

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner,

v.

HEADWATER RESEARCH LLC,
Patent Owner.

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

PATENT OWNER'S RESPONSE

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	OVERVIEW OF THE '403 PATENT.....	6
A.	The Claimed Device Messaging Agent and Secure Interprocess Communication Service.....	6
B.	The Challenged Claims.....	7
III.	LEVEL OF ORDINARY SKILL IN THE ART	8
IV.	CLAIM CONSTRUCTION.....	8
V.	THE PETITION AND THE ASSERTED REFERENCES	9
A.	TS-23.140	9
B.	Ogawa	10
C.	The Petition's Proposed Combination of TS-23.140 with Ogawa	13
VI.	LEGAL STANDARDS.....	14
VII.	THE IPR2024-00341 DECISION DOES NOT RESOLVE THE DISPOSITIVE ISSUE	15
VIII.	GROUND 1 FAILS FOR EVERY CHALLENGED CLAIM.....	18
A.	The Petition Fails to Show Its Proposed Combination Would Have Been Obvious, Because It Never Explains How That Combination Would Serve Its Intended Purpose of Allowing Recipient Applications to Read the Securely Transmitted Data	18
1.	The Intended Purpose of the Petition's Combination Is Secure Delivery of Data That Recipient Applications Can Read	19
2.	In the Petition's Combination, Only the MMS User Agent Can Decrypt the Data It Sends.....	22
3.	Neither TS-23.140 nor Ogawa Teaches How a Recipient Program Could Decrypt Inherent-Key Data.....	24

4.	The Petition’s Combination Is Inoperable for Its Intended Purpose and Therefore Not Obvious	26
B.	The Petition’s Combination Conflicts with the Purpose of Ogawa’s Inherent Key and Undermines Petitioner’s Own Rationale	29
C.	The Petition Does Not Show a Reasonable Expectation of Success ..	32
D.	The Petition Fails to Establish the Obviousness of a “Secure Interprocess Communication Service” in Its Proposed Combination	33
IX.	GROUND 2A–4D FAIL FOR THE SAME REASONS	34
X.	THE DEPENDENT CLAIMS ARE INDEPENDENTLY PATENTABLE	35
A.	Claim 11.....	35
B.	Claim 15.....	37
C.	Claim 16.....	37
D.	Claim 21.....	39
XI.	CONCLUSION	41

TABLE OF AUTHORITIES

Cases

<i>DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.</i> , 567 F.3d 1314 (Fed. Cir. 2009)	5, 29
<i>Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.</i> , 800 F.3d 1375 (Fed. Cir. 2015)	14
<i>In re Fritch</i> , 972 F.2d 1260 (Fed. Cir. 1992)	27
<i>In re Gordon</i> , 733 F.2d 900 (Fed. Cir. 1984).....	3, 27, 28
<i>In re Magnum Oil Tools Int’l, Ltd.</i> , 829 F.3d 1364 (Fed. Cir. 2016).....	15, 29, 39
<i>In re Ratti</i> , 270 F.2d 810 (C.C.P.A. 1959)	32
<i>In re Spinnoble</i> , 405 F.2d 578 (C.C.P.A. 1969)	27
<i>Intel Corp. v. Qualcomm Inc.</i> , 21 F.4th 784 (Fed. Cir. 2021)	27
<i>Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.</i> , 821 F.3d 1359 (Fed. Cir. 2016)	14, 32
<i>MaxLinear, Inc. v. CF CRESPE LLC</i> , 880 F.3d 1373 (Fed. Cir. 2018).....	18
<i>McGinley v. Franklin Sports, Inc.</i> , 262 F.3d 1339 (Fed. Cir. 2001)	4, 27, 28
<i>Medtronic, Inc. v. Teleflex Innovations S.à.r.l.</i> , 69 F.4th 1341 (Fed. Cir. 2023)	4, 28, 29
<i>Ohio Willow Wood Co. v. Alps S., LLC</i> , 735 F.3d 1333 (Fed. Cir. 2013).....	18
<i>Pers. Web Techs., LLC v. Apple, Inc.</i> , 848 F.3d 987 (Fed. Cir. 2017).....	15, 24, 29
<i>Plas-Pak Indus., Inc. v. Sulzer Mixpac AG</i> , 600 F. App’x 755 (Fed. Cir. 2015)....	32
<i>Tec Air, Inc. v. Denso Mfg. Mich. Inc.</i> , 192 F.3d 1353 (Fed. Cir. 1999)	27
<i>Wasica Fin. GmbH v. Cont’l Auto. Sys., Inc.</i> , 853 F.3d 1272 (Fed. Cir. 2017).....	14

Statutes

35 U.S.C. § 312(a)(3)	14
35 U.S.C. § 316(e).....	14

Other Authorities

Pat. Trial & Appeal Bd., <i>Consolidated Trial Practice Guide</i> (Nov. 2019)	14
---	----

PATENT OWNER'S EXHIBIT LIST

No.	Description
2001	Confidential License Agreement
2002	Final Judgment in <i>Headwater Research LLC v. Samsung Electronics Co., Ltd.</i> , No. 2:23-cv-00103-JRG-RSP (E.D. Tex. May 30, 2025)
2003	Day 3 trial transcript in <i>Headwater Research LLC v. Samsung Electronics Co., Ltd.</i> , No. 2:23-cv-00103-JRG-RSP (E.D. Tex. May 30, 2025)
2004	Excerpt of the January 23, 2024 deposition transcript of Jeff Sharkey in <i>Headwater Research, LLC v. Samsung Electronics Co., Ltd. et al.</i> , No. 2:22-CV-00422-JRG-RSP (E.D. Tex.) (redacted to remove any potential confidential information)
2005	Ben Schoon, <i>Google Pixel development reportedly moving almost entirely out of China</i> , 9to5Google.com, https://9to5google.com/2026/01/13/google-pixel-development-china-report/ , Jan. 13, 2026
2006	<i>TRUMP EFFECT: A Running List of New U.S. Investment in President Trump's Second Term</i> , The White House, https://www.whitehouse.gov/articles/2026/03/trump-effect-a-running-list-of-new-u-s-investment-in-president-trumps-second-term/ (Mar. 10, 2026)
2007	Matthew Gardner, <i>Four Big Tech Companies Avoid \$51 Billion in Taxes in Wake of One Big Beautiful Bill Act</i> , Institute of Taxation and Economic Policy, https://itep.org/trump-meta-tesla-alphabet-amazon-obbba-taxes/# (Feb. 6, 2026)
2008	<i>Investing in America 2025</i> , Google, available at https://blog.google/company-news/inside-google/company-announcements/investing-in-america-2025/ (last visited Mar. 23, 2026)
2009	<i>Apple and Corning Partner to Manufacture 100 Percent of iPhone and Apple Watch Cover Glass in Kentucky</i> , APPLE, https://www.apple.com/newsroom/2025/08/apple-corning-to-

	manufacture-all-iphone-apple-watch-cover-glass-in-kentucky/ (Aug. 6, 2025)
2010	Proposed Modified Agreed Protective Order
2011	Proposed Modified Agreed Protective Order (Changes Tracked Against Default)
2012	Declaration of Erik de la Iglesia in Support of Patent Owner's Response
2013	<i>Curriculum vitae</i> of Erik de la Iglesia
2014	September 21, 2026 Deposition Transcript of Patrick Traynor, Ph.D.
2015	Susmit Bagchi, <i>Distributed IPC Using Virtual Device Driver in Monolithic Kernel</i> , 2012 IEEE Int'l Conf. on Embedded & Real-Time Computing Systems & Applications (2012)
2016	Christophe Lizzi & Eric Gressier-Soudan, <i>A Real-Time IPC Service over ATM Networks for the Chorus Distributed System</i> , 1998 IEEE (1998)
2017	Excerpts from Bruce Schneier, APPLIED CRYPTOGRAPHY, SECOND EDITION: PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C (CLOTH) (1996), <i>available at</i> https://web.spms.ntu.edu.sg/~guojian/backup/phd/Books/Applied_Cryptography/ewtoc.html and https://web.spms.ntu.edu.sg/~guojian/backup/phd/Books/Applied_Cryptography/ch08/08-01.html

I. INTRODUCTION

Challenged U.S. Patent No. 9,232,403 (“’403 patent”) claims a mobile device in which a device messaging agent receives secure messages on behalf of multiple software applications and forwards each application’s data to a corresponding software process “on the secure interprocess communication service.” Ex. 1001 (’403 patent), claim 1. For the “secure” requirement, the Petition relies on a single mechanism: the MMS User Agent of TS-23.140 re-encrypts each application’s data with Ogawa’s “inherent encryption key 53” and then sends the encrypted data over a bus to the destination application. Pet. 18–20, 39–43; Ex. 1003 (Traynor Decl.) ¶¶95, 150–151.

