

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

CARBYNE BIOMETRICS, LLC,
Patent Owner.

IPR2024-00332
Patent 10,929,512 B1

Before JAMESON LEE, ARTHUR M. PESLAK, and
STEVEN M. AMUNDSON, *Administrative Patent Judges*.

PESLAK, *Administrative Patent Judge*.

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

I. INTRODUCTION

Apple Inc. (“Petitioner”) filed a Petition pursuant to 35 U.S.C. §§ 311–319 requesting an *inter partes* review of claims 1–6, 10–16, 20, and 21 (“the challenged claims”) of U.S. Patent No. 10,929,512 B1 (“the ’512 patent,” Ex. 1001). Paper 2. Petitioner filed a Declaration of Dr. Patrick McDaniel in support of the Petition. Ex. 1003. With our authorization, Petitioner also filed a stipulation concerning parallel district court litigation on April 29, 2024. Ex. 1029. Carbyne Biometrics, LLC (“Patent Owner”) filed a Preliminary Response. Paper 7 (“Prelim. Resp.”). Petitioner filed an authorized Preliminary Reply. Paper 8 (“Prelim. Reply”). Patent Owner filed an authorized Preliminary Sur-reply. Paper 9 (“Prelim. Sur-reply”).

We have authority, acting on the designation of the Director, to determine whether to institute an *inter partes* review under 35 U.S.C. § 314(a). *See* 37 C.F.R. § 42.4(a) (2023) (“The Board institutes the trial on behalf of the Director.”). Under 35 U.S.C. § 314(a), an *inter partes* review may not be instituted unless the information presented in the Petition shows “there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.”

Considering the Petition, the Preliminary Response, the Preliminary Reply, the Preliminary Sur-reply, as well as all supporting evidence, we conclude that the information presented in the Petition establishes a reasonable likelihood that Petitioner would prevail in its challenge of at least one claim of the ’512 patent as unpatentable. Pursuant to 35 U.S.C. § 314, we hereby institute an *inter partes* review of all challenged claims of the ’512 patent on the ground stated in the Petition.

Our factual findings, claim construction, and legal conclusions at this stage of the proceeding are based on the evidentiary record developed thus far. This decision to institute trial is not a final decision as to the unpatentability of the claims for which *inter partes* review is instituted. Our final decision will be based on the full record developed during trial.

A. Related Matters

The parties identify the following proceeding as a related matter: *Carbyne Biometrics, LLC v. Apple Inc.*, 1:23-cv-00324 (W.D. Tex.) (“Parallel District Court Proceeding”). Pet. 1; Paper 4, 2.

Petitioner also identifies the following terminated proceedings as related matters: *RightQuestion, LLC v. Samsung Electronics Co., Ltd.*, 2:21-cv-00238 (E.D. Tex.); *Samsung Electronics Co., Ltd. et al. v. RightQuestion, LLC*, IPR2022-00251 (PTAB) (hereinafter “the 251 IPR”); *Samsung Electronics Co., Ltd. et al. v. RightQuestion, LLC*, IPR2022-00244 (PTAB). Pet. 1–2.

B. Real Parties in Interest

Petitioner and Patent Owner each identifies itself and no others as a real party in interest. Pet. 1; Paper 4, 2.

C. The ’512 Patent

The ’512 patent is titled “Authentication Translation.” Ex. 1001, code (54). The ’512 patent issued on February 23, 2021, from Application No. 16/773,767 (“the ’767 patent application”), which was filed on January 27, 2020. *Id.* at codes (45), (21), (22). Application No. 16/773,767 claims priority through a series of continuation applications to Application No. 13/706,254, filed December 5, 2012, and also claims priority to Provisional

Application No. 61/587,387, filed January 17, 2012, and Provisional Application No. 61/569,112, filed December 9, 2011. *Id.* at codes (63), (60).

As background, the '512 patent explains that when “[p]roviding credentials to a service, whether via a mobile or other device,” “to make authentication easier for themselves, users will often engage in practices such as password re-use, and/or the selection of poor quality passwords, which render their credentials less secure against attacks.” Ex. 1001, 1:35–40.

Figure 1 of the '512 patent is reproduced below.

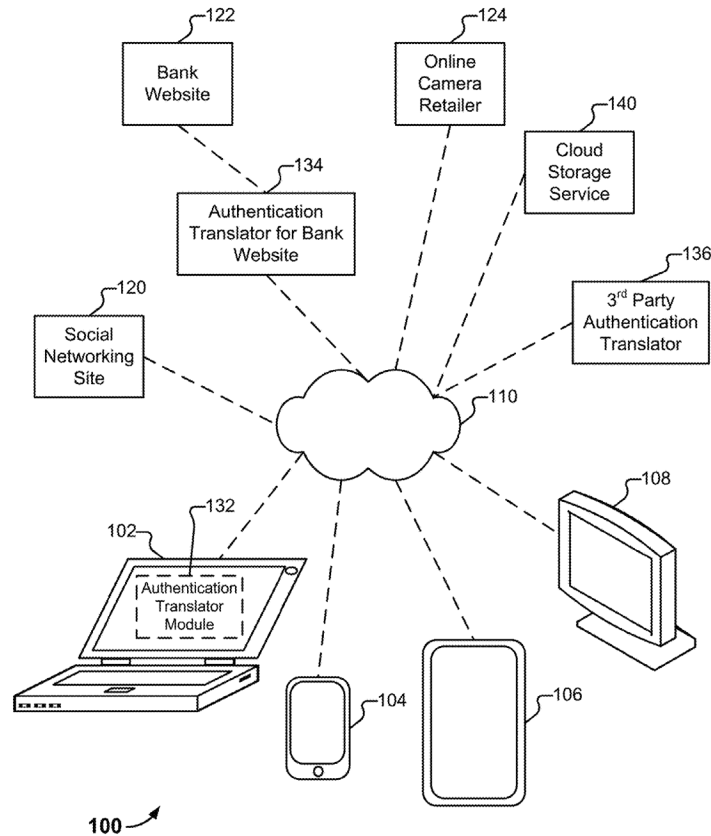


FIG. 1

Figure 1 “illustrates an embodiment of an environment in which authentication translation is provided,” where “a variety of client devices 102-108 connect, via one or more networks (represented as a single network

cloud 110) to a variety of services 120-124.” Ex. 1001, 2:37–42. The ’512 patent states that even though “[e]ach of services 120-124 requires a username and password (and/or a cookie) from a user prior to giving that user access to protected content and/or other features,” “users need not type such usernames and passwords into their devices whenever required by a service.” *Id.* at 2:59–65. According to the ’512 patent, “[i]nstead, users can authenticate themselves to an ‘authentication translator’ via an appropriate technique, and the authentication translator will provide the appropriate credentials to the implicated service on the user’s behalf.” *Id.* at 2:65–3:1. The ’512 patent also states that “authentication translators can be located in a variety of places within an environment,” as shown, for example, in notebook computer 102, which “includes an authentication translator module 132 that provides authentication translation services.” *Id.* at 3:2–6.

Figure 2 of the '512 patent is reproduced below.

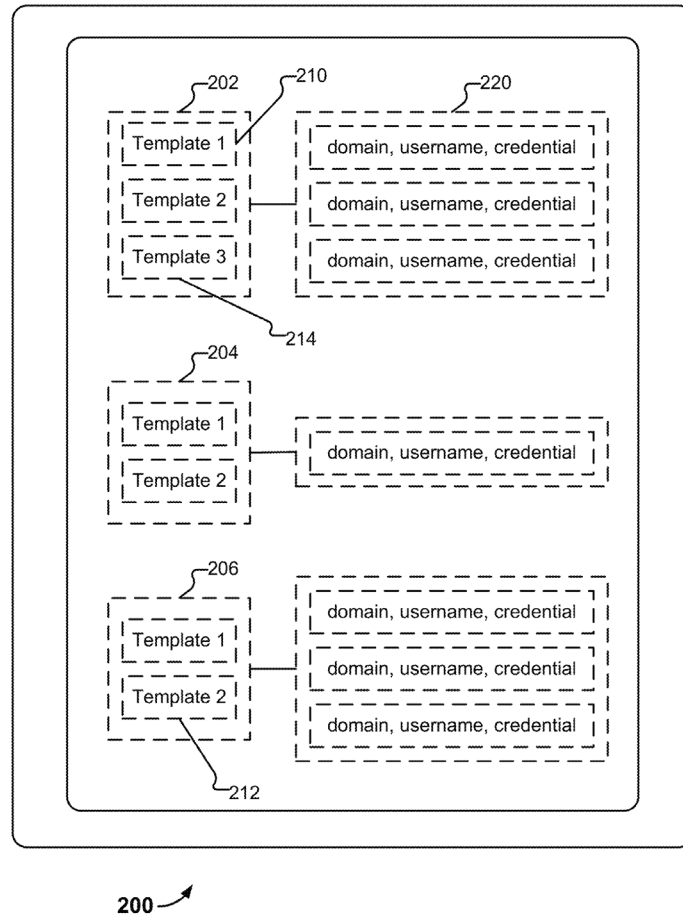


FIG. 2

Figure 2 “illustrates an embodiment of credential information stored on a device.” Ex. 1001, 3:13–14. The '512 patent describes user profiles 202–206 stored on device 200, “each of which contains a username and one or more templates (e.g., template 210) associated with the user.” *Id.* at 3:14–17. According to the '512 patent, “a template is a collection of biometric features” relating to, for example, “fingerprints,” “facial recognition, voiceprint, or retina scan technology.” *Id.* at 3:17–31. The '512 patent describes that “[a] profile is associated with a vault (e.g., vault 220),” which, “in turn, contains triples specifying a service provider/domain, a username,

and a credential,” and also “other sensitive user information, such as account numbers, address/phone number information, and health care data.” *Id.* at 3:51–56. According to the ’512 patent, “[t]he credential for a service provider/domain can be a password (e.g., for legacy servers), and can also take alternate forms (e.g., a cryptographic key for service providers supporting stronger authentication methods).” *Id.* at 3:56–59. The ’512 patent further describes that a secure storage may be used to store at least a portion of “profiles, templates, and vaults (collectively ‘authentication information’).” *Id.* at 3:60–61, 3:63–65; *see also id.* at 3:66–4:26, FIG. 3.

Figure 5 of the ’512 patent is reproduced below.

