

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

SAMSUNG ELECTRONICS CO. LTD., GOOGLE LLC,  
and SAMSUNG ELECTRONICS AMERICA, INC.,  
Petitioner,

v.

HEADWATER RESEARCH LLC,  
Patent Owner.

---

IPR2024-00341  
Patent 8,406,733 B2

---

Before HYUN J. JUNG, ROBERT J. WEINSCHENK, and  
GARTH D. BAER, *Administrative Patent Judges*.

JUNG, *Administrative Patent Judge*.

DECISION  
Granting Institution of *Inter Partes* Review  
*35 U.S.C. § 314*

## I. INTRODUCTION

### A. *Background and Summary*

Samsung Electronics Co. Ltd., Google LLC, and Samsung Electronics America, Inc. (collectively, “Petitioner”) filed a Petition (Paper 4, “Pet.”) requesting institution of an *inter partes* review of claims 1–17, 19, 21–27, 29, and 30 of U.S. Patent No. 8,406,733 B2 (Ex. 1001, “the ’733 patent”). Headwater Research LLC (“Patent Owner”) did not file a Preliminary Response.

Under 35 U.S.C. § 314, an *inter partes* review may not be instituted “unless . . . there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” Upon consideration of the Petition and for the reasons explained below, we determine that Petitioner has shown a reasonable likelihood of prevailing with respect to at least one of the challenged claims.

Thus, we institute an *inter partes* review of claims 1–17, 19, 21–27, 29, and 30 of the ’733 patent on the only presented challenge. 37 C.F.R. § 42.108(a) (“When instituting . . . review, the Board will authorize the review to proceed on all of the challenged claims and on all grounds of unpatentability asserted for each claim.”); *see also SAS Inst. Inc. v. Iancu*, 138 S. Ct. 1348, 1359–60 (2018).

### B. *Real Parties in Interest*

Petitioner identifies Samsung Electronics Co. Ltd., Google LLC, and Samsung Electronics America, Inc. as real parties in interest. Pet. 79. Patent Owner identifies itself as the real party in interest. Paper 6, 2.

### C. *Related Matters*

The parties identify *Headwater Research LLC v. Samsung Electronics Co., Ltd.*, 2:23-cv-00103 (E.D. Tex.) as a related matter. Pet. 79; Paper 6, 2.

Petitioner states that the parties “are also involved in case nos. 2:22-cv-00422 and 2:22-cv-00467, also in E.D. Tex.” Pet. 79. Patent Owner further identifies IPR2024-00342 as a related matter. Paper 6, 2. A related patent is challenged in IPR2024-00010.

*D. The '733 Patent (Ex. 1001)*

The '733 patent issued on March 26, 2013 from an application filed on May 1, 2012 that is a continuation of an application filed on March 2, 2009 and claims priority to four provisional applications, the earliest of which was filed on January 28, 2009. Ex. 1001, codes (22), (45), (60), (63), 1:7–21.

Figure 16 of the '733 is below reproduced.

