass a message that was sent to an agent and then decrypted. EX-1003, ¶142.

In MMS-Ogawa, encrypted messages (*e.g.*, received from VASPs via the MMS Relay/Server) are decrypted at the MMS User Agent, which is implemented to use Ogawa's decryption unit and a shared encryption key to decrypt messages that were encrypted using MMS-Ogawa Message Encryption. *Supra,* §§ III.A.3(c)-III.A.3(e); EX-1004, 19; EX-1003, ¶143. A POSITA would have understood that, in MMS-Ogawa, the service control device link agent is thus configured to "us[e] the encryption key" to "obtain a decrypted agent message," as claimed. EX-1003, ¶143.

Additionally and alternatively, ***under Patent Owner's claim interpretation***—which covers systems with only a single layer of symmetric encryption used in SSL/TLS—MMS-Ogawa's symmetric SSL/TLS encryption (*supra* §§ III.A.3(b), III.A.3(f)) alone also meets limitations [1d2] and [30d2], because messages encrypted using SSL/TLS must be decrypted using the same encryption key used to encrypt the message, and the result is a message for the agent that has been decrypted, *i.e.*, "a decrypted agent message" (under Patent Owner's interpretation). EX-1003, ¶144 (citing EX-1009, 6:59-7:17, 7:34-40, 8:1-5).

[1d3]/[30d3]-[30d4]

The claims require that the "decrypted agent message" include "a particular agent identifier and message content for delivery to a particular device agent of" the "plurality of device agents," where "the particular agent identifier identif[ies] the particular device agent."

In MMS-Ogawa, the MMS User Agent (the claimed "***service control device link agent***," discussed for [1a2]) receives encrypted ***messages*** from various value-added service applications provided by third-party VASPs (as discussed for [1d1]). As discussed for [1d2], the MMS User Agent decrypts those messages to obtain "decrypted agent messages," as claimed. The MMS User Agent then transports such application-specific data to other applications on the user device (the claimed "***plurality of device agents***," as discussed for [1b]). EX-1004, 54-55; EX-1003, ¶¶145-146; *see supra* §§ III.A.1.

The messages containing such application-specific data are a form of what TS-23.140 calls "[a]bstract messages": "information which is transferred between two MMS entities used to convey an MM and/or associated control information between these two entities." EX-1004, 14; EX-1003, ¶147. TS-23.140 says these messages comprise "a destination application identifier" and "additional application/implementation specific control information." EX-1004, 54-55. MM1-Re-

trieve.RES is an exemplary abstract message with a destination application identifier as well as "MMS control information and the MM content." *Id*., 56, 69; EX-1003, ¶147. "Upon reception of an abstract message containing a destination application identifier ([e.g.,] MM1_retrieve.RES…)," the MMS User Agent "route[s] the received MMS information on to the destination application that is referred to from the destination application identifier (based on the negotiated details upon application registration process)." EX-1004, 56; EX-1003, ¶148.

Based on these disclosures, a POSITA would have understood that MMS-Ogawa's "destination application identifier" (which is the "***associated device agent identifier***" discussed in the context of [1b]) is a "particular agent identifier" in MMS-Ogawa's "decrypted message" that "identifies the particular device agent" to which the message should be delivered. EX-1003, ¶149.

Additionally, while the '733 specification never uses the term "message content," a POSITA would have understood that the above-described application-specific "MMS control information and the MM content" in a message is "message content" that will likewise be delivered. EX-1003, ¶150.

Thus, a POSITA understood that MMS-Ogawa's "decrypted agent message" includes "a particular agent identifier and message content for delivery to a particular device agent of the plurality of device agents," where "the particular agent identifier identifies the particular device agent," as claimed. EX-1003, ¶151.

[1e]/[30e]

Element [1e] requires the "message content" to be "from a particular server of a plurality of servers communicatively coupled to the service control server link element." Element [30d1] recites that the "plurality of servers" be "communicatively coupled to" claim 30's "network element."

MMS-Ogawa's MMS Relay/Server is the claimed "service control server link element" in claim 1 (as discussed for [1c1]), and the claimed "network element" in claim 30 (as discussed for [30a2]). MMS-Ogawa's application-specific data from VAS Applications provided by third-party VASPs (discussed in the context of [1d1]) is "message content," as discussed for [1d3]. EX-1003, ¶¶152-153.

TS-23.140 discloses "several MMS VAS Applications… connected to an MMSE." EX-1004, 18. A POSITA understood that each VAS Application resides on a server associated with a Value-Added Service Provider (VASP) that communicates with MMS-Ogawa's MMS Relay/Server through interface MM7. EX-1004, 25-26, 41, 112 ("a VASP… provide[s] the service by sending a multimedia message to one or more subscribers or to a distribution list"); EX-1003, ¶154. TS-23.140 also shows numerous other "servers" that can communicate with MMS Relay/Server through various interfaces, including, *e.g.,* "External Server #1" and "External Server #N" (which use interface MM3), and "'Foreign' MMS Relay/Server (which uses interface MM4). EX-1004, 23-24, FIG. 3; EX-1003, ¶154.

Given the large number of servers that the MMS Relay/Server in MMS-Ogawa interfaces with, a POSITA understood that MMS-Ogawa's "message content" from a VAS Application provided by third-party VASPs (as discussed above for [1e]) was from "a particular server," and that "a plurality of servers" were "communicatively coupled to" MMS-Ogawa's MMS Relay/Server ("the service control server link element," as discussed above for [1c1]), as claimed. EX-1003, ¶¶155-157.

[1f]/[30f]

The claims require that the "service control device link agent" be "configured to," "based on the particular agent identifier, deliver the message content to the particular device agent over the agent communication bus." EX-1003, ¶158.

MMS-Ogawa's MMS User Agent is a "service control device link agent" (as discussed for [1a2]). It delivers application-specific data to a destination application on the end-user device using the destination application identifier that was included in the message received from the MMS Server/Relay (as discussed for [1b] and [1d3]). A POSITA understood that such communication would occur "through the agent communication bus" (discussed in the context of [1b]). MMS-Ogawa thus meets [1f]/[30f]. EX-1003, ¶158.

(b) Claim 2

Claim 2 recites a list of alternative servers ("or") that claim 1's "particular server" may comprise, including "a billing event server," or "a content management server." The '733 specification calls a server that "collects billing events," "and/or provides trusted third[-]party function for… ecommerce billing transactions" a "billing event server." EX-1001, 77:39-46. The '733 specification does not describe a "content management server," but describes "content billing" as a type of "content management." *Id.,* 16:53-54; EX-1003, ¶159.

In MMS-Ogawa, as discussed above for [1e], MMS is used by servers to provide "value added services" content such as news or weather to users. EX-1004, 14, 25-26 (§6.9); EX-1003, ¶160. A VASP server "provide[s] the service by sending a multimedia message to one or more subscribers or to a distribution list." EX-1004, 112. A POSITA understood that the VASP server manages various aspects of content provision, including determining which MM content is intended for distribution, cancelling MMs that have already been sent to a user agent, determining which subscribers receive MM content, "classif[ying] content of the MM based on e.g. media types/formats, size, presentation formats," "indicat[ing] a condition which needs to be met to allow delivery," etc. EX-1004, 87, 112-114; EX-1003, ¶¶160. TS-23.140 also discloses VAS applications generating Charging Data Records (CDR) "when submitting MMs to the MMS Relay/Server" "for the

purpose of billing and traceability." EX-1004, 18, 23, 163; *see also id*., 112-114 (describing billing services performed by VASPs, e.g., "indicat[ing] which party is expected to be charged for an MM submitted by the VASP," and "mark[ing] the [message] content… with a service code…"); EX-1003, ¶161.

