

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MICROSOFT CORPORATION,
Petitioner,

v.

UNILOC 2017 LLC,
Patent Owner.

IPR2020-00101
Patent 8,495,359 B2

Before THOMAS L. GIANNETTI, TREVOR M. JEFFERSON, and
CHRISTOPHER L. OGDEN, *Administrative Patent Judges*.

OGDEN, *Administrative Patent Judge*.

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

I. INTRODUCTION

Petitioner Microsoft Corporation (“Microsoft”) filed a Petition for *inter partes* review (Paper 2, “Pet.”) of claims 1–15 of U.S. Patent No. 8,495,359 B2 (Ex. 1001, “the ’359 patent”). Patent Owner Uniloc 2017 LLC (“Uniloc”) filed a Preliminary Response (“Prelim. Resp.”). Paper 8.

We may institute an *inter partes* review only if “the information presented in the petition . . . and any response . . . shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” 35 U.S.C. § 314(a) (2018). Applying that standard, we do not institute an *inter partes* review, for the reasons explained below.

II. BACKGROUND

A. RELATED PROCEEDINGS

The parties identify the following proceeding as relating to the ’359 patent: *Uniloc 2017 LLC v. Microsoft Corporation*, 8:19-cv-00783¹ (D.C. Cal. filed April 29, 2019). Pet. vi; Paper 6, 2.

B. REAL PARTIES IN INTEREST

Microsoft identifies only itself as the real party in interest. Pet. vi. Uniloc does not challenge that identification, and also only identifies itself as the real party in interest. Paper 6, 2.

C. THE ’359 PATENT (EX. 1001)

The ’359 patent relates to a system in which one computing device (the originator) sends an electronic communication to a recipient computing device, after encrypting the message using a key provided by a gateway server. Ex. 1001, 33–41.

¹ Uniloc incorrectly lists the docket number as 8:19-cv-00873. Paper 6, 2.

Figure 3B of the patent, reproduced below, depicts an embodiment of the invention:

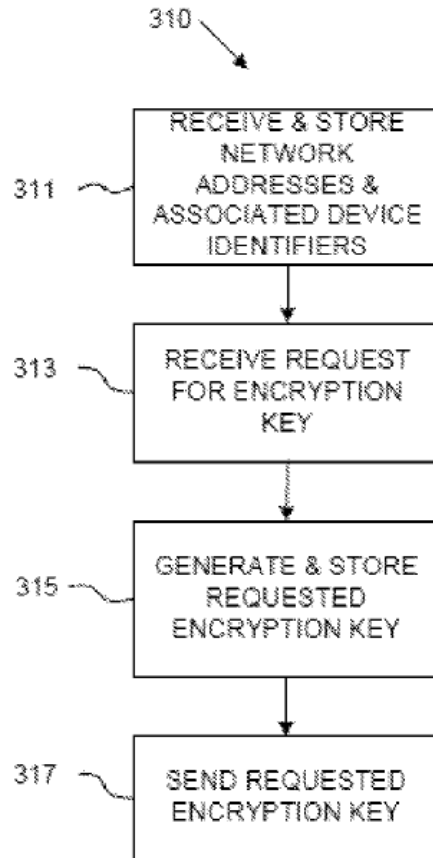


FIG. 3B

Figure 3B is a flowchart for a process (310) in which the gateway server interacts with the originator and receiver of the message. Ex. 1001, 6:60–61. Initially, in step 311, the gateway server receives and stores the network addresses and device identifiers of the devices it serves in the network. *Id.* at 6:61–64. Each device identifier “is generated by a process which operates on data indicative of the computing device’s configuration and hardware,” and “has a very high probability (e.g., greater than 99.999%) of being unique to the target device.” *Id.* at 4:3–5, 15–16.

In step 313, the gateway server receives, from the originator, a request for an encryption key associated with the recipient device. *Id.* at 6:64–65. In step 315, if the intended recipient computer exists within the gateway server’s database, the gateway server generates an encryption key unique to the intended recipient. *Id.* at 6:64–7:1. In step 317, the gateway server then sends the encryption key to the originator. *Id.* at 7:10–13. The originator uses the key to encrypt the message, and then sends the secure message over the network to the recipient computer. *Id.* at 6:56–59.

