

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

TELEFONAKTIEBOLAGET LM ERICSSON,
Patent Owner.

IPR2022-00850
Patent 11,039,312 B2

Before NATHAN A. ENGELS, SHARON FENICK, and
STEVEN M. AMUNDSON, *Administrative Patent Judges*.

AMUNDSON, *Administrative Patent Judge*.

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

I. INTRODUCTION

Apple Inc. (“Petitioner”) filed a Petition requesting an *inter partes* review of claims 1–3, 6, 8–12, and 15–18 in U.S. Patent No. 11,039,312 B2 (Exhibit 1001, “the ’312 patent”) under 35 U.S.C. §§ 311–319. Paper 1 (“Pet.”). Telefonaktiebolaget LM Ericsson (“Patent Owner”) filed a Preliminary Response. Paper 6 (“Prelim. Resp.”).

Under 37 C.F.R. § 42.4(a), we have authority to determine whether to institute an *inter partes* review. We may institute an *inter partes* review only if “the information presented in the petition filed under section 311 and any response filed under section 313 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). The “reasonable likelihood” standard is “a higher standard than mere notice pleading” but “lower than the ‘preponderance’ standard to prevail in a final written decision.” *Hulu, LLC v. Sound View Innovations, LLC*, IPR2018-01039, Paper 29 at 13 (PTAB Dec. 20, 2019) (precedential).

After considering the Petition, the Preliminary Response, and the evidence of record, and for the reasons explained below, we determine that Petitioner has not demonstrated a reasonable likelihood that it would prevail in proving the unpatentability of at least one claim challenged in the Petition. Hence, we deny the Petition and do not institute an *inter partes* review.

II. BACKGROUND

A. *Real Parties in Interest*

Petitioner identifies itself as the real party in interest. Pet. 76. Patent Owner identifies the following real parties in interest: Telefonaktiebolaget

LM Ericsson and Ericsson Inc. Paper 4, 2. The parties do not raise any issue about real parties in interest.

B. Related Matters

Petitioner states that it is “not aware of any disclaimers, reexamination certificates or petitions” for *inter partes* review of the ’312 patent. Pet. 76. Petitioner also states that the ’312 patent is “among three patents raised in” the following declaratory-judgment action: *Apple Inc. v. Telefonaktiebolaget LM Ericsson et al.*, No. 2:21-cv-460 (E.D. Tex. filed Dec. 17, 2021) (the “Texas case”). *Id.* at 73–74; *see* Ex. 2001 (Complaint filed Dec. 17, 2021).

Patent Owner states that “[t]here are no judicial or administrative matters that would affect, or be affected by, a decision in this proceeding.” Paper 4, 2. Patent Owner also states that Petitioner filed “a declaratory judgment action on December 17, 2021, in the Eastern District of Texas, captioned *Apple Inc. v. Telefonaktiebolaget LM Ericsson and Ericsson Inc.*, Case No. 2:21-cv-460, assigned to Judge Rodney Gilstrap.” Prelim. Resp. 5; *see id.* at 1.

C. The ’312 Patent (Exhibit 1001)

The ’312 patent, titled “Handling of Multiple Authentication Procedures in 5G,” issued on June 15, 2021, from an application filed on January 20, 2021. Ex. 1001, codes (22), (45), (54). The patent claims priority to the following applications: (1) International Patent Application No. PCT/EP2020/060968, filed on April 20, 2020; and (2) U.S. Provisional Patent Application No. 62/840,021, filed on April 29, 2019. *Id.* at 1:6–12, codes (60), (63). The patent states that the disclosure relates “generally to communications” and “more particularly to communication methods and

related devices and nodes supporting communications.” *Id.* at 1:17–19; *see id.* at code (57).

The ’312 patent explains that the 3rd Generation Partnership Project (3GPP) security standardization working group SA3 “has finalized the security specification for the Release 15 of the 5G System in [Technical Specification] TS 33.501.” Ex. 1001, 1:23–25. To protect communications between a user equipment (UE) and a core network (CN), TS 33.501 provides security protocols that “rely on multiple different security keys” organized in a hierarchy. *See id.* at 1:42–56. The hierarchy’s top level includes “the long-term key part of the authentication credential” that resides (1) “in the SIM card on the UE side” and (2) “in the unified data management/authentication credential repository and processing function (UDM/ARPF) on the Home Public Land Mobile Network (PLMN) side.” *Id.* at 1:56–61.

The ’312 patent also explains that a successful primary authentication between a UE and an Authentication Server Function (AUSF) “may lead to the establishment of the K_{AUSF} key” that “is not intended to leave the Home PLMN and is used for new features introduced in the 5G System.” Ex. 1001, 1:62–66. The new features include the following:

- (1) “the Steering of Roaming (SoR) security mechanism described in clause 6.14 of TS 33.501” and used for “the delivery of information about the list of preferred PLMNs from the UDM in the Home PLMN to the UE”; and
- (2) “the UE parameters update (UPU) via UDM control procedure security mechanism specified in clause 6.15 of TS 33.501” and used for “the delivery of UE parameter updates from the UDM in the Home PLMN to the UE.”

Id. at 4:28–32, 4:39–41.

The '312 patent identifies a problem when a UE “maintain[s] and use[s] in parallel two different 5G security contexts” associated with a first Visited PLMN and a second Visited PLMN that resulted from independent authentication procedures with the Home PLMN. *See* Ex. 1001, 4:47–5:18. In particular, the independent authentication procedures with the Home PLMN “may lead to two different K_{AUSF} keys in the HPLMN side and in the UE side.” *Id.* at 5:3–5. Hence, it “may not be clear which of the two different K_{AUSF} keys to use for services such as the SoR or the UDM parameter updates.” *Id.* at 5:5–7. Further, if “the UE and the AUSF K_{AUSF} keys are not synchronized,” then “there is a risk that the UE and the AUSF may use different K_{AUSF} keys for the SoR and SoR-like procedures leading to an integrity check failure.” *Id.* at 5:7–10.

The '312 patent addresses this problem by having the AUSF and the UE each determine whether the first security key or the second security key is the latest security key. *See* Ex. 1001, 8:38–9:20, 10:59–11:42, Figs. 7–10. The AUSF uses the latest security key to protect a message associated with a message protection request. *Id.* at 9:41–43, Fig. 7. The UE uses the latest security key to determine the contents of a protected message received from the Home PLMN. *Id.* at 11:63–65, Fig. 8. “The protected message may be a UDM parameter update message, a steering of roaming message, etc.” *Id.* at 11:66–67.

The '312 patent's Figure 3 (reproduced below) depicts a flowchart for managing multiple security keys delivered from a Home PLMN to a UE:

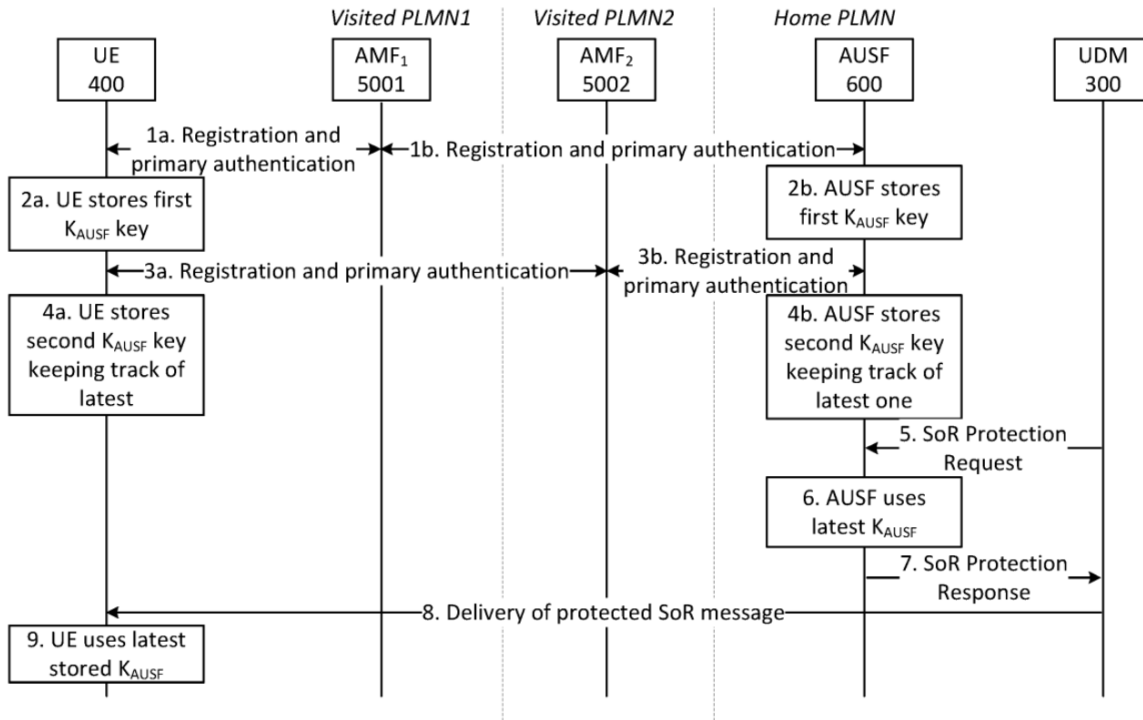


Figure 3

Figure 3 illustrates operations involving UE 400, AMF (Access Management Function) 5001 in a first Visited PLMN1, AMF 5002 in a second Visited PLMN2, AUSF 600 in the Home PLMN, and UDM (Unified Data Management) 300 in the Home PLMN. See Ex. 1001, 3:23–26, 7:7–8:37, Fig. 3.