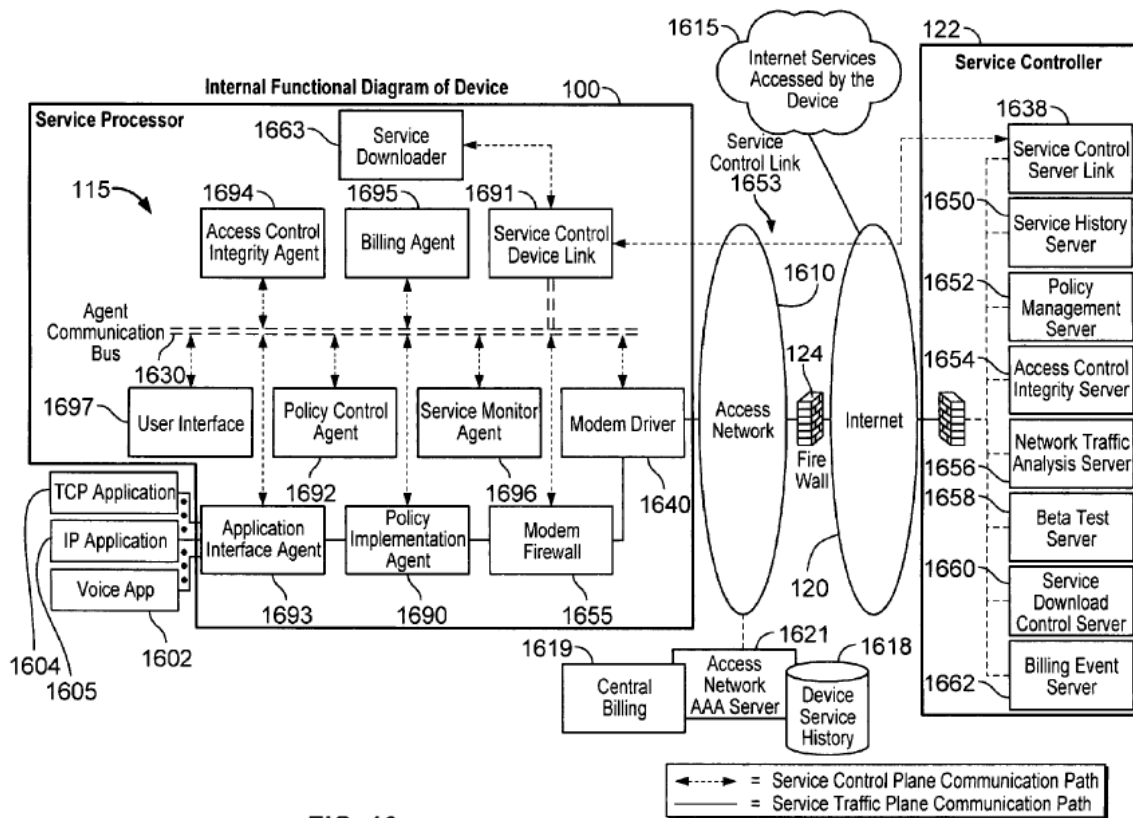


FIG. 16

Figure 16 shows “a functional diagram illustrating a device based service processor and a service controller.” Ex. 1001, 2:43–44. The '733

patent describes “[d]evices and methods for receiving control-plane communications from a network element over a secure service control link.”

*Id.* at code (57).

The network element includes a service control server link element that is communicatively coupled to a plurality of servers. The device includes a plurality of device agents communicatively coupled to a service control device link agent through an agent communication bus. The service control device link agent receives an encrypted agent message from the service control server link element over the secure service control link, uses an encryption key to obtain a decrypted agent message comprising a particular agent identifier and message content for delivery to the particular device agent, and, based on the particular agent identifier, delivers the message content to the particular device agent over the agent communication bus.

*Id.*

*E. Illustrative Claim*

The ’733 patent includes 30 claims, of which Petitioner challenges claims 1–17, 19, 21–27, 29, and 30. Of the challenged claims, claims 1 and 30 are independent, and claim 1 is below reproduced.

1. An end-user device comprising:
  - a modem for enabling communication with a network system over a service control link provided by the network system over a wireless access network, the service control link secured by an encryption protocol and configured to support control-plane communications between the network system and a service control device link agent on the end-user device;
  - 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
  - memory configured to store an encryption key, the encryption key shared between the service control device link agent and a service control server link element of the network system;

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,

using the encryption key, obtain a decrypted agent message, 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, the message content from a particular server of a plurality of servers communicatively coupled to the service control server link element, and

based on the particular agent identifier, deliver the message content to the particular device agent over the agent communication bus.

Ex. 1001, 163:47–164:12.

*F. Asserted Prior Art and Proffered Testimonial Evidence*

Petitioner identifies the following references as prior art in the asserted ground of unpatentability:

Name	Reference	Exhibit
Ogawa	US 8,195,961 B2, issued June 5, 2012	1005
TS-23.140	3GPP TS 23.140 v6.9.0 (2005-03); 3rd Generation Partnership Project; Technical Specification Group Terminals; Multimedia Messaging Service (MMS); Functional Description; Stage 2 (Release 6)	1004

Petitioner contends that TS-23.140 is prior art under § 102(b) and Ogawa is prior art under §§ 102(a) and 102(e).<sup>1</sup> Pet. 1. Petitioner also provides a Declaration of Dr. Patrick G. Traynor. Ex. 1003.

---

<sup>1</sup> The relevant sections of the Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112–29, 125 Stat. 284 (Sept. 16, 2011), took effect on March 16, 2013. Because the ’733 patent issued from an application filed before that date, our citations to 35 U.S.C. §§ 102 and 103 in this Decision are to their pre-AIA versions. *See also* Pet. 5 (stating that “[t]he ’733 Patent claims

*G. Asserted Ground*

Petitioner asserts that claims 1–17, 19, 21–27, 29, and 30 are unpatentable on the following ground:

<b>Claims Challenged</b>	<b>35 U.S.C. §</b>	<b>References/Basis</b>
1–17, 19, 21–27, 29, 30	103(a)	TS-23.140, Ogawa

Pet. 1.

II. ANALYSIS

*A. Legal Standards*

“In an [*inter partes* review], the petitioner has the burden from the onset to show with particularity why the patent [claim] it challenges is unpatentable.” *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016). This burden of persuasion never shifts to Patent Owner. *Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015). The Board may authorize an *inter partes* review if we determine that the information presented in the Petition shows that there is a reasonable likelihood that Petitioner will prevail with respect to at least one of the claims challenged in the petition. 35 U.S.C. § 314(a).

