

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,

Petitioner,

v.

HEADWATER RESEARCH LLC,

Patent Owner

IPR2026-00203
Patent No. 9,232,403

PATENT OWNER'S PRELIMINARY RESPONSE TO THE PETITION

TABLE OF CONTENTS

I. Introduction 1

II. The Petition fails to establish a reasonable likelihood of prevailing with respect to any challenged claim. 2

 A. The Petition’s obviousness theory places Ogawa’s decryption and decryption units only in the MMS User Agent within the MMS-Ogawa device. 3

 B. The Petition’s MMS-Ogawa combination includes no functionality for any application other than the MMS User Agent to decrypt data on the MMS-Ogawa device. 6

 C. The Petition’s reliance on other art and a prior IPR does not salvage the Petition’s MMS-Ogawa combination. 9

III. Conclusion 13

I. Introduction

The Petition alleges that a “secure interprocess communication service” would be obvious in the combination of TS-23.140 (which describes “MMS”) with Ogawa, based on a theory where it would be obvious for TS-23.140’s “MMS User Agent” to transfer data encrypted with an “inherent encryption key” to other recipient applications residing on the same device. But neither TS-23.140 nor Ogawa teaches any mechanism for transmitting encrypted data between different applications within the same device; for example, neither TS-23.140 nor Ogawa discloses how a receiving application would be able to *decrypt* any encrypted data received from an application residing on the same device.

The Petition does nothing to cure the deficiency of the references it relies upon. For instance, the Petition does not even *allege* that the receiving applications in its proposed combinations would have data decryption capabilities. And Ogawa itself (the sole reference the Petition relies on for details concerning encryption and decryption) suggests that Ogawa’s decryption unit for decrypting data encrypted using Ogawa’s “inherent” key exists *only* within the application on the device that encrypted the data in the first place. Indeed, Ogawa distinguishes the “inherent” key used for encryption and decryption *within* a device from a “shared” key used for encryption and decryption between distinct entities over a network, and Ogawa never suggests that its “inherent” key would be “shared” between applications as

would be necessary for the receiving application to decrypt (and thus understand) the data the Petition alleges would be sent between applications in its proposed combination of references.

Because the Petition fails to explain how either the Petition's references or the Petition's combination of those references satisfies the requirements of the sole independent claim 1, the Petition fails to show a reasonable likelihood of prevailing with respect to any challenged claim.

II. The Petition fails to establish a reasonable likelihood of prevailing with respect to any challenged claim.

The only independent claim of the '403 patent requires a "secure interprocess communication service." *See* Ex. 1001, claim 1. As explained below, the Petition's only theory as to how this limitation is satisfied is based on a theory wherein a MMS User Agent application residing on the MMS-Ogawa device would encrypt data using an inherent key and transmit the encrypted data to other applications residing on the device. The Petition fails to show the obviousness of this theory, because the Petition does not allege (and the prior art references mapped to claim 1 do not disclose) any mechanism by which a receiving application could decrypt the encrypted data received by the MMS-Ogawa User Agent.

A. The Petition’s obviousness theory places Ogawa’s decryption and decryption units only in the MMS User Agent within the MMS-Ogawa device.

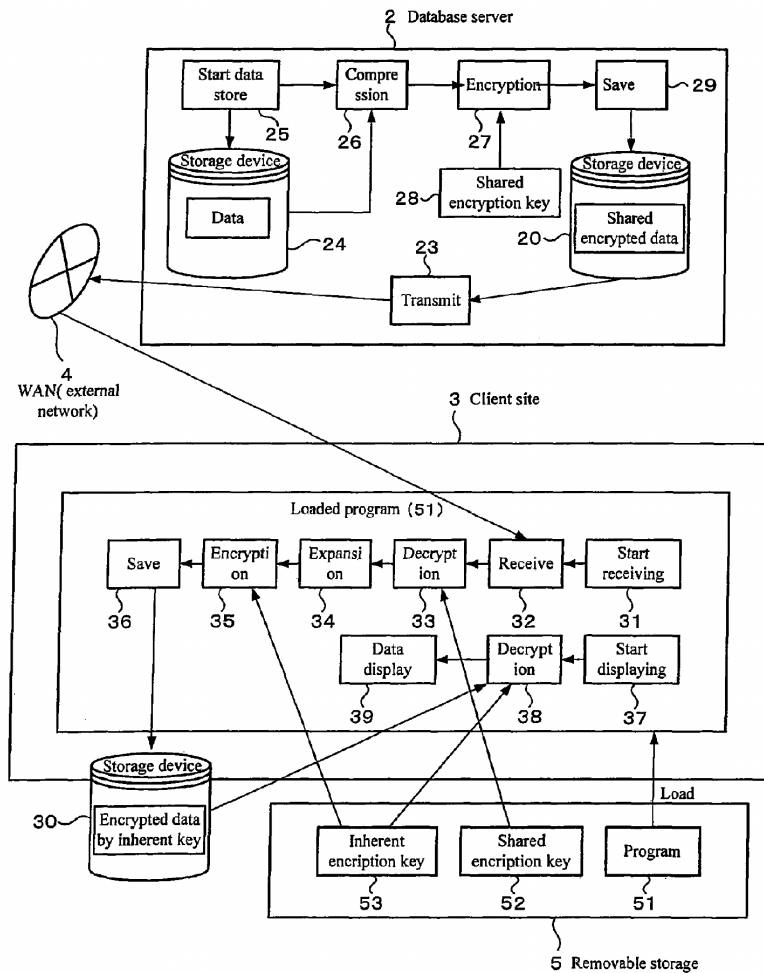
The Petition’s claim 1 invalidity theory relies on a combination of the teachings of TS-23.140 (Ex. 1004, which discusses an “MMS” protocol) and Ogawa (Ex. 1005). The Petition is explicit that in the proposed combination, “*Ogawa’s encryption and decryption units are implemented as part of the MMS User Agent in TS-23.140’s UE/device.*” Pet. 20.¹