That mechanism does not work as the Petition proposes. Ogawa generates its inherent key from an identification code “assigned during manufacturing” to a removable storage device, confines the key to a single program loaded from that device, and uses the key so that “unless there is a corresponding removable storage 5 which holds the inherent encryption key, there is no way to decrypt the saved data.” Ex. 1005 (Ogawa), 5:24–32, 5:44–47, 6:3–7, 8:44–50; Ex. 2012 (de la Iglesia Decl.) ¶¶43–46. In the Petition’s combination, only the MMS User Agent holds that key, so the chess, weather, and other applications to which the User Agent sends the encrypted data have no way to read it. Ex. 2012 ¶¶71–72. The Petition never

explains how any recipient application would decrypt what it receives, and neither TS-23.140 nor Ogawa supplies the missing mechanism. *Id.* ¶¶77–90.¹

Petitioner’s own expert confirmed this deficiency. Dr. Traynor agreed that “[a]t the end of the day, the application has to have access to decrypted data,” and that his analysis rests on “my assumption that the application at the end will get access to the data.” Ex. 2014 (Traynor Dep.), 42:20–25, 53:5–8. Yet he conceded that “I haven’t talked about how precisely the decryption is performed,” could not identify any paragraph of his declaration giving any entity other than the User Agent access to the inherent key, could not say whether different applications would receive the same key or different keys, offered no example of how the key would reach a destination application, and ultimately answered “I’m not sure how to answer this further than I have.” *Id.* 22:21–24, 27:7–29:11, 57:9–58:1, 58:14–61:11. He dismissed these questions as “implementation details” akin to the device’s case color, *id.* 23:14–24:1, 28:1–29:2, 59:9–15, but whether the scheme can deliver readable data is the entire point of the secure interprocess *communication* service the Petition alleges. Ex. 2012 ¶¶74–75.

¹ The challenged claims do not themselves require that any recipient decrypt data, or even that encryption be used. But Petitioner chose encryption with Ogawa’s inherent key as its sole source of security for the claimed interprocess communication service, and that choice makes sense only if the recipient can later decrypt the data. Ex. 2012 ¶68 n.2.

Nor does the Final Written Decision in IPR2024-00341 resolve the issue. The claims of related U.S. Patent No. 8,406,733 (“’733 patent”) addressed there recited only “an agent communication bus,” and the petition in that proceeding invoked Ogawa’s inherent key only for a single dependent claim. Ex. 1022 (IPR2024-00341 FWD), 4; Ex. 1038 (IPR2024-00341 Pet.), 69–74. That theory relied on a different decrypting entity—Ogawa’s display units 37–39, which reside in the same program 51 that performs the encryption—and applied only to data “intended for immediate display to the user.” Ex. 1038, 74; Ex. 1005, 5:24–32. Petitioner abandons that mapping here and puts nothing in its place. Ex. 2012 ¶¶53–59.

The Petition therefore fails for at least four independent reasons applicable to each ground.

First, the Petition never shows how its combination would serve its intended purpose. By Petitioner’s own account, the combination exists to deliver application data securely to destination applications so that each application “receive[s] data with correct format and content.” Ex. 1003 ¶96; *see* Ex. 1004 (TS-23.140), 14, 56. Data encrypted with a key that only the sender holds is useless to its recipient, so the combination is, at minimum, a “seemingly inoperative device” for delivering application data. Ex. 2012 ¶¶60–68, 87–90. A modification that renders the prior art “inoperable for its intended purpose” is not obvious, *In re Gordon*, 733 F.2d 900, 902 (Fed. Cir. 1984), and references that “would produce a ‘seemingly inoperative

device” “cannot serve as predicates for a prima facie case of obviousness,” *McGinley v. Franklin Sports, Inc.*, 262 F.3d 1339, 1354 (Fed. Cir. 2001); *see also Medtronic, Inc. v. Teleflex Innovations S.à.r.l.*, 69 F.4th 1341, 1349–50 (Fed. Cir. 2023) (affirming Board’s determination that petitioner failed to prove obviousness where proposed modification would destroy the reference’s “entire purpose, shared with the challenged claims”).

Second, Ogawa’s teachings undermine the very reason Petitioner offers for the modification. Petitioner contends that the inherent key would help “prevent unauthorized data access by, e.g., rogue software.” Pet. 20; Ex. 1003 ¶95. But Ogawa uses that key only to protect stored data on a computer that may be stolen, ties decryption to physical possession of the removable storage device, and never applies the key to data passed between programs. Ex. 1005, 8:44–56, 10:23–30, 10:41–49; Ex. 2012 ¶¶92–94. To make the combination work, Petitioner would have to give that device-bound key to every downloaded destination application, including applications that Dr. Traynor himself describes as ones “that should not be trusted with access to sensitive device data/functions.” Ex. 1003 ¶272; Ex. 2012 ¶¶96–99. That would place the key in the hands of the very software the encryption supposedly guards against. “An inference of nonobviousness is especially strong where the prior art’s teachings undermine the very reason being proffered as to why

a person of ordinary skill would have combined the known elements.” *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 567 F.3d 1314, 1326 (Fed. Cir. 2009).

Third, Petitioner has not shown a reasonable expectation of success. The Petition’s showing is a single conclusory clause that never addresses which entity would hold the inherent key, how the key would get there, or how the destination application would read the data. Pet. 19–20; Ex. 1003 ¶95; Ex. 2012 ¶100. Dr. Traynor conceded that Ogawa leaves out “lots of details,” that a key-distribution scheme may not be secure “if it’s done poorly,” and that “there are ways you could get it wrong too.” Ex. 2014, 33:23–34:9, 57:1–8, 59:16–24. No POSITA could reasonably expect success from a scheme whose essential details neither the Petition nor any asserted reference supplies. Ex. 2012 ¶¶101–103.

Fourth, the Petition never shows the claimed “secure interprocess communication service”—a service provided to the communicating processes by another component, such as the operating system—because the only security it describes is the User Agent’s own re-encryption, and it never identifies which entity would perform decryption. Ex. 2012 ¶¶32–33, 104.

Grounds 2A–4D incorporate the same deficient inherent-key mechanism and fail for the same reasons. *See* Pet. 71–72, 74–77, 82–85; Ex. 2012 ¶¶52, 111–112. Dependent claims 11, 12, 15, 16, and 21 also fail for additional, independent reasons.

Petitioner has not carried its burden of proving any challenged claim unpatentable, and the Board should confirm the patentability of claims 1–21.

II. OVERVIEW OF THE '403 PATENT

A. The Claimed Device Messaging Agent and Secure Interprocess Communication Service

The '403 patent describes a device-side service processor whose agents communicate with a network-side service controller over a secure service control link. Ex. 1001, 37:40–43, 68:9–48. On the device, a service control device link 1691 receives messages from the network and delivers their contents to the appropriate device agents over an agent communication bus 1630. *Id.* 41:42–43:4, 44:62–45:5, FIG. 16. The specification describes securing that bus in many ways. It explains that “there are multiple layers of security applied to the agent communication bus 1630 communication protocols,” including “point to point message exchange encryption using one or more keys that are partially shared or shared within the service processor 115 agent group,” and “a set of secure messages that can only be decoded or observed by the agents they are intended for.” *Id.* 41:59–42:6. Ex. 2012 ¶¶29–30.