When the recipient computer receives the encrypted message, it generates its own encryption key using its stored device identifier, and uses that key to decrypt the message. Ex. 1001, 7:20–23. The recipient computer “may also take the additional step of querying the server to determine if the computer purporting to send the secure communication, i.e., the sending computer, did, in fact, request the encryption key.” *Id.* at 7:32–36; *see also* 7:13–15 (“[T]he server . . . may provide confirmations to the receiving computer that the sending computer requested and was sent the encryption key.”). According to the ’359 patent, “[s]uch confirmation aids in building trust that the communication actually originated from the sending computer.” *Id.* at 7:15–17.

D. CHALLENGED CLAIMS AND ASSERTED GROUND OF
UNPATENTABILITY

Microsoft's sole ground for the *inter partes* review is summarized in the following table:

Claims Challenged	35 U.S.C. §	References
1–15	103 ²	Olkin, ³ Kim ⁴

Pet. 2. Microsoft argues that claims 1–15 of the '359 patent are unpatentable as obvious over Olkin in view of Kim. *See* Pet. 2, 11–40.

Independent claim 1, which follows, exemplifies the invention:

- [1.1] 1. A system for securing an electronic communication, the system comprising:
 - [1.2] a gateway server configured to:
 - receive and store a device identifier and a network address from a first computing device, wherein the device identifier is generated by the first computing device from a combination of user-configurable and non-user-configurable parameters of the first computing device and uniquely identifies the first computing device, and wherein the network address is associated with the first computing device;
 - [1.3] receive from a second computing device the network address for the first computing device and an encryption key request;
 - [1.4] derive an encryption key from the device identifier for the first computing device;

² Because the filing date of the '359 patent is before March 16, 2013, we apply the version of 35 U.S.C. § 103 that existed prior to the Leahy–Smith America Invents Act. *See* Pub. L. No. 112-29, § 3(n)(1), 125 Stat. 284, 293 (2011).

³ Olkin et al., US 7,376,835 B2, issued May 20, 2008 (Ex. 1003) (“Olkin”).

⁴ Kim et al., US 2009/0055648 A1, published Feb. 26, 2009 (Ex. 1004) (“Kim”).

- [1.5] send the encryption key to the second computing device, and
- [1.6] confirm to the first computing device that the encryption key was requested by the second computing device and was sent to the second computing device.

Ex. 1001, 8:40–60 (Microsoft’s reference numbers added). Claims 6 and 11 are also independent. *See id.* at 9:6–24, 10:1–23. Claims 2–5 depend from claim 1, claims 7–10 depend from claim 6, and claims 12–15 depend from claim 11. *See id.* at 8:61–10:35.

Microsoft relies on the declaration of Henry Houh, Ph.D, Ex. 1008. Uniloc does not presently contest Dr. Houh’s qualification to provide expert testimony on the subject matter of his declaration, and we have considered his testimony for the purpose of this decision. Uniloc did not provide a rebuttal expert at this stage of the proceeding.

III. ANALYSIS

Microsoft’s sole ground for seeking *inter partes* review of the ’359 patent is that claims 1–15 would have been obvious over Olkin in view of Kim. *See* Pet. 2. A claim is unpatentable for obviousness under 35 U.S.C. § 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 (2007). We typically consider “whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.” *Id.* at 418 (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)). A sufficient ground for obviousness in a petition must “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) (citing *KSR*, 550 U.S. at 418); *see also* 35 U.S.C. § 322(a)(3) (2018); 37 C.F.R. §§ 42.22(a)(2), 42.104(b)(4) (2019).

The obviousness inquiry requires an analysis of underlying factual considerations 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) any objective indicia of obviousness or non-obviousness (i.e., secondary considerations) that may be in evidence.⁵ *See Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

Based on the evidence and arguments presented in the Petition, and in light of Uniloc’s Preliminary Response, we are unable to conclude that Microsoft has demonstrated a reasonable likelihood of success on its obviousness ground, for the reasons discussed below.