Nowhere does the Petition allege that Ogawa’s decryption unit would be located anywhere *other* than the in Ogawa’s MMS User Agent. *See generally* Pet. For example, despite alleging that “MMS-Ogawa implements an interprocess bus for communications between applications” (Pet. 21), the Petition does not allege that Ogawa’s encryption or decryption units would be located within any of the applications that receive data from the MMS User Agent. Indeed, nowhere does the Petition describe (or allege) *any* decryption functionality for any application residing on the MMS-Ogawa device that would receive data from the MMS User Agent residing on the same device.

The Petition’s proposed combination, in which the encryption and decryption

¹ All emphases in quotations herein are added unless otherwise specified.

units would be located within only a single application (e.g., the MMS User Agent in the Petition’s MMS-Ogawa combination) within a device, is consistent with Ogawa’s teachings. Specifically, as shown in Figure 7 (cited by Pet. pp. 7, 14, 15, 19, 41 and reproduced below), Ogawa contemplates that both “Encryption” (35) and “Decryption” (33 and 38) components are located within a single “Loaded program (51),” and that encryption is used merely to save encrypted data to memory so that the *same* program can decrypt and display the data.



Ex. 1005, FIG. 7; *id.* at 6:10:10–18 (discussing the same program 51 “decrypt[ing]

the inherent key encrypted data... using the inherent encryption key” so that “the decrypted data are supplied to the display unit 39” within program 51).

Indeed, Ogawa teaches that the data is meant to be decrypted only using a “inherent” key that—unlike the “shared” key used to decrypt data transmitted over Ogawa’s external network—is inherent to a removable storage media that includes the program designed to encrypt, decrypt, and display the data, such that sharing of the inherent key *between* programs is not contemplated by Ogawa. *See* Ex. 1005, 8:44–47 (“[B]ecause the downloaded data is saved after 45 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.”). Nowhere does Ogawa teach or otherwise suggest that data would be encrypted by one application then transmitted to a *different* application for decryption using its encryption protocol, or that anything other than a single application stored on “Removable storage” (5) would have access to a decryption unit or the inherent key required to decrypt data encrypted with the inherent key.

In sum, the Petition’s theory (consistent with Ogawa’s own teachings) is that only the MMS User Agent within the MMS-Ogawa device would have access to a decryption unit for decrypting data. Neither the Petition nor Ogawa discloses any functionality for a *separate* application to receive and decrypt data that was encrypted using Ogawa’s inherent key.

B. The Petition’s MMS-Ogawa combination includes no functionality for any application other than the MMS User Agent to decrypt data on the MMS-Ogawa device.

The Petition’s only allegation that any “interprocess communication service” in its proposed combination of MMS with Ogawa is that “[a]s discussed [in] §VII.C.6 [of the Petition], interprocess communications [would be] secured using Ogawa’s inherent key” over a software bus. *See* Pet. 41.

The Petition’s Section VII.C.6 asserts that “internal communications [would be] protected using an inherent key.” Pet. 19–20. Elsewhere, the Petition provides slightly more detail, alleging that the message encrypted using the inherent key would be encrypted by the MMS “User Agent’s encryption unit” and “forwarded by the bus to a process of the destination application.” Pet. 59. In other words, the Petition alleges that the MMS User Agent would encrypt data using the inherent key, and send that encrypted data to a different application residing on the same device.