Where encryption is how the security is provided, the specification describes keys provided to the communicating agents. For example, the specification teaches “agent bus encryption using [a] shared key for all agents provided and updated by the secure server” and “agent level encryption using agent to agent shared keys in

which the secure server informs agents of the key and updates the key as appropriate.” Ex. 1001, 42:19–28. The bus may be “a variant of D-bus” or “another inter-process communication protocol or system, running a session bus in which all communications over the session bus can be secured, signed, encrypted or otherwise protected.” *Id.* 42:48–58; *see also id.* 88:9–22. Ex. 2012 ¶31.

These embodiments are illustrative, and confirm that for a workable encryption system for interprocess communications, the process receiving the encrypted data needs functionality (e.g., a decryption key) to read the encrypted data. Ex. 2012 ¶¶34–35.

B. The Challenged Claims

Petitioner challenges claims 1–21. Claim 1 is the only independent claim:

Claim 1: A mobile end-user-area device comprising:

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

[1B1] a device messaging agent to receive secure Internet data messages, on behalf of a plurality of software applications capable of execution on the device, and over a secure connection to a network message server reachable via the WWAN,

[1B2] wherein at least a subset of the secure Internet data messages contain an identifier for a corresponding one of the software applications and application data from a respective network application server corresponding to that application; and

[1C1] a secure interprocess communication service,

[1C2] wherein the device messaging agent, for each message in the subset of the secure Internet data messages, maps the identifier to the corresponding one of the software applications in order to forward the

application data on the secure interprocess communication service to a software process corresponding to the identified software application.

Ex. 1001, claim 1 (bracketed labels from Petition’s Claim Listing Appendix, Pet. 86); Ex. 2012 ¶36.

III. LEVEL OF ORDINARY SKILL IN THE ART

Petitioner proposes that a person of ordinary skill in the art (“POSITA”) would have had at least a bachelor’s degree in computer science, electrical engineering, or a related field, and 3–5 years of experience in services and application implementation in communication networks. Pet. 4; Ex. 1003 ¶33. Patent Owner’s arguments do not depend on the level of skill, and they apply equally under Petitioner’s formulation. Ex. 2012 ¶37.

IV. CLAIM CONSTRUCTION

Petitioner proposes no express constructions. Pet. 4–5. While all terms should be given their plain meaning, in the context of the ’403 patent, a POSITA would have understood that an “interprocess communication service” is not merely a communication path between two processes that is implemented by the processes themselves, but instead contemplates a service that is provided to the processes by some component. There thus must exist a specific “service” on which the messages are delivered, rather than the processes simply communicating in some secure fashion. *See* Ex. 2012 ¶¶32–33, 38.

V. THE PETITION AND THE ASSERTED REFERENCES

A. TS-23.140

TS-23.140 is a 3GPP standard describing the Multimedia Messaging Service (“MMS”). Ex. 1004, 10. An MMS User Agent on user equipment exchanges multimedia messages with an MMS Relay/Server over interface MM1. *Id.* 14, 17–19, 23–24. MMS may also transport “Application Data,” which TS-23.140 defines as “[i]nformation / data specific to an application other than the MMS User Agent / VASP which is intended to be transported without alteration by using MMS.” *Id.* 14. When an abstract message carries a destination application identifier, “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 (based on the negotiated details upon application registration process) without presentation to the user.” *Id.* 56. Ex. 2012 ¶¶39–40.

TS-23.140 is explicit that it does *not* teach how messages are routed from the MMS User Agent to any destination application: “[d]etails of these applications or how an MMS User Agent or an MMS VAS Application would interface with them are outside the scope of this specification,” and “[t]he application registration process is outside the scope of this specification.” Ex. 1004, 54. Ex. 2012 ¶41.

B. Ogawa

Ogawa is titled “Removable Storage Device and Associated Methodology of Data Encryption.” Ex. 1005, cover. It describes a client site that receives data encrypted with a “shared encryption key” from a database server, decrypts it, expands it, and then re-encrypts it with an “inherent encryption key 53” before saving it to a local storage device. *Id.* 5:58–6:9. Ex. 2012 ¶42.

Importantly, Ogawa uses the two keys differently. The “shared” key is, as the name suggests, distributed between multiple entities: Ogawa describes “processing operations that distribute the shared encryption keys” through a Diffie-Hellman exchange, after which “the distribution of keys is carried out between the data input site 1 and the client site 3.” Ex. 1005, 6:42–43, 7:1–24. The inherent key is not. It “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.* 6:3–7. The removable storage may be “a USB memory device, flash drive, zip disk, floppy disk, compact disc, miniSD, or even DVD RAM.” *Id.* 5:48–51. While the inherent key can be stored in temporary memory by a program that is derived from the removable storage device, it is not described as being distributed beyond the single program derived from the removable storage device itself. Ex. 1005, 8:11–15, 8:26–31, claims 1, 12, 15; Ex. 2012 ¶¶43–44.

All of Ogawa's client-side units responsible for encryption and decryption using the inherent key (including encryption unit 35 and decryption unit 38) "are implemented as a single computer executable instruction set 51," which Ogawa describes as a single "loaded program (51)" that is "loaded to the client site 3 from a memory of the removable storage." Ex. 1005, 5:24–32, 5:44–47, FIG. 1. When a user later wants to view the stored encrypted data, the same program's decryption unit 38 "will decrypt the inherent key encrypted data stored on the storage device 30, using the inherent encryption key 53 stored on the removable storage 5," and the decrypted data are displayed. *Id.* 6:10–18; *see id.* 8:24–34. Ex. 2012 ¶45.

Ogawa explains that the inherent key is not distributed beyond the program derived from the removable storage itself for security purposes: "because the downloaded data is saved after being encrypted with an inherent encryption key, unless there is a corresponding removable storage 5 which holds the inherent encryption key, there is no way to decrypt the saved data. Therefore, if a laptop with downloaded data is stolen, and if the removable storage 5 is secured separately the data of the laptop remains secure." Ex. 1005, 8:44–50; *see also id.* 10:58–63 (data "may only be decrypted only with the same PC and same removable storage"). When Ogawa contemplates others reading inherent-key data, it does not create an electronic copy of the key untethered to its removable storage device or provide another program access to the inherent key. It instead relies on the intended reader

having access to the specific removable hardware that includes the decryption program: a group member who needs to decrypt “must borrow a removable storage device” that contains the necessary inherent key and decryption program. *Id.* 10:41–49. This ties the security (including the decryption program itself) to physical possession of the removable storage device, such that only users who have access to this device can read the inherent-key-encrypted data. Ex. 2012 ¶¶46–47.

Furthermore, when Ogawa *does* pass encrypted data between two separate programs (across devices, rather than on the same device), it uses what it describes as a “shared” key rather than an “inherent” key which is tied to a removable storage device. Unlike the shared key, which Ogawa distributes between sites using a key-exchange protocol, the inherent key is never applied to data passed from one program to another. And in the one instance where Ogawa passes data between programs on the same device, the receiving program already holds the key needed to read the data, and the inherent key is never used. In that FIG. 9 embodiment, which adds a second layer of transport encryption (“TCP2”) to the FIG. 1 system, a TCP2 program 60 removes the TCP2 encryption and passes the data to program 51: “the received data are decrypted with the decryption unit 63 in TCP2 and are supplied in the sending unit 64 and are sent to the receiving unit 32 of the program 51.” Ex. 1005, 10:23–28. Because “[t]he other processes are completed similarly as shown in the system of FIG. 1,” the data program 51 receives is the shared-key-

encrypted data that program 51 then decrypts with the shared key it already holds, just as in FIG. 1. *Id.* 5:59–65, 10:4–8, 10:28–30; Ex. 2012 ¶48.