A POSITA understood that a VASP server that manages content delivery and billing for that content, as taught in TS-23.140, is both a "content management server" because it manages billing for content delivery and a "billing event server" because it creates CDRs for the purpose of billing—thus meeting claim 2. EX-1003, ¶161.

(c) Claims 3-4

Claim 3 requires claim 1's "message content" to "comprise[] information associated with a service usage." Claim 4 requires claim 3's "information" comprise "information about one or more" of several alternatives, including "a service usage value," "a projected service usage value," "a service plan time remaining before end of period," or "a service usage plan limit." EX-1003, ¶162.

In MMS-Ogawa, the "VASP may mark the content of the message with a service code that may be transferred by the MMS Relay/Server in the form of charging information for use by the billing system to properly bill the user for the service being supplied." EX-1004, 113. A POSITA understood that because TS-23.140's service code includes information that allows a billing system to properly

bill for a service, the information indicates the ***value*** of the service being used by the user, thus constituting a "service usage value." EX-1003, ¶163.

A VASP can also mark an abstract message (intended for a destination application on the user device) to indicate that the VASP will "take over the charge for the sending of a reply-MM… from the recipient(s)" and associated "reply-charging limitations." EX-1004, 37-38 (§7.1.10); EX-1003, ¶164. "Within submission of an MM," the VASP indicates "willingness to pay the charge for one reply-MM," and "may define a reply-charging limitation request (e.g. may specify the latest time of submission of the reply-MMs or a maximum size of reply-MMs)." *Id*., 38. Upon receiving the VASP's MM, the MMS Relay/Server "pass[es] the indication" of the reply-charging and associated "limitations" "when routing" the MM to the user. *Id*.; *see also id.*, 70; EX-1003, ¶164.

A POSITA understood that information indicating that the VASP will cover the charge of a reply-MM is information about an anticipated service usage—*i.e.,* "a projected service usage value," as claimed. EX-1003, ¶165. Additionally, a POSITA understood that information regarding time limitations imposed on the offered reply-MM service constitutes "a service plan period time duration," "a service plan time remaining before end of period," and a "service usage plan limit," as claimed, because the information provided to the user device is regarding time-based limits on the reply-charging service usage. EX-1003, ¶165; EX-1004, 38.

A POSITA also understood the above-identified information is "associated with a service usage," as required by claim 3. EX-1003, ¶¶165.

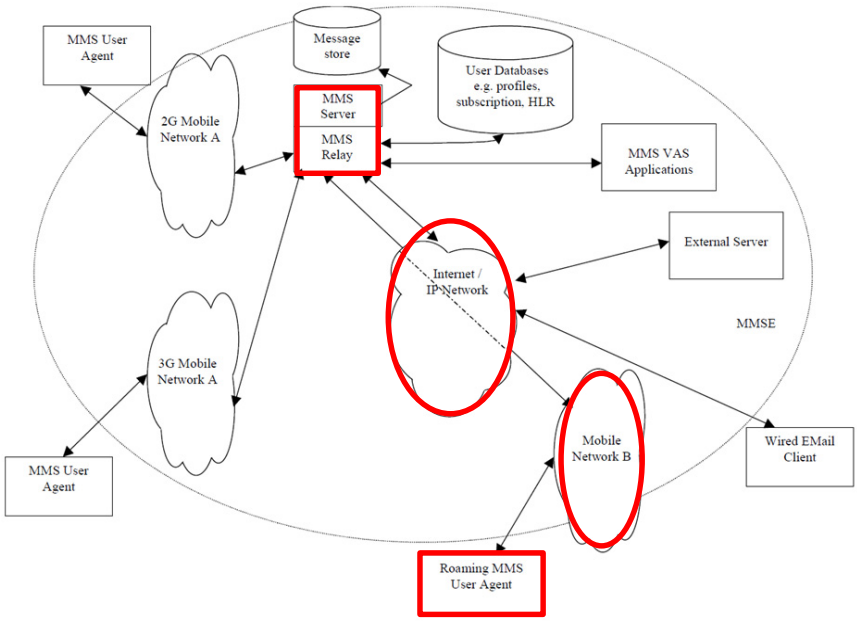
(d) Claim 5

Claim 5 requires claim 1's "message content" to be "based, at least in part, on a user preference." In MMS-Ogawa, the MMS Relay/Server can adjust the characteristics of a message and its content, including its presentation format and whether content is streamed, based on the user preferences before delivering the message to the user's device. EX-1004, 35-36. TS-23.140 expressly describes the MMS Relay/Server converting media type/format based on user settings/preferences. For example, "MM contents may be… delivered as non-streaming MM elements, or made available for streaming retrieval," with the "***MMS Relay/Server decid[ing] whether to use streaming based on*** the media type and the media format of the subjected MM contents, capability negotiation and/or ***user settings/preferences***." *Id*. The "***MMS Relay/Server may convert media types and/or formats of MM contents*** to make it available for streaming retrieval" by the MMS User Agent. *See id.* MMS-Ogawa thus meets claim 5. EX-1003, ¶166.

(e) Claim 6

Claim 6 requires claim 1's "message content" to "comprise[] information associated with a roaming service usage or a roaming service cost."

The MMS-Ogawa user device is configured to use the MMS service as described in TS-23.140. *Supra* § III.A.3(f). TS-23.140 discloses its "MMS User Agent" communicating with the MMS Relay/Server while "[r]oaming." EX-1004, 17, FIG. 2, 19-20.



EX-1004, Figure 2 (annotated)

Part of the MMS service described in TS-23.140 (and implemented in MMS-Ogawa) involves notification about incoming MMs sent to an MMS User Agent. EX-1003, ¶¶167-168. TS-23.140 discloses the MMS Relay/Server sending the MM1-_notification.REQ abstract message to an MMS User Agent that includes an "indication about ***charging related information*** if recipient has to pay for the retrieval [of the incoming MM] or ***roaming condition***." EX-1004, 55-56, 67-68; EX-1003, ¶168.

A POSITA understood that the above-described message content included in MM1_notification.REQ constitutes information "associated with a roaming service usage," as claimed, because information on whether receipt of a message will incur roaming charges is information associated with usage of a roaming service. EX-1003, ¶169. Thus, in MMS-Ogawa, "message content" in MM1_notification.REQ comprises "information associated with a roaming service usage or a roaming service cost," as claimed. EX-1003, ¶169.

(f) Claim 7

Claim 7 requires claim 1's "message content" to "comprise[] a service offer, an advertisement, or a transaction offer." For example, TS-23.140 discloses messages sent by a third-party VASP to the MMS Relay/Server for sending to an MMS User Agent—*see* [1d1]-[1d3] *supra*—that include a classification indicating the message is an advertisement. EX-1004, 112 ("[S]ection [8.7.1] addresses… operations necessary for a VASP to ***provide the service*** by sending a multimedia message ***to one or more subscribers***…"), Figure 8 (showing "data flow of MM7 message distribution"), 115 (listing information in an MM7 message to a MMS Relay/Server, including "[m]essage class" indicating the "[c]lass of MM (***advertisement***…)."), 63 ("Figure 6 illustrates some of [MM1] transactions," including "notifications of new MMs, retrieval of MMs…"), 69, 73 (listing information in an MM1 message, including "[m]essage class" of "***advertisement***…"); EX-1003,

¶¶170-171. Thus, in MMS-Ogawa, "message content" includes "a service offer, an advertisement, or a transaction offer." EX-1003, ¶¶170-171.