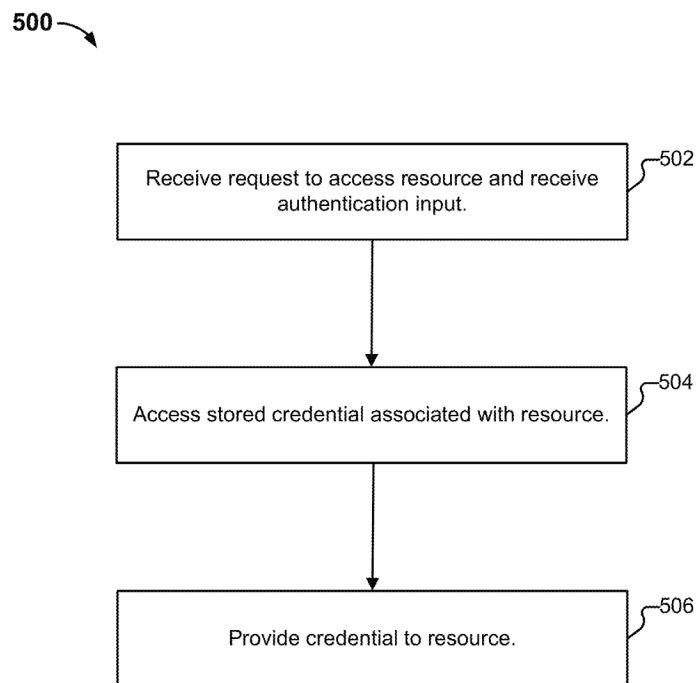


FIG. 5

Figure 5 “illustrates an embodiment of a process for performing authentication translation.” Ex. 1001, 6:18–19. The ’512 patent describes one exemplary process which begins at step 502 as follows:

Suppose Alice wishes to sign into social networking website 120. She directs a web browser application installed on client 102 to the social networking website. Authentication translator module 132 recognizes, from the context of Alice’s actions (e.g., that she is attempting to access site 120 with her browser) that she would like to access a particular resource. Authentication translator module 132 prompts Alice (e.g., by a popup message or via a sound) to provide biometric information (e.g., to use the integrated fingerprint reader on her laptop). . . .

Module 132 compares Alice’s supplied biometric data to the templates stored on her computer. If a suitable match is found, and if an entry for site 120 is present in the applicable vault, at 504, a previously stored credential associated with the resource is accessed. In particular, the username and password for the website, as stored in a vault, such as vault 220, are retrieved from the vault.

Finally, at 506, the credential is provided to the resource. For example, Alice’s username and password for site 120 are transmitted to site 120 at 506.

Id. at 6:22–48.

D. Illustrative Claim

Claims 1, 11, and 21 are independent claims. Claim 1 is representative of the claimed subject matter and is reproduced below:

1. A system, comprising:
a first processor of a first device, wherein the first processor is configured to:
based at least in part on a request associated with a user to access an external resource, establish a secure connection with the external resource; and

communicate with a second processor using a restricted interface, wherein the second processor is configured to:

receive a biometric input from a sensor, wherein the biometric input corresponds to at least one of a fingerprint, a feature usable for facial recognition, a voiceprint, a feature usable for a retina scan, or a typing feature; and

access a record stored in a secure storage, wherein the record is associated at least with the external resource;

retrieve, from the record, at least one of a password, a cookie, or a cryptographic key;

perform a cryptographic operation;

in response to determining that there is a match between the biometric input and a stored biometric template accessed by the second processor, facilitate a login of the user to the external resource at least in part by transmitting, via the established connection, output based at least in part on the at least one of the password, the cryptographic key, or the cookie retrieved from the record, and wherein the user is logged in to the external resource based at least in part on the output; and

perform a secure backup of the record to a storage service, wherein a second device associated with the user is registered with the storage service, and wherein the record is downloaded from the storage service by the second device; and

a memory coupled to the first processor and configured to provide the first processor with instructions.

Ex. 1001, 10:62–11:31.

E. Prior Art and Asserted Grounds

Petitioner asserts that claims 1–6, 10–16, 20, and 21 would have been unpatentable on the following ground (Pet. 9):

Claim(s) Challenged	35 U.S.C. §	References/Basis
1–6, 10–16, 20, and 21	103(a) ¹	Kesanupalli, ² Challener, ³ Cheng ⁴

II. ANALYSIS

A. Discretionary Denial of Institution Under 35 U.S.C. § 314(a)

Patent Owner contends that we should exercise our discretion to deny institution under 35 U.S.C. § 314(a) and *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020) (precedential). Prelim. Resp. 13–26. Patent Owner analyzes the factors set forth in *Fintiv* in light of the Parallel District Court Proceeding. *Id.* at 16–26.

In the Petition, Petitioner contends that we should not exercise our discretion to deny institution under 35 U.S.C. § 314(a) and provides its analysis of the factors set forth in *Fintiv* in light of the Parallel District Court Proceeding. Pet. 72–74. In the Petition, Petitioner also stipulates that if we institute trial, “it will not pursue the same grounds raised in this Petition in the Parallel District Court Litigation.” *Id.* at 73–74 (citing *Sand Revolution*

¹ The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112–29, 125 Stat. 284, 287–288 (2011), amended 35 U.S.C. §§ 102 and 103. Because the ’138 patent claims priority to an application filed before March 16, 2013 (the effective date of the amendments), the pre-AIA version of § 103 applies.

² U.S. Patent No. 8,799,666 B2 (issued Aug. 5, 2014) (Ex. 1006, “Kesanupalli”).

³ U.S. Patent No. 8,099,789 B2 (issued Jan. 17, 2012) (Ex. 1007, “Challener”).

⁴ U.S. Patent Application Publication No. 2004/0117636 A1 (published June 17, 2004) (Ex. 1008, “Cheng”).

II, LLC v. Cont'l Intermodal Grp.–Trucking LLC, IPR2019-01393, Paper 24 at 7 (PTAB June 16, 2020)). Subsequently, as noted above, we authorized Petitioner to file a stipulation. *See* Ex. 1029. Petitioner's stipulation provides that if we institute trial in this case, Petitioner "(i) will not pursue the grounds [raised in this proceeding] in the Parallel District Court Litigation and (ii) will not pursue any other ground that reasonably could have been raised during the IPR (should it be instituted) in the Parallel District Court Litigation." Ex. 1029, 1.

Patent Owner counters that "Petitioner is using its late 'stipulation' to game the *Fintiv* process and get two bites at the invalidity apple." Prelim. Resp. 25. Patent Owner contends that "Petitioner's stipulation does not in fact guarantee the reduction of *any* duplicate effort," and asserts that "Petitioner has already positioned itself to combine the petitioned art with art that Petitioner will argue it 'could **not** have reasonably been raised' in the IPR petitions, such as system art, in the district court in order to avoid the consequences of its stipulation." *Id.* at 23.

Analysis

The Director of the USPTO has proscribed an interim procedure for discretionary denials in AIA post-grant proceedings with parallel district court litigation. *See* Ex. 1025, Memorandum to Members of the PTAB from Director Vidal, dated June 21, 2022 ("Memorandum"). In the Memorandum, the Director states that "[w]hen a petitioner stipulates not to pursue in a parallel district court proceeding the same grounds as in the petition or any grounds that could have reasonably been raised in the petition, it mitigates concerns of potentially conflicting decisions and duplicative efforts between the district court and the PTAB." *Id.* at 7.

Further, when such a stipulation is provided, “the grounds the PTAB resolves will differ from those present in the parallel district court litigation” and “the PTAB will not discretionarily deny institution of an IPR.” *Id.*

In this case, Petitioner provides a stipulation that falls within the contours of the Memorandum. Ex. 1029, 1. Petitioner’s stipulation meets the requirements of a stipulation pursuant to *Sotera Wireless, Inc. v. Masimo Corp.*, IPR2020-01019, Paper 12 at 18–19 (PTAB Dec. 1, 2020) (precedential as to § II.A), and, therefore, the Director’s Memorandum governs our determination here.

For the foregoing reasons, in accordance with the Director’s Memorandum, we do not exercise our discretion to deny institution under 35 U.S.C. § 314(a) due to the parallel district court litigation.

B. Discretionary Denial of Institution Under 35 U.S.C. § 325(d)

Patent Owner contends we should exercise our discretion under 35 U.S.C. § 325(d) and deny institution because Petitioner relies on the references that are the same or substantially the same as the references that were previously considered by the Office (including the Board) and Petitioner has failed to demonstrate that the Office (including the Board) erred in evaluating the art. Prelim. Resp. 26–35; *see also id.* at 7–11.

Although “Petitioner acknowledges that *another* Kesanupalli reference was ‘previously presented to the Office,’” Petitioner contends that “neither Challenger nor Cheng is similar—let alone cumulative—to Johansson, or any reference that was before the Board.” Pet. 76–77. Petitioner further contends that “the Office overlooked specific teachings in a manner that demonstrates material error relative to the Kesanupalli/Challenger/Cheng ground advanced in this Petition.” *Id.* at 78.

i. Analytical Framework Under 35 U.S.C. § 325(d)

The statute provides that “the Director may take into account whether, and reject the petition . . . because, the same or substantially the same prior art or arguments previously were presented to the Office.” 35 U.S.C.

§ 325(d). Our Consolidated Trial Practice Guide (“CTPG”) indicates that the decision whether to deny institution on this basis “is a fact-dependent decision, in which the Board balances the petitioner’s desire to be heard against the interest of the patent owner in avoiding duplicative challenges to its patent.” Patent Trial and Appeal Board Consolidated Trial Practice Guide, 62 (Nov. 2019), available at <https://www.uspto.gov/sites/default/files/documents/tpgnov.pdf>.

We use a two-part framework to analyze a request to exercise discretion to deny institution under § 325(d). First, we determine “whether the same or substantially the same art previously was presented to the Office or whether the same or substantially the same arguments previously were presented to the Office.” *Advanced Bionics, LLC v. MED-EL*

Elektromedizinische Geräte GmbH, IPR2019-01469, Paper 6 at 8 (PTAB Feb. 13, 2020) (precedential). Second, “if either condition of [the] first part of the framework is satisfied,” then we consider “whether the petitioner has demonstrated that the Office erred in a manner material to the patentability of [the] challenged claims.” *Id.* In applying this framework, we refer to the non-exclusive factors delineated in *Becton, Dickinson & Co. v. B. Braun Melsungen AG*, IPR2017-01586, Paper 8 (PTAB Dec. 15, 2017)

(precedential as to § III.C.5, first para.). These factors are: a) the similarities and material differences between the asserted art and the prior art involved during examination; b) the cumulative nature of asserted art and the prior art

evaluated during examination; c) the extent to which the asserted art was evaluated during examination, including whether the prior art was the basis for rejection; d) the extent of overlap between the arguments made during examination and the manner in which Petitioner relies on the prior art or Patent Owner distinguishes the prior art; e) whether Petitioner has pointed out sufficiently how the Examiner erred in its evaluation of the asserted prior art; and f) the extent to which additional evidence and facts presented in the Petition warrant reconsideration of the prior art or arguments. *Id.* at 17–18.