C. The Petition’s Proposed Combination of TS-23.140 with Ogawa

The Petition’s proposed Ground 1 combination implements Ogawa’s decryption and encryption units “as part of TS-23.140’s MMS User Agent application.” Pet. 14–15; Ex. 1003 ¶¶83–84; Ex. 2012 ¶49. The combination also adds a software bus between the User Agent and other applications. Pet. 16–18.

For the “secure” requirement, the Petition’s Ground 1 combination proposes “to include Ogawa’s re-encryption functionality in MMS-Ogawa’s User Agent—e.g., to secure decrypted application data received over MM1 before transmitting it to any other component on the user device.” *Id.* 19–20; Ex. 1003 ¶95. Thus, “MMS-Ogawa’s interprocess communications are secured using Ogawa’s inherent key when data is routed by the User Agent over TS-23.140’s software bus for interprocess communications ... to a destination application.” Pet. 41; Ex. 1003 ¶¶150–151. In other words, rather than Ogawa’s program 51 (which is loaded from the removable storage device) storing the encrypted data for later retrieval by that same program, in the proposed combination, that program 51 would encrypt the data and send that encrypted data to a *different* program. Ex. 2012 ¶¶50–51.

That re-encryption is the Petition’s only basis for the “secure” requirement in every ground. Grounds 2A–2C substitute Cole’s modem and Sathish’s D-Bus but

rely on the bus “secured as discussed supra §VII.C.6.” Pet. 71–72. Grounds 3A–4D add Papineau and Ellison to MMS-Ogawa unchanged. *Id.* 74–77, 82–85. Ex. 2012 ¶52.

VI. LEGAL STANDARDS

In an inter partes review, “the burden of persuasion is on the petitioner to prove ‘unpatentability by a preponderance of the evidence,’ 35 U.S.C. § 316(e), and that burden never shifts to the patentee.” *Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015). The Petition defines the scope of the entire IPR proceeding, because “[i]t is of the utmost importance that petitioners in the IPR proceedings adhere to the requirement that the initial petition identify ‘with particularity’ the ‘evidence that supports the grounds for the challenge to each claim.’” *Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1369 (Fed. Cir. 2016) (quoting 35 U.S.C. § 312(a)(3)). Thus, a petitioner may not shift to new theories in reply, *Wasica Fin. GmbH v. Cont’l Auto. Sys., Inc.*, 853 F.3d 1272, 1286 (Fed. Cir. 2017), or introduce argument or evidence that “it could have presented earlier, e.g., to make out a prima facie case of unpatentability”, Pat. Trial & Appeal Bd., Consolidated Trial Practice Guide 73 (Nov. 2019) (*available at* <https://www.uspto.gov/sites/default/files/documents/tpgnov.pdf>).

A petitioner “cannot employ mere conclusory statements”; it “must instead articulate specific reasoning, based on evidence of record, to support the legal

conclusion of obviousness.” *In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016). Furthermore, the petitioner must explain how its proposed combination would actually work: a “clear, evidence-supported account of the contemplated workings of the combination is a prerequisite to adequately explaining and supporting a conclusion that a relevant skilled artisan would have been motivated to make the combination and reasonably expect success in doing so.” *Pers. Web Techs., LLC v. Apple, Inc.*, 848 F.3d 987, 994 (Fed. Cir. 2017).

VII. THE IPR2024-00341 DECISION DOES NOT RESOLVE THE DISPOSITIVE ISSUE

The Petition leans heavily on the Final Written Decision in IPR2024-00341 and on the Director’s September 16, 2025 memorandum regarding prior findings. Pet. 1, 8–21, 26–44; Ex. 1022; Ex. 1023. But no prior finding addressed the issue presented here. *See* Ex. 2012 ¶53.

The ’733 claims addressed in that proceeding recited “a plurality of device agents communicatively coupled to the service control device link agent through an agent communication bus.” Ex. 1022, 4. They did not require that the bus be *secure*. The issues Patent Owner contested there concerned whether TS-23.140’s destination applications were separate from the MMS User Agent and whether a POSITA would have implemented a bus at all. *Id.* 45–49; Ex. 2012 ¶54. The Board resolved those issues and nothing more.

The inherent-key theory on which Petitioner now relies played no part in IPR2024-00341's challenge to the independent claims. The petition there invoked Ogawa's inherent key only for dependent claim 27 of the '733 patent. And that was an entirely *different* theory about how the inherent key would be used and where the data encrypted via the inherent key would be sent, because under the IPR2024-00341 theory, Ogawa's own display units 37–39 would decrypt the inherent-key data. Ex. 1038, 69–74. Specifically, Petitioner argued that “[b]ecause both the MMS User Agent and MMS-Ogawa's display units 37-39 use the same key for encryption and decryption,” the inherent key was “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. 1038, 74. Those display units are part of the same Ogawa program that encrypts the data in the first place. *See, e.g.*, Ex. 1005, 5:24–32 & FIG. 1. Ex. 2012 ¶55.

The instant Petition sets forth an entirely different theory, wherein third-party downloaded applications (e.g., chess and weather applications)—rather than display units 37-39 that Ogawa discloses are within the same program that encrypts the data—are alleged to be the recipients of the encrypted data rather than any display units. Pet. 29–30, 36–39, 44; Ex. 2014, 41:19–22. The Petition identifies no recipient even allegedly capable of decrypting data using the inherent key, and indeed does not even *mention* Ogawa's “display unit[s]” (i.e., the receiving and

decrypting entities that the theory in IPR2024-00341 relied on for different claim language). Furthermore, when asked at his deposition “which entity is doing the decryption in your proposed combination,” Petitioner’s expert did not even *mention* Ogawa’s display units as being the entity that would do so. *See* Ex. 2014, 53:12–54:10; *see generally id.* (no mention of Ogawa’s display units throughout his entire deposition); Ex. 2012 ¶57. The instant IPR thus does not adopt the same display unit decryption theory proposed in IPR2024-00341. This is for good reason: the ’403 patent’s claim 1 recites a “secure *interprocess* communication service,” whereas Ogawa implements its display units in the same program 51 that performs the original encryption. Ex. 1005, 5:24–32; Ex. 2012 ¶¶56, 58. Indeed, the IPR2024-00341 petition made clear that the “display unit” theory only applied to “data received by the MMS User Agent... that was intended for *immediate display to the user*” (i.e., data immediately rendered on the device’s display without first being delivered to a separate downloaded application such as a chess or weather application). Ex. 1038, 74; Ex. 2012 ¶58.

Furthermore, IPR2024-00341’s claim 27 theory identified only a single agent capable of receiving and decrypting the data. That mapping was consistent with claim 27’s recitation of only a single “particular agent” that must share the claimed “second encryption key.” In contrast, claim 1 of the ’403 patent requires the device messaging agent, “for *each message* in the subset of the secure Internet data

messages,” to forward application data “on the secure interprocess communication service,” which the instant Petition maps as the subset of messages that include “abstract messages” intended for destination applications. Accordingly, even if the IPR2024-00341 theory were correct as to claim 27 of the ’733 patent, it would establish nothing about whether the Petition’s different theory satisfies the different requirements of the ’403 patent. Ex. 2012 ¶59.

Preclusion principles thus do not apply. Collateral estoppel turns on “the identity of the issues that were litigated.” *Ohio Willow Wood Co. v. Alps S., LLC*, 735 F.3d 1333, 1342 (Fed. Cir. 2013). Before applying it, “[t]he Board must decide whether the [claims at issue] present materially different issues that alter the question of patentability.” *MaxLinear, Inc. v. CF CRESPE LLC*, 880 F.3d 1373, 1377 (Fed. Cir. 2018). Here, the issues are different, because a different theory is presented against materially different claim limitations (including the requirement of a “secure interprocess communication service”). Accordingly, the obviousness of the instant Petition’s proposed combination, which involves transmission of inherent-key-encrypted data to third-party applications which do not have any mechanism for decryption, was never presented or decided, and thus cannot have preclusive effect here.