Petitioner contends that the challenged claims of the ’733 patent are unpatentable under § 103. Pet. 1. A claim is unpatentable under § 103 if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406

---

priority to a provisional application filed January 28, 2009 (‘Critical Date’”).

(2007). The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) where in evidence, so-called secondary considerations. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). When evaluating a combination of teachings, we must also “determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.” *KSR*, 550 U.S. at 418 (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)). Whether a combination of elements produces a predictable result weighs in the ultimate determination of obviousness. *Id.* at 416–417.

#### *B. Level of Ordinary Skill in the Art*

Petitioner argues that a person of ordinary skill in the art “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,” and that “[a]dditional graduate education could substitute for professional experience, and vice versa.” Pet. 2 (citing Ex. 1003 ¶¶ 1–15, 21, 22).

Based on the preliminary record, we adopt Petitioner’s asserted level of ordinary skill to determine whether there is a reasonable likelihood that Petitioner would prevail with respect to at least one of the claims challenged in the Petition.

#### *C. Claim Construction*

In an *inter partes* review, the claims are construed using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. [§] 282(b), including construing the claim in accordance with the ordinary and customary meaning of such claim as understood by one of

ordinary skill in the art and the prosecution history pertaining to the patent.

37 C.F.R. § 42.100(b) (2021); *see Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005) (en banc).

Petitioner states that “[c]laim terms are construed herein using the standard used in civil actions,” and Petitioner is “not conceding that each Challenged Claim satisfies all statutory requirements, nor waiving arguments that can only be raised in district court.” Pet. 2.

In asserting how its proposed combination would have included the limitations of claims 1 and 30, Petitioner argues what certain claim terms would have encompassed or would have been understood to mean based on the Specification of the ’733 patent. *See, e.g.*, Pet. 20 (arguing that “end-user device” includes “networked” devices) (citing Ex. 1001, 5:65–6:28, 6:49–56, 8:3–15, 8:60–9:15; Ex. 1003 ¶ 99), 20–21 (arguing that “modem” includes modems for 2G and 3G communications over a wireless access network) (citing Ex. 1001, 12:61–13:32, 25:29–45, 27:38–44, 29:52–53, 33:59–65, 34:24–27; Ex. 1003 ¶ 100), 21 (arguing that “one or more servers performing one or more server functions would meet the claimed ‘network system’”) (citing Ex. 1001, 16:13–26, 17:8–11, 68:20–37, Figs. 16–20; Ex. 1003 ¶ 101), 23–24 (arguing that “service control link” “can provide an efficient and flexible control plane communication link” for controlling a service and would have been understood to be provided when implemented for communication) (citing Ex. 1002, 76, 99–100; Ex. 1003 ¶¶ 107, 108), 25 (arguing that “network element” is any element that is part of a network) (citing Ex. 1001, 23:46–54, Figs. 1–8; Ex. 1003 ¶ 113), 26 (arguing that “control-plane communications” would have been understood to include communications across a network for supervising and control of services