In operation 1a, UE 400 “registers over an access type (e.g., 3GPP or non-3GPP) to” AMF 5001 in the first Visited PLMN1. Ex. 1001, 7:16–18, Fig. 3. In operation 1b, a primary authentication occurs, and AUSF 600 and UE 400 establish a first K_{AUSF} key. *Id.* at 7:18–22, Fig. 3.

In operation 2a, UE 400 stores the first K_{AUSF} key. Ex. 1001, 7:24–25, Fig. 3. In operation 2b, AUSF 600 stores the first K_{AUSF} key. *Id.* at 7:24–25, Fig. 3.

In operation 3a, UE 400 “registers over an access type (e.g., non-3GPP or 3GPP) to” AMF 5002 in the second Visited PLMN2. Ex. 1001, 7:26–28, Fig. 3. In operation 3b, a primary authentication occurs, and AUSF 600 and UE 400 establish a second K_{AUSF} key. *Id.* at 7:28–31, Fig. 3.

In operation 4a, UE 400 stores the second K_{AUSF} key and “keeps track of the latest K_{AUSF} key.” Ex. 1001, 7:34–36, Fig. 3. In operation 4b, AUSF 600 stores the second K_{AUSF} key and “keeps track of the latest K_{AUSF} key.” *Id.* at 7:34–36, Fig. 3.

In operation 5, UDM 300 in the Home PLMN “may send a message protection request (e.g., a SoR protection request or a UPU protection request, etc.)” to AUSF 600 in the Home PLMN. Ex. 1001, 7:38–43, Fig. 3. In operation 6, AUSF 600 “determines the latest K_{AUSF} key and uses the latest K_{AUSF} key” to “protect the message associated with the message protection request.” *Id.* at 7:43–46, Fig. 3. In operation 7, AUSF 600 “sends a protection message response” to UDM 300. *Id.* at 7:46–47, Fig. 3. In operation 8, UDM 300 “transmits the protection message response (e.g., a protected SoR message, a protected UPU message, etc.)” to UE 400. *Id.* at 7:48–50, Fig. 3. In operation 9, UE 400 “uses the latest stored K_{AUSF} key to determine the contents of the protection message response.” *Id.* at 7:50–53, Fig. 3.

D. The Challenged Claims

Petitioner challenges the following claims:

- independent method claim 1 for an Authentication Server Function;
- claims 2, 3, 6, 8, and 9 that depend directly or indirectly from claim 1;

- independent apparatus claim 10 for an Authentication Server Function;
- claims 11 and 12 that depend directly from claim 10;
- independent method claim 15 for an electronic device, such as a UE; and
- claims 16–18 that depend directly or indirectly from claim 15.

Pet. 5–6, 42–73.

Claims 1 and 15 exemplify the challenged claims and read as follows (with numbers and letters added for reference purposes):¹

1. [1pre] A method by an Authentication Server Function, AUSF, of a home public land mobile network, PLMN, configured to communicate through an interface with electronic devices, the method comprising:

[1a] receiving a first authentication request from a first PLMN that is authenticating an electronic device;

[1b] obtaining a first security key used for integrity protection of messages delivered from the home PLMN to the electronic device, wherein the first security key is obtained in response to successful authentication based on the first authentication request;

[1c] receiving a second authentication request from a second PLMN that is authenticating the electronic device;

[1d] obtaining a second security key used for integrity protection of the messages delivered from the home PLMN to the electronic device, wherein the second security key is obtained in response to successful authentication based on the second authentication request;

[1e] receiving a message protection request;

¹ We use the same numbers and letters that the parties use to identify the claim language.

[1f] determining which of the first security key and the second security key is a latest security key; and

[1g] using the latest security key to protect a message associated with the message protection request.

15. [15pre] A method in an electronic device configured to communicate through a wireless air interface with a home public land mobile network, PLMN, and visiting PLMNs, the method comprising:

[15a] transmitting a first authentication request to a first PLMN to authenticate the electronic device;

[15b] generating a first security key used for integrity protection of messages delivered from the home PLMN to the electronic device upon successful authentication based on the first authentication request;

[15c] transmitting a second authentication request to a second PLMN to authenticate the electronic device;

[15d] generating a second security key used for integrity protection of the messages delivered from the home PLMN to the electronic device upon successful authentication based on the second authentication request;

[15e] receiving a protected message from the home PLMN;

[15f] determining which of the first security key and the second security key is a latest security key; and

[15g] using the latest security key to determine contents of a message received from the home PLMN.

Ex. 1001, 38:17–39, 40:58–41:11.

E. The Asserted References

For its challenges, Petitioner relies on the following references:

Name	Reference	Exhibit
Tiwari	WO 2020/208996 A1, published October 15, 2020 (based on an application filed March 12, 2020, and claiming priority to an application filed April 8, 2019)	1004
Werner	US 2012/0310882 A1, published December 6, 2012 (based on an application filed June 1, 2012)	1007
Wang	US 2010/0064344 A1, published March 11, 2010 (based on an application filed May 26, 2006)	1011
S3-172482	3GPP TSG SA WG3 (Security) Meeting #88Bis, S3-172482, titled “Discussion on Protection of Network Steering Information” (October 2017)	1014

Pet. 5–6. Petitioner asserts that Werner, Wang, and S3-172482 qualify as prior art under § 102(a)(1) and that Tiwari qualifies as prior art under § 102(a)(2). *Id.* at 6; *see* 35 U.S.C. § 102(a)(1)–(2).

At this stage of the proceeding, Patent Owner does not dispute that each reference qualifies as prior art. *See, e.g.*, Prelim. Resp. 23–40.

F. The Asserted Challenges to Patentability

Petitioner asserts the following challenges to patentability:

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1, 9, 10, 15, 16	102/103	Tiwari
1–3, 9–12, 15, 17, 18	103	Tiwari, Werner
6, 8	103	Tiwari, Wang
6, 8	103	Tiwari, Werner, Wang
15, 16	103	Tiwari, S3-172482
15–18	103	Tiwari, Werner, S3-172482

Pet. 5–6, 42–73.

G. Testimonial Evidence

To support its challenges, Petitioner relies on the declaration of Narayan B. Mandayam, Ph.D. (Exhibit 1003, “Mandayam Decl.”). Dr. Mandayam states, “I have been retained by counsel for” Petitioner as “an expert witness to provide assistance regarding” the ’312 patent. Ex. 1003 ¶ 1. Dr. Mandayam also states, “I received a bachelor degree (with Honors) in 1989 from the Indian Institute of Technology, Kharagpur, and M.S. and Ph.D. degrees in 1991 and 1994 from Rice University, Houston, TX, all in electrical engineering.” *Id.* ¶ 7.

Petitioner also relies on the declaration of Friedhelm Rodermund (Exhibit 1015, “Rodermund Decl.”). Mr. Rodermund states, “I have been retained in this matter by” Petitioner “to provide testimony regarding 3GPP’s standard business practices for record keeping and publishing technical specifications, change request proposals, reports, and other documents developed during the course of standards activities carried out by the 3rd Generation Partnership Project (‘3GPP’) and the European Telecommunications Standards Institute (‘ETSI’).” Ex. 1015 ¶ 1. Mr. Rodermund also states, “As an ETSI Project Manager and Secretary, from June 1998 to December 2004, I have personal knowledge of 3GPP’s standard business and records keeping practices,” and “I continued following 3GPP’s work ever since.” *Id.* ¶ 3.

III. DISCRETIONARY DENIAL

Patent Owner argues that we should exercise our discretion under § 314(a) to deny institution because “each *Fintiv* factor weighs in favor of denying institution” in view of the Texas case. *See* Prelim. Resp. 1–3, 5–21;

35 U.S.C. § 314(a); *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020) (precedential).

For the reasons explained below, we determine that Petitioner has not demonstrated a reasonable likelihood that it would prevail in proving the unpatentability of at least one claim challenged in the Petition. *See infra* §§ IV.E–IV.G. Hence, we do not consider discretionary denial under § 314(a).

IV. PATENTABILITY ANALYSIS

A. *Legal Principles: Anticipation*

“[T]o demonstrate anticipation, the proponent must show ‘that the four corners of a single, prior art document describe every element of the claimed invention.’” *Net MoneyIN, Inc. v. VeriSign, Inc.*, 545 F.3d 1359, 1369 (Fed. Cir. 2008) (quoting *Xerox Corp. v. 3Com Corp.*, 458 F.3d 1310, 1322 (Fed. Cir. 2006)). The prior-art document “must not only disclose all elements of the claim within the four corners of the document, but must also disclose those elements ‘arranged as in the claim.’” *Id.* (quoting *Connell v. Sears, Roebuck & Co.*, 722 F.2d 1542, 1548 (Fed. Cir. 1983)). Hence, a patent challenger cannot rely on portions from different, unrelated embodiments in a prior-art document to demonstrate anticipation. *See id.* at 1369, 1371.