VIII. GROUND 1 FAILS FOR EVERY CHALLENGED CLAIM

A. The Petition Fails to Show Its Proposed Combination Would Have Been Obvious, Because It Never Explains How That

**Combination Would Serve Its Intended Purpose of Allowing
Recipient Applications to Read the Securely Transmitted Data**

**1. The Intended Purpose of the Petition’s Combination Is
Secure Delivery of Data That Recipient Applications
Can Read**

In the Petition’s combination, the transmission of encrypted data to destination applications has only one possible purpose: secure transmission of data that allows recipient destination applications to actually *read* and *use* that data. Ex. 2012 ¶60.

This intended purpose—secure transmission of data to entities that will be able to decipher that data—follows from common sense. Encryption protects data on its way to a recipient who is meant to use it. Ex. 2012 ¶61. Data that no one can ever decrypt is meaningless. Ex. 2012 ¶62. Thus, a transmission scheme in which the sender encrypts and nothing downstream can decrypt is not useful, and certainly would not have been obvious to a POSITA. Ex. 2012 ¶63.

Petitioner’s own expert acknowledges that the system cannot serve its intended purpose if the destination application cannot ultimately obtain access to decrypted data: “At the end of the day, *the application has to have access to decrypted data.*” Ex. 2014, 42:20–25 (emphasis added); *id.* at 53:22–24 (“The destination application has to be able to get access to that data somehow, which implies decryption.”). See Ex. 2012 ¶64.

The understanding that destination applications will need to *read* the encrypted data transmitted to them is further confirmed by the destination applications, such as chess and weather applications, the Petition relies upon, which need to be able to read the chess moves or weather forecasts they receive. *See* Pet. 29 (discussing a “chess application” that “initially need[s] to register with the appropriate MMS User Agent” in order to send and receive data) (quoting Ex. 1004, 54); *id.* at 44 (discussing data “for moving opponent chess pieces”); *id.* at 6 (discussing providing “weather forecasts” “to MMS users”) (quoting Ex. 1004, 14). Of course, chess moves and weather forecasts are useful to these applications only if the applications can actually *read* them. Dr. Traynor agreed: his analysis rests on “my assumption that the application at the end will get access to the data so that applications like chess or weather are useful,” with “the assumption being that that application can use it.” Ex. 2014, 53:5–8, 55:9–13; *see also* *id.* 43:4–11 (“[F]or applications like chess, the destination application would need to see the contents of the message.”). Ex. 2012 ¶65.

The intended purpose of the Petition’s combination, in short, is to deliver application data securely to destination applications *that can read and use that data*. Ex. 2012 ¶¶66–67.

Accordingly, any sensible implementation of the Petition’s proposal requires that the data the User Agent encrypts before sending over the bus can later be

decrypted, so the destination application can use it. That requirement comes from Petitioner's reliance on encryption for security (and the purpose of that encryption—to allow the recipient applications to securely make use of the transmitted data), rather than from the claims themselves. Ex. 2012 ¶68.

Ogawa itself supports the understanding that any sensible encryption scheme requires a mechanism for any recipient to decrypt the encrypted data. Every time Ogawa encrypts data with its inherent key, it also provides the program that will later decrypt that data. Ex. 1005, 6:7–18, 8:24–34. The inherent key's design goal is to *preserve* decryptability for the holder of the removable storage while denying it to everyone else. *Id.* 8:44–50; Ex. 2012 ¶69. A POSITA would have readily recognized that encryption alone is not a difficult problem; the more complex problem is encrypting data in a way that allows the intended recipient to *decrypt* the data while simultaneously *preventing* unintended recipients from doing so. Ex. 2012 ¶70. Ogawa solves this problem by tying decryption to a physical removable storage, but as explained in further detail below, the Petition offers no suitable mechanism for ensuring secure decryptability in the Petition's proposed combination of TS-23.140 with Ogawa.

2. In the Petition's Combination, Only the MMS User Agent Can Decrypt the Data It Sends

The Petition is explicit that Ogawa's encryption and decryption units are placed inside the MMS User Agent. Pet. 14–15, 18–20; Ex. 1003 ¶¶83–84, 95, 101–102. The User Agent decrypts the incoming message, reads the destination application identifier, re-encrypts the data with the inherent key, and sends it over the bus. Ex. 2014, 42:6–14. No other entity is given the inherent key. The network does not have it. *Id.* 27:3–6. No destination application, operating-system service, or proxy is given it anywhere in the Petition or Dr. Traynor's declaration. Pet. 18–20, 39–43; Ex. 1003 ¶¶93–97, 146–151; Ex. 2014, 57:9–59:15; Ex. 2012 ¶¶51, 71, 73.

Accordingly, the data the User Agent encrypts and sends can never be decrypted by or for its recipient. Thus, the encryption step the Petition adds in an attempt to read on the “secure interprocess communication service” claim language defeats the very purpose for which Petitioner added it. The Petition's combination is simply inoperable; a chess application will receive moves it cannot read, and the weather application will receive a forecast it cannot analyze. Ex. 2012 ¶72.

Dr. Traynor did not dispute that his declaration leaves this problem entirely unaddressed. Asked where his declaration explains how a destination application would be able to read inherent-key data, he answered: “I haven't talked about how precisely the decryption is performed, but I look to the '403 patent and its spec for

guidance.” Ex. 2014, 22:21–24. He could not identify any paragraph describing any entity other than the User Agent having access to the inherent key. *Id.* 27:7–29:11. He could not say whether each destination application would receive the same inherent key or a different one, offering only that “I would imagine that different keys are used for different applications” (even though Ogawa describes only a *single* inherent key tied to a removable storage device to decrypt inherent-key encrypted data within a specific device). *Id.* 57:9–58:1; Ex. 1005, 6:3–7; Ex. 2012 ¶¶74, 98. Asked for “one example as set forth in your declaration as to how the inherent keys in Ogawa are distributed to the destination application,” he offered none. Ex. 2014, 58:14–59:15. And when asked for a single paragraph number to which Patent Owner could respond in addressing any theory regarding how the recipient application would be able to read the inherent-key-encrypted data, he answered: “Again, I’m not sure how to answer this further than I have.” *Id.* 61:2–11.

Instead, Dr. Traynor repeatedly characterized these questions as “implementation details” comparable to the device’s battery, screen size, and case color. *Id.* 23:14–24:1, 28:1–29:2, 47:20–48:2, 50:18–51:1, 59:9–15. They are not. A larger or smaller battery has nothing to do with whether the Petition’s proposed encryption scheme can deliver readable data to its recipients—the whole point of the “secure interprocess communication service” alleged to be present in the proposed combination. Ex. 2012 ¶75. Whether the mechanism Petitioner relies on to arrive

at the claims produces a workable result goes to the heart of the obviousness inquiry. *See Pers. Web*, 848 F.3d at 993–94 (vacating where the Board “nowhere clearly explained, or cited evidence showing, how the combination of the two references was supposed to work”). And Petitioner did not even attempt to elicit any details of how the combination would work on redirect. Ex. 2014, 61:22–23. Accordingly, the Petition and supporting materials fail to set forth any coherent way in which the Petition’s proposed combination could operate in the manner Petitioner alleges it could. Ex. 2012 ¶76.

3. Neither TS-23.140 nor Ogawa Teaches How a Recipient Program Could Decrypt Inherent-Key Data

Neither TS-23.140 nor Ogawa discloses how any application other than the program holding Ogawa’s inherent key could decrypt data encrypted with that key. Ex. 2012 ¶77.

TS-23.140 mentions encryption by the MMS User Agent only “on an end-user to end-user basis,” Ex. 1004, 19, and says nothing about encrypting or decrypting data passed from the User Agent to a destination application on the same device. It instead leaves the interface between the User Agent and those applications “outside the scope of this specification.” *Id.* 54. Ex. 2012 ¶78.