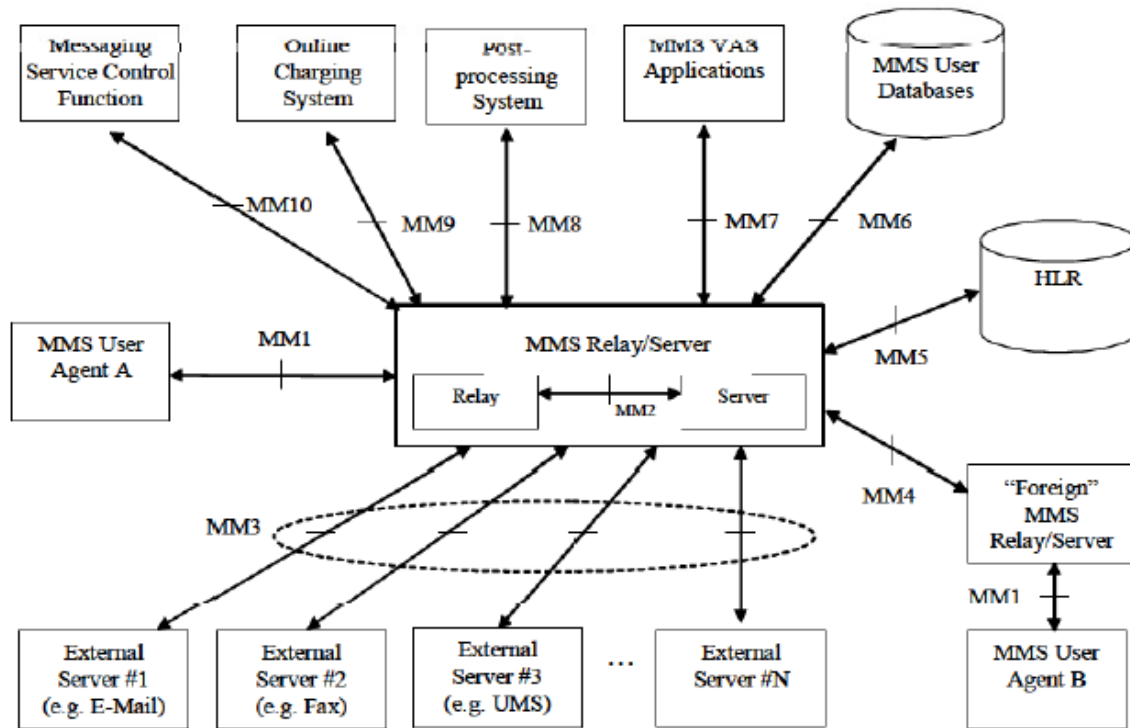
delivered to a device) (citing Ex. 1001, 8:60–9:15, 9:23–24, 37:36–43, 68:19–28; Ex. 1003 ¶ 116), 27–28 (arguing that “service control device link agent” can be any component, possibly implemented in software, that performs some function for a service control device link) (citing Ex. 1001, 15:58–16:12, 37:43–62, 42:51–52, claim 26; Ex. 1003 ¶ 118), 29 (arguing that “device agent” includes software component and can be on a device) (citing Ex. 1001, 15:58–16:2, 42:51–52; Ex. 1003 ¶ 120; Ex. 1029, 12; Ex. 1021, 13–23; Ex. 1038, 17), 36–37 (arguing that “encrypted agent message” includes “an encrypted message sent to an agent”) (citing Ex. 1003 ¶ 139), 38 (arguing that “decrypted agent message” includes “a message that was sent to an agent and then decrypted”) (citing Ex. 1003 ¶ 142), 40 (arguing that “message content” includes multimedia messaging service control information and multimedia content) (citing Ex. 1003 ¶ 150).

At this stage, we do not need to interpret expressly any claim term. *Realtime Data, LLC v. Iancu*, 912 F.3d 1368, 1375 (Fed. Cir. 2019) (“The Board is required to construe ‘only those terms that . . . are in controversy, and only to the extent necessary to resolve the controversy.’”) (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)). We apply Petitioner’s understanding of the claim terms as above described.

*D. Asserted Obviousness Based on TS-23.140 and Ogawa*

*1. TS-23.140 (Ex. 1004)*

TS-23.140 “defines the stage 2 and stage 3 description of the non-realtime Multimedia Messaging Service, MMS.” Ex. 1004, 10.<sup>2</sup> Figure 3 of TS-23.140 is below reproduced.



**Figure 3: MMS Reference Architecture**

“Figure 3 shows the MMS Reference Architecture.” Ex. 1004, 24. TS-23.140 defines “MMS User Agent” as an “application residing on a UE [“User Equipment”]. . . or an external device that performs MMS-specific operations on a user’s behalf and/or another application’s behalf.” *Id.* at 14. The MMS User Agent can provide application layer functionalities, such as

<sup>2</sup> We, like Petitioner, cite to page numbering at the top center of each page, not the exhibit page numbering.

“the decryption and encryption of an MM on end-user to end-user basis.” *Id.* at 19; *see also id.* at 41 (stating “authentication mechanisms based on public/private key cryptography and certificates may also be used”).

“The MMS Relay/Server is responsible for storage and handling of incoming and outgoing messages and for the transfer of messages between different messaging systems” (Ex. 1004, 17) and “for storage and notification, reports, and general handling of messages” (*id.* at 21). *See also id.* at 23–25 (describing further the MMS Relay/Server).

MMS VAS Applications are “[a]pplications providing Value Added Services (e.g. news service or weather forecasts) to MMS Users.” Ex. 1004, 14; *see also id.* at 18, 23, 41 (describing further MMS VAS Applications). “MMS may also be used to transport data specific to applications.” *Id.* at 54. “Abstract messages that are sent by an MMS User Agent or an MMS VAS Application on behalf of an originating application shall contain a destination application identifier.” *Id.* at 55. “If the destination application resides on a receiving MMS User Agent, the MMS User Agent shall immediately route the received MMS information on to the destination application that is referred to from the destination application identifier.” *Id.* at 56.

## 2. *Ogawa (Ex. 1005)*

Ogawa is “directed to encryption methodologies and a portable storage device for storing data thereto.” Ex. 1005, 1:17–19. Ogawa describes a “data encryption system” and “associated methodology to compresses and encrypt data based on a shared encryption key.” *Id.* at 3:18–21. Components are “operably linked via an external wide area telecommunication network 4,” such as a wide area network (“WAN”) or the Internet. *Id.* at 3:44–54.