These factors “should be read broadly . . . to apply to any situation in which a petition relies on the same or substantially the same art or arguments previously presented to the Office during a proceeding *pertaining to the challenged patent.*” *Advanced Bionics*, Paper 6 at 10 (emphasis added). If, after review of factors (a), (b), and (d), we determine the same or substantially the same art or arguments previously were presented to the Office, then factors (c), (e), and (f) relate to whether the petitioner demonstrates that the Office erred in a manner material to patentability of the challenged claims. *Id.*

ii. Analysis

None of Kesanupalli, Challener, or Cheng were of record during prosecution of the ’512 patent. Ex. 1001, code (56); Ex. 1002. Further, the Examiner did not issue any rejections during prosecution based on any of Kesanupalli, Challener, and Cheng or combination of these references and consequently, no arguments for patentability to overcome any rejections were made. *See generally* Ex. 1002. Patent Owner argues that Kesanupalli was cited in the prosecution of four continuation patents in the family of the ’512 patent. Prelim. Resp. 7, 26. The four continuation patents, however,

do not pertain to the challenged claims in the '512 patent. Based on the foregoing, we find that the same or substantially the same art or arguments were not presented to the Office during prosecution of the '512 patent.

The 251 IPR involved a challenge to claims 1–4, 6–15, and 17–21 of the '512 patent over Johansson (U.S. Patent No. 8,776,214 B1) and Kesanupalli (U.S. 2011/0138450 A1 (Ex. 2030) (“Kesanupalli 450”)). *Samsung v. RightQuestion, LLC*, IPR2022-00251, Paper 17 at 15–26 (PTAB June 9, 2022). Kesanupalli 450 is substantially similar to the Kesanupalli reference relied on by Petitioner. *See* Prelim. Resp. 30–31 (comparing disclosure of the references). Neither Challenger nor Cheng were part of any challenge before the Board in the 251 IPR. *RightQuestion*, Paper 17 at 10.

In the 251 IPR, the petitioner relied on Kesanupalli 450 to disclose the “restricted interface” recited in claim 1. *RightQuestion*, Paper 17 at 24. The Board found that “Petitioner does not explain sufficiently, let alone with particularity, how or why Kesanupalli’s secure communication using SSL v# protocol (alone or in combination with Johansson) discloses or teaches the claimed ‘restricted interface.’” *Id.* at 25. The Board further found that “Petitioner’s declarant also makes this same statement verbatim, without more, and with no further explanation or additional citations to evidence” and gave the testimony of the declarant “little or no weight.” *Id.* The Board, “constrained by” the petition in the 251 IPR, denied institution. *Id.*

In this case, Petitioner’s relies on Challenger, not Kesanupalli for disclosure of a restricted interface between a first processor and a second processor. Pet. 35–37. The denial of institution on the Johansson/ Kesanupalli 450 ground in the 251 IPR is, thus, of little import here.

The 251 IPR also involved a challenge based on Shah (US 2008/0059804 A1) and Owen (US 7,780,080 B2). *RightQuestion*, Paper 17 at 10. Patent Owner argues that Shah describes a Trusted Platform Module (TPM) reference. Prelim. Resp. 37. In the 251 IPR, the Board denied institution of the Shah and Owen ground because it determined that neither Shah nor Owen nor the combination taught the recited secure storage. *RightQuestion*, Paper 17 at 40. This determination is, thus, of little import here because Petitioner relies on Cheng for the secure backup. Pet. 54–55.

Based on the foregoing, we find that the same or substantially the same art or arguments were not made to the Board in the 251 IPR.

Because neither the same nor substantially the same art or arguments were made to the Office during prosecution of the '512 patent or in the 251 IPR, we determine that the first prong of the *Advanced Bionics* framework is not satisfied. Since the first prong of the *Advanced Bionics* framework is not satisfied, we need not reach the second prong of the *Advanced Bionics* framework. Accordingly, we decline to exercise our discretion to deny institution under § 325(d).

C. Overview

A claim is unpatentable under § 103(a) 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). The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in

the art; and (4) when in evidence, objective indicia of non-obviousness (i.e., secondary considerations).⁵ *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

The Supreme Court explained in *KSR International Co. v. Teleflex Inc.* that

[o]ften, it will be necessary for a court to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.

550 U.S. at 418 (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006) (“[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.” (alteration in original))).

“Whether an ordinarily skilled artisan would have been motivated to modify the teachings of a reference is a question of fact.” *WBIP, LLC v. Kohler Co.*, 829 F.3d 1317, 1327 (Fed. Cir. 2016) (citations omitted). “[W]here a party argues a skilled artisan would have been motivated to combine references, it must show the artisan ‘would have had a reasonable expectation of success from doing so.’” *Arctic Cat Inc. v. Bombardier Recreational Prods. Inc.*, 876 F.3d 1350, 1360–1361 (Fed. Cir. 2017) (quoting *In re Cyclobenzaprine Hydrochloride Extended-Release Capsule Patent Litig.*, 676 F.3d 1063, 1068–1069 (Fed. Cir. 2012)).

⁵ No evidence of secondary considerations has been presented at this stage of the proceeding.

D. Level of Ordinary Skill in the Art

Petitioner contends that

Persons of Ordinary Skill in the Art (‘POSITA’) at the time of the claimed invention would have had a bachelor’s degree in an electrical engineering, computer engineering, computer science, or a related field, and at least two years of experience in the research, design, development, and/or testing of authentication techniques, and related firmware and software, or the equivalent, with additional education substituting for experience and vice versa.

Pet. 6 (citing Ex. 1003 ¶¶ 18–21). Petitioner further states that “a person with less formal education but more experience, or more formal education but less experience, could have also met the relevant standard for POSITA.”

Id. (citing Ex. 1003 ¶¶ 18–21). Patent Owner, at this stage of the proceeding, does not dispute Petitioner’s definition of the person of ordinary skill in the art. Prelim. Resp. 11.

For the purposes of this Decision, we apply Petitioner’s proffered level of skill in the art, with the exception of the phrase “at least” which injects potential ambiguity into the level of skill, because it appears consistent with the problems addressed in the ’512 patent and the prior art.

E. Claim Construction

We apply the same claim construction standard used by Article III federal courts and the International Trade Commission, both of which follow *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc). 37 C.F.R. § 42.100(b). The claim construction standard includes construing claims in accordance with the ordinary and customary meaning of such claims as understood by one of ordinary skill in the art at the time of the invention. *See id.* at 1312–14. In construing claims in accordance with their ordinary and customary meaning, we take into account the specification and prosecution history. *Id.* at 1315–17.

If the specification “reveal[s] a special definition given to a claim term by the patentee that differs from the meaning it would otherwise possess[,] . . . the inventor’s lexicography governs.” *Phillips*, 415 F.3d at 1316 (citing *CCS Fitness, Inc. v. Brunswick Corp.*, 288 F.3d 1359, 1366 (Fed. Cir. 2002)). Another exception to the general rule that claims are given their ordinary and customary meaning is “when the patentee disavows the full scope of a claim term either in the specification or during prosecution.” *Uship Intellectual Props., LLC v. U.S.*, 714 F.3d 1311, 1313 (Fed. Cir. 2013) (quoting *Thorner v. Sony Comput. Ent. Am., LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012)).

Petitioner asserts that “for purposes of this proceeding, and as set forth below, the terms of the challenged claims should be given their plain and ordinary meaning.” Pet. 6–7 (citing Ex. 1003 ¶¶ 52–56). In particular, Petitioner contends that plain and ordinary meaning of “‘*restricted interface*’ is an interface that limits accessibility.” *Id.* at 7 (citing Ex. 1003 ¶ 53).

In support of its proposal, Petitioner explains:

In the ’512 patent specification, disclosure of such an interface is sparse. For an example device that “includes a large and insecure storage 302 attached to a fast processor 304, and a smaller but secure storage 306 attached to a dedicated processor 308 and a sensor 310 (*e.g.*, a camera or a fingerprint reader),” the specification refers to access limitations in connection with an application programming interface (API). [Ex. 1001], 4:6–8 (“users cannot access the secure storage area, and the fast processor can only communicate with the dedicated processor/sensor via a restricted API”). Thus, [a person of ordinary skill in the art] would understand *restricted interface* to at least include an API that limits accessibility to a secure storage, a fingerprint sensor, or a dedicated processor. [Ex. 1003] ¶53.

Pet. 7.

Patent Owner does not address Petitioner’s proposed construction of “restricted interface” but reserves the right to do so during trial. Prelim.

Resp. 11.

Based on Petitioner’s explanations, which are supported by the cited evidence, including the example given in the specification of the ’512 patent, we determine, preliminarily, that a “restricted interface” is an interface that limits accessibility and includes within its scope a restricted API.

We determine that it is not necessary for purposes of this Decision for us to expressly construe any other claim term. *See Realtime Data, LLC v. Iancu*, 912 F.3d 1368, 1375 (Fed. Cir. 2019) (“The Board is required to construe ‘only those terms . . . that are in controversy, and only to the extent necessary to resolve the controversy.’”)(quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

The parties are free to address the construction of “restricted interface” or any other claim term in subsequent briefing during trial.

F. Ground 1: Alleged Obviousness of Claims 1–6, 10–16, 20, and 21 over Kesanupalli, Challenger, and Cheng

Petitioner contends claims 1–6, 10–16, 20, and 21 would have been obvious over Kesanupalli, Challenger, and Cheng. Pet. 10–72. Petitioner supports its contentions with the Declaration of Dr. Patrick McDaniel. Ex. 1003. Patent Owner disputes Petitioner’s contentions. Prelim. Resp. 35–56. Patent Owner did not submit an expert declaration with the Preliminary Response.

We begin with brief summaries of Kesanupalli, Challenger, and Cheng, and then address the parties’ respective contentions.

1. Kesanupalli (Ex. 1006)

Kesanupalli is titled “Secure User Authentication Using Biometric Information.” Ex. 1006, code (54). Kesanupalli states that “it is desirable to provide a user authentication method and system that provides a more secure authentication of the user than commonly used password-based methods and systems” and that “biometric information provides an additional level of security when used in systems and procedures related to authentication of a user.” *Id.* at 1:59–62, 2:35–38.

Kesanupalli describes the systems and methods performing biometric user authentication in several steps as follows:

Initially, a user enrolls with the biometric user authentication system by binding their user credentials with the user’s biometric template (a “fingerprint template” in specific implementations). The biometric template contains information related to the user’s biometric characteristics (also referred to as “biometric information”) obtained from a biometric sensor that scans or reads the user’s biometric characteristics, such as a fingerprint. A user identification process identifies a particular user among multiple enrolled users (e.g., multiple users enrolled with a particular device, system or biometric sensor). A user verification process verifies that the user who provides their biometric information is who they claim to be by comparing the user’s biometric information with the biometric template obtained during enrollment of that user.

Ex. 1006, 3:15–29.

Kesanupalli describes that “[d]uring an example enrollment process that uses a fingerprint sensor as the biometric sensor, a user swipes their finger across the fingerprint sensor several times to create a fingerprint template,” which “contains qualitative fingerprint information that allows the user’s fingerprint to be distinguished from fingerprints associated with other users.” Ex. 1006, 3:32–35. According to Kesanupalli, “after creating

a fingerprint template, the user (or a web server or other system) provides user credentials, such as a password, cryptographic key, random seed, and the like.” *Id.* at 3:41–44. The fingerprint template and user credentials are then bound together and stored in a secure storage device. *Id.* at 3:44–47.