Ogawa also does not teach how inherent-key-encrypted data might be passed between two different programs on a device in a secure manner that would allow the receiving program to access the data. Ex. 2012 ¶79.

As discussed above, Ogawa deliberately uses two different kinds of keys. Its shared key is distributed between sites through a Diffie-Hellman exchange. Ex. 1005, 6:42–43, 7:1–24. Dr. Traynor’s own declaration says so: “[t]he shared encryption key is distributed to both data input site 1 and client site 3.” Ex. 1003 ¶56; Ex. 2012 ¶¶80, 82.

Ogawa’s inherent key is fundamentally different from Ogawa’s shared key. It is “generated from an inherent identification code that was assigned during manufacturing and stored on the internal memory device of the removable storage 5.” Ex. 1005, 6:3–7. The fact that the “inherent key” is derived from the identification code that is inherent to the removable storage device is what makes the key “inherent.” The decryption process can perform decryption only by using the *same* inherent code. *Id.* 8:65–9:14. The code passes only from the removable storage to the client program that uses it (which client program itself is loaded from the removable storage). *Id.* 5:44–47, 8:10–19, 8:24–34. Dr. Traynor could identify no Ogawa embodiment in which the inherent key is not stored on or derived from the removable storage. Ex. 2014, 29:18–32:16, 35:14–19 (“I don’t recall reading that”); Ex. 2012 ¶81.

Ogawa explicitly teaches that its inherent key is closely tied to the removable storage device that is the focus of its invention. *See* Ex. 1005, 8:44–50 (“[U]nless there is a corresponding removable storage 5 which holds the inherent encryption key, there is no way to decrypt the saved data.”); *id.* at 10:58–63 (noting that data “may only be decrypted only with the same PC and same removable storage”). When another person wants to read inherent-key data, the key is not electronically transmitted to that person via a bus; instead, that person “must borrow a removable storage device” that contains the key. *Id.* 10:41–49. Even Ogawa’s group-sharing embodiment, in which multiple removable storage devices each contain “the same program (or encryption key),” shares the key only by duplicating the physical removable storage among the members of a group—not by handing the key to other programs on the same device. *Id.* 5:54–58; Ex. 2012 ¶¶83–84. And only one program (a program derived from the removable storage device itself) ever uses the inherent key. Ogawa’s encryption unit 35 and decryption unit 38 are both part of “a single computer executable instruction set 51,” which is itself derived from the removable storage device. Ex. 1005, 5:24–32, 5:44–47, 6:1–18; Ex. 2012 ¶85.

4. The Petition’s Combination Is Inoperable for Its Intended Purpose and Therefore Not Obvious

As noted above, neither Ogawa nor TS-23.140 discloses or suggests any mechanism for how a destination application in the proposed combination would be

able to read the inherent-key-encrypted data transmitted from the MMS User Agent in the proposed combination. And the Petition itself provides no explanation for how this capability would be present in its proposed combination. Ex. 2012 ¶87.

The Federal Circuit has long held that a modification rendering the prior art inoperable for its intended purpose is not an obvious one. In *Gordon*, the court reversed an obviousness rejection premised on turning a prior-art strainer upside down, because doing so would have rendered the device “inoperable for its intended purpose.” 733 F.2d at 902. The court later explained that it “has previously found a proposed modification inappropriate for an obviousness inquiry when the modification rendered the prior art reference inoperable for its intended purpose.” *In re Fritch*, 972 F.2d 1260, 1265 n.12 (Fed. Cir. 1992). And “[i]f references taken in combination would produce a ‘seemingly inoperative device,’ ... such references teach away from the combination and thus cannot serve as predicates for a prima facie case of obviousness.” *McGinley*, 262 F.3d at 1354 (citing *In re Spinnoble*, 405 F.2d 578, 587 (C.C.P.A. 1969)); accord *Tec Air, Inc. v. Denso Mfg. Mich. Inc.*, 192 F.3d 1353, 1360 (Fed. Cir. 1999). The Federal Circuit recently reaffirmed this principle in an IPR appeal, holding that the Board “did not err in determining the destruction of [the reference’s] entire purpose, shared with the challenged claims, was probative of whether [the petitioner’s] modifications would have been obvious.” *Medtronic*, 69 F.4th at 1349–50.

The Petition’s combination fails this test. TS-23.140’s transmission of application data has the purpose of delivering data to the destination application “without alteration.” Ex. 1004, 14, 56. The Petition modifies it so that the destination application receives data encrypted using a key that only the User Agent holds, with no articulated way to restore the encrypted data to its unencrypted form.² That modification renders TS-23.140’s application-data transport inoperable for its intended purpose, and the resulting combination is, at minimum, a “seemingly inoperative device” for delivering usable application data. *Gordon*, 733 F.2d at 902; *McGinley*, 262 F.3d at 1354. Ex. 2012 ¶88. And delivering usable application data to the identified software process is a purpose TS-23.140 shares with the challenged claims. Ex. 1001, claim 1. Modifying a reference in a way that destroys such a

² The ’403 patent itself, when it discusses encryption, does not present this problem because it discloses that encryption can involve “encryption using one or more keys that are partially shared or shared within the service processor 115 agent group.” E.g., Ex. 1001, 41:59–42:4; *see also id.* 42:19–28 (keys “provided and updated by the secure server”). However, this approach is incompatible with the Petition’s proposed reliance on Ogawa’s *inherent key* for encryption, which is not shared and not designed to be shared. Ex. 2012 ¶89.

shared purpose “counsels against a motivation to make such modifications.”
Medtronic, 69 F.4th at 1349.

Patent Owner’s argument does not depend on either reference disparaging Petitioner’s modification, and it does not depend on any claim requirement. It depends only on the Petition. Petitioner chose the inherent key as its sole source of security in the alleged “secure interprocess communication service,” assigned that mechanism the purpose of protecting data delivered to destination applications, but never explained how the destination applications could read the data. Ex. 2012 ¶90. And as noted above, a petitioner “cannot employ mere conclusory statements” to fill that gap. *Magnum Oil*, 829 F.3d at 1380; *see Pers. Web*, 848 F.3d at 994. Ground 1 fails for every challenged claim on this basis alone.

B. The Petition’s Combination Conflicts with the Purpose of Ogawa’s Inherent Key and Undermines Petitioner’s Own Rationale

Even apart from the inoperability of the combination, Petitioner has not shown that a POSITA would have been motivated to make it. Ex. 2012 ¶91. “An inference of nonobviousness is especially strong where the prior art’s teachings undermine the very reason being proffered as to why a person of ordinary skill would have combined the known elements.” *DePuy Spine*, 567 F.3d at 1326. That is the case here.

Petitioner's stated reason for applying the inherent key to bus communications is that doing so "would have improved data security in MMS-Ogawa's UE/device and would have helped, e.g., prevent unauthorized data access by, e.g., rogue software." Pet. 20; Ex. 1003 ¶¶95. Ogawa provides no support for that rationale. Ogawa uses its inherent key for a single purpose: protecting files saved to a local disk so that they are useless if the computer is stolen without the separately secured removable storage. Ex. 1005, 8:44–56. Ogawa's own example is a salesperson who carries only the removable storage and downloads data to a customer's PC, where "there is no way of decrypting the data unless there is a corresponding removable storage 5." *Id.* 8:51–56. That rationale concerns data at rest on a machine that may be lost. It says nothing about messages passed between processes on a running device. Ex. 2012 ¶¶92–93.

When Ogawa *does* pass data from one program to another on the same device, it does not use the inherent key, and the receiving program already holds the key it needs. In FIG. 9, the TCP2 program removes only the TCP2 transport encryption and passes the data to program 51, which decrypts it with the shared key it already holds, just as in FIG. 1. Ex. 1005, 5:59–65, 10:23–30; Ex. 2012 ¶¶94. Ogawa thus teaches that its inherent key is for storage, not for inter-program transfer. Petitioner identifies no disclosure in Ogawa, TS-23.140, or any other reference that applies a storage-bound key like Ogawa's to communications between applications. Pet. 18–

20. The Petition’s citation to Yami (Ex. 1039) as background for securing interprocess communications (Pet. 19–20) does not cure this deficiency. Yami is not part of any ground, and neither the Petition nor Dr. Traynor relies on Yami for how a recipient application would obtain an inherent key like Ogawa’s in a way that would not undermine the security motivations behind the inherent key. *Id.*; Ex. 1003 ¶¶93, 95; Ex. 2012 ¶95.