We analyze the anticipation issues according to these principles.

B. *Legal Principles: Obviousness*

A patent may not be obtained “if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed

invention pertains.” 35 U.S.C. § 103. An obviousness analysis involves underlying factual inquiries including (1) the scope and content of the prior art; (2) differences between the claimed invention and the prior art; (3) the level of ordinary skill in the art; and (4) where in evidence, objective indicia of nonobviousness, such as commercial success, long-felt but unsolved needs, and failure of others.² *Graham v. John Deere Co.*, 383 U.S. 1, 17–18, 35–36 (1966); *Apple Inc. v. Samsung Elecs. Co.*, 839 F.3d 1034, 1047–48 (Fed. Cir. 2016) (en banc). When evaluating a combination of references, an obviousness analysis should address “whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007).

We analyze the obviousness issues according to these principles.

C. Level of Ordinary Skill in the Art

Factors pertinent to determining the level of ordinary skill in the art include (1) the educational level of the inventor; (2) the type of problems encountered in the art; (3) prior-art solutions to those problems; (4) the rapidity with which innovations are made; (5) the sophistication of the technology; and (6) the educational level of workers active in the field. *Envtl. Designs, Ltd. v. Union Oil Co.*, 713 F.2d 693, 696–97 (Fed. Cir. 1983). Not all factors may exist in every case, and one or more of these or other factors may predominate in a particular case. *Id.* These factors are not exhaustive, but merely a guide to determining the level of ordinary skill in the art. *Daiichi Sankyo Co. v. Apotex, Inc.*, 501 F.3d 1254, 1256 (Fed. Cir.

² The record does not include evidence or argument regarding objective indicia of nonobviousness.

2007). Moreover, the prior art itself may reflect an appropriate skill level. *Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001).

Petitioner asserts that a person of ordinary skill in the art at the time of the alleged invention “would have had at least a Bachelor’s degree in an academic area emphasizing electrical engineering or a similar discipline, and at least two years of experience in the field working with, teaching, or researching wireless communication networks.” Pet. 18. Petitioner also asserts that “[s]uperior education could compensate for a deficiency in work experience, and *vice-versa*.” *Id.* Dr. Mandayam’s testimony supports Petitioner’s assertions. See Ex. 1003 ¶¶ 17–18.

Patent Owner does not address the level of ordinary skill in the art. See, e.g., Prelim. Resp. 1–4, 23–40.

Based on the current record and for purposes of analysis, we accept Petitioner’s description of an ordinarily skilled artisan as consistent with the ’312 patent and the asserted prior art.

D. Claim Construction

We construe claim terms “using the same claim construction standard” that district courts use to construe claim terms in civil actions under 35 U.S.C. § 282(b). See 37 C.F.R. § 42.100(b) (2022). Under that standard, claim terms “are given their ordinary and customary meaning, which is the meaning the term would have to a person of ordinary skill in the art at the time of the invention.” *Power Integrations, Inc. v. Fairchild Semiconductor Int’l, Inc.*, 904 F.3d 965, 971 (Fed. Cir. 2018) (citing *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005) (en banc)). The meaning of claim terms may be determined by “look[ing] principally to the intrinsic evidence of record, examining the claim language itself, the written

description, and the prosecution history, if in evidence.” *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 469 F.3d 1005, 1014 (Fed. Cir. 2006) (citing *Phillips*, 415 F.3d at 1312–17).

Petitioner contends that “no formal claim constructions are necessary.” Pet. 18.

Patent Owner contends that claim construction “is not necessary for the Board to construe claim terms to deny institution.” Prelim. Resp. 3–4.

Based on the current record, we determine that no claim term requires an explicit construction to decide whether Petitioner satisfies the “reasonable likelihood” standard for instituting trial. “[O]nly those terms need be construed that are in controversy, and only to the extent necessary to resolve the controversy.” *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999); see *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017).

*E. Alleged Anticipation by or Obviousness
over Tiwari: Claims 1, 9, 10, 15, and 16*

Petitioner contends that claims 1, 9, 10, 15, and 16 are unpatentable under § 102 as anticipated by Tiwari or under § 103 as obvious over Tiwari. See Pet. 5, 42–49, 55–70. Below, we provide an overview of Tiwari, and then we consider patentability issues raised by the parties. For the reasons explained below, Petitioner does not establish sufficiently for purposes of institution that Tiwari anticipates or renders obvious the subject matter of claims 1, 9, 10, 15, and 16.

1. OVERVIEW OF TIWARI (EXHIBIT 1004)

Tiwari is a WIPO patent application publication titled “Procedure to Provide Integrity Protection to a UE Parameter During UE Configuration

Update Procedure,” filed on March 12, 2020, and published on October 15, 2020. Ex. 1004, codes (22), (43), (54). Tiwari claims priority to a patent application filed in India on April 8, 2019. *Id.* at code (30).

Tiwari describes a problem when “a UE is registered to two different” Public Land Mobile Networks (PLMNs) that “are not equivalent PLMNs via a 3GPP access and non-3GPP access” and “the UE has two 5G security contexts,” e.g., security keys, “at the various network nodes.” Ex. 1004 ¶ 5; *see id.* ¶¶ 2–3. In that conventional scenario, the Authentication Server Function (AUSF) “has one K_{AUSF} ” (security key) after the latest authentication, namely “the K_{AUSF} resulting from the latest authentication,” because “the AUSF would overwrite the K_{AUSF} in storage” during the latest authentication. *Id.* ¶¶ 5, 24. If the Unified Data Management (UDM) “decides to send steering information to the UE and sends a message containing steering information” and requesting the AUSF “to provide integrity protection to the steering information,” the AUSF “calculates the [Medium Access Control] MAC-I for integrity protection of the message using the K_{AUSF} resulting from the latest authentication.” *Id.* ¶ 5. But because the AUSF has one K_{AUSF} and the UE has two, i.e., one K_{AUSF} for each of the two different PLMNs, “it is unclear to the UE which K_{AUSF} the AUSF has used for the calculation of the MAC-I for integrity protection of the steering of roaming message.” *Id.*

Tiwari addresses the AUSF one-key problem by having (1) the AUSF and the UE each store a first K_{AUSF} and a first PLMN ID during a first authentication procedure when the UE registers to a first visited PLMN and (2) the AUSF and the UE each store a second K_{AUSF} and a second PLMN ID during a second authentication procedure when the UE registers to a second

visited PLMN. Ex. 1004 ¶¶ 22–24, 34. In contrast to the prior art, the AUSF does not overwrite the K_{AUSF} in storage during the second authentication procedure. *Id.* ¶ 24. Thus, the AUSF and the UE each store “two tuples of K_{AUSF} and PLMN IDs.” *Id.* ¶¶ 24, 34.

Tiwari’s Figure 1 (reproduced below) depicts the steps in a procedure that addresses the AUSF one-key problem:

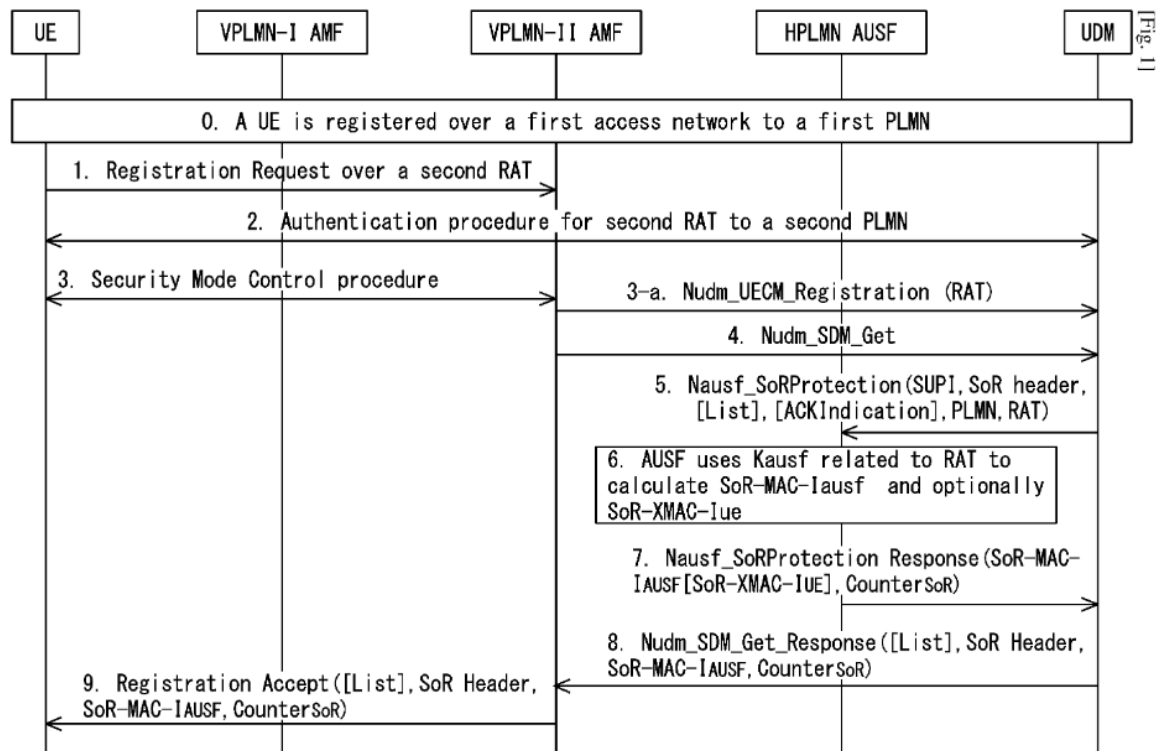


Fig. 1

Figure 1 illustrates operations involving a UE, an AMF in a first visited PLMN (VPLMN-I), an AMF in a second visited PLMN (VPLMN-II), an AUSF in the home PLMN (HPLMN), and a UDM. Ex. 1004 ¶¶ 12, 21–33.