Kesanupalli further describes that “[d]uring an example user identification process (also referred to as a user verification process), a user swipes their finger across a fingerprint sensor” so as to determine “whether the user’s fingerprint information matches a fingerprint template associated with the fingerprint sensor.” Ex. 1006, 3:52–56. According to Kesanupalli, “[i]f the user’s fingerprint information matches a fingerprint template, the user’s credentials are released to the user and/or a service or process requesting the user verification.” *Id.* at 3:56–59.

Figure 2 of Kesanupalli is reproduced below.

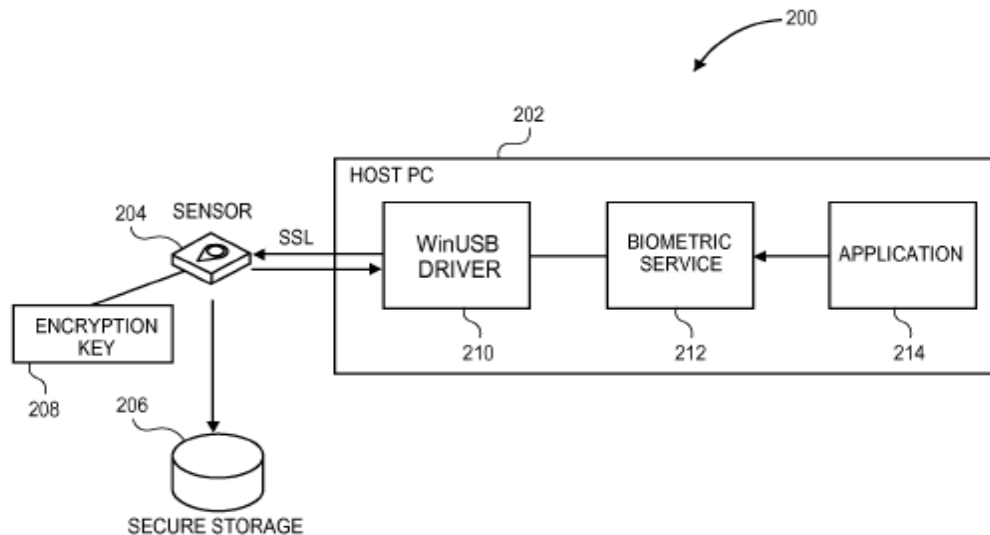


FIG. 2

Figure 2 shows an example system 200 capable of performing biometric user enrollment and authentication. Ex. 1006, 2:1–2. System 200 comprises

Host PC 202, biometric sensor 204, encryption key 208, and secure storage 206. *Id.* at 6:26–49. In the example, biometric sensor 204 is a fingerprint sensor that “creates a secure communication with Host PC 202 using SSL v3 protocol or other secure communication technique.” *Id.*

2. *Challenger (Ex. 1007)*

Challenger is titled “Apparatus and Method for Enabling Applications on a Security Processor.” Ex. 1007, code (54). Challenger’s invention “relates to securely protecting computer data, and more particularly to security processors provided in computer systems to implement security features.” *Id.* at 1:7–9. As background, Challenger describes a way to secure information known as the Trusted Platform Module:

Another way to secure information is known as the Trusted Platform Module (TPM) specification from the Trusted Computing Group (TCG). In this specification, a standard chipset including a programmable microcontroller is provided on a computer’s circuit board during manufacturing, and is used to store and secure information of the computer system that is desired to be protected, i.e., enable effective trusted computing features. The security architecture (i.e., the functions and the application program interface (API)) that runs on the microcontroller, can be referred to as a TPM. A TPM can offer a variety of features, including a random number generator, facilities for secure generation of cryptographic keys, and abilities to limit the use of keys, e.g., to signing and verification, and/or encryption and decryption.

Id. at 1:18–31.

Figure 1 of Challenger is reproduced below.

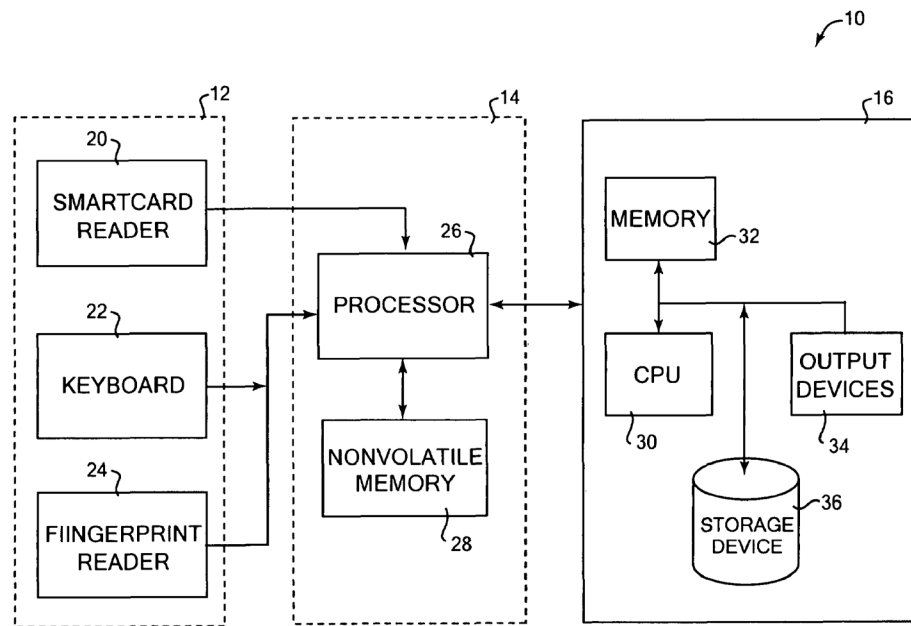


FIG. 1

Figure 1 of Challenger is a block diagram depicting a computer system 10 including an input portion 12 on the left, a security portion 14 in the center, and a standard portion 16 on the right. Ex. 1007, 3:46–47, 3:56–57.

Challenger discloses that “[s]ystem 10 includes a security architecture such as a Trusted Platform Module (TPM) from the Trusted Computing Group (TCG), or other security system suitable for . . . securing data and functions of the system 10 from unauthorized access and manipulation.” *Id.* at 3:51–56.

Challenger discloses “[i]nput portion 12 can include a variety of different input devices,” such as “card reader 20, keyboard 22, and/or fingerprint reader 24,” “which allow a user to input data to the system 10 and authenticate the user’s identity to the system.” Ex. 1007, 3:58–62.

Challenger also discloses “[s]ecurity portion 14 of system 10 is used to secure the data and applications of the system for access and use only by

authorized users.” Ex. 1007, 4:9–11. “For example, processor 26 can implement a TPM security architecture, which is a well-known standard for securing computer data” and “is implemented on a secure, dedicated chipset incorporated into a motherboard or other circuitry of a computer by the manufacturer.” *Id.* at 4:24–28. Challenger also describes a “nonvolatile memory 28 . . . included in security portion 14 and . . . connected to the processor 26.” *Id.* at 4:57–58. According to Challenger, “memory 28 is a secure memory which cannot be easily tampered with to read its data contents.” *Id.* at 4:61–63.

Challenger’s “standard portion 16 of system 10 is connected to the processor 26 and includes remaining standard components of the system,” such as “a microprocessor or CPU 30, memory 32 (random access memory (RAM), read-only memory (ROM), etc.), output devices 34 (video monitor, audio speakers, printer, etc.) and other typical computer components.” Ex. 1007, 5:15–21.

3. *Cheng (Ex. 1008)*

Cheng is titled “System, Method and Apparatus for Secure Two-Tier Backup and Retrieval of Authentication Information.” Ex. 1008, code (54). Cheng states that “[b]iometrics-based authentication is emerging as a reliable method that offers better security than traditional authentication including automated personal identification technologies.” *Id.* ¶ 4. According to Cheng, the “invention provides new ways to backup and restore data generated and stored on portable biometrics-based authentication devices.” *Id.* ¶ 7.

Cheng states that “[a] foundational aspect of the present invention is the concept of a two-tier backup encryption structure having a first

encryption means for enciphering lower tier data and a second encryption means for enciphering upper tier data,” where “[t]he lower tier data contain encrypted electronic identity such as private keys and associated certificates” and “[t]he upper tier data contain the encrypted lower tier data, restore validation script, and biometrics data.” Ex. 1008 ¶¶ 7–8. Figure 1 of Cheng is reproduced below:

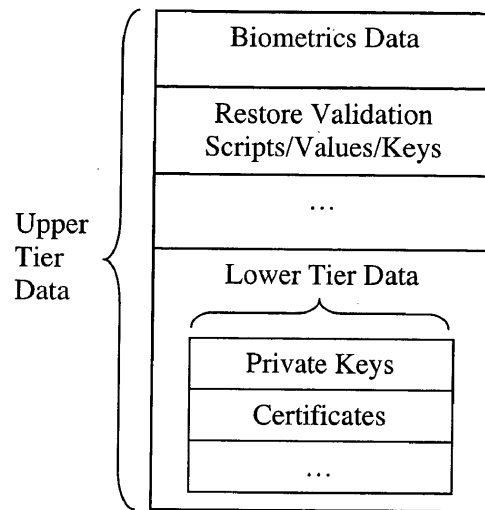


FIG. 1

Figure 1 “shows a two-tier backup encryption structure that allows the decryption of lower tier data only when upper tier data has been decrypted and validated.” *Id.* ¶ 15.

Cheng describes an embodiment of backup data as follows:

In a preferred embodiment, the device obtains a first encryption key from a first user service bureau. The lower tier data is encrypted with this first encryption key. Then, the device obtains a second encryption key from a second user service bureau, which may or may not be the same as the first user service bureau, and the upper tier data are further encrypted using the second encryption key, generating a multiple-encrypted backup file. The multiple-encrypted backup file is then copied to a storage medium of user’s choice.

Ex. 1008 ¶ 8.

Cheng further describes an embodiment of restoring backup data as follows:

To restore the multiple-encrypted backup data onto a new biometrics-based authentication device, the user first needs to enroll the relevant biometrics in the new device and upload the multiple-encrypted backup data onto the device, then contact the corresponding user service bureau to obtain an access clearance to the encrypted lower and upper tier encryption keys. The access clearance enables the device to establish a secure connection with the user service bureau service. Upon establishing the secure connection, the restore process begins automatically. The device first requests the upper tier data decryption key from the user service bureau server to decipher the encrypted upper tier data. The device then compares the decrypted backup biometrics data with the newly enrolled biometrics data. If they match, then the newly enrolled biometrics data are replaced with the decrypted backup biometrics data. Only then, will the system confirm the match to the user service bureau server and request the lower tier decryption key. Once the lower tier decryption key is received, the lower tier data is deciphered and stored in the device. This completes the restore process. If they do not match, the restore process is terminated.

Ex. 1008 ¶ 9.