The Petition’s proposal of sending an encrypted message over a software bus from the MMS User Application to receiving applications raises the obvious question of how each recipient application would be able to decrypt the encrypted data it receives from the MMS User Agent.² Such decryption has *at least* two

² Of course, it would not make sense to encrypt a message for transmission to a

requirements. First, Ogawa teaches that decryption occurs using a “decryption unit.” See Ex. 1005, FIG. 7. Second, Ogawa teaches that decryption of data requires the same key that was used to encrypt the data. See, e.g., Ex. 5 at FIG. 7 (showing the “Shared encryption key” and “Inherent encryption key” being required to decrypt messages encrypted using the shared and inherent keys, respectively). Indeed, the Petition elsewhere acknowledges that in order to decrypt encrypted messages in accordance with Ogawa’s teachings, the recipient entity “needs to have the shared encryption key used to encrypt the message to enable decryption.” Pet. 52. Thus, to perform decryption of data encoded with Ogawa’s inherent key, a recipient application would need both (1) a “decryption unit” as well as (2) access to Ogawa’s inherent key.

However, the Petition does not allege *either* of these requirements to be satisfied in MMS-Ogawa. For instance, as discussed above, the Petition alleges that “**Ogawa’s encryption and decryption units are implemented as part of the MMS User Agent** in TS-23.140’s UE/device.” Pet. 20. The Petition is entirely silent as to how any application that would *receive* data from the MMS User Application within the combined device would have access to either a decryption unit or Ogawa’s

recipient application if the recipient application was unable to *decrypt* that encrypted message.

inherent key required to utilize such a decryption unit.

The Petition's failure to explain how the recipient applications in the MMS-Ogawa device have both a decryption unit and the inherent key is not trivial, because the Petition asserts that sharing a key used for encryption requires a secure protocol to avoid unintended recipients from accessing the key and using it to decrypt messages not meant for those unintended recipients. For instance, the Petition explains that exchange of a shared encryption key between a MMS User Agent residing on a device and a MMS VAS Application residing on a network application server is possible because the communication pathway between these two entities would "[be] secured using TLS/SSL." Pet. 53. In other words, the Petition contends that because a MMS User Agent (which resides on the MMS-Ogawa user device) and a MMS VAS Application (which resides on a separate network application server) communicate using a protocol that is secured *independently* of the shared key (i.e., TLS/SSL), the key can be securely shared between the sender and recipient.

However, the Petition does not allege that TLS/SSL would be (or even could be) used for transmission of data *within* the MMS-Ogawa user device. Nor does the Petition propose any *other* means of securely sharing an encryption key between a MMS User Application and other recipient applications. Instead, the use of "Ogawa's inherent key" is the *only* security mechanism alleged to secure what the Petition describes as "TS-23.140's software bus for interprocess communications"

from a “User Agent... to a destination application.” *See* Pet. 41.

In sum, the Petition does not (and cannot) explain why a POSITA would have been motivated to *encrypt* data for transmission to a recipient application, given that the Petition fails to articulate (much less establish the obviousness of) any mechanism for the recipient application to *decrypt* the received data. Accordingly, the Petition fails to establish the obviousness of its proposed combination at least as that combination relates to the “secure interprocess communication service” limitation.

C. The Petition’s reliance on other art and a prior IPR does not salvage the Petition’s MMS-Ogawa combination.

The Petition makes allegations regarding Ex. 1039 (the “Yami” reference) and a prior IPR petition filed by Samsung against claims of another patent, but these arguments do nothing to salvage the deficiency of Google’s MMS-Ogawa theory in this proceeding. *See* Pet. 19–20 (relying on Ex. 1039 and IPR2024-00341).

First, the Petition alleges that “securing interprocess communications between applications using encryption was well-documented,” relying on the Yami reference as purported evidence of this contention. *See* Pet. 19–20 (citing Ex. 1039, Abstract, [0001]-[0004], [0007]-[0008]). But the Petition does not explain how this alleged teaching of Yami suggests the obviousness of the Petition’s *MMS-Ogawa* combination. For instance, Yami teaches the use of two distinct encryption keys for

interprocess communication; [1] a “generated symmetric [encryption] key” which is “then encrypted using [2] a static symmetric encryption key”; it is the “decrypted [symmetric] encryption key” which “is then used to decrypt the job data” sent between applications. *See, e.g.*, Ex. 1039, Abstract.

Unlike Yami, the Petition’s theory relies on encrypting data for interprocess communication using an *inherent* key, rather than any *shared* or *symmetric* key. *See* Pet. 21 (alleging that “communications between applications... are secured using Ogawa’s inherent key”). Accordingly, the obviousness of Yami’s disclosure of encrypting data for transmission between applications is irrelevant to the obviousness of the Petition’s MMS-Ogawa combination, which uses a different type of key that is not alleged or disclosed to be shared between applications on the MMS-Ogawa device, as would be required for a receiving application to decrypt the encrypted data.