To make its proposal work, Petitioner would need to get the inherent key (or the ability to decrypt with it) to each destination application, and do so in a way that would satisfy each of the claim requirements (including the “interprocess communication service” requirement). Petitioner never proposes that modification, and for good reason. Petitioner’s destination applications are third-party applications downloaded to the device. Ex. 2014, 41:19–22; Pet. 29, 82–84; Ex. 1004, 54. Dr. Traynor himself describes those applications as ones “that should not be trusted with access to sensitive device data/functions.” Ex. 1003 ¶272; Ex. 2012 ¶96. Distributing a single device-bound decryption key to every such application would place it in the hands of the very “rogue/unauthorized software” Petitioner says the encryption guards against. Ex. 1003 ¶95; Pet. 20. Ex. 2012 ¶97. The security benefit Petitioner invokes as its motivation would disappear.

It would also abandon what makes Ogawa’s inherent key work. Ogawa ties decryption to possession of the corresponding removable storage device. Ex. 1005,

8:44–50, 10:58–63. A key handed to every downloaded application on a handset is no longer bound to any physical guarantee of security. Ex. 2012 ¶¶99. A POSITA reading Ogawa would not have been led to discard the defining feature of the very key Petitioner selected. *See In re Ratti*, 270 F.2d 810, 813 (C.C.P.A. 1959) (holding a combination requiring “a change in the basic principles under which the [reference’s] construction was designed to operate” not obvious); *see also Plas-Pak Indus., Inc. v. Sulzer Mixpac AG*, 600 F. App’x 755, 759–60 (Fed. Cir. 2015) (affirming nonobviousness where proposed combinations would have altered one reference’s “principle of operation” or rendered another “inoperable for its intended purpose”).

C. The Petition Does Not Show a Reasonable Expectation of Success

For the same reasons, Petitioner has not shown a reasonable expectation of success in achieving the claimed invention through its proposed combination. *Intelligent Bio-Sys.*, 821 F.3d at 1367. The Petition’s showing consists of a single clause asserting that POSITAs “would have reasonably expected success,” followed by the same security rationale discussed above. Pet. 19–20; Ex. 1003 ¶¶95; Ex. 2012 ¶¶100. Neither the Petition nor the declaration addresses how the destination application would read the data, which entity would hold the inherent key, or how the key would reach it. Ex. 2014, 22:21–24, 27:7–29:11, 58:14–61:11.

Dr. Traynor’s deposition testimony confirms that these omissions matter. He acknowledged that Ogawa provides only “some high level mechanisms for key generation, but there are lots of details that aren’t included here,” and that he would look to outside standards such as FIPS 140-2 to fill them in. *Id.* 33:23–34:9, 35:4–8. He agreed that how an encryption key is distributed can determine whether a system is in fact “secure,” acknowledging that “if it’s done poorly” the overall system will not be “secure.” *Id.* 59:16–24. And he conceded that “there are many different ways to deliver data securely, and there are ways you could get it wrong too.” *Id.* 57:1–8. A reasonable expectation of success cannot rest on a scheme whose essential details neither the Petition nor any asserted reference supplies, particularly when Petitioner’s own expert acknowledges the implementation details matter. Ex. 2012 ¶¶101–103.

D. The Petition Fails to Establish the Obviousness of a “Secure Interprocess Communication Service” in Its Proposed Combination

As noted above, an “interprocess communication service” is not simply communication functionality implemented by the communicating processes, but is instead a service that is provided to the processes by some other component (e.g., the operating system). Ex. 2012 ¶¶32–33, 104. The Petition does not specify how the encryption and decryption functionality between the MMS User Agent and destination application in its proposed combination actually satisfies a “secure

interprocess communication service” as it would have been understood by a POSITA (because, e.g., the Petition does not describe what entities are actually responsible for providing the actual alleged secure communication path such as which entity is responsible for decryption), such that they have not established its obviousness. Ex. 2012 ¶104. To the extent Petitioner is allowed to introduce a more specific theory in this regard, Patent Owner reserves the right to introduce additional evidence and argument explaining why any new proposal does not satisfy the claim requirement.

IX. GROUNDS 2A–4D FAIL FOR THE SAME REASONS

Every remaining ground incorporates MMS-Ogawa’s inherent-key mechanism unchanged. Grounds 2A–2C add Cole’s WWAN and WLAN modems and Sathish’s D-Bus, but they rely on “the bus secured as discussed supra §VII.C.6” (i.e., secured with Ogawa’s inherent key). Pet. 63–72; Ex. 1003 ¶¶211–236. Sathish’s D-Bus is “an example of a device inter-process communication channel used to send information between applications”; it supplies no key distribution. Ex. 1031, 10:56–62. Grounds 3A–3D add Papineau for claims 7–9, and Grounds 4A–4D add Ellison for claim 10 (and, in Grounds 4B–4D, claims 1–6 and 13–21), without altering how MMS-Ogawa secures communications on the device. Pet. 74–77, 80, 82–85. None of Cole, Sathish, Papineau, or Ellison is cited for a recipient

application's ability to decrypt inherent-key data. Ex. 2012 ¶¶111–112. Each ground therefore fails for the reasons set out in Section VIII.

X. THE DEPENDENT CLAIMS ARE INDEPENDENTLY PATENTABLE

Because every ground fails as to claim 1, every dependent claim survives. The following dependent claims are independently patentable for additional reasons. Ex. 2012 ¶113.

A. Claim 11

Claim 11 requires that the device messaging agent send secure upload Internet data messages, “at least a subset” of which “are sent responsive to a corresponding request received on the secure interprocess communication channel from a corresponding one of the software applications,” and that each such message contain “an identifier for a respective network application server corresponding to the requesting software application.” Ex. 1001, claim 11; Ex. 2012 ¶114.

First, the Petition never shows that any request is received on a *secure* channel. The Petition's combination secures only one direction: the User Agent re-encrypts data before sending it *to* a destination application. Pet. 18–20, 41. For the reverse direction, the Petition says only that “communication between MMS-Ogawa's User Agent application and other applications on the user device occur over MMS-Ogawa's bus (‘secure interprocess communication service’).” Pet. 49; *see* Ex. 1003 ¶¶170–175. It never explains how a request *from* an application is

secured. Under Petitioner’s inherent-key theory, the requesting application would itself need Ogawa’s inherent key and encryption unit, features which the Petition never alleges would be included within any application (and which would contradict Ogawa’s design goal of providing encryption and decryption capabilities only to the single program derived from the removable storage device). *Supra* §§ VIII.A.2–3. Ex. 2012 ¶115.

Second, the Petition does not show the claimed identifier. Petitioner relies on TS-23.140’s “destination application identifier.” Pet. 50–51. That identifier, as its name indicates, identifies the destination *application* to which a VAS Application routes the data. Ex. 1004, 55–56. The Petition itself describes the identifier as being “*for use by the VAS Application* to route the message to the correct destination application.” Pet. 51. Nowhere does TS-23.140 describe the identifier as being used by the “destination application” in order to route the message to a VAS application, and the Petition identifies no such disclosure. An identifier of an application is not “an identifier for a respective network application server,” (Ex. 2012 ¶116), and the Petition never explains how TS-23.140 would even allegedly be modified in any obvious manner to arrive at this requirement. Accordingly, claim 11 (and claim 12, which depends from claim 11) is not obvious under the Petition’s theory. Ex. 2012 ¶¶116–118.