Ogawa's encryption "may be utilized to enhance security over networks to effectively tunnel data over the network 4," such as "conventional TCP/IP (Transmission Control Protocol/Internet Protocol) or UDP (User Datagram Protocol), encryption communication, such as IPsec (Internet Protocol Security) or SSL (Secure Socket Layer)." Ex. 1005, 3:61–4:4.

In one embodiment, "if a start instruction is issued by the client starting unit 31 at the client site 3, the shared key encrypted data will be received by the receive unit 32 from the database server 2 via network 4." Ex. 1005, 5:59–62; *see also id.* at 6:42–7:21 (describing Fig. 2 and the processing operations for distributing shared encryption keys). That "received shared key encrypted data will be decrypted using the shared encryption key 52 which was supplied to decryption unit 33 and beforehand stored on the removable storage 5." *Id.* at 5:62–65.

"Data that was expanded by the decompression unit 34 is re-encrypted by the encryption unit 35, using an inherent encryption key 53 that was stored on the removable storage 5." Ex. 1005, 6:1–3. "[E]ncryption key 53 is generated from an inherent identification code that was assigned during manufacturing and stored on the internal memory device of the removable storage 5." *Id.* at 6:4–7.

Figure 7 of Ogawa is below reproduced.

Figure 7

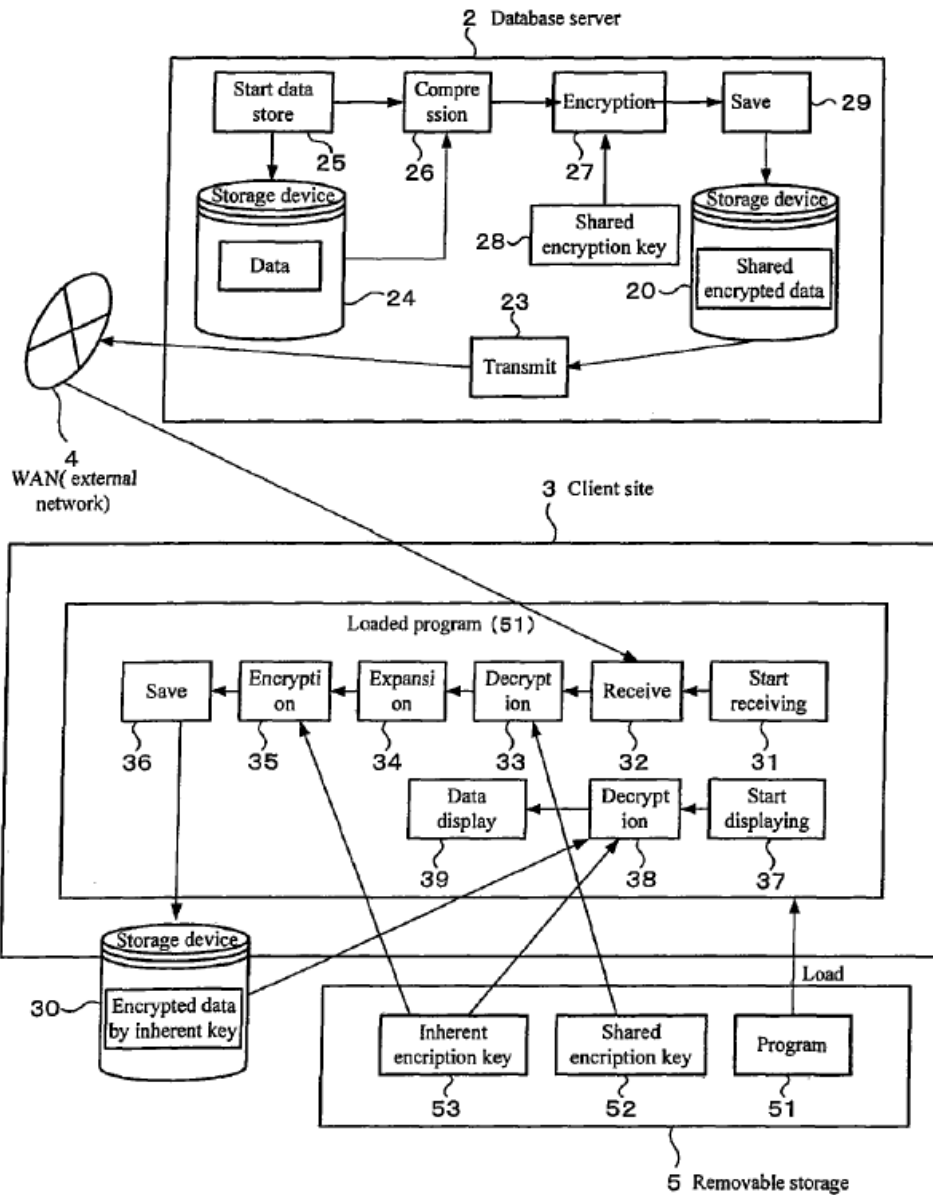


Figure 7 shows “a high level block diagram of an exemplary encryption methodology where the encryption takes place on the database server.” Ex. 1005, 3:4–5. “[D]atabase server 2 is integrated with the

function of a data input site 1[,] and the database server 2 and the client site 3 are connected through the external network 4.” *Id.* at 9:16–20.