(g) Claim 8

Claim 8 requires claim 1's "message content" to "comprise[] information from a third party configured to provide control of a service or a billing for a service." TS-23.140 discloses a third-party value-added service provider (VASP) that controls a service and associated VAS Application(s) in the MMS environment and delivers ***services*** (*e.g.*, news, weather services), via abstract messages, to the MMS User Agent. EX-1004, 14, 34, 112.

As described for claim 2, the VASP controls the content included in abstract messages intended for MMS User Agents, and is therefore configured to control the service. EX-1003, ¶¶172-174. As discussed for claims 3-4, the VASP is configured to control a reply-charging service by activating and setting limitations for it. The VASP is also configured to provide billing for such services by generating and providing a CDR (described for claim 2). EX-1003, ¶175. Thus, in MMS-Ogawa, the content in VASP abstract messages "comprise information from a third party configured to provide control of a service or billing for a service," as claimed.

Alternatively, to the extent claim 8's "third party" is read to require an entity that is ***not*** claim 1's "particular server," it would have been obvious to use the

VASP server to provide User Agents (via the Relay/Server) information controlled by some other source. EX-1003, ¶176. A POSITA understood that a VASP server could be implemented to act as an intermediary server that receives VAS messages from other entities (third-party servers)—*e.g.*, third-party news applications/sources (*e.g.,* blogs, news servers, weather stations)—from which third-party data for the value-added services are retrieved and then transmitted by the VASP to the MMS Relay/Server for delivery to user devices. *Id*. Such an implementation would have desirably allowed a single value-added service provider to offer a wide variety of content from many sources. *Id.* (citing EX-1035 and EX-1036). In such an implementation, the VASP would be implemented to create messages with content originating from third-party sources and then transmit them to MMS User Agent(s). EX-1003, ¶176. Because each third-party source would originate content (*e.g.,* news, weather), such third-parties would control messages sent to the VASP—and would be "configured to ***provide control of***… [the] service" that originates at the third-party server. EX-1003, ¶176.

(h) Claim 9

Claim 9 requires claim 1's "message content" to "comprise[]" one of several alternatives, including "an agent instruction," "or an agent configuration."

TS-23.140 discloses that "[t]he application identifier of the destination application [and] some additional application/implementation specific control information" are "present in an abstract message." EX-1004, 55. The "additional application/implementation specific control information" allows the abstract message to be delivered to the correct destination. EX-1003, ¶¶177-178 (citing EX-1004, 55). For example, such information includes data "distinguishing between multiple instances of the same application" so that a particular instance of the receiving application can be targeted. *Id*. Such information may include data "specifying a particular logical channel" used to address a particular part of the application, *e.g.*, a discussion thread. *Id*.

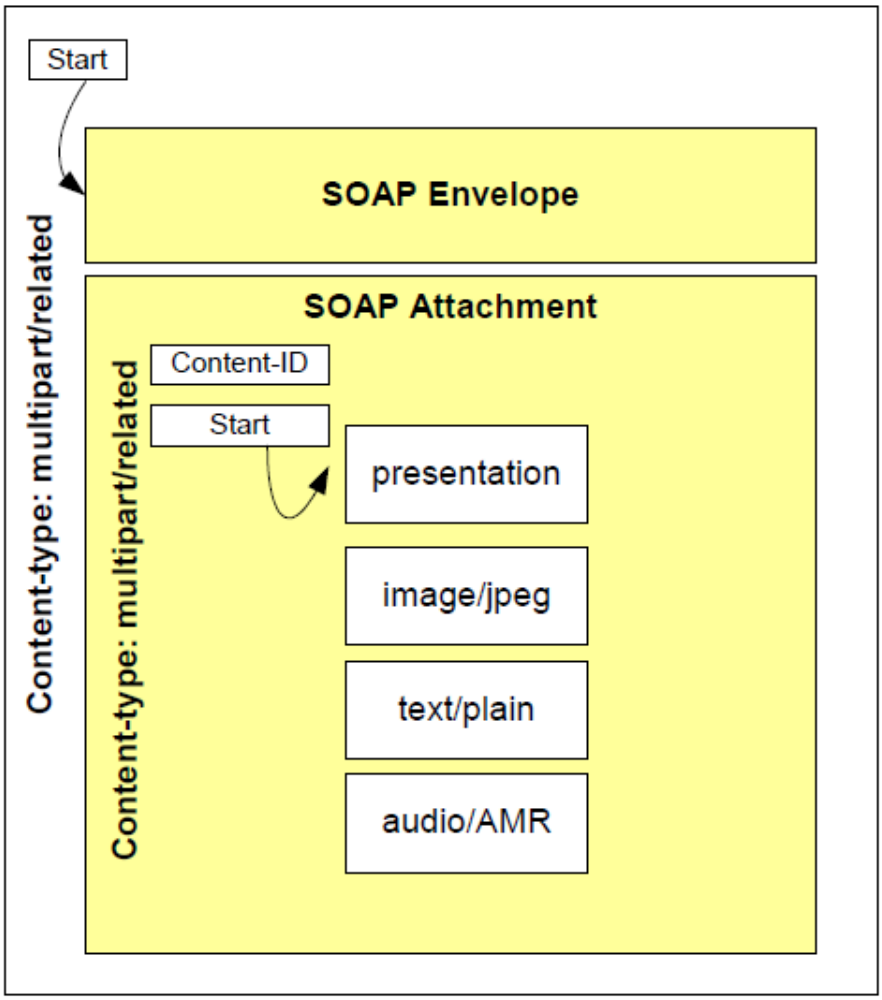
A POSITA understood that such data constitutes "an agent configuration," as claimed, because it has details regarding how the destination application is configured. EX-1003, ¶179. Using this data allows the abstract message to be delivered to the correct location in/instance of the application. *Id*. Such data also constitutes "an agent instruction," as claimed, because it instructs the destination application to use a "particular logical channel" for addressing. EX-1003, ¶¶179-180.

(i) Claim 10

Claim 10 requires claim 1's "message content" to "comprise[] software or a media file." TS-23.140 discloses that a VASP "provide[s]" its "service by ***send-***

ing… multimedia message[s] to" users. EX-1004, 112. TS-23.140 further discloses that MM7 messages from VASPs can "carry a SOAP attachment," which includes "[m]ultimedia content, e.g. audio, image… or a combination of… media types and/or formats." *Id.*, 15, 133; *see also id.*, 113 (explaining that an "originator" (VASP) provides to the MMS Relay/Server "information about the nature of the content in the message" such as "***media types/formats***"); EX-1003, ¶181.

A POSITA understood that such multimedia content would be delivered in a file container and would constitute a ***media file***. EX-1003, ¶182. Indeed, TS-23.140 discloses the structure of the SOAP attachment that carries such content:



EX-1004, 133

Thus, in MMS-Ogawa, "message content" comprises a "media file," as claimed, because a POSITA understood a multimedia message including media such as image and audio would include a ***file*** containing the media. EX-1003, ¶183.

(j) Claim 11

Claim 11 requires claim 1's "message content" to "comprise[] information associated with a service policy."