A. LEVEL OF ORDINARY SKILL IN THE ART

The level of ordinary skill in the pertinent art at the time of the invention is one of the factual considerations relevant to obviousness. *See Graham*, 383 U.S. at 17. It is also pertinent to interpreting the patent claims, *see Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005) (en banc). To assess the level of ordinary skill, we construct a hypothetical “person of ordinary skill in the art,” from whose vantage point we assess obviousness and claim interpretation. *See In re Rouffet*, 149 F.3d 1350, 1357

⁵ Because neither party has presented evidence of objective indicia of obviousness or non-obviousness, we do not address this consideration in our decision. *See* Pet. 40 (stating that Microsoft is unaware of any secondary considerations of non-obviousness).

(Fed. Cir. 1998). This legal construct “presumes that all prior art references in the field of the invention are available to this hypothetical skilled artisan.” *Id.* (citing *In re Carlson*, 983 F.2d 1032, 1038 (Fed. Cir. 1993)).

Citing testimony of Dr. Houh, Microsoft argues that a person of ordinary skill in the art “would have a bachelor’s degree in computer science, electrical and/or computer engineering, or equivalent training, and two years of experience in computer networking and information security.” Pet. 9 (citing Ex. 1008 ¶ 43 (Dr. Houh’s testimony to that effect)). For the purpose of its Preliminary Response, Uniloc does not dispute Microsoft’s assertion. *See* Prelim. Resp. 10–11.

We find that Microsoft’s proposed level of ordinary skill is consistent with the teachings of the ’359 patent and the cited prior art. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001) (holding that the prior art itself may provide evidence as to the appropriate level of ordinary skill). Therefore, we adopt Microsoft’s uncontested formulation as the level of ordinary skill for this decision.

B. CLAIM CONSTRUCTION

The Board interprets patent claims using the same claim construction standard that would be used to construe the claims in a civil action under 35 U.S.C. § 282(b). 37 C.F.R. § 42.100(b) (2019). Under this standard, we generally give claim terms their “ordinary and customary meaning . . . as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.” *Id.* The ordinary and customary meaning is the meaning the claim language would have to a person of ordinary skill at the

time of the invention, in the context of the entire patent including the specification. *See Phillips*, 415 F.3d at 1312–13.

Microsoft contends that the claims of the '359 patent “do not require proposed constructions that differ from the claim language in order for the Board to compare the prior art to the claims.” Pet. 9. Likewise, Uniloc “contends that no claim terms require specific construction to resolve the unpatentability issues presented” in the Petition. Prelim. Resp. 10.

In light of the parties’ arguments and evidence, we agree with the parties that it is unnecessary to expressly construe any claim terms for our determination of whether to institute an *inter partes* review. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (“[W]e need only construe 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))). Nevertheless, our interpretation of the '359 patent claims is informed by the disclosure and prosecution history, and we will discuss our interpretation of pertinent claim terms in the context of our analysis in the section below.

A. COMPARISON OF THE CHALLENGED CLAIMS WITH THE PRIOR ART

1. *Overview of Olkin*

Olkin describes a communication system for sending and receiving email messages and other communications via transactions with a “key server.” Pet. 12 (citing Ex. 1003, 21:27–43, 21:57–58); Prelim. Resp. 12 (citing Ex. 1003, 8:44–56).