Referencing Figure 1, Tiwari explains that when the UDM decides to send steering information to the UE, the UDM sends a message containing certain information, including a specified PLMN ID, to the AUSF. Ex. 1004 ¶ 27, Fig. 1. After receiving the message from the UDM, the AUSF retrieves the K_{AUSF} corresponding to the PLMN ID specified by the UDM.

Id. ¶ 28. After retrieving the K_{AUSF} corresponding to the specified PLMN ID, the AUSF uses the retrieved K_{AUSF} to apply integrity protection to a message the AUSF sends to the UDM. *Id.* ¶¶ 28–29, Fig. 1.

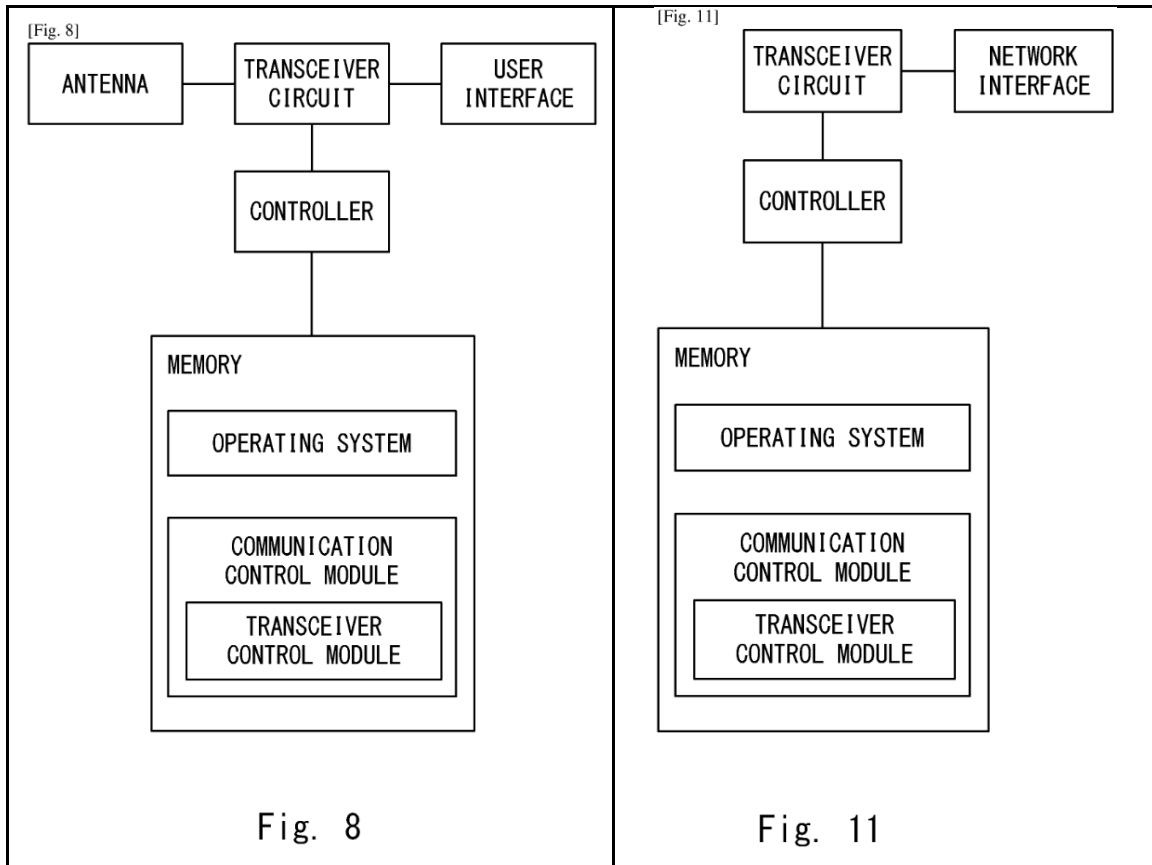
Then, the UDM sends a protected message to the AMF of the PLMN corresponding to the PLMN ID specified by the UDM. Ex. 1004 ¶ 30, Fig. 1. After receiving the protected message from the UDM, the AMF of the PLMN corresponding to the specified PLMN ID sends a “Registration Accept” message to the UE. *Id.* ¶ 31, Fig. 1. After receiving the “Registration Accept” message, the UE verifies the PLMN used to send the message and retrieves the K_{AUSF} corresponding to the PLMN ID. *Id.* ¶ 32, Fig. 1. After retrieving the K_{AUSF} corresponding to the PLMN ID, the UE uses the retrieved K_{AUSF} to verify the integrity protection applied to the message. *Id.* ¶ 32. If correct, “the UE may return a registration acknowledgement message to the UDM.” *Id.*

Tiwari explains that when the UDM decides to notify the UE of changes in steering information or perform the UE parameters update (UPU) procedure, the UDM may select “a PLMN from the first PLMN and the second PLMN when the first PLMN and second PLMN are different and are not equivalent PLMNs.” Ex. 1004 ¶¶ 35, 44. The UDM selection criteria for a PLMN include the following:

- (1) 5G access type, e.g., “3GPP access is preferred over non-3GPP access”;
- (2) PLMN congestion, e.g., use “the PLMN which is least congested or is not congested”; and
- (3) the “PLMN that the UE latest authenticated to,” i.e., because “some UEs may not support the feature of storing multiple K_{AUSFS} .”

Id. ¶¶ 35, 44.

Tiwari's Figures 8 and 11 (reproduced below) depict block diagrams of the main components of a UE and an AUSF, respectively:



Above on the left, Figure 8 illustrates a UE including an antenna, a transceiver circuit, a user interface, a controller, and a memory. Ex. 1005 ¶¶ 12, 114, Fig. 8. Above on the right, Figure 11 illustrates an AUSF including a transceiver circuit, a network interface, a controller, and a memory. *Id.* ¶¶ 12, 117, Fig. 11.

2. INDEPENDENT CLAIM 1

(a) Preamble [1pre] and Limitations [1a], [1b], [1c], [1d], and [1e]

Petitioner provides an analysis supported by Dr. Mandayam's testimony about how Tiwari discloses claim 1's preamble and limitations [1a], [1b], [1c], [1d], and [1e]. See Pet. 42–47; Ex. 1003 ¶¶ 87–93.

At this stage of the proceeding, Patent Owner does not dispute that Tiwari discloses claim 1's preamble and limitations [1a], [1b], [1c], [1d], and [1e]. *See, e.g.*, Prelim. Resp. 3, 25–28. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015).

We need not decide whether Petitioner establishes sufficiently for purposes of institution that Tiwari discloses claim 1's preamble and limitations [1a], [1b], [1c], [1d], and [1e] because, as explained below, Petitioner does not establish sufficiently for purposes of institution that Tiwari discloses limitations [1f] and [1g]. *See infra* §§ IV.E.2(b)–(c).

(b) Limitation [1f]

Claim 1 recites “determining which of the first security key and the second security key is a latest security key.” Ex. 1001, 38:36–37.

Petitioner contends that Tiwari discloses this limitation because:

- (1) “Tiwari teaches that the AUSF stores two security keys from two separate authentications”; and
- (2) “Tiwari additionally teaches” that “the UE has two 5G security contexts (e.g[sic] Security Keys) at the various network nodes.”

Pet. 47 (alteration by Petitioner) (quoting Ex. 1004 ¶ 7) (citing Ex. 1003 ¶ 94; Ex. 1004 ¶¶ 5, 24). Petitioner also contends that “it is well-known” from Tiwari's teachings “for the AUSF to use the security key from the latest authentication for integrity protection of an incoming message.” *Id.* at 47–48 (citing Ex. 1004 ¶ 5).

Further, Petitioner asserts that it “would have been obvious to” an ordinarily skilled artisan to “use the key from the latest authentication when more than one security [key] is stored, and in order for the AUSF to use the

security key from the latest authentication, it must determine whether the first security key or the second security key is the latest.” Pet. 48 (citing Ex. 1003 ¶ 94).