TS-23.140 discloses that, for "prepaid customer[s]," prior to sending a message to an MMS User Agent, the MMS Relay/Server performs a credit check based on "criteria" that depend on information included ***in*** the message (*e.g.*, size, content type) to see if the customer can send or retrieve such messages. EX-1004, 36. Depending on the credit check result and message content, the Relay/Server decides whether to deliver the message to the customer. *Id.*; EX-1003, ¶¶184-185. A POSITA understood that an MMS service for prepaid customers that predicates message delivery to a user based on criteria like message size and content type is a "service policy," as claimed. EX-1003, ¶185 (citing EX-1001, 8:62-9:3). A POSITA likewise understood that the criteria TS-23.140 discloses to determine whether a service will be delivered are "information associated" with that service policy. EX-1003, ¶185. Thus, messages that are successfully delivered to the MMS User Agent of a prepaid customer, as disclosed in TS-23.140, "comprise[] information" that satisfies the service policy of a prepaid service and is thus "associated with a service policy," as claimed. *Id.*

(k) Claim 12

Claim 12 requires claim 1's "message content" to "comprise[]service usage accounting information."

As discussed earlier regarding [1f], messages sent from a VASP to the MMS User Agent are transmitted through the MMS Relay/Server. EX-1003, ¶186.

TS-23.140 also discloses VASP messages (*e.g.*, MM7_submit.REQ) classified as "accounting" messages, and that the Relay/Server can forward VASP messages to User Agents. EX-1004, 115, 112, 68, 72-73, 30; EX-1003, ¶187. Further, VASPs generate billing information such as a charging data record (CDR) (or other billing information related to VASP messages) that are sent to the Relay/Server for delivery to User Agents. EX-1004, 17, 18, 23, 154, 41; *see also* discussion for claim 2.

Per TS-23.140, a user is alerted of charges associated with a service so that the user can decide whether to use that service. EX-1003, ¶188; EX-1004, 45, 56, 38. Given TS-23.140's disclosures that there may be charges associated with using a VASP service (and messages received therefrom), and that users may be alerted of charges associated with such service, a POSITA would have had reason to implement (and would have reasonably expected success implementing) MMS-Ogawa to provide messages with this information to the MMS User Agent. EX-1003, ¶188. This would have allowed the user to be aware of service charges being incurred because of receiving messages associated with the VASP service. *Id.* (citing EX-1004, 66-67, 38). Such content would constitute "service usage accounting information," as claimed. EX-1003, ¶188.

(l) Claim 13

Claim 13 requires that claim 1's "service control device link agent is further configured to send a device message to the service control server link element over the service control link." As described for claim 1, the MMS User Agent (the "service control device link agent," as discussed for [1a2]) communicates with the MMS Relay/Server (the "service control server link element," as discussed for [1c1]) over MM1 (the "service control link," as discussed for [1a]). EX-1003, ¶189.

TS-23.140 discloses that MMS is used to transport data between two MMS User Agents or between an MMS User Agent and a MMS VAS Application. EX-1004, 54-56. Because communications between the MMS User Agent and MMS VAS Applications occurs through the MMS Relay/Server, such communications use interface MM1. EX-1003, ¶189; EX-1004, 24-25.

Moreover, as described for claim 3, TS-23.140 supports a reply-charging capability whereby the message sender (*e.g.*, the VASP) indicates that it will cover charges for a recipient's (*e.g.*, the MMS User Agent's) reply message. EX-1003, ¶190. In response, the MMS User Agent submits a reply to the MMS Relay/Server and marks the message "reply-MM," indicating that the MMS User Agent is using the reply charging service offered by the sender. EX-1004, 37-39 (§7.1.10).

The '733 specification does not describe a "device message." Based on the

claim's plain language, a POSITA understood that because the MMS User Agent's reply message is from MMS-Ogawa's end-user device, it is a "device message," as claimed. EX-1003, ¶191. Moreover, because communications between the MMS User Agent and MMS Relay/Server happen over MM1, the reply-MM message is sent "over the service control link," as claimed. *Id.*

(m) Claim 14

Claim 14 requires claim 13's "device message" to "comprise[] a service usage report or an integrity report."

As discussed for claim 13, TS-23.140 discloses that a VASP sending an MM can utilize a reply-charging functionality whereby the VASP offers to pay for a reply message by the recipient (a MMS User Agent). EX-1003, ¶192. A POSITA understood that reply charging is an offered service, and therefore the recipient's (MMS User Agent) reply to the message (the reply-MM) constitutes a usage of the service. *Id*. Moreover, the reply-MM includes information regarding (***a report of***) this service usage by "mark[ing] the MM as a reply-MM," and "includ[ing] the message ID of the original MM which it replies to." EX-1004, 37-39.

(n) Claim 15

Claim 15 requires claim 13's "device message" to "comprise[] a user response." A POSITA understood MMS-Ogawa's reply-MM (described for claim 13) "comprises a user response" because it responds to a message received from an

originator (a VASP) and is sent when a "user intends to send" this message. EX-1004, 37-39; EX-1003, ¶193.

(o) Claim 16

Claim 16 requires claim 15's "user response" to "comprise[] an acknowledgement of a roaming cost or a roaming usage."

As discussed for claim 6, TS-23.140 discloses that the "MMS User Agent" may communicate with the MMS Relay/Server while "[r]oaming." EX-1004, 17, FIG. 2, 19-20. Further, the MMS Relay/Server can recommend to the User Agent a particular retrieval mode to retrieve a particular message, "based on different factors," including "roaming conditions." EX-1004, 19-20. The recommendation can include an "indication about ***charging*** related information if recipient has to pay for the retrieval or ***roaming condition***," explaining why the retrieval mode is recommended for the MM. *Id.*, 67; EX-1003, ¶194.

The end user then "make[s] a decision whether to download the MM." *Id.*, 19. The MMS User Agent "ask[s] for end user confirmation before any… retrieval of an MM triggered by an application due to charging…" *Id.*, 56. After confirmation, the MMS User Agent requests to retrieve the message from the MMS Relay/Server. *Id.*, 19-20, 56.

Because the user is notified of a service cost while roaming and can decide whether or not to retrieve a message, a POSITA understood that such a user response (carried out by the MMS User Agent) requesting message delivery after being notified of a roaming cost or usage is an "***acknowledgement***" of roaming cost and/or usage, as claimed, of services while the device is roaming. EX-1003, ¶¶195-196.

(p) Claim 17

Claim 17 requires claim 15's "user response" to "comprise[] an acknowledgment of" various alternatives, including "a service usage." A POSITA understood the user response (described for claim 15) "comprises an acknowledgement of… a service usage" because when the user sends a reply message marked as a reply-MM, the message ID of the original (replied-to) message is provided (EX-1004, 37-39), and the user acknowledges that the offered reply-charging service was accepted and used. EX-1003, ¶197.

(q) Claim 19

Claim 19 requires claim 1's "end-user device" to include "a user interface," and requires "the particular device agent" to be "configured to assist in presenting a notification through the user interface, the notification being based on the message content." MMS-Ogawa's User Agent is on an end-user device (as discussed

for [1pre]), which includes destination applications that are "particular device agent[s]" (as discussed for [1d3]).

TS-23.140 discloses "MM presentation" and "presentation of notifications to the user." EX-1004, 19 ("[T]he MM may be ***displayed*** to the end user with or without any pre-notice."); *see also id.*, 16 (Figure 1, showing end-user devices including displays), 155 (Figure A.1, similar). Given the well-known use of user interfaces on devices to facilitate content presentation to a user, a POSITA understood TS-23.140's user device to include a "user interface," as claimed, on, *e.g.,* a display. EX-1003, ¶¶198-199. Alternatively, such an implementation would have been a conventional and obvious way to implement what TS-23.140 describes, and is nothing more than utilizing familiar, known components (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, ¶199.