Olkin's Figure 11, reproduced below, illustrates an example of such a system:

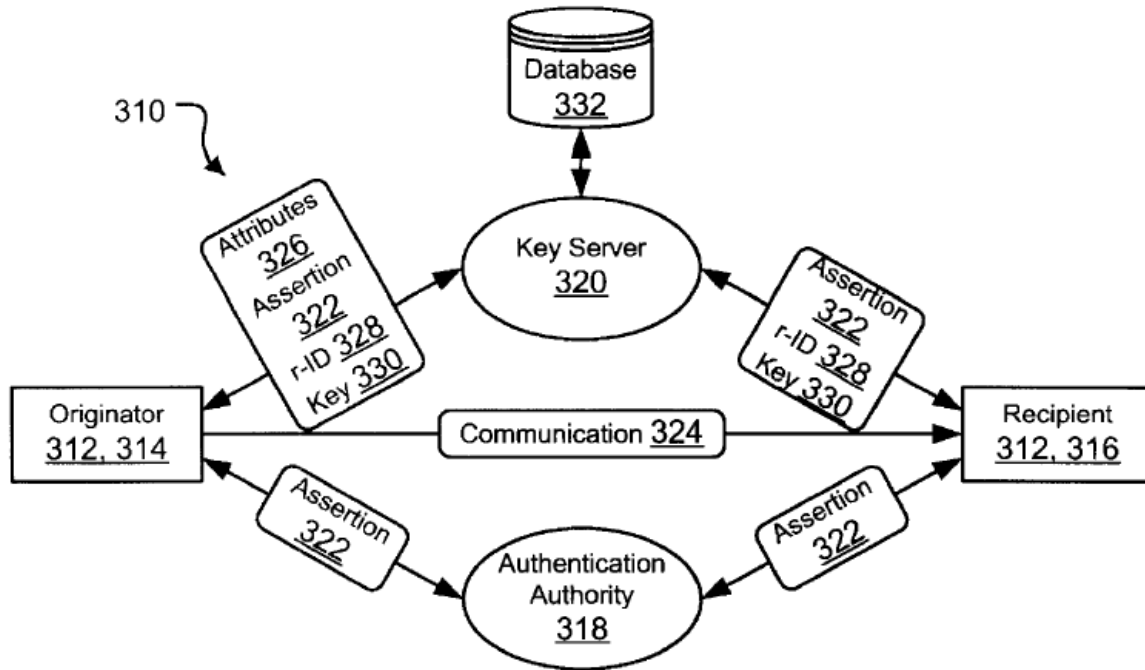


FIG. 11

Figure 11 is a block diagram with four basic components: communication originator 314, communication recipient 316, key server 320, and authentication authority 318. Ex. 1003, 26:38–41. Originator 314 and Recipient 316 will at some point independently authenticate themselves with authentication authority 318, and receive authentication assertion 322, which they will use to authenticate themselves with key server 320. *Id.* at 26:42–55.

Olkin's system uses "conversation keys." Pet. 12. These are symmetric keys that "flow[] from a single source to one or more destinations." Ex. 1003, 21:48–50. When originator 314 wishes to obtain a conversation key in order to send secure messages to one or more recipients including recipient 316, it contacts key server 320 and provides it with

authentication assertion 322 and attributes 326 for intended communication 324. *Id.* at 26:56–60. These attributes 326 may include a list of intended recipients 316 for the communication. *Id.* at 26:60–62. Key server 320 confirms the originator’s authentication assertion 322 and creates “a key 330 suitable to encrypt the communication 324,” which it sends back to originator 314 for use in encrypting the communication. *Id.* at 63–67.

Alternatively to having key server 320 create and send an encryption key to the originator at its request, originator 314 “can instead send the key 330 to the key server 320 and ask it to associate that key 330 with a resource ID 328”; the originator can then use its own key to encrypt future communications within the system. *See id.* at 27:1–3; *see also id.* at 22:37–38 (the key server either “creates the keys . . . or it can receive them from source participants.”).

When recipient 316 receives an encrypted message from originator 314, recipient 316 can ask key server 320 (using its authentication assertion 322 and resource ID 328) for a key for decrypting the message. Ex. 1003, 27:15–21. Key server 320 verifies authentication assertion 322 and also checks that recipient 316 “is an intended one for the communication 324 that the resource ID 328 specifies, using the list of intended recipients 316 that the originator 314 previously provided in the attributes 326.” *Id.* at 27:21–26. Key server 320 then sends the key to recipient 316 for use in decrypting the communication. *Id.* at 27:30–31.