Patent Owner disputes that Tiwari discloses limitation [1f]. See Prelim. Resp. 3, 25–28. Specifically, Patent Owner asserts that Tiwari “does not determine which key is the latest security key” but instead “stores each key with a network ID so that the integrity of a message is checked using the key associated with a particular network’s identity.” *Id.* at 25 (citing Ex. 1004 ¶¶ 24, 32). Patent Owner asserts that Tiwari describes a problem with an AUSF keeping only the latest key when “the UE is registered to different PLMNs, because ‘it is unclear to the UE which K_{AUSF} the AUSF has used for the calculation of the [Medium Access Control] MAC-I for integrity protection of the steering of roaming message.’” *Id.* at 25 (alteration by Patent Owner) (quoting Ex. 1004 ¶ 5). Patent Owner further asserts that the AUSF one-key problem arises because a conventional AUSF “has one K_{AUSF} , namely the K_{AUSF} resulting from the latest authentication,” since “the AUSF [] overwrite[s] the K_{AUSF} in storage during [a second] authentication procedure.” *Id.* (alterations by Patent Owner) (emphases omitted) (quoting Ex. 1004 ¶¶ 5, 24); see *id.* at 26–27, 36.

Patent Owner asserts that Tiwari teaches the following steps to resolve the AUSF one-key problem:

- (1) the AUSF “store[s] a second K_{AUSF} in addition to the first one together with the PLMN ID of the access network”;
- (2) the UE associates each key with a network ID (PLMN ID) by storing “two tuples of K_{AUSF} and PLMN IDs”; and
- (3) when the UE receives a message, it “retrieves the K_{AUSF} associated with the . . . PLMN identity from storage and

selects this key to be used for verifying the integrity protection applied by the AUSF.”

Prelim. Resp. 25–26 (alterations by Patent Owner) (emphases omitted)
(quoting Ex. 1004 ¶¶ 24, 32)

Additionally, Patent Owner contends that Petitioner does not address “this ready-made solution” to the AUSF one-key problem but instead “relies on its expert’s testimony to circularly argue that ‘for the AUSF to use the security key from the latest authentication,’ ‘it would have been obvious to . . . use the key from the latest authentication when more than one security [key] is stored.’” Prelim. Resp. 27 (quoting Pet. 48).

Further, Patent Owner asserts that Petitioner’s “attempt to analogize Tiwari to the claims makes little sense” because Petitioner points to (1) the prior-art AUSF one-key problem “where only one key exists at a time due to overwriting” by the AUSF and (2) Tiwari’s solution to that problem “using tuples of a key and a network ID, not determining which key is the latest key.” Prelim. Resp. 28 (citing Pet. 47–48). Patent Owner also asserts that in both the prior-art problem and Tiwari’s solution “there is no determination of whether ‘the first security key’ or ‘the second security key’ is the ‘latest security key,’ as claimed.” *Id.*

Based on the current record, Petitioner does not establish sufficiently for purposes of institution that Tiwari discloses limitation [1f]. *See* Pet. 47–48; Prelim. Resp. 23–28; Ex. 1003 ¶ 94. As Patent Owner asserts, Tiwari “does not determine which key is the latest security key” but instead “stores each key with a network ID so that the integrity of a message is checked using the key associated with a particular network’s identity.” *See* Prelim. Resp. 25; Ex. 1004 ¶¶ 21–35, 44, Fig. 1.

In particular, Tiwari addresses the AUSF one-key problem by having (1) the AUSF and the UE each store a first K_{AUSF} and a first PLMN ID during a first authentication procedure when the UE registers to a first visited PLMN and (2) the AUSF and the UE each store a second K_{AUSF} and a second PLMN ID during a second authentication procedure when the UE registers to a second visited PLMN. Ex. 1004 ¶¶ 22–24, 34. Thus, the AUSF and the UE each store “two tuples of K_{AUSF} and PLMN IDs.” *Id.* ¶¶ 24, 34.

Tiwari explains that when the UDM decides to send steering information to the UE, the UDM sends a message containing certain information, including a specified PLMN ID, to the AUSF. Ex. 1004 ¶ 27, Fig. 1. After receiving the message from the UDM, the AUSF retrieves the K_{AUSF} corresponding to the PLMN ID specified by the UDM. *Id.* ¶ 28. The AUSF does not “determin[e] which of the first security key and the second security key is a latest security key.” *See id.* ¶¶ 21–33, Fig. 1.

Further, after a UE receives a “Registration Accept” message, the UE verifies the PLMN used to send the message and retrieves the K_{AUSF} corresponding to the PLMN ID. Ex. 1004 ¶ 32, Fig. 1. The UE does not “determin[e] which of the first security key and the second security key is a latest security key.” *See id.* ¶¶ 21–33, Fig. 1.

Tiwari discloses that the UDM may select a PLMN for message transmission based on the “PLMN that the UE latest authenticated to.” Ex. 1004 ¶¶ 35, 44. But Petitioner does not contend that an ordinarily skilled artisan would have been motivated to modify Tiwari’s AUSF or UE to employ that selection criterion. *See* Pet. 47–48; Ex. 1003 ¶ 94.

Petitioner's contention that "it is well-known for the AUSF to use the security key from the latest authentication for integrity protection of an incoming message" mischaracterizes Tiwari's disclosure. *See* Pet. 47–48 (citing Ex. 1004 ¶ 5); Ex. 1004 ¶¶ 5, 24. Specifically, Tiwari discloses that a conventional AUSF, i.e., one not operating according to Tiwari's asserted improvement, "has one K_{AUSF} " after the latest authentication, namely "the K_{AUSF} resulting from the latest authentication," because "the AUSF would overwrite the K_{AUSF} in storage" during the latest authentication. Ex. 1004 ¶¶ 5, 24. Thus, a conventional AUSF uses "the K_{AUSF} resulting from the latest authentication" because the AUSF has no other option, not because the AUSF "determin[es] which of the first security key and the second security key is a latest security key" according to limitation [1f].

(c) Limitation [1g]

Claim 1 recites "using the latest security key to protect a message associated with the message protection request." Ex. 1001, 38:38–39.

Petitioner contends that Tiwari discloses this limitation because "Tiwari teaches that it was well-known for the AUSF to use the security key resulting from the latest authentication for integrity protection of an incoming message." Pet. 48–49 (citing Ex. 1003 ¶ 96; Ex. 1004 ¶ 5).

Patent Owner disputes that Tiwari discloses limitation [1g] for the reasons Patent Owner disputes that Tiwari discloses limitation [1f]. *See* Prelim. Resp. 3, 25–28.

Based on the current record, Petitioner does not establish sufficiently for purposes of institution that Tiwari discloses limitation [1g]. *See* Pet. 48–49; Prelim. Resp. 23–28; Ex. 1003 ¶ 96. Because Tiwari does not disclose "determining which of the first security key and the second security

key is a latest security key” according to limitation [1f], Tiwari does not disclose using the result of such a determination according to limitation [1g]. See Ex. 1004 ¶¶ 21–35, 44, Fig. 1. Rather, Tiwari discloses using the K_{AUSF} associated with the appropriate PLMN identity for integrity protection, or the sole stored K_{AUSF} in the case of a UE that does not support storing multiple K_{AUSFs} . *Id.*

(d) Conclusion Concerning Claim 1

Because Petitioner does not establish sufficiently for purposes of institution that Tiwari discloses limitations [1f] and [1g], Petitioner does not establish sufficiently for purposes of institution that Tiwari anticipates or renders obvious claim 1’s subject matter. See Pet. 47–49; Ex. 1003 ¶¶ 94, 96; *supra* §§ IV.E.2(b)–(c). Hence, Petitioner does not demonstrate a reasonable likelihood of prevailing in proving claim 1 unpatentable under § 102 as anticipated by Tiwari or under § 103 as obvious over Tiwari.

3. INDEPENDENT CLAIMS 10 AND 15

Claims 10 and 15 include limitations identical or similar to limitations [1f] and [1g]. Compare Ex. 1001, 38:36–39, with *id.* at 40:5–8, and *id.* at 41:8–11; see Prelim. Resp. 3 (characterizing the limitations as similar).

Because Petitioner does not establish sufficiently for purposes of institution that Tiwari discloses limitations [1f] and [1g], Petitioner does not establish sufficiently for purposes of institution that Tiwari discloses the identical or similar limitations in claims 10 and 15 or that Tiwari anticipates or renders obvious the subject matter of claims 10 and 15. See Pet. 47–49; Ex. 1003 ¶¶ 94, 96; *supra* §§ IV.E.2(b)–(d). Hence, Petitioner does not demonstrate a reasonable likelihood of prevailing in proving claims 10

and 15 unpatentable under § 102 as anticipated by Tiwari or under § 103 as obvious over Tiwari.

4. DEPENDENT CLAIMS 9 AND 16

Claim 9 depends directly from claim 1. Ex. 1001, 39:43–46.

Claim 16 depends directly from claim 15. *Id.* at 41:12–14. Hence, claim 9 incorporates all of claim 1’s limitations, and claim 16 incorporates all of claim 15’s limitations. See 35 U.S.C. § 112(d).

Because Petitioner does not establish sufficiently for purposes of institution that Tiwari anticipates or renders obvious the subject matter of claims 1 and 15, Petitioner does not establish sufficiently for purposes of institution that Tiwari anticipates or renders obvious the subject matter of claims 9 and 16. See *supra* §§ IV.E.2(b)–(d), IV.E.3.