B. Claim 15

Claim 15 requires that “access by the software applications to the interprocess communication channel is subject to a security policy.” Ex. 1001, claim 15. Petitioner contends that access by the applications is “subject to a security policy” because the bus is encrypted with the inherent key, so that access requires “a specific encryption key.” Pet. 55; Ex. 1003 ¶¶191; Ex. 2012 ¶¶119. But in the Petition’s combination no software application holds that key. *Supra* § VIII.A.2. A key that no application can obtain does not govern applications’ “access” to anything; it simply prevents every application from reading what it receives. Ex. 2012 ¶¶120. Accordingly, claim 15 is not obvious under the Petition’s theory.

C. Claim 16

Claim 16 requires that “at least one of the secure Internet data messages comprises multiple identifier/data pairs.” Ex. 1001, claim 16. Petitioner offers two theories, neither of which succeeds. Ex. 2012 ¶¶122.

Petitioner first contends that when an unavailable User Agent returns to coverage, the MMS Relay/Server “delivers the group of collected messages,” and that this group is a single message comprising multiple identifier/data pairs. Pet. 56–57; Ex. 1003 ¶¶193–194. A group of the claimed messages, however, is not a claimed message. TS-23.140 specifies how a User Agent retrieves an MM: “[t]he recipient MMS User Agent shall issue an MM1_retrieve.REQ to the recipient MMS

Relay/Server to initiate the retrieval process,” providing “a reference, e.g., URI, for the MM,” and “[t]he MMS Relay/Server shall respond with an MM1_retrieve.RES, which contains MMs control information and the MM content.” Ex. 1004, 69. Each request and response concerns a single MM. Ex. 2012 ¶¶123–124. Dr. Traynor identified the MM1_retrieve.RES as his example of a secure Internet data message containing an identifier. Ex. 2014, 8:16–9:7. Yet he conceded that he knows of no TS-23.140 disclosure of an MM1_retrieve.RES carrying more than one MM—“I don’t have a direct reference”—and could not identify where his declaration addresses the question. *Id.* 12:24–14:12; Ex. 2012 ¶125.

Petitioner alternatively contends that lower-layer radio protocols would have aggregated multiple HTTP messages within a single RLC or MAC frame. Pet. 57–58; Ex. 1003 ¶¶195–198. But the claimed “secure Internet data messages” are the messages the device messaging agent receives “over a secure connection to a network message server.” Ex. 1001, claim 1. Petitioner’s device messaging agent is the MMS User Agent, which Petitioner says “sits at the application layer,” well above the radio link protocols. Pet. 62; Ex. 1003 ¶208; Ex. 2012 ¶126. The User Agent never receives an RLC protocol data unit or a MAC transport block. Ex. 2012 ¶127. Nor does concatenating or multiplexing segments of lower-layer data units create “identifier/data pairs” within a secure Internet data message. Ex. 2012 ¶128. Dr. Traynor could not say at which layer the MM1_retrieve.RES would reside and

had no recollection of offering any opinion on the subject. Ex. 2014, 9:8–10:7; Ex. 2012 ¶129. The Petition’s lower-layer theory is precisely the sort of conclusory assertion that cannot carry Petitioner’s burden. *Magnum Oil*, 829 F.3d at 1380. Claim 16 is not shown to be obvious.

D. Claim 21

Claim 21 requires that “at least one of the applications and the network application server corresponding to that application authenticate with each other prior to passing application data via the device messaging agent and network message server.” Ex. 1001, claim 21. Petitioner relies on TS-23.140’s application registration process. Pet. 62–63; Ex. 1003 ¶¶209–210; Ex. 2012 ¶130.

The Petition fails to show that TS-23.140’s registration constitutes mutual authentication. TS-23.140 describes registration in a single note: the application “provisions an MMS User Agent or an MMS VAS Application with its application identification value and may negotiate with the MMS User Agent or MMS VAS Application the details (amount and format) of information to be exchanged between the two entities.” Ex. 1004, 54. “The application registration process is outside the scope of this specification,” and it “may be an inherent process e.g., in the application’s integration into a mobile phone.” *Id.* Dr. Traynor agreed that the note describes two things—provisioning an application identification value and negotiating the amount and format of information—and pointed to nothing else. Ex.

2014, 36:11–37:22, 40:4–41:2; Ex. 2012 ¶131. However, merely providing some identifier and agreeing on data format does not necessarily verify any application’s identity or credentials. Ex. 2012 ¶132.

The Petition also fails to show that a destination application residing on an end-user device would *ever* register with an MMS VAS Application. TS-23.140 states that an application registers “with the appropriate MMS User Agent *or* MMS VAS Application.” Ex. 1004, 54 (emphasis added). A POSITA would have understood that the “appropriate MMS User Agent or MMS VAS Application” was the MMS User Agent or MMS VAS Application residing on the same physical device as the application, because that is the User Agent or VAS Application that the application interacts with most directly (and the User Agent or VAS Application would perform the requisite coordination with remote User Agents or VAS Applications). Ex. 2012 ¶133. Dr. Traynor agreed that a device application “might do so locally with its MMS user agent.” Ex. 2014, 38:22–39:5. Although he speculated that the User Agent “may then need to, as a proxy or on behalf of application, further register with the MMS VAS application,” *id.* 39:3–5, but TS-23.140 describes no such step and Dr. Traynor provided no support for his assertion. And registration with the device’s own User Agent is not the application and the network application server “authentica[ting] with each other.” Ex. 2012 ¶134.

Dr. Traynor further cites to authentication between a VASP and the MMS Relay/Server, alleging that “TS-23.140 also discloses the MMS-Relay Server ‘authenticat[ing] the VASP during each session established for message submission... before any transactions will be allowed by the MMS Relay/Server.’” Ex. 1003 ¶210. But this is authentication between the MMS Relay/Server and a VASP, *not* between a device application and its network application server. Ex. 1004, 41; Ex. 1003 ¶210; Ex. 2012 ¶135. And nowhere does the Petition or Dr. Traynor explain how this VASP to Relay/Server authentication could satisfy the claim language. The Petition therefore fails to show that claim 21 would have been obvious for this additional reason.

XI. CONCLUSION

Petitioner has not carried its burden of proving any challenged claim unpatentable. Patent Owner respectfully requests that the Board enter a final written decision confirming the patentability of claims 1–21 of the ’403 patent.

Date: October 8, 2026

/James A. Milkey/
James A. Milkey, Reg. No. 79,503
Russ August & Kabat
12424 Wilshire Blvd., 12th Floor
Los Angeles, CA 90025

Counsel for Patent Owner

CERTIFICATION REGARDING WORD COUNT

Pursuant to 37 C.F.R. §42.24(d), Patent Owner certifies that there are 9,543 words in the paper excluding the portions exempted under 37 C.F.R. §42.24(a)(1).

Date: October 8, 2026

/James A. Milkey/
James A. Milkey, Reg. No. 79,503
Russ August & Kabat
12424 Wilshire Blvd., 12th Floor
Los Angeles, CA 90025

Counsel for Patent Owner

CERTIFICATE OF SERVICE (37 C.F.R. § 42.6(e)(1))

The undersigned hereby certifies that the above document was served on October 8, 2026 by filing this document through the Patent Trial and Appeal Case Tracking System (P-TACTS) as well as delivering a copy via electronic mail upon the following attorneys of record for the Petitioner:

Anant K. Saraswat, Reg. No. 76,050
Turhan F. Sarwar, *pending admission pro hac vice*
George T. Scott, Reg. No. 62,859
Wolf, Greenfield & Sacks, P.C.
600 Atlantic Avenue
Boston, MA 02210-2206
ASaraswat-PTAB@wolfgreenfield.com
TSarwar-PTAB@wolfgreenfield.com
GScott-PTAB@wolfgreenfield.com

Date: October 8, 2026

/James A. Milkey/
James A. Milkey, Reg. No. 79,503
Russ August & Kabat
12424 Wilshire Blvd., 12th Floor
Los Angeles, CA 90025

Counsel for Patent Owner