2. *Overview of Kim*

Kim describes a scheme for “identity based encryption (IBE).” Ex. 1004 ¶ 23. The scheme allows “any string to be used as a valid public key.”

Id. ¶ 24. The key may therefore include a string representing an identity, such as an email address, of the intended recipient. *Id.*

In an exemplary embodiment, an intended recipient of a communication transmits “seed information” to an originating device, which may include information about the device’s hardware, as well as user credentials. *Id.* at ¶¶ 28, 31–33. The originating device generates a public encryption key for encrypting its communications, using the predetermined seed information and the user credentials. *Id.* ¶ 31. To decrypt these messages, the recipient device generates and keeps a “secret key based on the seed information and the credential according to the IBE scheme.” *Id.* ¶ 34.

3. *Claim 1*

(a) Microsoft’s Arguments

Microsoft asserts that the combination of Olkin and Kim teaches every limitation of claim 1, and that it would have been obvious to combine the two references in the way recited in claim 1. *See* Pet. 11–29. According to Microsoft, Olkin discloses “conversation keys,” but does not explain how they are generated. Pet 12–13. Therefore, Microsoft argues that a person of ordinary skill in the art would have naturally looked to Kim, which discloses details of generating keys meeting the limitations of claim 1. *Id.* at 13–14.

The preamble (1.1) recites “[a] system for securing an electronic communication.” Ex. 1001, 8:40. This system includes three devices: a “gateway server,” a “first computing device” (the recipient), and a “second computing device (the originator). *See* Ex. 1001, 8:40–53; *see also* Prelim. Resp. 3–4 (explaining that the first computing device is the recipient, and the

second computing device is the originator). As recited in the claim, the gateway server is “configured to” perform a series of steps. Ex. 1001, 8:42. Microsoft identifies these three devices in Olkin’s Figure 11 and supporting text. *See* Pet. 15–16.

Limitations 1.2 and 1.3 recite steps in which the gateway server does the following: (1.2) generates a “device identifier” based on user-configurable and non-user-configurable parameters, and (1.3) receives an “encryption key request” from the second computing device (the originator). *See* Ex. 1001, 8:43–53. Microsoft argues that a combination of Olkin and Kim meets limitation 1.2, and that Olkin alone teaches limitation 1.3. *Id.* at 15–23.⁶

Limitation 1.4 requires that the gateway server be configured to “derive an encryption key from the device identifier for the first computing device.” Ex. 1001, 8:54–55. Microsoft concedes that Olkin does not explicitly disclose deriving an encryption key from a device identifier, but argues that a person of ordinary skill in the art “would understand this limitation to be taught by the combination of Olkin and Kim.” Pet. 24. According to Microsoft, “Kim teaches that an encryption key can be generated using seed information (which includes non-configurable information . . .) plus personal information (configurable).” *Id.* (emphasis omitted). Thus, Microsoft argues that “using the teachings of Kim, a [person of ordinary skill in the art] implementing Olkin would use both configurable

⁶ In its Preliminary Response, Uniloc does not specifically dispute Microsoft’s contentions for the preamble 1.1 and limitations 1.2–1.3. *See* Prelim. Resp. 21–30 (arguing only with respect to limitations 1.4–1.6).

and non-configurable data to generate an encryption key.” *Id.* at 25 (citing Ex. 1008 ¶ 66).

Limitation 1.5 requires that the gateway server be configured to “send the encryption key to the second computing device.” Ex. 1001, 8:56.

Microsoft argues that “Olkin satisfies this limitation” because as shown in Olkin’s Figure 11 (reproduced above), “the generated encryption key is sent back to the originator (the second computing device).” Pet. 26 (quoting Ex. 1003, 26:63–67) (citing Ex. 1008 ¶ 67).