TS-23.140 also discloses presenting, in a manual message retrieval mode, a "pre-notice" notification about a multimedia message (MM) to the user so that the user can decide whether to request retrieving and viewing the MM. EX-1004, 19-20; EX-1003, ¶200. In particular, the MMS Relay/Server sends a "MM1_notification.REQ" message to the MMS User Agent to notify it of content included in an upcoming MM, *e.g.*, details about the MM's class and size. EX-1004, 61, 67-68. Based on these disclosures, a POSITA understood that the pre-notice notification is

based on message content in MM1_notification.REQ received from the MMS Relay/Server. EX-1003, ¶200. As discussed above, in MMS-Ogawa, notifications (including pre-notice notifications) are displayed/presented using a ***user interface*** of the end-user device. EX-1003, ¶200.

A POSITA also understood that MMS-Ogawa's destination application "assists" in presenting this notification, as claimed. EX-1003, ¶201. MM1_notification.REQ is an abstract message and the MMS User Agent "***immediately*** route[s]" content of such messages to the destination application specified in the message (*see* discussion above regarding [1f]) "without present[ing the content] to the user." EX-1004, 57, 67-68; EX-1003, ¶201. Given that the MMS User Agent routes information intended to be presented to a user (*e.g.*, an option to accept/retrieve an MM) to a ***destination application***, and given that the User Agent itself does not present such information to the user, a POSITA would have understood TS-23.140 to teach its destination applications "assist[ing]" with presentation of such notifications, either because the destination application itself presents the notification to the user, or because it sends pertinent information to another component responsible for displaying such notifications (*see* discussion *infra* regarding claim 27), thereby causing the notification to be displayed. EX-1003, ¶201.

Further, TS-23.140 teaches a received MM (intended for a destination application) containing visual content. EX-1003, ¶202; EX-1004, 15, 20, 30. A

POSITA would have understood that a destination application that receives an MM would be configured to assist in presenting the notification of any visual content contained in the received MM. EX-1003, ¶202. Alternatively, a POSITA would have had reason to implement the destination application to assist in providing such presentations to the user visually, because it was conventional and obvious for messages containing visual content to be presented visually to users. *Id.*; EX-1004, 35-36. A POSITA would have reasonably expected success with such an implementation. EX-1003, ¶202.

A POSITA thus understood the device agents in MMS-Ogawa to be "configured to assist in presenting a notification through the user interface, the notification being based on the message content," as claimed. EX-1003, ¶203.

(r) Claim 21

Claim 21 requires claim 1's "service control link" (interface MM1, as discussed for [1a]) to "support[] asynchronous transmissions" by claim 1's "service control server link element" (the MMS Relay/Server, as discussed for [1c1]). The '733 Patent uses the term "asynchronous" to encompass transmissions that occur in response to a server receiving a user request for the transmission, or as a result of polling. *See, e.g.*, EX-1001, 38:19-32, 43:16-19, 69:23-24; EX-1003, ¶204. A POSITA thus understood that the term "asynchronous transmissions" encompasses

transmissions by a server sent to a client in response to a request from the client. EX-1003, ¶204.

TS-23.140 discloses the MMS Relay/Server using MM1 (the ***service control server link element*** in MMS-Ogawa) to transmit messages in response to receiving a trigger event from the MMS User Agent based on, *e.g.,* a user action. EX-1003, ¶¶205-206; EX-1004, §7.1.2 ("Upon reception of an MM the recipient ***MMS Relay/Server… shall generate a notification to the recipient MMS User Agent***"), §7.1.2.1 (MMS User Agent requests retrieval of the message upon receipt of the notification), §8.1.5.1 ("MMS User Agent… issue[s] an MM1_retrieve.REQ to the… MMS Relay/Server to initiate the retrieval process"), §5.1.1.1. A POSITA thus understood that MM1 (the claimed ***service control link***) in MMS-Ogawa supports asynchronous transmissions, consistent with how this term is used in the '733 specification. EX-1003, ¶¶205-207.

(s) Claim 22

Claim 22 requires claim 1's "service control link" (MM1, as discussed for [1a]) "support[] periodic transmissions" by "the service control link element" (the MMS Relay/Server, as discussed for [1c1]).

TS-23.140 discloses that, "[f]or discovery of incoming messages from external messaging systems different mechanisms may be utilized, e.g. [by] ***periodic polling*** for messages on External Server, ***followed by retrieval by the MMS User***

Agent via the MMS Relay/Server." EX-1004, 90-91, 59-61; EX-1003, ¶208. An obvious way to implement TS-23.140's "periodic polling" was by implementing the MMS Relay/Server to aggregate messages between periodic requests from the MMS User Agent and send the aggregated messages upon receipt of a periodic polling message. EX-1003, ¶¶209-210 (citing EX-1004, 59-60, Figure 6). As with all transmissions between the MMS Relay/Server and the MMS User Agent, a POSITA understood that such "periodic" retrieval of message(s) from External Server(s) via the MMS Relay/Server (or pre-notifications associated with such messages) occurred over MM1. EX-1003, ¶¶210-211. A POSITA also understood that the MMS Relay/Server's transmissions over MM1 responding to periodic polling from the MMS User Agent would likewise be periodic whenever network conditions permitted—thus meeting claim 22. *Id.*

A POSITA also had reason to ensure that MM1 "***support[ed]*** periodic transmissions" by the MMS Relay/Server to the MMS User Agent, since this would have beneficially allowed the MMS Relay/Server to (1) immediately respond to periodic requests for content (*e.g.,* at the frequency that a MMS User Agent indicated using TS-23.140's "periodic polling") whenever network conditions permitted, and (2) facilitate other periodic communications from external servers (*e.g.,* periodic news/weather updates). EX-1003, ¶212. A POSITA would reasonably have expected success doing so, since periodic server-client communications were

commonplace before the Critical Date. EX-1003, ¶212 (citing EX-1039, 12:53-60, EX-1040, 2:59-64).

(t) Claims 23-24

Claim 23 requires claim 1's "service control device link agent" (the MMS User Agent, as discussed for [1a2]) to be "configured to send" or "receive" a "device credential" to "the network system" (of which the MMS Relay/Server is a part, as discussed for [1a]) "during a service authorization sequence." EX-1003, ¶213. Claim 24 requires that the "device credential" comprise one of several alternatives, *e.g.*, a "phone number," "identification number," or "device identifier."

When submitting an MM message, an originating MMS User Agent provides an address of the recipient in a recipient address field that is transmitted to the MMS Relay/Server. EX-1004, 57-58. The recipient's address can be "an E.164 (MSIDN) or RFC2822 address." *Id.* The address can be a "PLMN address" such as "a local telephone number, or a numeric short code". *Id*. The message also includes the "address of the originator" (the originating MMS User Agent and its device), which has the same address format. *See id.* Such addresses each constitute a device credential because they identify the originating or receiving entity. *Id.*; EX-1003, ¶214. Thus, when an MMS User Agent sends a MM message, the MMS User Agent sends a "device credential" to the MMS Relay/Server. EX-1003, ¶214.

TS-23.140 also discloses that an "originator MMS User Agent may support a request for the sender's address to be hidden from the recipient(s)." EX-1004, 36-37. "If the originator's MMS Relay/Server does not allow address hiding (anonymous messages)… a message containing a request for address hiding shall be rejected." *Id*. MMS Relay/Server may thus reject or authorize the address-hiding request and either authorize use of this service as part of the message-sending sequence or reject the use of this service during the message-sending sequence. EX-1003, ¶215. For example, if "MMS Relay/Server does not allow address hiding… MMS Relay/Server shall return an error information to the originator MMS User Agent." EX-1004, 36. A POSITA understood this sequence of communications for requesting an address hiding service to constitute a "service authorization sequence," as claimed. EX-1003, ¶215.