4. Claims 1, 11, and 21

Petitioner provides a limitation-by-limitation analysis of independent claims 1, 11, and 21,⁶ mapping the prior art to the claim limitations. Pet. 27–60, 67–72. Petitioner also provides contentions concerning reasons to combine Kesanupalli and Challener, and Kesanupalli, Challener, and Cheng, and a reasonable expectation of success in the combination. *Id.* at 21–27.

⁶ For ease of reference, we use Petitioner’s claim limitation identifiers in our analysis.

Patent Owner contends that Petitioner's expert's declaration should be given no weight as to motivation-to-combine and reasonable-expectation-of-success analyses (Prelim. Resp. 36–42); Petitioner has not established that a POSITA would have combined Kesanupalli and Challener given Kesanupalli's exposure of the user's biometrics to the non-secure portion of the device during enrollment, which directly contradicts the teachings of Challener (*id.* at 42–49); Petitioner has not established that a POSITA would have combined Challener and Cheng because Cheng discloses that biometrics do not need to be securely protected (*id.* at 49–54); and Petitioner failed to show that a POSITA would have had a reasonable expectation of success adding Cheng to the Kesanupalli-Challener system (*id.* at 54–56).

With this background, we analyze the parties' respective contentions.

[1.0]: A system, comprising:

Petitioner contends that the combination of Kesanupalli and Challener teaches the preamble. Pet. 27 (citing Ex. 1003 ¶¶ 92–95). Petitioner contends that Kesanupalli discloses system 200, sensor 204, and secure storage 206 “capable of performing biometric user enrollment and authentication.” *Id.* (citing Ex. 1006, Abst., 2:1–2, Figs. 2, 11, 12). Petitioner provides the following annotated version of Figure 2 of Kesanupalli (*id.*):

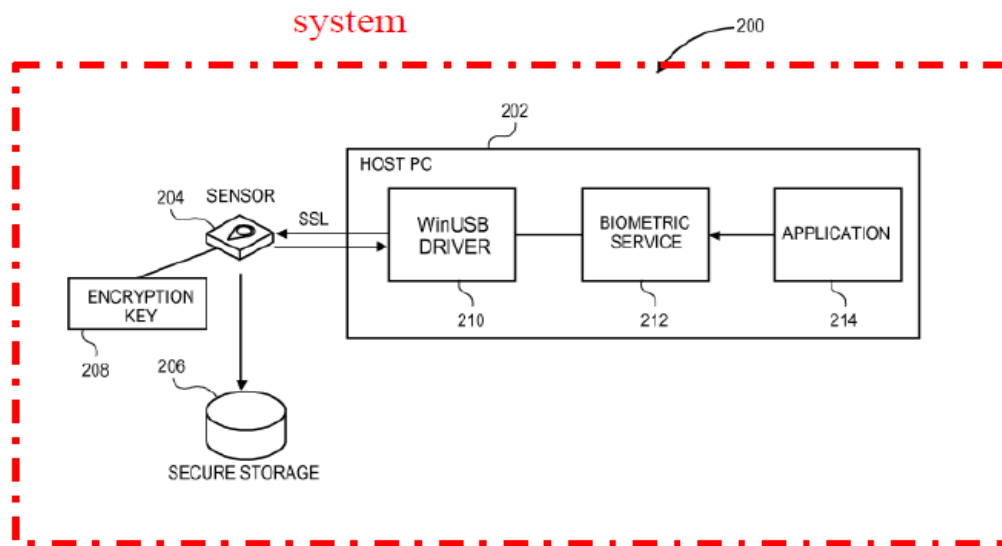


Figure 2 is a block diagram of an “example system.” Ex. 1006, 2:1–2. Petitioner adds a red rectangle with broken lines around Figure 2 with the word “system.” According to Petitioner, an ordinarily skilled artisan would have applied Challenger’s “known architecture . . . to Kesanupalli . . . to form the system.” *Id.* at 28 (citing Ex. 1003 ¶¶ 74–84; Ex. 1007, 3:45–4:65, Figs. 1, 3).

Patent Owner does not dispute Petitioner’s contentions concerning the preamble. *See generally* Prelim. Resp.

We reviewed the evidence cited by Petitioner and find it sufficiently discloses the subject matter of the preamble. Therefore, we need not address whether the preamble is limiting.

[1.1A]: a first processor of a first device, wherein the first processor is configured to:

Petitioner contends that Kesanupalli and Challenger individually and in combination teach this limitation. Pet. 29.

Petitioner contends that Kesanupalli’s “[b]iometric sensor 204, its secure storage 206, and Host PC 202 . . . constitute *a device* that provides

authentication translation and ultimately communicates user credentials to web servers.” Pet. 29 (citing Ex. 1003 ¶¶ 99; Ex. 1006, Abst., 2:54–3:3, 4:3–11, 4:36–50, 6:11–49, Fig. 2).

Petitioner next contends that an ordinarily skilled artisan “would have implemented Kesanupalli’s system 200 and techniques performed by the system using the TPM-based architecture of Challenger” resulting in “the functions of HOST PC 202 . . . including communication with an external resource . . . implemented as *first processor*, which is a general processor shown in Challenger as general microprocessor 30.” Pet. 30 (citing Ex. 1003 ¶¶ 74–79, 100; Ex. 1006, 2:54–3:3, 6:11–25, 9:58–10:12; Ex. 1007, 5:15–25, Fig. 1).

Patent Owner does not address Petitioner’s contentions for this limitation other than to dispute Petitioner’s reasons for combining Kesanupalli and Challenger with a reasonable expectation of success. *See generally* Prelim. Resp. As discussed in detail below after considering Patent Owner’s contentions, we find Petitioner’s reasons for combining Kesanupalli and Challenger with a reasonable expectation of success sufficient based on the record before us at this stage of the proceeding.

We reviewed the evidence cited by Petitioner for this limitation and find it sufficient for institution.

[1.1B]: [wherein the first processor is configured to] based at least in part on a request associated with a user to access an external resource, establish a secure connection with the external resource;

Petitioner contends that the combination of Kesanupalli and Challenger teaches this limitation. Pet. 31 (citing Ex. 1003 ¶¶ 102–111).

Petitioner first contends that, in Kesanupalli, “the user visits an *external resource* (website) to enroll with the resource and create, and store,

the user's fingerprint template and user credentials associated with the website.” Pet. 31 (citing Ex. 1006, 5:33–43, Figs. 7, 11). For subsequent visits by the user, after enrollment, the user requests that “the external resource initiate an authentication translation procedure.” *Id.* (citing Ex. 1006, 2:54–3:3, 4:36–5:14, Figs. 10, 11). According to Petitioner, this results in establishing a connection “between application 214 of PC 202 and the external resource,” “application 214 is executing on the *first processor* of PC 202,” and “the first processor establishes a connection, via the Internet, with a web server of the website.” *Id.* at 32 (citing Ex. 1003 ¶¶ 101–105; Ex. 1006, 2:54–3:3, 4:36–50, 6:11–50, 7:67–8:4, 9:58–10:1, Fig. 9 (block 914)).

Petitioner next contends that “Challener confirms that a *first processor*, microprocessor 30 of a standard portion of a system, performs typical device functions including input/output (communications), which would include Kesanupalli's connections to external resources.” Pet. 32–33 (citing Ex. 1007, 5:15–25). Petitioner argues that Kesanupalli discloses “the connection between PC 202 and the web server as a ‘**secure communication link**,’ which is a *secure connection*.” *Id.* at 33 (citing Ex. 1003 ¶¶ 104, 110; Ex. 1006, 7:54–8:5, 12:62–67).

Petitioner reproduces the following annotated version of Kesanupalli's Figure 12 (Pet. 33):

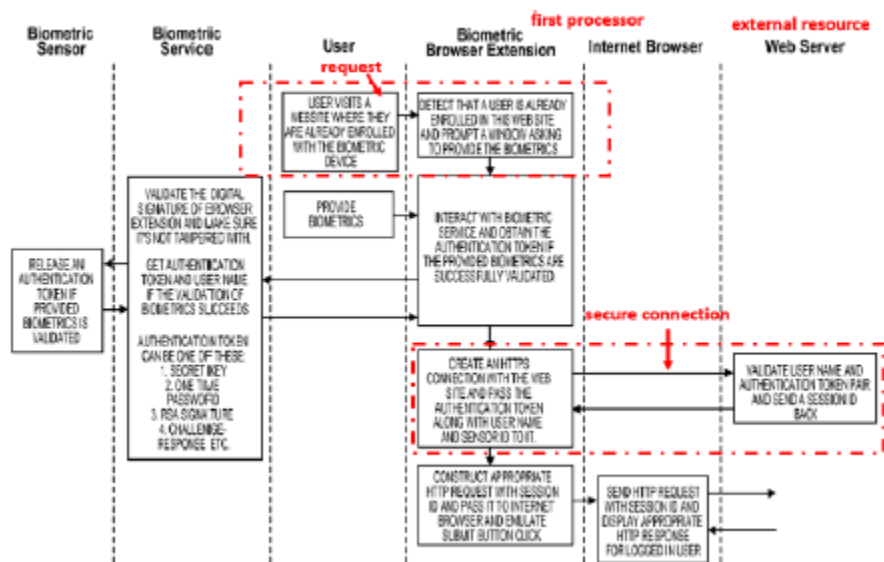


Figure 12 is a block diagram illustrating “a procedure for identifying and authenticating a user of a biometric authentication system.” Ex. 1006, 2:22–24. Petitioner adds red rectangles in broken lines with associated text identifying where it contends Figure 12 shows a “request,” a “first processor,” an “external resource,” and a “secure connection.” According to Petitioner, annotated Figure 12 “illustrates actions for authenticating a user, including those performed by a ‘user’ and those performed by the *first processor* . . . or the external resource’s web server,” and “also shows communication over the *secure connection* between the first processor and the webserver providing the *external resource*.” Pet. 33 (citing Ex. 1003 ¶ 108; Ex. 1006, Fig. 12)).

Patent Owner does not address Petitioner’s contentions for this limitation. *See generally* Prelim. Resp.

We reviewed the evidence cited by Petitioner and find it sufficient for institution.

[1.1C]: and [the first processor is configured to] communicate with a second processor using a restricted interface,

Petitioner contends that the combination of Kesanupalli and Challener teaches this limitation. Pet. 34 (citing Ex. 1003 ¶¶ 112–120).

Petitioner first contends that an ordinarily skilled artisan “would have been motivated to build on the functions of Challener’s TPM-based security architecture using a specialized security processor—a *second processor* such as illustrated by Challener’s security processor 26.” Pet. 34 (citing Ex. 1003 ¶¶ 74–79). In the combination, “[t]he first processor (Kesanupalli’s HOST PC 202 functionality operating in standard portion 16 of Challener’s TPM framework) *is configured to communicate with* [Challener’s security processor 26], *a second processor*.” *Id.* at 35 (citing Ex. 1003 ¶¶ 113–114; Ex. 1006, 6:39–42).