Limitation 1.6 requires that the gateway server be configured to “confirm to the first computing device that the encryption key was requested by the second computing device and was sent to the second computing device.” Ex. 1001, 8:58–60. Microsoft argues that “Olkin in combination with Kim satisfies this limitation.” Pet. 26. According to Microsoft, the recited confirmation step takes place in Olkin’s disclosure when the recipient device obtains a key from the key server. Pet. 27 (quoting Ex. 1003, 27:15–30). Microsoft contends that when the recipient asks for a key to decrypt a message from the originator, “[t]he key server checks that the recipient was intended to receive the message by using the list previously provided by the originator (the second computing device).” *Id.* (citing Ex. 1003, 27:22–26). Thus, according to Microsoft, “by sending the key to the recipient, the key server (gateway server) is confirming that the encryption key was originally requested by and sent to the originator.” *Id.* (citing Ex. 1003, 27:21–30; Ex. 1008 ¶ 69). Microsoft notes that Olkin’s key server performs checks to verify that the communication is authorized, and “[i]f all the checks do not pass, the key server would not send the encrypted key

back to the recipient for decryption.” *Id.* at 28 (citing Ex. 1003, 27:21–30; Ex. 1008 ¶ 71).

(b) Discussion

Among other arguments, Uniloc contends that the combination of Olkin and Kim fails to satisfy the confirmation step recited in limitation 1.6. *See* Prelim. Resp. 25–30. According to Uniloc, Olkin only teaches that key server 320 provides a decryption key to recipient 316, but “[t]here exists no disclosure within the entirety of Olkin that the key server 320 confirms in any manner with the recipient 316 that the key 330 was provided to the originator 314.” *Id.* at 28. Uniloc argues that Microsoft’s argument that confirmation takes place when key server 320 provides the recipient a key “is conclusory in that it attempts to read into the disclosure of Olkin that which was never intended to be taught or suggested by Olkin.” *Id.* at 29. Uniloc also contends that Olkin does not implicitly teach a confirmation step, because “sending the key to the recipient does not implicitly identify any of a myriad of operations that could have possibly been performed by either of the originator and/or the key server.” *Id.*

We agree with Uniloc that Olkin does not explicitly or implicitly disclose that its key server is configured to confirm to the recipient device “that the encryption key was requested by the [originator] and was sent to the [originator].” Ex. 1001, 8:58–60.

First, the mere fact that Olkin’s key server gives a key to the recipient for decrypting a message does not necessarily mean that the key server sent the originator an encryption key at its request. Although, in one embodiment, Olkin’s key server provides a key upon request from an originator, Olkin also teaches that originator 314 “can instead send the key 330 to the key

server 320 and ask it to associate that key 330 with a resource ID 328,” which the originator can then use to encrypt future communications. Ex. 1003, 27:1–3; *see also id.* at 22:37–38 (the key server either “creates the keys . . . or it can receive them from source participants.”). In this latter case, originator 314 need never have requested an encryption key, and key server 320 need never have sent an encryption key back to the originator. Thus, the mere fact that Olkin’s key server performs all checks and successfully provides a key to the recipient for decrypting a message does not necessarily mean that “the encryption key was requested by the second computing device and was sent to the second computing device,” as claim 1 requires. Ex. 1001, 8:58–60.

Second, even if a recipient in Olkin’s system were able to reliably infer, from the key server’s actions in sending it a key, that the key server had sent an encryption key to the message originator at the originator’s request, the specification of the ’359 patent, and its prosecution history, do not support Microsoft’s theory that such an inference may constitute the act of “confirm[ing]” as recited in limitation 1.6. Claim 1 recites “a gateway server configured to” perform the confirmation step. Ex. 1001, 8:42, 58–60. Thus, it is the gateway server—not the recipient—that must be configured to perform the confirmation step in its entirety. The confirmation step must be more than simply an inference that the recipient makes based on its understanding of how the key server typically operates.

The prosecution history of the ’359 patent supports this understanding that the “confirm” step is an independent affirmative action by the gateway server, and more than simply an inference by the recipient. During

prosecution, the inventor added limitation 1.6 to distinguish over a prior art reference. Ex. 1002, 45–46. According to the inventor’s counsel,

a recipient computing device may receive a communication that contains the correct encryption key, but for security purposes the recipient computing device may wish to verify that the sending computing device was originally authorized to receive the encryption key and in fact obtained the encryption key legitimately via the trusted gateway server. *The confirmation step is therefore an independent verification step for authenticating the communication.*

Ex. 1002, 46 (emphasis added).