Thus, a POSITA understood that the MMS User Agent (the "service control device link agent," as discussed for [1a2]) is "configured to send a device credential" (TS-23.140's originator and recipient addresses) to "the network system" (because it is sent to the MMS Relay/Server, per the discussion regarding [1a]) during a "service authorization request"—a sequence of communications between MMS User Agent and MMS Relay/Server regarding authorization for an address hiding service, discussed above, as part of the message transmission. EX-1003, ¶216. A POSITA likewise understood the originator and recipient addresses constituted "a

phone number," "identification number," or "device identifier," as required by claim 24. EX-1003, ¶216 (citing EX-1004, 57-58).

(u) Claim 25

Claim 25 requires claim 1's "transmission over a service control link" to be "within an ambient service." The specification never uses the term "within an ambient service," or explain what it means. The '733 patent appears to use the term "ambient" service to encompass any service that the user may pay for or receive for free (*e.g.*, pay as you go sessions, news service, etc.) ***beyond*** a "basic" calling plan/service for the user's user device. EX-1003 (citing EX-1001, 67:37-53).

TS-23.140 discloses that the "VASP may mark the content of the message with a service code that may be transferred by the MMS Relay/Server in the form of charging information for use by the billing system to properly bill the user for the service being supplied." EX-1004, 113; EX-1003, ¶¶217-218. Because each such message is coded with charging information for that message, a POSITA would have understood that the user would be billed (and would have to pay for) the service used, that this service was beyond the "basic" messaging service described in TS-23.140. EX-1003, ¶218. A POSITA understood that such service was an ***ambient service***, as claimed. *Id.*

Additionally, the VASP in TS-23.140 transmits services that are similar to those identified as "ambient services" in the '733 Patent. The '733 Patent lists "a

news service, eReader, PND service, ***pay as you go*** session Internet" as exemplary ambient services. EX-1001, 67:37-53. Similarly, VASPs provide, via messages sent by a VAS application, "news services or weather forecasts" to users. EX-1004, 14.

Since VASPs send transmissions to MMS User Agents through MM1 (the "service control link," as discussed for [1a]), a POSITA understood that transmissions of messages related to these services are "within an ambient service," as claimed. EX-1003, ¶¶219-223; *see also id*, ¶¶221-222 (citing EX-1032, and noting that even if the '733 Patent had used the term "ambient service" in its ordinary meaning as used in the field, the claim would still be obvious).

(v) Claim 26

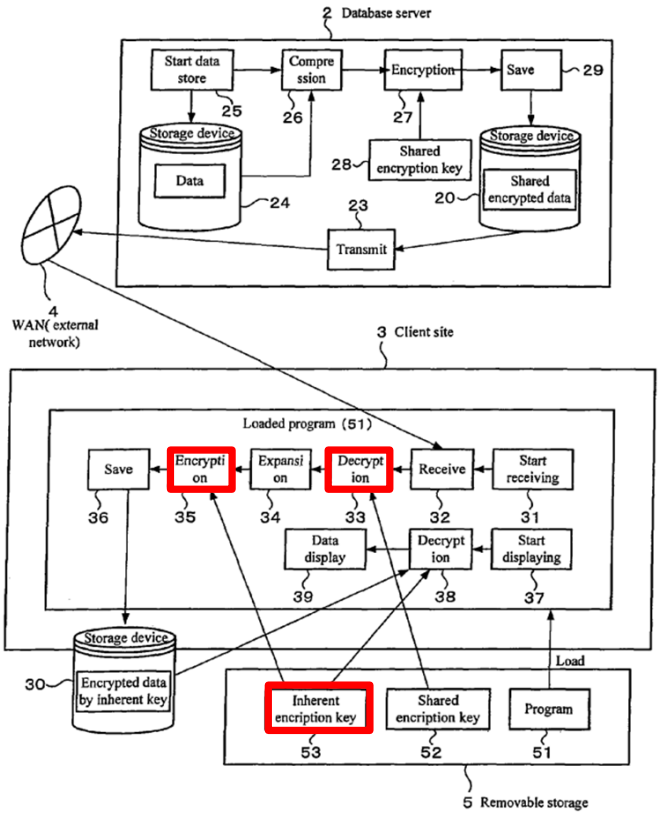
Claim 26 requires claim 1's "particular device agent" to "comprise[] software." MMS-Ogawa's destination applications (the "device agents," as discussed for [1b]) "comprise software," as claimed. EX-1003, ¶224; EX-1004, 54 (§7.1.18: describing registration for application data transport using MMS, where the registering entity is a "downloadable application" on a "mobile phone").

(w) Claim 27

Claim 27 calls the encryption key recited in claim 1 "a first encryption key," and requires claim 1's "service control device link agent" to be "configured to encrypt the message content using a ***second*** encryption key before delivering the message content to the particular agent." EX-1003, ¶225.

TS-23.140's MMS User Agent (the "***service control device link agent***," as discussed for [1a2]/[30a2]) is responsible for receiving a message from TS-23.140's MMS Relay/Server, decrypting the message using a first encryption key, and sending message content to a destination application (the "***particular device agent***," as discussed for [1d3]/[30d3]-[30d4]). EX-1003, ¶226.

As discussed *supra* §III.A.3(d), Ogawa discloses an encryption unit for re-encrypting data for, *e.g.*, transmission within the user device. EX-1005, 5:59-6:9; EX-1003, ¶227. In Ogawa, a message received and decrypted at the client (using receive unit 32 and encryption unit 33) is converted back to its original format (using decompression/expansion unit 34), and encrypted again by encryption unit 35, using an "inherent encryption key 53" before being transmitted within the client device, *e.g.*, for storage. EX-1005, 5:59-6:26, 5:24-25; EX-1003, ¶227. Inherent encryption key 53 is a second encryption key different from the first encryption key used to encrypt/decrypt data transmitted between server and client. EX-1003, ¶227.



EX-1005, FIG.7 (annotated)

As discussed *supra* §III.A.3(d), a POSITA had reason to include the encryption functionality as part of MMS-Ogawa's User Agent—*e.g.*, to secure decrypted received data before transmitting it to any other component on the user device—and would have reasonably expected success with such an implementation. EX-1003, ¶228.

A POSITA would further have been motivated to implement MMS-Ogawa's user device to secure/encrypt message content (received from, *e.g.*, the MMS Re-

lay/Server) using a ***different*** encryption key than the one used to decrypt the received data (*e.g.*, Ogawa's disclosed inherent key) prior to delivery to device storage or a destination application, as taught by Ogawa. EX-1003, ¶229 (citing EX-1037); EX-1005, 6:1-26. Such internal encryption within the device using an inherent key was expressly taught by Ogawa and would have improved security of data in MMS-Ogawa's user device when stored on the device or when transmitted within the device, and would have helped, *e.g.*, prevent unauthorized viewing or use of the data by rogue/unauthorized software on the device. EX-1003, ¶229.