Petitioner next contends that “based on the ’512 patent’s limited description, [a person of ordinary skill in the art] would understand ‘*restricted interface*’ to at least include an API⁷ that limits accessibility to a secure storage, a [fingerprint] sensor, or a dedicated processor.” Pet. 35 (citing Ex. 1003 ¶¶ 114–119). Petitioner argues that “Challener’s secure processor 26—the *second processor*—implements a security architecture that includes API functions used in its communication with other components, including general microprocessor 30—the *first processor*.” *Id.* at 36 (citing Ex. 1003 ¶¶ 117–118; Ex. 1007, 4:9–24, Fig. 1). According to Petitioner, “a TPM-based API, such as provided by Challener’s secure processor 26, provides restrictions by the way of a set of rules or restrictions [a person of ordinary skill in the art] would understand are defined by the TPM standard for access to the security portion of the system.” *Id.* at 37 (citing Ex. 1003 ¶¶ 51, 117–119).

⁷ As used herein, “API” refers to an application programming interface.

Petitioner next contends that using Challenger’s architecture in Kesanupalli “provides communication between . . . microprocessor 30 . . . of a general portion of the TPM-based system . . . and . . . secure processor 26 . . . of a security portion of the TPM-based system.” Pet. 37. According to Petitioner, this communication is via a restricted interface, i.e., “an API of the TPM security architecture of the security processor” and “is merely [the] predictable use of a known element according to its established function in the TPM architecture.” *Id.* (citing Ex. 1003 ¶ 118).

Patent Owner does not address Petitioner’s contentions for this limitation. *See generally* Prelim. Resp.

We reviewed the evidence cited by Petitioner and find it sufficient for institution.

[1.2]: wherein the second processor is configured to: receive a biometric input from a sensor, wherein the biometric input corresponds to at least one of a fingerprint, a feature usable for facial recognition, a voiceprint, a feature usable for a retina scan, or a typing feature; and

Petitioner contends that the combination of Kesanupalli and Challenger teaches this limitation. Pet. 38 (citing Ex. 1003 ¶¶ 121–124).

Petitioner specifically contends that Kesanupalli’s “sensor 204 receives a biometric input of a ‘fingerprint’ from a ‘fingerprint sensor.’” Pet. 39 (citing Ex. 1006, 6:31–36, 9:10–24, Fig. 9). Petitioner further contends that Kesanupalli “suggests other biometric information including those further recited in the recited group,” i.e., “facial characteristics, eye characteristics, voice characteristics.” *Id.* (citing Ex. 1006, 2:31–35).

Patent Owner does not address Petitioner’s contentions for this limitation. *See generally* Prelim. Resp.

We reviewed the evidence cited by Petitioner and find it sufficient for institution.

[1.3]: *[wherein the second processor is configured to] access a record stored in a secure storage, wherein the record is associated at least with the external resource;*

Petitioner contends that the combination of Kesanupalli and Challener teaches this limitation. Pet. 40 (citing Ex. 1003 ¶¶ 125–134).

Petitioner contends that the ordinarily skilled artisan would understand that the combination of Kesanupalli and Challener “has a security processor—a *second processor on the device*—executing the functions of Kesanupalli’s sensor 204, which include” this limitation. Pet. 40.

Petitioner further contends that after a user’s enrollment with an external resource, Kesanupalli discloses “[u]ser **credentials** and other information may be **stored** within biometric sensor 204, in a **secure storage 206**, or any other storage mechanism.” Pet. 41 (quoting Ex. 1006, 6:45–47 (emphasis by Petitioner)). According to Petitioner, “[t]he stored user’s credential bound with a biometric template is a *record*, which is *stored on the first device* in a secure storage” and “is *associated at least with the external resource* as the credential and/or template are associated with the website.” *Id.* (citing Ex. 1003 ¶ 129; Ex. 1006, 5:33–41, 8:47–53; Ex. 1019).

Petitioner next contends both Kesanupalli and Challener disclose secure storage. Pet. 42 (citing Ex. 1003 ¶ 131; Ex. 1006, 6:45–47, Fig. 2; Ex. 1007, 4:57–65, Fig. 1).

Patent Owner does not address Petitioner’s contentions for this limitation. *See generally* Prelim. Resp.

We reviewed the evidence cited by Petitioner and find it sufficient for institution.

[1.4]: [wherein the second processor is configured to] retrieve, from the record, at least one of a password, a cookie, or a cryptographic key;

Petitioner contends that the combination of Kesanupalli and Challenger teaches this limitation. Pet. 43 (citing Ex. 1003 ¶¶ 135–139).

Petitioner contends that, in Kesanupalli’s enrollment process, “the record (template and credential) is stored in secure storage 206 of the first device” and “one type of user credential is a *cryptographic key* and another is a *password*.” Pet. 43 (citing Ex. 1006, 3:41–44). According to Petitioner, “subsequent visits by the user to the external resource initiate an authentication translation procedure,” and “[i]f successfully authenticated, the . . . security processor executing functions of sensor 204, *retriev[es] from the record* the user credential (e.g., password or key) to release the credential to the requesting resource (website via PC 202).” *Id.* at 43–44 (citing Ex. 1003 ¶ 138; Ex. 1006, 5:9–14), 44–45 (reproducing Figure 9 of Kesanupalli annotated by Petitioner to illustrate retrieval of user credentials upon successful authentication at step 908), 45–46 (arguing “[i]f the user’s fingerprint information matches a fingerprint template, the user’s **credentials are released** to the user and/or a service or process requesting the user verification.” (citing Ex. 1006, 3:65–4:1)).

Patent Owner does not address Petitioner’s contentions for this limitation. *See generally* Prelim. Resp.

We reviewed the evidence cited by Petitioner and find it sufficient for institution.

[1.5]: [wherein the second processor is configured to] perform a cryptographic operation;

Petitioner contends that the combination of Kesanupalli and Challenger teaches this limitation. Pet. 46 (citing Ex. 1003 ¶¶ 140–144).

Petitioner contends that Figure 9 of Kesanupalli discloses “the procedure retrieves credentials associated with the user based on the fingerprint information (block 908). The **procedure then decrypts the user credentials** (block 910).” Pet. 47 (quoting Ex. 1006, 9:17–21 (emphasis by Petitioner)). Petitioner next contends that the ordinarily skilled artisan “would have implemented the sensor 204 functions using a *second processor* according to the TPM-based architecture of Challenger” which “also confirms a security processor *is configured to perform a cryptographic operation.*” *Id.* at 48 (citing Ex. 1003 ¶ 143; Ex. 1007, 4:24–36).

Patent Owner does not address Petitioner’s contentions for this limitation. *See generally* Prelim. Resp.

We reviewed the evidence cited by Petitioner and find it sufficient for institution.

[1.6]: *[wherein the second processor is configured to]*

[1.6A]: *in response to determining that there is a match between the biometric input and a stored biometric template accessed by the second processor,*

[1.6B]: *facilitate a login of the user to the external resource at least in part by transmitting, via the established connection, output based at least in part on the at least one of the password, the cryptographic key, or the cookie retrieved from the record, and wherein the user is logged in to the external resource based at least in part on the output; and*

Petitioner contends that the combination of Kesanupalli and Challenger teaches these limitations. Pet. 48 (citing Ex. 1003 ¶¶ 145–156).

For limitation 1.6A, Petitioner contend that “Kesanupalli’s authentication procedure includes determining that there is *a match between the biometric input (e.g., fingerprint information) and a stored biometric template (e.g., fingerprint template)*” and “then **authenticates the**

fingerprint information (block 904).” Pet. 49 (citing Ex. 1006, 6:34–47, 9:12–18). According to Petitioner, “[v]alidating or authenticating means matching the template and the biometric input.” *Id.* at 50 (citing Ex. 1003 ¶ 143). Petitioner further contends that the device shown in Figure 2 of Kesanupalli in response “to ‘on-chip matching’ performed by sensor 204, the user credential is retrieved from secure storage 206 of sensor 204 and provided to application 214 of PC 202 for communication to the external resource (*e.g.*, website).” *Id.* at 50–51 (citing Ex. 1006, 6:11–49).

For limitation 1.6B, Petitioner contends that “in Kesanupalli’s procedure, the security processor executing the functions of sensor 204 (the *second processor*) *facilitate[s] a login of the user to the external resource*” by “retriev[ing] the credentials from secure storage (206) and transmits, via the HOST PC 202, the credentials (*e.g.*, password, cryptographic key) to the external resource-transmitting the credential to the website, thereby *transmitting output* to the external resource (website).” Pet. 51 (citing Ex. 1006, 9:10–24). Referring to its contentions for limitation 1.1B, Petitioner contends that “[s]ensor 204 . . . sends the decrypted credentials to the website by sending the credentials to application 212 of the PC 202 . . . and . . . application 214 communicates it to the website via this *established connection* between the first processor and the external resource.” *Id.* at 51–52 (citing Ex. 1006, 4:1–5, 4:51–63, 5:59–6:25), 33 (“Kesanupalli describes the connection between PC 202 and the web server as a ‘secure communication link.’” (emphasis omitted)). Petitioner further contends that Kesanupalli and the ’512 patent describe communication of decrypted credentials in like manner, *i.e.*, “in terms of SSL (now TLS) or HTTPS protocols.” *Id.* at 52 (citing Ex. 1001, 5:7–15; Ex. 1003 ¶ 151). According

to Petitioner, an ordinarily skilled artisan would have understood that “when Kesanupalli communicates the credentials ‘to the Web site to **complete** the user authentication process,’ the user login has occurred.” *Id.* at 56–57 (citing Ex. 1003 ¶¶ 154–155; Ex. 1006, 5:22–24, Fig. 12).

Patent Owner does not address Petitioner’s contentions for these limitations. *See generally* Prelim. Resp.

We reviewed the evidence cited by Petitioner and find it sufficient for institution.

[1.7]: *[wherein the second processor is configured to]*

[1.7A]: *perform a secure backup of the record to a storage service,*

[1.7B]: *wherein a second device associated with the user is registered with the storage service, and*

[1.7C]: *wherein the record is downloaded from the storage service by the second device; and*

Petitioner contends that the combination of Kesanupalli, Challenger, and Cheng teaches limitation 1.7 including subparts 1.7A, 1.7B, and 1.7C. Pet. 54 (citing Ex. 1003 ¶¶ 157–175).

For limitation 1.7A, Petitioner contends that “Cheng discloses a ‘biometrics-based authentication device,’ and a *secure backup* of data of this first device by creating ‘backup file(s)’ of the encrypted data, and providing these backup file(s) to a user service bureau, a *storage service*.” Pet. 55 (citing Ex. 1008 ¶¶ 2, 23–29). Petitioner also contends that Cheng discloses backing-up data, i.e., “user authentication information, such as ‘private keys, certificates, and other data held within the device’ and ‘user’s biometric information.’” Pet. 56 (citing Ex. 1008, ¶¶ 7, 8, 30, Figs. 3A, 3B). According to Petitioner, because Kesanupalli’s record contains the types of data referred to in Cheng, combining Kesanupalli and Cheng would

predictably “create[] a backup of the record (*e.g.*, backup file(s)) that is protected from unauthorized access (*e.g.*, by encryption) and transmit[] it to a storage service (*e.g.*, user service bureau).” *Id.* (citing Ex. 1003 ¶¶ 165–169).