F. Alleged Obviousness over Tiwari and Werner: Claims 1–3, 9–12, 15, 17, and 18

Petitioner contends that claims 1–3, 9–12, 15, 17, and 18 are unpatentable under § 103 as obvious over Tiwari and Werner. See Pet. 5, 42–53, 55–73. Above, we provided an overview of Tiwari. See *supra* § IV.E.1. Below, we provide an overview of Werner, and then we consider obviousness issues raised by the parties. For the reasons explained below, Petitioner does not establish sufficiently for purposes of institution that the combined disclosures in Tiwari and Werner teach the subject matter of claims 1–3, 9–12, 15, 17, and 18.

1. OVERVIEW OF WERNER (EXHIBIT 1007)

Werner is a U.S. patent application publication titled “Key Value Data Storage,” filed on June 1, 2012, and published on December 6, 2012.

Ex. 1007, codes (22), (43), (54). Werner discloses technologies relating to key-value data storage and synchronization. *Id.* ¶¶ 2, 5, 30–31, code (57).

Werner explains that:

- (1) a key-value pair is “a data structure expressed in the form <key, value>”;
- (2) the key is “an identifier”; and
- (3) the value is “the data being stored in the key-value pair.”

Ex. 1007 ¶ 31. “The key can identify, for example, the application and the type of data stored in the associated value.” *Id.*

Werner also explains that key-value pairs “are typically small pieces of data not stored as files like documents or other larger pieces of data.” *Id.* ¶ 29.

Werner's Figure 1 (reproduced below) depicts an example system for storing and synchronizing key-value pairs:

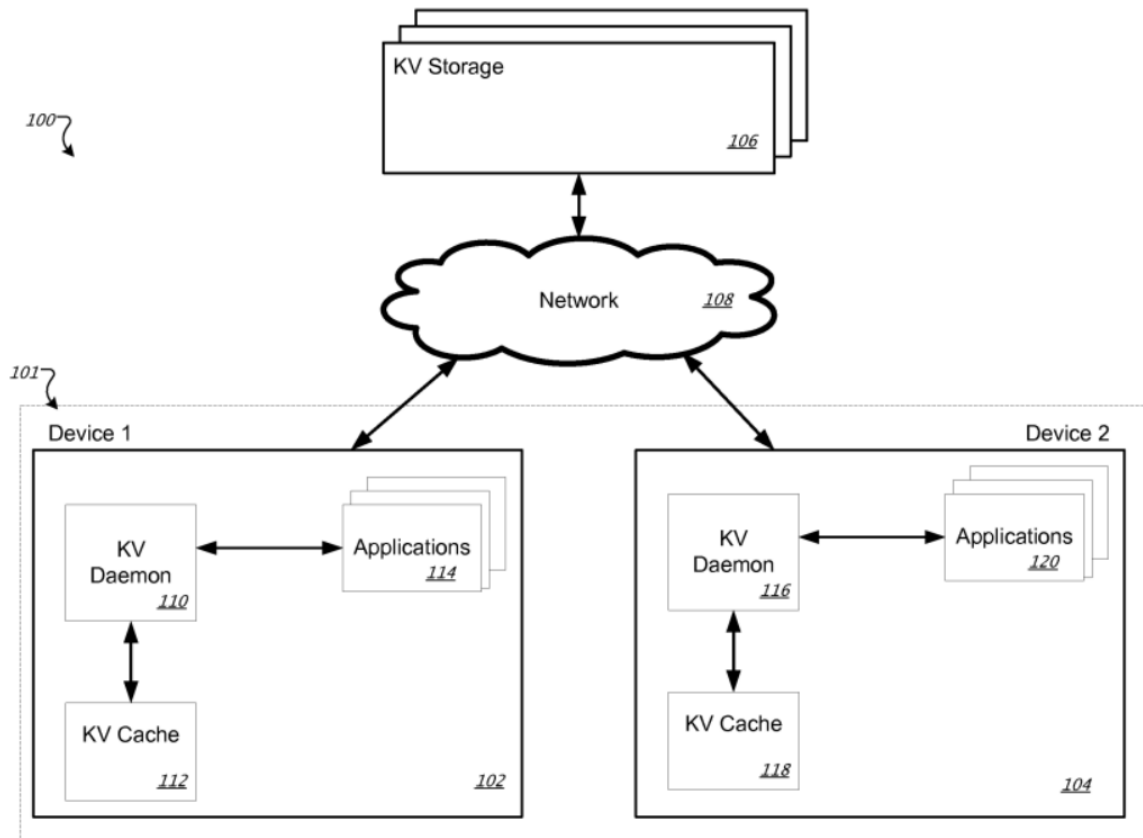


FIG. 1

Figure 1 illustrates example system 100 for storing and synchronizing key-value pairs including “a first device 102, a second device 104, and a remote storage location 106.” Ex. 1007 ¶¶ 16, 25, Fig. 1. “The first device 102, second device 104, and remote storage location 106 are coupled together using one or more networks 108.” *Id.* ¶ 26, Fig. 1. “The remote storage location 106 can be a single storage location or multiple storage locations” and “can include one or more computing devices.” *Id.* ¶ 27.

“The first device 102 includes one or more applications 114, a key-value daemon 110, and a key-value cache 112.” Ex. 1007 ¶ 29, Fig. 1. “The second device 104 similarly includes one or more applications 120, a key-

value daemon 116, and a key-value cache 118.” *Id.* ¶ 29, Fig. 1. “The applications 114 and application 120 can” include “the same applications” that “generate new key-value pairs based on changes to a running application.” *Id.* ¶ 29.

“The key-value daemon 110 receives key-value pairs from applications 114 as well as from the remote storage location 106” and includes logic for “resolving conflicts between key-value pairs from different devices.” Ex. 1007 ¶ 32. “The key-value cache 112 allows the key-value daemon 110 to store both notifications and received key-value pairs.” *Id.* ¶ 33. “Additionally, the key-value cache 112 can store key-value pairs received from the remote storage location 106.” *Id.* ¶ 34.

“The remote storage location 106 receives key-value pairs from devices, e.g., the first device 102 and the second device 104 for storage and to provide synchronization.” Ex. 1007 ¶ 36. “The remote storage location 106 also provides notifications to the first device 102 and the second device 104.” *Id.* ¶ 37. For instance, “when the first device 102 pushes a new key-value pair to the remote storage location 106, the remote storage location 106 can notify the second device 104 of the new key-value pair (e.g., if the second device 104 is associated with the same account and has the same application).” *Id.* “The second device 104 can then request the corresponding key-value pair (e.g., immediately or at some later time) for incorporation with the corresponding application 120 of the second device 104.” *Id.*

Werner discloses an example where applications 114 include “a stocks application” for providing, among other things, “stock price quotes” for selected companies. Ex. 1007 ¶ 30. “A user can modify a listing of

companies” presented by the stocks application, e.g., by adding “a new stock to the listing.” *Id.* “If the user modifies the listing, a new key-value pair can be generated that represents the new listing or the change in the listing.” *Id.* Then, “a key-value pair indicating a new stock listing can be sent from the first device 102 to the remote storage location 106.” *Id.* ¶ 39. “The remote storage location 106 both stores the key-value pair and sends a notification to the second device 104.” *Id.* “The second device 104 can then request the key-value pair, for example using the key value daemon 116,” and can use the requested key-value pair “to synchronize the stocks listing in the corresponding stocks application of the second device 104.” *Id.*

Werner's Figure 5 (reproduced below) depicts a flowchart for an example conflict resolution:

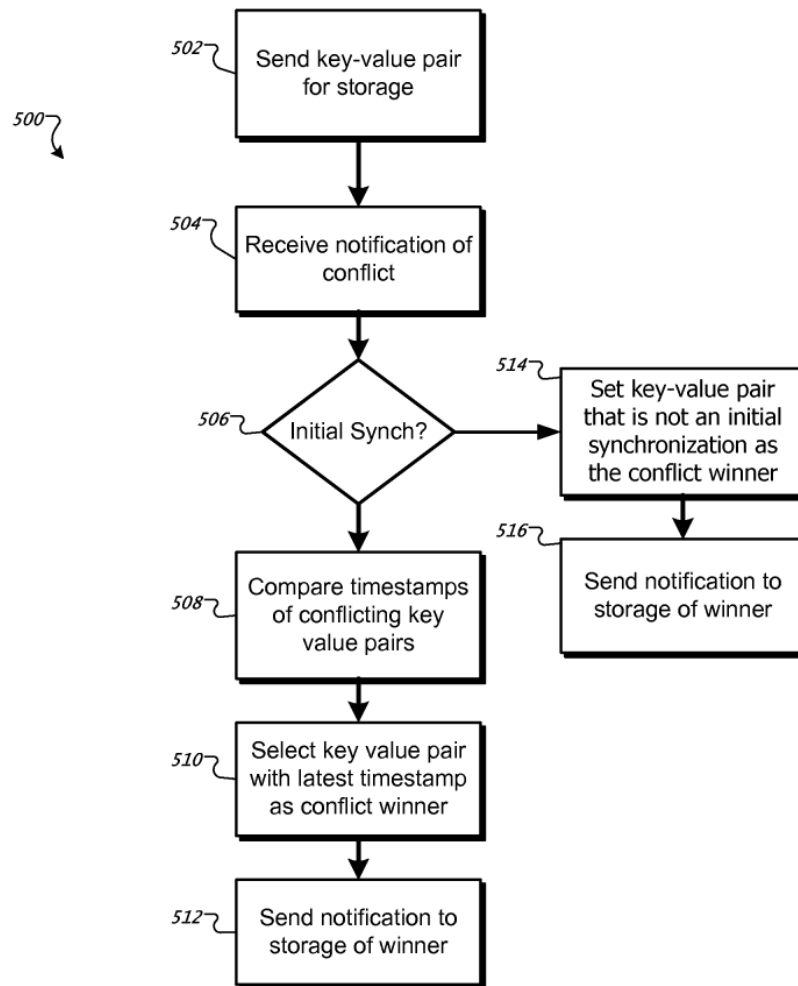


FIG. 5

Figure 5 illustrates “an example process 500 for client side conflict resolution” performed by “one or more computing devices, for example, by the first device 102” in Figure 1. Ex. 1007 ¶¶ 20, 62, Fig. 5.