Finally, Microsoft has not sufficiently explained why a person of ordinary skill in the art would have modified Olkin’s system by adding an independent verification step. Olkin uses “conversation keys,” which are associated with a flow of messages “from a single source to one or more destinations.” Ex. 1003, 21:48–50. In Olkin’s system, the originator sends the messages to members of a recipient list, but the intended recipients on that list need not be authenticated before, or even after, the originator sends the message. *See* Ex. 1003, 9:55–60 (an intended recipient need not be registered with the system when the originator requests the key); *id.* at 10:3–7 (alternatively, the security server “need not be concerned with whether the receivers . . . are registered”). Microsoft has not adequately explained why, in Olkin’s system, where messages may be broadcast to multiple recipients before those recipients are even registered, a person of ordinary skill in the art would have had reason to independently verify to the recipients that the originator asked for, and was sent, an encryption key.

For the above reasons, we determine that Microsoft has not adequately shown that Olkin teaches or suggests limitation 1.6 of claim 1. Microsoft does not point to any passage in Kim that would supply the

missing teaching. *See* Pet. 26–29. Nor do Microsoft’s arguments regarding limitations 1.1–1.5 demonstrate that the combination of Olkin and Kim teaches limitation 1.6. *See id.* at 11–26. Thus, we determine that Microsoft has not demonstrated a reasonable likelihood of prevailing in showing that claim 1 would have been obvious over Olkin in combination with Kim.

4. *Claim 2–15*

Like claim 1, independent claims 6 and 11 both include a “confirmation” step similar to limitation 1.6. *See* Ex. 1001, 9:22–24 (“confirming to the first computing device that the encryption key was requested by the second computing device and was sent to the second computing device”); *see id.* at 10:16–18 (“querying, by the recipient computing device, the gateway server for confirmation that the sending computing device requested the first encryption key”). Microsoft’s argument regarding limitation 1.6 is identical to the argument for the corresponding limitation in claim 6, *see* Pet. 26–29, and substantially the same as the argument for the corresponding limitation in claim 11, *see id.* at 35–37.

The remaining claims 2–5, 7–10, and 12–15 depend from claims 1, 6, or 11, and thus include the “confirmation” step of the base claims. Microsoft’s analysis only addresses the added limitations of each dependent claim, and does not provide further argument or evidence relevant to limitation 1.6 or the corresponding limitations in claims 6 and 11. *See* Pet. 29–32, 38–40.

Thus, for the same reasons given above as to claim 1, we determine that Microsoft has not sufficiently shown that claims 2–15 would have been obvious over Olkin in combination with Kim. *See In re Fine*, 837 F.2d 1071,

1076 (Fed. Cir. 1988) (“Dependent claims are nonobvious under section 103 if the independent claims from which they depend are nonobvious.”)

B. CONCLUSION

After considering the evidence and arguments presented in the Petition and Preliminary Response, we determine that Petitioner has not demonstrated a reasonable likelihood of prevailing in proving that at least one challenged claim of the '359 patent is unpatentable. Therefore, we deny the Petition.

IV. ORDER

In consideration of the foregoing, it is ORDERED that the Petition is *denied*, and no trial is instituted.

IPR2020-00101
Patent 8,495,359 B2

For PETITIONER:

Todd M. Siegel
Andrew M. Mason
Robert F. Scotti
Joseph T. Jakubek
KLARQUIST SPARKMAN, LLP
todd.siegel@klarquist.com
andrew.mason@klarquist.com
robert.scotti@klarquist.com
joseph.jakubek@klarquist.com

For PATENT OWNER:

Ryan Loveless
Brett Mangrum
James Etheridge
Jeffrey Huang
ETHERIDGE LAW GROUP
ryan@etheridgelaw.com
brett@etheridgelaw.com
jim@etheridgelaw.com
jeff@etheridgelaw.com