“When a start instruction is sent from the saving start unit 25, the compression unit 26 will compress the saved data in the storage device 24,” and “[t]he compressed data is supplied to the encryption unit 27 and encrypted by the shared encryption key 28.” Ex. 1005, 9:22–26. “[T]he share key encrypted data are saved in the storage device 20.” *Id.* at 9:26–27. “Data encrypted by the shared encryption key saved in the storage device 20 is sent to the network 4 through a sending unit 23 which is requested from client site 3.” *Id.* at 9:31–33.

### 3. *Independent Claim 1*

Petitioner argues that, to the extent the preamble is limiting, the user device of TS-23.140 would have been understood to be “[a]n end-user device.” Pet. 20 (citing Ex. 1003 ¶¶ 99; Ex. 1004, 14).

For “a modem for enabling communication with a network system over a service control link provided by the network system over a wireless access network,” Petitioner argues that its proposed combination would have a modem for communicating between an MMS Relay/Server and VAS applications that is implemented for communications and facilitates transmitting control information. Pet. 21–24 (citing Ex. 1003 ¶¶ 102–107, 109, 110; Ex. 1004, 14, 18, 23, 55–56, Fig. 3); *see also id.* at ii (labeling the limitation “1a”).

For “the service control link secured by an encryption protocol,” Petitioner relies on SSL/TLS used to secure the interface between MMS User Agent and MMS Relay/Server. Pet. 24–25 (citing Ex. 1001, 17:2–26, 87:62–88:7, 98:42–44; 99:26–29; 101:65–67; Ex. 1003 ¶¶ 111, 112); *see also id.* at ii (labeling the limitation “1a1”).

For “and configured to support control-plane communications between the network system and a service control device link agent on the end-user device,” Petitioner argues that interface MM1 between MMS User Agent and MMS Relay/Server would be understood to meet the above-quoted limitation because it facilitates transmitting control information. Pet. 25–28 (citing Ex. 1001, 8:60–9:15; Ex. 1003 ¶¶ 114, 115, 117–119; Ex. 1004, 14, 19, 21, 23–24, 30–31, 35–36, 55–56); *see also id.* at ii (labeling the limitation “1a2”).

For “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,” Petitioner argues that TS-23.140’s VAS Applications would have been understood to be device agents that are communicatively coupled to other applications. Pet. 28–30 (citing Ex. 1001, 42:48–61; Ex. 1003 ¶¶ 121–124; Ex. 1004, 54–55, 56; Ex. 1038, 24); *see also id.* at ii (labeling the limitation “1b”). Petitioner alternatively argues that one of ordinary skill in the art would have implemented communications between the MMS User Agent and other applications over a bus with a reasonable expectation of success. *Id.* at 30–31 (citing Ex. 1003 ¶¶ 125–126). Petitioner also argues that TS-23.140’s “destination application identifier” teaches “device agents identifiable by an associated device agent identifier.” *Id.* at 31 (citing Ex. 1003 ¶ 127; Ex. 1004, 54–56)

For “memory configured to store an encryption key,” Petitioner argues that its proposed combination includes the recited memory. Pet. 32 (citing Ex. 1003 ¶¶ 128–129); *see also id.* at ii (labeling the limitation “1c”). Petitioner also provides an argument based on Patent Owner’s interpretation

from related litigation. *Id.* at 32–33 (citing Ex. 1003 ¶¶ 130–132; Ex. 1021, 3–12, 25–32; Ex. 1038, 8, 29).

For “the encryption key shared between the service control device link agent and a service control server link element of the network system,” Petitioner argues that TS-23.140’s MMS User Agent would be a “service control device link agent” and the MMS Relay/Server and interface MM1 would have been understood to be a “service control server link element of the network system.” Pet. 33–35 (citing Ex. 1001, 68:19–40; Ex. 1003 ¶¶ 133, 134); *see also id.* at ii (labeling the limitation “1c1”). Petitioner also relies on Ogawa’s encryption key. *Id.* at 35 (citing Ex. 1003 ¶¶ 135, 136). Petitioner further provides arguments based on Patent Owner’s interpretation from related litigation. *Id.* at 35–36 (citing Ex. 1003 ¶ 137).