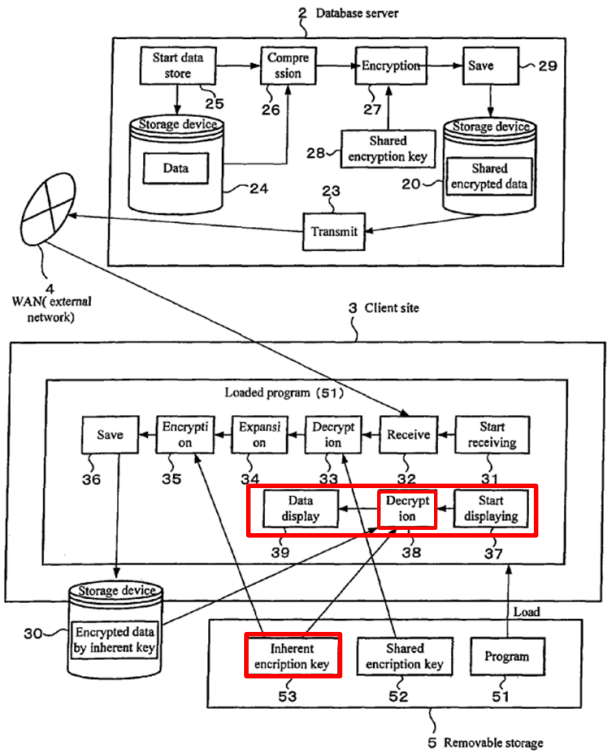
A POSITA would also have had reason to implement MMS-Ogawa's User Agent such that it performed any intermediary functions/steps between decryption (*e.g.*, by Ogawa's unit 33) and re-encryption (*e.g.*, by Ogawa's unit 35) that were required to ensure that the destination (on the user device) received data with correct format and content. EX-1003, ¶230 (citing EX-1005, 5:65-6:3). A POSITA would have reasonably expected success implementing MMS-Ogawa's User Agent to perform the intermediary functions described in Ogawa, as discussed above—*e.g.*, by incorporating Ogawa's expansion unit 34—because the prior art components would continue to perform functions they performed prior to the combination. EX-1003, ¶230. For example, the MMS User Agent would continue to receive, decrypt, and send data within the user device, and Ogawa's expansion and encryption units (implemented as part of the MMS User Agent) would continue to

convert decrypted data into its original format before encrypting it for use within the user device. *Id.*

Claim 27 also requires "the second encryption key" to be "shared by the service control device link agent and the particular agent."

As noted for claim 19, MMS-Ogawa's user device is capable of displaying messages to a user. EX-1003, ¶¶231-232; EX-1004, 16 (Figure 1), 19, 155 (Figure A.1). As discussed below, a POSITA had reason to implement the display functionality in the MMS-Ogawa user device such that it could display data that was encrypted using Ogawa's inherent key 53 (pursuant to Ogawa's teachings discussed above). EX-1003, ¶232.

Ogawa teaches using "display units 37-39" to "provide the necessary functionality for rendering decoded data to a display of" the client; in order to "render" and display data stored on the client, Ogawa teaches decrypting the data using the same inherent key 53 that encryption unit 34 used to encrypt the data for storage within the device. EX-1005, 5:24-30, 6:10-18; EX-1003, ¶233.



EX-1005, FIG. 7 (annotated)

Based on Ogawa's teachings, a POSITA had reason to implement MMS-Ogawa's user device to incorporate Ogawa's display units 37-39 to be able to decrypt and display data encrypted using Ogawa's inherent key 53. EX-1003, ¶234. A POSITA would have reasonably expected success implementing MMS-Ogawa's user device to use Ogawa's display units 37-39 to perform the decryption and display functions described in Ogawa, because the prior art components would continue to perform functions they performed prior to the combination. EX-1003, ¶234.

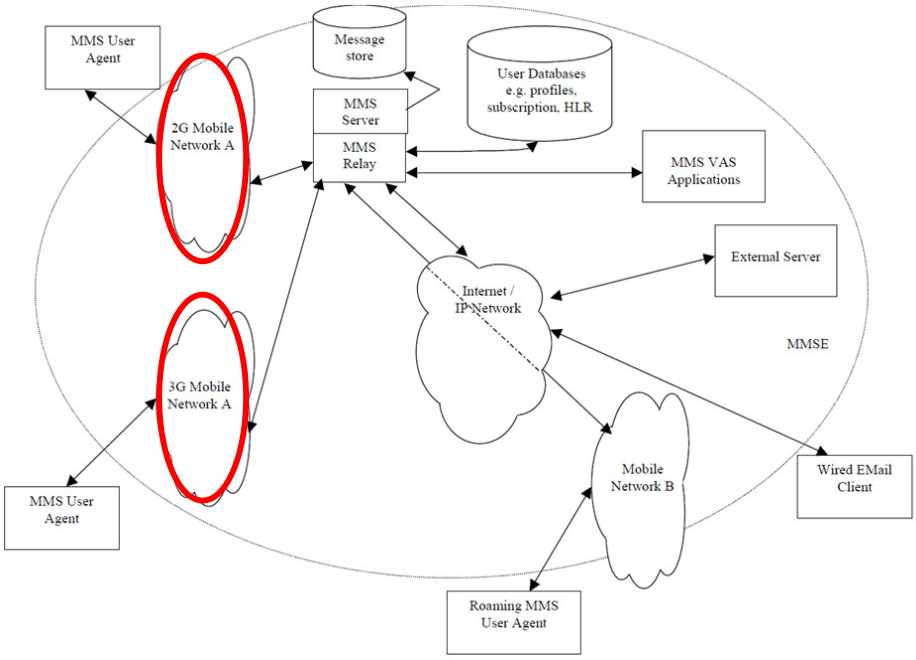
In such an implementation, for data received by the MMS User Agent from the MMS Relay/Server that was intended for immediate display to the user, a POSITA understood that MMS-Ogawa's display units 37-39 collectively constituted a destination application in the user device that performed display functions on behalf of an entity (*e.g.*, client, server, another application), thus constituting one of the "***plurality of device agents***" for [1b], and "***a particular device agent***" for [1d3], in claim 1. EX-1003, ¶234.

Because both the MMS User Agent and MMS-Ogawa's display units 37-39 use the same key for encryption and decryption, a POSITA would also have understood that the inherent key (the claimed ***second encryption key***) is ***shared*** by encryption unit 35 in the MMS User Agent (***the service control device link agent,*** as claimed) and the destination display units 37-39 (***the particular agent***, as claimed). EX-1003, ¶235.

(x) Claim 29

Claim 29 requires claim 1's "service control link" which is "configured to support control-plane communications" to be configured for such communications "using an Internet protocol." As described with reference to [1a], [1a1], and [1a2], MM1 in MMS-Ogawa (the claimed "service control link") supports control-plane communications. Moreover, communications between the MMS User Agent and the MMS Relay/Server occur over wireless networks that use an Internet protocol.

EX-1003, ¶236. In FIG. 2 reproduced below, a 2G mobile network and a 3G mobile network each facilitate communications between a MMS User Agent and the MMS Relay/Server. *Id*.



EX-1004, Figure 2 (annotated)

TS-23.140 explains that the "basis of connectivity between these different networks shall be provided by the ***Internet Protocol*** and its associated set of messaging protocols." EX-1004, 17. "This approach enables messaging in 2G and 3G wireless networks to be compatible with messaging systems found on the Internet." *Id*. Given these disclosures in TS-23.140, a POSITA would have understood that each of the 2G and 3G networks use an Internet protocol. EX-1003, ¶237. Alternatively, this would have been a conventional, obvious way to implement what TS-

23.140 describes, and is nothing more than utilizing familiar, known components to achieve a predictable, desirable result of enabling TS-23.140's user agent to send and receive data over the Internet. *KSR*, 550 U.S. at 416; EX-1003, ¶237.