In step 502, a “key-value pair is sent for storage.” Ex. 1007 ¶ 63, Fig. 5. In step 504, a “notification of a conflict is received.” *Id.* ¶ 64, Fig. 5. “The notification indicates that the sent key-value pair is out of sequence relative to a key-value pair received from another device.” *Id.* ¶ 64.

In step 506, a “determination is made as to whether one of the conflicting key-value pairs represents an initial synchronization” because an initial synchronization for a new device may provide “default settings to applications that could override user modifications to applications if synchronized.” Ex. 1007 ¶ 65, Fig. 5.

If “the conflicting key-value pairs do not include a key-value pair from an initial synchronization,” in step 508 “the timestamps associated with each respective key value pair are compared.” Ex. 1007 ¶ 66, Fig. 5. Next in step 510, the “key-value pair with the latest timestamp is selected as the conflict winner.” *Id.* ¶ 67, Fig. 5. “The latest timestamp identifies the key-value pair for the most recent change to the application by the user.” *Id.* ¶ 67. Then in step 512, a “notification of the conflict winner is sent to the remote storage location.” *Id.* ¶ 67, Fig. 5.

If “the conflicting key-value pairs include a key-value pair from an initial synchronization,” in step 514 “the key-value pair that is not an initial synchronization is [selected as] the conflict winner.” Ex. 1007 ¶ 68, Fig. 5. Then in step 516, a “notification of the conflict winner is sent to the remote storage location.” *Id.* ¶ 68, Fig. 5.

2. WHETHER WERNER CURES THE DEFICIENCIES |IN TIWARI FOR CLAIMS 1, 10, AND 15

(a) Limitation [1f] and the Related Limitations in Claims 10 and 15

Claim 1 recites “determining which of the first security key and the second security key is a latest security key.” Ex. 1001, 38:36–37.

Claims 10 and 15 include identical limitations. *Id.* at 40:5–6, 41:8–9.

Petitioner contends that the combined disclosures in Tiwari and Werner teach limitation [1f] and the related limitations in claims 10 and 15.

See Pet. 48, 57, 67–68. Specifically, Petitioner asserts that “Werner recognizes scenarios where there may be conflicting key-value pairs between devices.” *Id.* at 48, 67 (citing Ex. 1003 ¶ 95; Ex. 1007 ¶ 65). Petitioner also asserts that in “those scenarios, the ‘key-value pair with the latest timestamp is selected as the conflict winner.’” *Id.* at 48, 67 (quoting Ex. 1007 ¶ 67). According to Petitioner, “Werner’s teachings, applied to Tiwari, would cause the AUSF to use timestamps to identify the key with the latest timestamp to be used for integrity protection and verification.” *Id.* at 48, 68 (citing Ex. 1003 ¶ 66; Ex. 1007 ¶¶ 66–68).

Patent Owner disputes that the combined disclosures in Tiwari and Werner teach limitation [1f] and the related limitations in claims 10 and 15. See Prelim. Resp. 3, 32–38. Specifically, Patent Owner asserts that Petitioner “cites Werner for its disclosure of resolving conflicts between key-value pairs.” *Id.* at 32. Patent Owner then contends that Werner’s disclosure “is wholly unrelated to Tiwari and the technology at issue in this case.” *Id.*

Additionally, Patent Owner contends that (1) Werner’s key is “an identifier” and (2) Werner’s value is “the data being stored in the key-value pair.” Prelim. Resp. 32 (quoting Ex. 1007 ¶ 31). Patent Owner also contends that Werner’s key is not “a security key that is used for determining the contents of a protected message, as in Tiwari and the claimed invention.” *Id.* at 33.

Based on the current record, Petitioner does not establish sufficiently for purposes of institution that the combined disclosures in Tiwari and Werner teach limitation [1f] and the related limitations in claims 10 and 15. See Pet. 47–48, 57, 67–68; Prelim. Resp. 32–38; Ex. 1003 ¶¶ 94–95, 118,

137–138. As Patent Owner contends, Werner’s key is not “a security key that is used for determining the contents of a protected message, as in Tiwari and the claimed invention.” See Prelim. Resp. 33; Ex. 1007 ¶¶ 30–31.

Specifically, Werner explains that:

- (1) a key-value pair is “a data structure expressed in the form <key, value>”;
- (2) the key is “an identifier”; and
- (3) the value is “the data being stored in the key-value pair.”

Ex. 1007 ¶ 31. The key uniquely identifies the kind of data populating the value field and does not change when the data changes. See *id.* ¶¶ 30–31. For example, a particular key may denote that the data populating the value field concerns stock information or weather information, e.g., key = 1111 for stock information and key = 1112 for weather information. *Id.* ¶¶ 30–31, 39, 45, 48, 52.

Werner’s data-identifying key has no relation to Tiwari’s security key K_{AUSF} or the security keys required by claims 1, 10, and 15. In Werner’s system, a given key-value pair does not have different keys at different times or a “latest” key. See Ex. 1007 ¶¶ 30–31. Instead, a given key-value pair has only one key that does not change when the data changes. See *id.* ¶¶ 30–31.

For these reasons and the reasons discussed above for the challenge based on Tiwari alone, neither Tiwari nor Werner discloses “determining which of the first security key and the second security key is a latest security key” as required by claims 1, 10, and 15. See *supra* §§ IV.E.2(b), IV.E.3.

(b) Limitation [1g] and the Related Limitations in Claims 10 and 15

Claim 1 recites “using the latest security key to protect a message associated with the message protection request.” Ex. 1001, 38:38–39. Claim 10 includes an identical limitation, and claim 15 includes a similar limitation. *Id.* at 40:7–8, 41:10–11.

Petitioner contends that the combined disclosures in Tiwari and Werner teach limitation [1g] and the related limitations in claims 10 and 15. *See* Pet. 49, 57, 68–69. Specifically, Petitioner asserts that “Werner recognizes scenarios where there may be conflicting key-value pairs between devices.” *Id.* at 49, 68 (citing Ex. 1007 ¶ 65). Petitioner also asserts that in “those scenarios, the ‘key-value pair with the latest timestamp is selected as the conflict winner.’” *Id.* at 49, 68 (quoting Ex. 1007 ¶ 67). According to Petitioner, “Werner’s teachings, applied to Tiwari, would cause the AUSF to use timestamps to identify the key with the latest timestamp to be used for integrity protection and verification.” *Id.* at 49, 69 (citing Ex. 1003 ¶ 66; Ex. 1007 ¶¶ 66–68).

Patent Owner disputes that the combined disclosures in Tiwari and Werner teach limitation [1g] and the related limitations in claims 10 and 15 for the reasons Patent Owner disputes that the combined disclosures in Tiwari and Werner teach limitation [1f] and the related limitations in claims 10 and 15. *See* Prelim. Resp. 3, 32–38.

Based on the current record, Petitioner does not establish sufficiently for purposes of institution that the combined disclosures in Tiwari and Werner teach limitation [1g] and the related limitations in claims 10 and 15. *See* Pet. 48–49, 57, 68–69; Prelim. Resp. 32–38; Ex. 1003 ¶¶ 96–97, 119, 139–140. Because neither reference discloses “determining which of the

first security key and the second security key is a latest security key” according to limitation [1f] and the related limitations in claims 10 and 15, neither reference discloses using the result of such a determination according to limitation [1g] and the related limitations in claims 10 and 15. *See* Ex. 1004 ¶¶ 21–35, 44, Fig. 1; Ex. 1007 ¶¶ 23–31, 62–68, Fig. 5; *supra* §§ IV.E.2(b)–(c), IV.E.3.

3. ALLEGED REASONS FOR COMBINING THE TEACHINGS OF THE REFERENCES

Petitioner contends that an ordinarily skilled artisan would have been motivated to combine Werner’s teachings with Tiwari’s teachings because “Tiwari and Werner both”:

- (1) concern “security in communication systems”;
- (2) concern “communication systems that use keys for security”;
- (3) recognize “challenges concerning managing key-value pairs among different devices”;
- (4) “use pairs of keys that are used by different devices in the system”; and
- (5) “discuss using the latest key when multiple keys are present.”