For “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,” Petitioner argues that MMS User Agent receives over interface MM1 data from MMS Relay/Server. Pet. 36 (citing Ex. 1003 ¶ 138); *see also id.* at ii (labeling the limitation “1d1”). Petitioner also argues that the messages would have been encrypted in the proposed combination. *Id.* at 37 (citing Ex. 1003 ¶ 140). Petitioner further provides arguments based on Patent Owner’s interpretation from related litigation. *Id.* (citing Ex. 1003 ¶ 141).

For the service control device link agent being configured to, “using the encryption key, obtain a decrypted agent message,” Petitioner argues that, in its proposed combination, encrypted messages are decrypted at the MMS User Agent. Pet. 37–38 (citing Ex. 1003 ¶ 143); *see also id.* at ii (labeling the limitation “1d2”). Petitioner also provides arguments based on

Patent Owner's interpretation from related litigation. *Id.* at 38 (citing Ex. 1003 ¶ 144).

For “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,” Petitioner argues that, in its proposed combination, encrypted messages are decrypted at the MMS User Agent to obtain the recited “decrypted agent messages” for applications on other devices. Pet. 39–40 (citing Ex. 1003 ¶¶ 145–148, 151; Ex. 1004, 14, 54–55, 56, 59); *see also id.* at ii (labeling the limitation “1d3”). Petitioner also argues that “destination application identifier” would have been understood to be the recited “particular agent identifier.” *Id.* at 40 (citing Ex. 1003 ¶ 149).

For “the message content from a particular server of a plurality of servers communicatively coupled to the service control server link element,” Petitioner argues that application-specific data from VAS Applications provided by VAS providers communicating through the MMS Relay/Server teach the above-quoted limitation. Pet. 41–42 (citing Ex. 1003 ¶¶ 152–157; Ex. 1004, 23–24, 25–26, 41, 112, Fig. 3); *see also id.* at iii (labeling the limitation “1e”).

For “based on the particular agent identifier, deliver the message content to the particular device agent over the agent communication bus,” Petitioner argues that, in its proposed combination, the MMS User Agent delivering application-specific data to a destination application based on a destination application identifier would have been understood to occur over an “agent communication bus.” Pet. 42 (citing Ex. 1003 ¶ 158); *see also id.* at iii (labeling the limitation “1f”).

*a) Petitioner's Asserted Reason for Combining*

Petitioner argues that TS-23.140 would have been implemented with a modem because “it was well-known to use a *modem* to enable communications over the networks described in TS-23.140,” “would have been a conventional and obvious way to implement what TS-23.140 describes,” and would have been “nothing more than utilizing familiar, known components to achieve a predictable result of facilitating TS-23.140’s communications.” Pet. 9–10 (citing Ex. 1003 ¶¶ 61–63; Ex. 1004, 14, 17–19, 23–24; Ex. 1008 ¶¶ 27–28, 44, Figs. 1, 4); *see also id.* at 19 (summarizing the proposed combination). Petitioner also argues that there would have been a reasonable expectation of success in implementing a modem in TS-23.140. *Id.* at 10 (citing Ex. 1003 ¶ 63).

According to Petitioner, “TS-23.140 explains that network communications between the MMS User Agent and the MMS Relay/Server use the MM1 Transfer Protocol.” Pet. 10 (citing Ex. 1003 ¶¶ 64–65; Ex. 1004, 24, Fig. 4; Ex. 1018). Petitioner argues that one of ordinary skill in the art would have secured MM1 with an SSL/TLS protocol because “it was conventional and well-known for client-server communications to use SSL/TLS to achieve secure communications,” “TS-23.140 contemplates implementations which use ‘transport layer security mechanisms’ (*e.g.*, SSL/TLS) to secure communication links,” and “such an implementation is nothing more than utilizing familiar, known protocols to achieve a predictable result.” *Id.* at 10–11 (citing Ex. 1003 ¶¶ 66–69); *see also id.* at 19 (summarizing the proposed combination). Petitioner also argues that there would have been a reasonable expectation of success in implementing MM1 to use SSL/TSL. *Id.* at 11 (citing Ex. 1003 ¶ 70).

Petitioner further argues that “TS-23.140 does not provide details regarding how to implement additional end-user-to-end-user encryption beyond SSL/TLS.” Pet. 12 (citing Ex. 1003 ¶¶ 71–72). According to Petitioner, “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” and Ogawa discloses how to implement symmetric encryption. *Id.* (citing Ex. 1003 ¶¶ 72, 73; Ex. 1005, 3:61–4:4, 9:16–34).

Petitioner contends that one of ordinary skill in the art would have implemented Ogawa’s symmetric data encryption technique because it “would have achieved a system ‘having improved security’ and providing ‘an end-user to end-user’ security solution for MMS applications,” “would have been particularly beneficial for ‘enterprise applications,’” and would have been implementing a known method or technique to a known system or device to achieve predictable results. Pet. 12–13 (citing Ex. 1003 ¶¶ 74–76) *see also id.* at 19 (summarizing the proposed combination). Petitioner also contends that there would have been a reasonable expectation of success. *Id.* at 13 (citing Ex. 1003 ¶¶ 77–79).