For limitation 1.7B, Petitioner contends that Cheng describes a process of restoring backup data onto a new device which “includes *register[ing] a second device associated with the user* with Cheng’s user service bureau, *the storage service.*” Pet. 57 (citing Ex. 1008 ¶¶ 45–47), 58 (reproducing Cheng’s Figure 4 with Petitioner’s annotations which, according to Petitioner, show that “Cheng discloses a second device such as a user’s new device *is registered* with the storage service.” (citing Ex. 1003 ¶¶ 170–171)).

For limitation 1.7C, Petitioner contends that “Cheng describes data is *downloaded* from the service bureau, *storage service*, by the *second device.*” Pet. 58–59 (citing Ex. 1003 ¶¶ 172–174; Ex. 1008 ¶¶ 9, 39, 48, Figs. 4A, 4B). According to Petitioner, an ordinarily skilled artisan “would recognize that applying Cheng’s teachings to Kesanupalli’s record would be a predictable benefit to Kesanupalli/Challener system” of saving user’s time “in recreating the data in the record (*e.g.*, biometric template and/or user credential).” *Id.* at 59 (citing Ex. 1003 ¶ 174).

Patent Owner does not address Petitioner’s contentions for these limitations. *See generally* Prelim. Resp.

We reviewed the evidence cited by Petitioner and find it sufficient for institution.

[1.8]: a memory coupled to the first processor and configured to provide the first processor with instructions.

Petitioner contends that the combination of Kesanupalli and Challener teaches this limitation. Pet. 59 (citing Ex. 1003 ¶¶ 176–180).

Petitioner contends that an ordinarily skilled artisan would have understood that Kesanupalli’s main memory “is *coupled* to the *first processor* and configured to provide the processor with *instructions* such as those that execute the functions of Host PC 202 and sensor 204.” Pet. 59–60 (citing Ex. 1003 ¶¶ 177–178; Ex. 1006, 5:59–66, 14:49–15:18). Petitioner further contends that “Challener confirms a memory 36 is coupled to a general microprocessor 30—a *first processor*.” *Id.* at 60 (citing Ex. 1007, 5:26–40, 7:67–8:7).

Patent Owner does not address Petitioner’s contentions for this limitation. *See generally* Prelim. Resp.

We reviewed the evidence cited by Petitioner and find it sufficient for institution.

Motivation to Combine Kesanupalli and Challener

Petitioner argues that “Kesanupalli discloses the authentication techniques espoused by the ’512 patent.” Pet. 18. Petitioner contends that an ordinarily skilled artisan “would have understood Kesanupalli’s techniques are achieved through [general or specialized] processor(s) executing the described functions including those of sensor 204 . . . and Host PC 202. *Id.* at 18–19 (citing Ex. 1003 ¶¶ 74–79; Ex. 1006, 5:62–64, 6:11–17, 6:28–49, 9:58–10:12). Petitioner next contends that Challener is an example of a “Trusted Platform Module (TPM) security architecture” that is “based on specifications from Trusted Computing Group (TCG)” and is a

“well-known platform for implementing secure systems and for securely handling sensitive information.” *Id.* at 19 (citing Ex. 1003 ¶¶ 45–51, 77).

Petitioner argues that an ordinarily skilled artisan “would have been motivated to apply Challenger’s teachings of a TPM-type security architecture to Kesanupalli’s techniques to provide a security processor . . . in a secure portion communicating with a general processor . . . in a standard portion with API-mediated interfaces of the second processor in between.” *Id.* at 21 (citing Ex. 1003 ¶¶ 80–84), 23–24 (“Challenger’s description of its TPM-based security architecture includes *both* secure storage (nonvolatile memory 28) for secure data . . . *and* fingerprint reader 24 behind a security processor 26 that ‘implements the particular security features and functions (e.g., API functions, algorithms)’ in a system that includes secure and non-secure portions.” (citing Ex. 1007, 3:67–4:23, 4:57–5:9)). According to Petitioner, the “combination would have produced the obvious, beneficial, and predictable results of a standardized and widely-deployed security architecture (TPM) for implementation of Kesanupalli’s techniques.” *Id.* at 21.

Petitioner next contends that an ordinarily skilled artisan would have had a reasonable expectation of success in combining Kesanupalli and Challenger because “TPMs were well-known, standard and widely-deployed in the industry” and Kesanupalli “suggests the use[] of specialized processors.” Pet. 24 (citing Ex. 1003 ¶¶ 51, 84; Ex. 1006, 9:64–10:1; Ex. 1007, 1:18–31).

Motivation to Combine Kesanupalli, Challenger, and Cheng

Petitioner contends that an ordinarily skilled artisan “would have been motivated to apply Cheng’s teachings of backing-up data of a device, such

as the data of Kesanupalli’s device including biometric information and credentials for user authentication.” Pet. 24 (citing Es. 1003 ¶¶ 85–91). Petitioner further contends that “because Kesanupalli’s stored biometric information and credentials are personal data,” an ordinarily skilled artisan would have been motivated to employ Cheng’s backup technique. *Id.* at 25 (citing Ex. 1003 ¶ 88).

Petitioner next contends that because Cheng is “pertinent to known risks of theft and loss of devices and recovery of data that [a person of ordinary skill in the art] would have been motivated to address by combining Cheng with Kesanupalli/Challenger.” Pet. 26. Petitioner argues that “Cheng provides a benefit of the desired back up of personal data [such as biometric information and secret keys] to provide access to it in other user devices in a ‘reliable and secure way[.]’” *Id.* (citing Ex. 1003 ¶ 90).

Petitioner next contends that an ordinarily skilled artisan would have had a reasonable expectation of success because “[a]dding a backup feature would merely have been applying a known technique to a known device (method, or product) ready for improvement to yield predictable results.” *Id.* at 27 (citing Ex. 1003 ¶ 91).

Patent Owner’s Contentions

Patent Owner provides four contentions addressed to motivation to combine and reasonable expectation of success. Prelim. Resp. 36–56.

i. Sufficiency of Petitioner’s Expert Declaration

Patent Owner contends that we should give no weight to the testimony of Dr. McDaniel in connection with Petitioner’s motivation-to-combine and reasonable-expectation-of-success contentions. Prelim. Resp. 36. In support of this contention, Patent Owner provides a table reproducing side-by-side

various statements from pages 22–27 of the Petition with paragraphs 81 and 91 (as allegedly representative of paragraphs 81–91) of Dr. McDaniel’s declaration testimony. *Id.* at 37–41. Patent Owner argues that Dr. McDaniel’s cited testimony “is nearly identical to the analysis in the Petition.” *Id.* at 37. According to Patent Owner, the “Board has previously held in situations like this when an expert adds nothing beyond what is already found in the Petition, that the expert testimony should be given little to no weight.” *Id.* at 41 (citing *RightQuestion, LLC*, Paper 17 at 24).

For the following reasons, this contention is unavailing based on the present evidentiary record.

In *Xerox Corp. v. Bytemark, Inc.*, IPR2022-00624, Paper 9, 15–17 (PTAB Aug. 24, 2022) (precedential), the Board accorded “little weight” to declaration testimony that contains a *verbatim* restatement of a petition’s arguments without additional supporting evidence or reasoning. In *Xerox*, the Board held that the critical inquiry is whether a declaration is conclusory and unsupported and whether it discloses underlying facts or data on which the opinion is based. *Xerox*, Paper 9 at 15 (quoting 37 C.F.R. § 42.65(a) (“Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight.”)); *see also RightQuestion*, Paper 17 at 23 (“Petitioner’s declarant makes these same statements verbatim, without more, and with no additional citations to evidence.”).

Patent Owner ignores Dr. McDaniel’s testimony summarizing the relevant disclosures from Kesanupalli, Challener, and Cheng. Ex. 1003 ¶¶ 61–73. Patent Owner also ignores Dr. McDaniel’s testimony of the specific basis for his opinion that a person of ordinary skill in the art would have

been motivated to combine Kesanupalli and Challener with a reasonable expectation of success. Ex. 1003 ¶¶ 74–80. This testimony contains specific detailed citations to the references in support of Dr. McDaniel’s opinions.

We, thus, find that Dr. McDaniel’s testimony, taken as a whole, in support of the Petition is supported sufficiently at this stage of the proceeding. Consequently, we do not give his testimony little to no weight because portions of it are repeated in the Petition.

ii. Kesanupalli and Challener Combination

Patent Owner contends that an ordinarily skilled artisan “would not have been motivated to combine Kesanupalli’s system with Challener’s TPM disclosures because Kesanupalli’s system would expose a user’s biometric data that Challener would want to keep in the ‘secure portion’ to the ‘standard portion’ (aka the non-secure portion).” Prelim. Resp. 42.

Patent Owner argues Petitioner acknowledges that “Challener has crafted this architecture to avoid disclosing the biometric information such as the biometric template, to the non-secure portion (i.e., ‘standard portion 16’).” Prelim. Resp. 44 (quoting Pet. 38). Patent Owner argues that the benefit of using Challener’s architecture is defeated by Kesanupalli because in Kesanupalli, “the user’s *biometrics* are being provided to the browser extension.” *Id.* at 44–45 (reproducing Kesanupalli’s Figure 11). Patent Owner argues that an ordinarily skilled artisan would have understood “that the browser extension of Kesanupalli would have been operating as part of the browser” which “would operate in the standard portion of Challener.” *Id.* at 45 (citing Ex. 1006, 7:33–37, Fig. 6; Ex. 1007, 5:15–25.). According to Patent Owner, “when the enrollment process described in Kesanupalli

Figure 11 above is run, the browser extension running in the standard portion would have access to the user's biometric templates and information" which would be "contrary to Challenger's purpose of segregating the 'secure' and 'standard' portions of system 10." *Id.* at 46. Patent Owner further argues that an ordinarily skilled artisan "reading Challenger and its segregation of data would not be motivated to add Kesanupalli and its open disclosure of user's biometrics to the standard portion of the device." *Id.* at 47.

In the Preliminary Reply, Petitioner argues that Patent Owner's contention "rests on bodily incorporation rather than a combination of teachings." Prelim. Reply 4. Petitioner also argues that "Challenger by API-mediated interfaces, restricts the form of communications between secure and standard portions, but does not prohibit particular communications." *Id.* at 5 (citing Pet. 21, 34–38; Ex. 1003 ¶¶ 69, 80–84).

Patent Owner, in turn, contends that it is not relying on bodily incorporation but rather its "argument goes to why a [person of ordinary skill in the art] would *not* have been motivated to combine the references." Prelim. Sur-reply 3.