Pet. 28–29 (citing Ex. 1004 ¶ 5, code (57); Ex. 1007 ¶¶ 5–15, 65–67, Figs. 1, 5); *see id.* at 48–49, 68–69 (citing Ex. 1003 ¶ 66; Ex. 1007 ¶¶ 66–68).

Further, Petitioner asserts that an ordinarily skilled artisan “would have found it obvious to implement the integrity protection procedure of Tiwari with Werner’s key management approach, which compares timestamps to determine which of the keys is the latest.” Pet. 29 (citing Ex. 1003 ¶ 65).

Patent Owner disputes that an ordinarily skilled artisan would have been motivated to combine Werner's teachings with Tiwari's teachings. See Prelim. Resp. 35–38. Regarding Petitioner's contention that "Tiwari and Werner both" recognize "challenges concerning managing key-value pairs among different devices," Patent Owner asserts that "Tiwari does not recognize challenges concerning managing a key (the identity of an application and type of data stored in the associated value) and a value (encoding of data in a form interpretable by the application)." *Id.* at 36 (citing Pet. 28; Ex. 1007 ¶ 31). Patent Owner also asserts that Petitioner's contention "addresses a non-existent problem in Tiwari," i.e., "managing key-value pairs among different devices," because "Tiwari already solved its stated problem of knowing which security key (K_{AUSF}) to use for integrity protection across different Public Land Mobile Networks (PLMNs) by storing tuples of a security key and network ID." *Id.* (citing Pet. 28; Ex. 1004 ¶¶ 5, 24). According to Patent Owner, "[t]here is simply no 'challenge' relating to 'managing key-value pairs' in Tiwari," contrary to Petitioner's contention. *Id.*

Further, Patent Owner asserts that an ordinarily skilled artisan "would not have thought to add timestamps for synchronizing data within applications across a user's devices, e.g., stock lists, to keys for accessing different PLMNs using the same device" because "[s]uch a person reading Tiwari would have understood that the tuples already distinguish the keys among the different PLMNs, and, therefore, would not have considered application-data-synchronization concepts to solve a non-existent problem." Prelim. Resp. 38.

Based on the current record, Petitioner does not establish sufficiently for purposes of institution that an ordinarily skilled artisan would have had a reason to combine Werner's teachings with Tiwari's teachings. *See* Pet. 28–30; Prelim. Resp. 35–38; Ex. 1003 ¶¶ 63–66. Petitioner's contentions that “Tiwari and Werner both” (1) concern “security in communication systems,” (2) concern “communication systems that use keys for security,” and (3) recognize “challenges concerning managing key-value pairs among different devices” mischaracterize Tiwari and Werner. *See* Pet. 28.

Specifically, Werner does not concern “security in communication systems” or “communication systems that use keys for security.” *See, e.g.,* Ex. 1007 ¶¶ 5–15, 23–39, 45, 62–68, code (57), Figs. 1, 5. Instead, Werner discloses technologies relating to key-value data storage and synchronization. *Id.* ¶¶ 2, 5, 30–31, code (57). While Werner notes that “key-value pairs can be securely stored and synchronized,” Werner does not disclose how to protect key-value pairs, *e.g.,* by using cryptographic keys for security or by using some other method. *See, e.g., id.* ¶¶ 14, 33, 36, 45, code (57).

Additionally, Tiwari does not recognize “challenges concerning managing key-value pairs among different devices” because, among other things, Tiwari does not mention key-value pairs. *See, e.g.,* Ex. 1004 ¶¶ 5, 21–35, 44, Fig. 1. Tiwari's tuple containing a K_{AUSF} and a PLMN ID is not “a data structure expressed in the form <key, value>” where the key is “an identifier” and the value is “the data being stored in the key-value pair.” *See* Ex. 1004 ¶ 24; Ex. 1007 ¶ 31. In Tiwari's system, a K_{AUSF} operates to provide integrity protection for messages, not as “an identifier” for data. *See, e.g.,* Ex. 1004 ¶¶ 1, 3, 5, 28, 32, code (57), Fig. 1.

Also, as discussed above, Werner’s data-identifying key has no relation to Tiwari’s security key K_{AUSF} or the security keys required by claims 1, 10, and 15. *See supra* § IV.E.2(b).

Further, as Patent Owner asserts, an ordinarily skilled artisan “would not have thought to add timestamps for synchronizing data within applications across a user’s devices, e.g., stock lists, to keys for accessing different PLMNs using the same device” because “[s]uch a person reading Tiwari would have understood that the tuples already distinguish the keys among the different PLMNs, and, therefore, would not have considered application-data-synchronization concepts to solve a non-existent problem.” *See Prelim. Resp.* 38.

In short, Petitioner identifies no sound reason that would have prompted an ordinarily skilled artisan to combine Werner’s teachings with Tiwari’s teachings to yield the claimed invention. *See Pet.* 28–30; *Ex. 1003 ¶¶* 63–66.

4. CONCLUSION CONCERNING CLAIMS 1, 10, AND 15

Because Petitioner does not establish sufficiently for purposes of institution that (1) the combined disclosures in Tiwari and Werner teach limitations [1f] and [1g] and the related limitations in claims 10 and 15 and (2) an ordinarily skilled artisan would have been motivated to combine Werner’s teachings with Tiwari’s teachings, Petitioner does not establish sufficiently for purposes of institution that the combined disclosures teach the subject matter of claims 1, 10, and 15. *See Pet.* 28–30, 47–49, 57, 67–69; *Ex. 1003 ¶¶* 63–66, 94–97, 118–119, 137–140; *supra* §§ IV.F.2–IV.F.3. Hence, Petitioner does not demonstrate a reasonable likelihood of

prevailing in proving claims 1, 10, and 15 unpatentable under § 103 as obvious over Tiwari and Werner.

5. DEPENDENT CLAIMS 2, 3, 9, 11, 12, 17, AND 18

Claims 2, 3, and 9 depend directly or indirectly from claim 1. Ex. 1001, 38:40–60, 39:43–46. Claims 11 and 12 depend directly from claim 10. *Id.* at 40:9–31. Claims 17 and 18 depend directly or indirectly from claim 15. *Id.* at 41:15–42:4. Hence, claims 2, 3, 9, 11, 12, 17, and 18 incorporate all of the limitations of the respective base claims. *See* 35 U.S.C. § 112(d).

Because Petitioner does not establish sufficiently for purposes of institution that the combined disclosures in Tiwari and Werner teach the subject matter of claims 1, 10, and 15, Petitioner does not establish sufficiently for purposes of institution that the combined disclosures teach the subject matter of claims 2, 3, 9, 11, 12, 17, and 18. *See supra* §§ IV.F.2–IV.F.4.

*G. Petitioner's Other Challenges:
Claims 6, 8, and 15–18*

Petitioner contends that the following claims are unpatentable under § 103 as obvious over the following combinations of references:

- claims 6 and 8 obvious over Tiwari and Wang;
- claims 6 and 8 obvious over Tiwari, Werner, and Wang;
- claims 15 and 16 obvious over Tiwari and S3-172482;
and
- claims 15–18 obvious over Tiwari, Werner, and S3-172482.

Pet. 5–6, 53–55, 58–73.

Claims 6 and 8 depend directly or indirectly from claim 1. Ex. 1001, 39:19–23, 39:38–42. Claims 16–18 depend directly or indirectly from claim 15. *Id.* at 41:12–42:4. Hence, claims 6, 8, and 16–18 incorporate all of the limitations of the respective base claims. See 35 U.S.C. § 112(d).

Petitioner does not rely on Wang or S3-172482 to cure the deficiencies in Tiwari and Werner for limitations [1f] and [1g] and the related limitations in claims 10 and 15. See Pet. 31–42, 47–49, 57, 67–69. Hence, Petitioner does not demonstrate a reasonable likelihood of prevailing in proving claims 6, 8, and 15–18 unpatentable under § 103 as obvious based on the challenges that add Wang or S3-172482 to either Tiwari alone or Tiwari and Werner.

V. CONCLUSION

After considering the Petition, the Preliminary Response, and the evidence of record, and for the reasons discussed above, we determine that Petitioner has not demonstrated a reasonable likelihood that it would prevail in proving the unpatentability of at least one claim challenged in the Petition. Hence, we deny the Petition and do not institute an *inter partes* review.

VI. ORDER

Accordingly, it is

ORDERED that the Petition is denied and no trial is instituted.

IPR2022-00850
Patent 11,039,312 B2

PETITIONER:

W. Karl Renner
Thomas A. Rozylowicz
Jennifer J. Huang
FISH & RICHARDSON P.C.
IPR50095-0100IP1@fr.com
PTABInbound@fr.com
renner@fr.com
rozylowicz@fr.com
jhuang@fr.com

PATENT OWNER:

Scott W. Hejny
Nicholas Mathews
McKOOL SMITH, P.C.
shejny@mckoolsmith.com
nmathews@mckoolsmith.com