Petitioner additionally argues that one of ordinary skill in the art would have implemented Ogawa’s decryption and encryption units in TS-23.140 because, for example, it would have “beneficially allowed the MMS User Agent to decrypt an encrypted message,” and the ability to “securely store data on a user device was a desirable feature that would have helped prevent, e.g., theft.” Pet. 13–15 (citing Ex. 1003 ¶¶ 80–82) *see also id.* at 19 (summarizing the proposed combination). Petitioner further argues

that there would have been a reasonable expectation of success. *Id.* at 15 (citing Ex. 1003 ¶ 83).

Petitioner additionally contends that Ogawa teaches the well-known technique of storing an encryption key in memory connected to each device that encrypts or decrypts communications. Pet. 15 (citing Ex. 1003 ¶ 84; Ex. 1005, 3:18–34, 4:48–57, 5:59–65, 6:64–7:21, Figs. 1, 7). Petitioner further contends that there were limited ways of ensuring that the same key is used. *Id.* at 15–16 (citing Ex. 1003 ¶ 85).

In Petitioner’s view, one of ordinary skill in the art would have stored Ogawa’s key in the memory of the user device in TS-23.140 “to facilitate decryption of encrypted messages received from the MMS Relay/Server” and “to implement the symmetric encryption teachings of Ogawa.” Pet. 16–17 (citing Ex. 1003 ¶¶ 87, 88; Ex. 1005, 3:61–4:7, 5:41–47, 9:21–34, Fig. 7). Petitioner also argues that the proposed modification would have been implementing a known method to known systems to achieve a predictable result and would have been a design choice. *Id.* at 18 (citing Ex. 1003 ¶¶ 89–94; Ex. 1009, 3:25–27). Petitioner further argues that there would have been a reasonable expectation of success. *Id.* (citing Ex. 1003 ¶ 95).

*b) Petitioner Shows a Reasonable Likelihood of Prevailing*

Based on the present record, Petitioner shows a reasonable likelihood of prevailing in its challenge to claim 1 as unpatentable over TS-23.140 and Ogawa.

*4. Claims 2–17, 19, 21–27, 29, and 30*

Petitioner argues with citations to the record that its proposed combination of TS-23.140 and Ogawa would have rendered obvious claims 2–17, 19, 21–27, 29, and 30. Pet. 20, 24–31, 33–76.

For the reasons discussed above, we preliminarily determine that Petitioner demonstrates a reasonable likelihood of prevailing with respect to its obviousness challenge to independent claim 1. We, therefore, institute review on all challenged claims on the only ground set forth in the Petition. 37 C.F.R. § 42.108(a); *see also SAS*, 138 S. Ct. at 1354.

### III. CONCLUSION

After considering the evidence and arguments presented in the Petition and the cited evidence, we determine that Petitioner has demonstrated a reasonable likelihood of prevailing in proving that at least one of claims 1–17, 19, 21–27, 29, and 30 of the '733 patent is unpatentable, and thus, we institute an *inter partes* review of all challenged claims on the only presented challenge. 37 C.F.R. § 42.108(a).

At this stage of the proceeding, the Board has not made a final determination as to the patentability of any challenged claim or any underlying factual and legal issues.

### IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that, pursuant to 35 U.S.C. § 314(a), an *inter partes* review of claims 1–17, 19, 21–27, 29, 30 of U.S. Patent No. 8,406,733 B2 is instituted with respect to all grounds set forth in the Petition; and

FURTHER ORDERED that, pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4(b), *inter partes* review of U.S. Patent No. 8,406,733 B2 shall commence on the entry date of this Order, and notice is hereby given of the institution of a trial.

IPR2024-00341  
Patent 8,406,733 B2

For PETITIONER:

W. Karl Renner  
Jeremy J. Monaldo  
Karan Jhurani  
Turhan F. Sarwar  
Gregory F. Corbett  
FISH & RICHARDSON P.C.  
axf-ptab@fr.com  
jjm@fr.com  
jhurani@fr.com  
Gregory.Corbett@wolfgreenfield.com  
TSarwar-PTAB@wolfgreenfield.com

FOR PATENT OWNER:

Reza Mirzaie  
Dale Chang  
Amy E. Hayden  
James A. Milkey  
Neil Rubin  
Philip X. Wang  
RUSS, AUGUST & KABAT  
rmirzaie@raklaw.com  
dchang@raklaw.com  
ahayden@raklaw.com  
jmilkey@raklaw.com  
nrubin@raklaw.com  
pwang@raklaw.com