For the following reasons, Patent Owner's contention does not undercut Petitioner's showing based on the present evidentiary record at this stage of the proceeding.

Patent Owner bases this contention on cherry picking a statement from page 38 of the Petition that Challenger's "restrictions limit access and thereby protect the functions and data in the security portion of a TPM-based security architecture (*e.g.*, sensor 204 and the secure storage 206) from being misused by an untrusted or malicious program." Prelim. Resp. 44 (emphasis

omitted). This statement needs to be read in context in order to understand its import. This statement in the Petition is based on paragraph 119 of Dr. McDaniel's declaration. *See* Pet. 38. The prior sentence of paragraph 119 explains that "Challener's architecture limits access to security functions and data on the secure processor . . . using TPM standardized techniques, a *restricted interface*." Ex. 1003 ¶ 119. From this, we understand that Petitioner relies on Challener to show that a restricted interface protects data on Challener's secure processor 26 and memory 28 from being misused by a malicious program. *See* Pet. 14 (reproducing Challener Figure 1 with annotations). Patent Owner does not argue that Kesanupalli's browser extension is a malicious program, nor does Patent Owner direct us to disclosure in Challener that secure information is not or should not be shared with Challener's standard portion. Prelim. Resp. 46

Patent Owner also ignores Kesanupalli's disclosure that "the biometric service communicates a response to the random challenge to web server 604 using *a secure communication link*." Ex. 1006, 8:2–4 (emphasis added); *see also* Pet. 33 (reproducing and annotating Figure 12 of Kesanupalli to illustrate secure connection between browser extension and external resource). Likewise, the web site communicates a "secret key to the user's computing device via a secure connection between the Web site and the user's computing device." *Id.* at 4:59–61. This further undercuts Patent Owner's argument concerning lack of a motivation to combine because it shows that Kesanupalli protects data transmitted to and from its standard portion and the external resource by using a secure link.

Finally, Patent Owner's argument that a person of ordinary skill in the art *would not* have been motivated to combine Kesanupalli and Challener is

merely attorney argument. Patent Owner's contention does not directly address Petitioner's stated reasons for combining Kesanupalli and Challener which are supported by Dr. McDaniel's testimony. As just discussed, we find that Dr. McDaniel's testimony is sufficiently supported at this stage of the proceeding.

Based on the present record at this stage of the proceeding, Patent Owner's contention does not undercut Petitioner's showing of why a person of ordinary skill in the art would have combined Kesanupalli and Challener.

iii. Kesanupalli, Challener, and Cheng Combination

Patent Owner contends that "Cheng . . . and Challener fundamentally handle biometric data in different ways and a [person of ordinary skill in the art] would not have combined them due to these differences." Prelim. Resp. 49–50. According to Patent Owner, "[r]ather than put the biometric templates in a secure processing area that is cordoned off from the standard portion, Cheng openly admits there is no need to restrict what can access a user's biometrics because biometrics are 'substantially difficult if not impossible to replicate.'" *Id.* at 52 (citing Ex. 1008 ¶ 46).

In the Preliminary Reply, Petitioner argues that Patent Owner "mistakes differences for conflict where it characterizes Cheng as not needing to store biometrics in a security portion . . . despite the Petition's demonstration that Kesanupalli-Challener teach storage of biometrics." Prelim. Reply 5. Petitioner further contends that "Cheng actually secures such data" by using encryption. *Id.* (citing Pet. 55–58; Ex. 1003 ¶¶ 167, 169).

For the following reasons, Patent Owner's contention does not undercut Petitioner's showing based on the present evidentiary record at this stage of the proceeding.

Cheng discloses an example embodiment where "[a] user's biometric-based authentication device becomes unavailable due to loss, damage, destruction, theft, etc." Ex. 1008 ¶¶ 44–45. Paragraph 46, in its entirety, states:

The user obtains a new biometrics-based authentication device. There is no need to report the unavailability of the old one since it is substantially difficult if not impossible to replicate the user's biometric information due to the nature of each individual's uniqueness.

Ex. 1008 ¶ 46.

Contrary to Patent Owner's assertion (Prelim. Resp. 52), paragraph 46 of Cheng does not "admit[] there is no need to restrict what can access a user's biometrics." Rather, Cheng states that "[t]he new biometric-based authentication device establishes a *secure connection with a user service bureau*, begins the restore process and downloads backup data from storage." Ex. 1008 ¶ 48. This paragraph shows that Cheng, in fact, places restrictions on access to biometric information. Consequently, the portion of Cheng cited by Patent Owner, when read in context, appears to be of little import to whether a person of ordinary skill in the art would have been motivated to combine Kesanupalli, Challener, and Cheng.

Based on the present record at this stage of the proceeding, Patent Owner's contention does not undercut Petitioner's showing of why a person of ordinary skill in the art would have combined Kesanupalli, Challener, and Cheng.

iv. Reasonable Expectation of Success

Patent Owner contends that Petitioner “failed to show that a [person of ordinary skill in the art] would have had a reasonable expectation of success adding Cheng to the Kesanupalli/Challener system.” Prelim. Resp. 54 (emphasis omitted). According to Patent Owner, “the Cheng backup cannot simply be added to the two-processor architecture [of Challener] without doing more and Petitioner fails to address this.” *Id.* at 56. Patent Owner further argues that “safeguards would need to be put in place so that the data in the secure portion of Challener would not be exposed to the non-secure portion in the backup process” and “[n]either Petitioner nor its expert explain why a [person of ordinary skill in the art] would reasonably believe the data could get from Challener’s secure portion to the backup location securely.” *Id.*

For the following reasons, Patent Owner’s contention does not undercut Petitioner’s showing based on the evidentiary record at this stage of the proceeding.

“[A] conclusion of obviousness requires a reasonable expectation of success.” *Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1365 (Fed. Cir. 2016) (citing *KSR*, 550 U.S. at 421). Further, “the ‘predictable result’ discussed in *KSR* refers not only to the expectation that prior art elements are capable of being physically combined, but also that the combination would have worked for its intended purpose.” *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 567 F.3d 1314, 1326 (Fed. Cir. 2009) (citations omitted).

Patent Owner ignores the safeguards in the backup process relied on by Petitioner. Petitioner contends that it “would have been straightforward

for [a person of ordinary skill in the art] to implement widely practiced porting of code to a TPM environment” for “**generating secure back up** of authentication information.” Pet. 55 (citing Ex. 1003 ¶¶ 158–164; Ex. 1017; Ex. 1008 ¶¶ 2, 23–28; Ex. 1019). Dr. McDaniel’s testimony that “at least by 2006, it was common to securely backup critical TPM data by encrypting the TPM data for external storage and later decryption during a recovery procedure” adequately supports Petitioner’s contention. Ex. 1003 ¶ 160; *see also id.* ¶ 162 (testifying that an ordinarily skilled artisan “would readily implement the techniques in the secure processor by porting the code to the native TPM environment and have a reasonable expectation of success”). Dr. McDaniel’s testimony on this point is supported by Exhibit 1018. *Id.* This evidence is sufficient to show that the combination would have worked for its intended purpose.

Based on the present record at this stage of the proceeding, Patent Owner’s contention does not undercut Petitioner’s showing that a person of ordinary skill in the art would have combined Kesanupalli, Challener, and Cheng with a reasonable expectation of success.

Summary of Motivation to Combine/Reasonable Expectation of Success

For all the foregoing reasons, based on the present record, and after considering all of Patent Owner’s contentions, we find that Petitioner has sufficiently shown that a person of ordinary skill in the art would have been motivated to combine Kesanupalli, Challener, and Cheng with a reasonable expectation of success.

Summary of Claim 1

For all the foregoing reasons, Petitioner establishes a reasonable likelihood that claim 1 would have been unpatentable over Kesanupalli, Challenger, and Cheng.

Claims 11 and 21

For independent claims 11 and 21, Petitioner relies on its contentions for various limitations of claim 1. *See* Pet. 67–71. With respect to the preamble of claim 11 ([11.0]: *A method, comprising:*) and the preamble of claim 21 ([21.0]: *A computer program product embodied in a non-transitory computer readable storage medium and comprising computer instructions for:*), Petitioner argues that to the extent they are limiting, Kesanupalli and Challenger render them obvious. *Id.* at 68–69, 71–72.

Patent Owner does not provide separate arguments for claims 11 and 21 apart from claim 1. *See generally* Prelim. Resp.

We reviewed Petitioner’s evidence and arguments for claims 11 and 21, and for the reasons discussed above with respect to claim 1, determine that Petitioner has shown a reasonable likelihood that claims 11 and 21 would have been unpatentable over Kesanupalli, Challenger, and Cheng.

5. Claims 2–6, 10, 12–16, and 20

These claims depend directly or indirectly from one of claims 1 or 11. Ex. 1001, 11:32–49, 11:61–62, 12:31–47, 12:59–60. Petitioner sets forth evidence and argument as to why Kesanupalli, Challenger, and Cheng allegedly render claims 2–6, 10, 12–16, and 20 unpatentable. Pet. 60–67, 69.

Patent Owner does not provide separate arguments for these claims. *See generally* Prelim. Resp.

We reviewed Petitioner's evidence and arguments and determine that Petitioner has shown a reasonable likelihood that these dependent claims would have been unpatentable over Kesanupalli, Challenger, and Cheng.

III. CONCLUSION

Based on the present record, we determine that Petitioner demonstrates a reasonable likelihood that it would prevail in establishing that at least one challenged claim of the '512 patent is unpatentable. We, thus, institute an *inter partes* review of all challenged claims of the '512 patent based on the ground in the Petition. At this stage of the proceeding, we have not made a final determination under 35 U.S.C. § 318(a) with respect to the unpatentability of any challenged claim.⁸

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that, pursuant to 35 U.S.C. § 314(a), an *inter partes* review of the '512 patent is instituted with respect to challenged claims 1–6, 10–16, 20, and 21 and the ground set forth in the Petition; and

FURTHER ORDERED that, pursuant to 35 U.S.C. § 314(a) and 37 C.F.R. § 42.4(b), *inter partes* review of the '512 patent shall commence on the entry date of this Order, and notice is hereby given of the institution of a trial.

⁸ Patent Owner is cautioned that any arguments not raised in the Patent Owner Response may be deemed waived. *See In re NuVasive, Inc.*, 842 F.3d 1376, 1379–1382 (Fed. Cir. 2016) (holding that a patent owner waived an argument addressed in a preliminary response by not raising the same argument in the patent owner response).

IPR2024-00332
Patent 10,929,512 B1

FOR PETITIONER:

David W. O'Brien
Hong Shi
Kelly Gehrke Lyle
HAYNES AND BOONE, LLP
david.obrien.ipr@haynesboone.com
hong.shi.ipr@haynesboone.com
kelly.lyle@haynesboone.com

FOR PATENT OWNER:

Richard A. Kamprath
George Fishback
McKOOL SMITH, P.C.
rkamprath@mckoolsmith.com
gfishback@mckoolsmith.com