Second, the Petition points to a prior petition brought by Samsung in IPR2024-00341 (the “-341 petition”), in which Samsung alleged that Ogawa’s inherent keys could be used to “secur[e] communications within MMS-Ogawa’s UE/device.” Pet. 20. Tellingly, Google’s Petition does *not* allege that Samsung’s -341 petition involved combining MMS and Ogawa in the same way Google’s MMS-Ogawa combination is alleged to operate. Nor could Google make such an allegation, because Samsung’s -341 petition alleged that “Ogawa’s *display units 37-*

39” would “perform the decryption and display functions described on Ogawa” (Ex. 1038, 73), a theory found nowhere in the instant Petition. And Ogawa’s FIG. 7 is clear that its display units are *part of* program 51 (which the Petition points to as performing actions, such as encrypting and decrypting data, attributable to the MMS User Agent rather than any application that would receive data from the MMS User Agent).

Because Google’s Petition does not rely on the same theory that Samsung did in the -341 petition, the Board need not consider whether Samsung’s -341 petition theory satisfies the claim requirements.³ But Headwater additionally notes that Samsung’s theory, *even if* applied, has notable deficiencies as applied to the claims at issue here. For instance, Samsung’s -341 petition theory in this regard was limited to the scenario where “data [is] received by the MMS User Agent... that was intended for immediate display to the user.” Ex. 1038, 74. Even assuming such a theory *were* both obvious and identical to the theory Google presents in the instant Petition (it is not⁴), such a theory would not satisfy the requirement that “the device

³ Nor could details which are present in Samsung’s Petition, but *not* present in Google’s Petition, be relevant here because “[a]rguments must not be incorporated by reference from one document into another document.” 37 C.F.R. §42.6(a)(3).

⁴ As noted herein, Samsung’s combination is a *different* combination than Google’s

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” limitation of [1C2].

Specifically, Google’s Petition maps the “subset of secure Internet data messages” to the subset of “abstract messages” that “are ‘used to transport data specific to applications’ other than the MMS User Agent” (Pet. 35; *see also* Pet. 3, 34), and the Petition does not allege that “*each*” of those messages contain data for immediate display of data (i.e., the messages that Samsung’s -341 petition theory for claim 27 was limited to). Google’s theory is clearly *not* that “subset of secure Internet data messages” is limited to the precise subset of messages intended for

MMS-Ogawa combination and would not render obvious the asserted claims of the ’403 patent under the theory presented in Google’s Petition. But even if the Board’s findings in IPR2024-00341 were arguably relevant for persuasive value, Patent Owner notes that it did not make separate arguments regarding the validity of claim 27 of U.S. Patent No. 8,406,733 in IPR2024-00341 because that claim was not asserted in the corresponding district court proceeding (and is not of similar claim scope as the independent claim at issue here).

immediate display, as Google’s Petition does not even *mention* “immediate display” or “display” of data to the user. *See generally* Petition. Thus, Samsung’s theory wherein encrypted data could only be sent for messages that are “intended for immediate display” does nothing to explain how there would be a “secure interprocess communication service” applicable to “each” message in the “subset” of messages identified by Google’s Petition.

Furthermore, Ogawa discloses that its “display units 37–39” (i.e., what Samsung’s -341 petition alleges would include decryption capability—*see* Ex. 1038 at 73) are part of the same program (51) that receives encrypted data over a network (i.e., the functionality that Google’s Petition attributes to the “MMS User Agent”—*see* Pet. 14–15). *See* Ex. 1005, FIG. 7 (depicting 37, 38, and 39 as being part of program 51). Given that these entities would be part of the *same application* as the MMS User Agent under the Petition’s MMS-Ogawa combination, there is no explanation of how data would be transmitted to those units via a “secure *interprocess communication service*” (a term not at issue in claims challenged by the -341 petition claims) as the ’403 patent claims require.

III. Conclusion

For each of the foregoing reasons (and the reasons articulated in Patent Owner’s Request for Discretionary Denial), Patent Owner respectfully requests that the Board deny Google’s Petition.

Date: March 27, 2026

Respectfully submitted,

/James A. Milkey/

James A. Milkey, Reg. No. 79,503
RUSS, AUGUST & KABAT
12424 Wilshire Blvd., 12th Fl.
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 2,781 words in this paper excluding the portions exempted under 37 C.F.R. §42.24(a)(1).

Date: April 27, 2026

Respectfully submitted,

/James A. Milkey/
James A. Milkey, Reg. No. 79,503
RUSS, AUGUST & KABAT
12424 Wilshire Blvd., 12th Fl.
Los Angeles, CA 90025

Counsel for Patent Owner

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

The undersigned hereby certifies that the above document was served on March 27, 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 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: April 27, 2026
RUSS AUGUST & KABAT
12424 Wilshire Blvd., 12th Fl.
Los Angeles, CA 90025
Phone: (310) 826-7474

/James A. Milkey/
James A. Milkey
Reg. No. 79,503
Attorney for Patent Owner