Thus, because communications in MMS-Ogawa occur over MM1, including control plane communications, MMS-Ogawa meets the requirement that the "service control link" (MM1, as described for [1a2]) "is configured to support control-plane communications using an Internet Protocol," as claimed. EX-1003, ¶238.

IV. PTAB DISCRETION SHOULD NOT PRECLUDE INSTITUTION

A. 35 U.S.C. §325(d) – *Advanced Bionics*

The references advanced in this Petition were not previously before the Office. *See generally* EX-1002. Thus, the Office has not considered the references or combinations presented in this Petition. Moreover, the same or substantially the same arguments were not previously presented to the Office. Indeed, there could be no overlap between the arguments made before the Office because the Examiner issued no prior art rejections during prosecution. *Id*.

Further, material error occurred during prosecution because Examiner failed to consider systems of the above-presented grounds, and how they rendered obvious every claim feature of the Challenged Claims. Indeed, Petitioners have shown a reasonable likelihood that at least one of the Challenged Claims is unpatentable over the applied art on the current record. *Supra* §III.A; *see Tokyo Ohka Kogyo Co., Ltd.*

v. Fujifilm Elec. Materials U.S.A., Inc., PGR2022-00010, Paper 9, 8-9 (PTAB June 6, 2022). Therefore, §325(d) discretionary denial is not warranted.

B. 35 U.S.C. §314(a) - *Fintiv*

The Petition's merits are compelling, which "alone demonstrates that the PTAB should not discretionarily deny institution under *Fintiv*." EX-1020, 4-5. Moreover, the *Fintiv* factors do not favor denial.

Factor 1 favors institution because Google is not a party in the EDTX litigation and no litigation party (Samsung, Headwater) has requested a litigation stay.

Factor 2 favors institution because Google is not a party in the EDTX litigation, and the Court's trial date for the litigation parties (Samsung, Headwater) is speculative and subject to change. The Board will likely issue its Final Written Decision around June 2025, 5-6 months after the currently scheduled trial date (January 6, 2025). EX-1022, 1. However, as the PTAB has recognized, "scheduled trial dates are unreliable and often change." EX-1020, 8.

Factor 3 favors institution because Google is not a party in the EDTX litigation. Moreover, Petitioners diligently filed this Petition months ahead of the one-year time bar for Samsung, while the EDTX Litigation is in its early stages. Indeed, by the anticipated institution decision deadline in June/July 2024, the litigation will still be in early stages—fact and expert discovery will be ongoing and the *Markman* hearing will not have occurred. *Id.*

Factor 4 favors institution because Google is not a party in the EDTX litigation and Samsung stipulates to not pursue the IPR grounds in the EDTX litigation. EX-1023. Thus, "[i]nstituting trial here serves overall system efficiency and integrity goals by not duplicating efforts and by resolving materially different patentability issues." *Apple, Inc. v. SEVEN Networks, LLC*, IPR2020-00156, Paper 10, 19 (June 15, 2020); *Sand Revolution II, LLC v. Continental Intermodal Group-Trucking LLC*, IPR2019-01393, Paper 24, 12 (June 16, 2020); *Google LLC v. Flypsi, Inc.*, IPR2023-00360, Paper 9, 36-39 (August 2, 2023).

Factor 5 favors institution because Google is not a party in the EDTX litigation, so the parties in the EDTX litigation are not the same.

Factor 6 favors institution because the merits of this Petition are compelling.

V. CONCLUSION AND FEES

The Challenged Claims are unpatentable. Please charge fees to Deposit Account 06-1050.

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

A. Real Party-In-Interest Under 37 C.F.R. § 42.8(b)(1)

Samsung Electronics Co., Ltd. ("Samsung") and Google LLC ("Google") are the petitioners and real parties-in-interest. Samsung Electronics America, Inc. is an additional real-party-in-interest.

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

The '733 Patent is the subject of *Headwater Research LLC v. Samsung Electronics Co., Ltd. et al.*, 2:23-cv-00103, E.D. Tex., filed March 10, 2023. Samsung and Headwater are also involved in case nos. 2:22-cv-00422 and 2:22-cv-00467, also in E.D. Tex.

Petitioners are not aware of any other disclaimers, reexamination certificates, or IPR petitions addressing the '733 Patent.

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

Petitioners provide the following designation of counsel.

Lead Counsel	Backup counsel
W. Karl Renner, Reg. No. 41,265 Fish & Richardson P.C. 60 South Sixth Street, Suite 3200 Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 Email:IPR39843-0164IP1@fr.com	Jeremy J. Monaldo, Reg. No. 58,680 Karan Jhurani, Reg. No. 71,777 60 South Sixth Street, Suite 3200 Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 IPR39843-0164IP1@fr.com Gregory F. Corbett, pending admission *pro hac vice* Turhan F. Sarwar, pending admission *pro*

	hac vice Wolf, Greenfield & Sacks, P.C. 600 Atlantic Avenue Boston, MA 02210 Tel: 617-646-8000 Fax: 617-646-8646 Gregory.Corbett@wolfgreenfield.com TSarwar-PTAB@wolfgreenfield.com

D. Service Information

Please address all correspondence and service to the address listed above. Petitioners consent to electronic service by email at IPR39843-0164IP1@fr.com Gregory.Corbett@wolfgreenfield.com, and TSarwar-PTAB@wolfgreenfield.com (referencing No. 39843-0164IP1).

Respectfully submitted,

Dated 01/23/2024

/Karan Jhurani/

W. Karl Renner, Reg. No. 41,265
Jeremy J. Monaldo, Reg. No. 58,680
Karan Jhurani, Reg. No. 71,777
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

(Control No. IPR2024-00341)

Attorneys for Petitioner Samsung

Gregory F. Corbett,
pending admission *pro hac vice*,
Turhan F. Sarwar,
pending admission *pro hac vice*,
Wolf, Greenfield & Sacks, P.C.
600 Atlantic Avenue
Boston, MA 02210
T: 617-646-8000
F: 617-646-8646

Attorneys for Petitioner Google

CERTIFICATION UNDER 37 CFR § 42.24

Under the provisions of 37 CFR § 42.24(d), the undersigned hereby certifies that the word count for the foregoing Petition for *Inter Partes* Review totals 13,987 words, which is less than the 14,000 allowed under 37 CFR § 42.24.

Dated 01/23/2024

/Karan Jhurani/

W. Karl Renner, Reg. No. 41,265
Jeremy J. Monaldo, Reg. No. 58,680
Karan Jhurani, Reg. No. 71,777
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

Attorneys for Petitioner Samsung

Gregory F. Corbett,
pending admission *pro hac vice*,
Turhan F. Sarwar,
pending admission *pro hac vice*,
Wolf, Greenfield & Sacks, P.C.
600 Atlantic Avenue
Boston, MA 02210
T: 617-646-8000
F: 617-646-8646

Attorneys for Petitioner Google

CERTIFICATE OF SERVICE

Pursuant to 37 CFR §§ 42.6(e)(4)(i) *et seq.* and 42.105(b), the undersigned certifies that on January 23, 2024, a complete and entire copy of this Petition for *Inter Partes* Review, Powers of Attorney, and all supporting exhibits were provided via Federal Express, to the Patent Owner, by serving the correspondence address of record as follows:

Headwater Research LLC
Outside Firm 1
110 North College Avenue, Suite 1116
Tyler, TX 75702

/Michael Stanwyck/
Michael Stanwyck
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
(202) 626-7790