Trials@uspto.gov
571-272-7822

Paper 26
Entered: July 1, 2025

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*.

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
35 U.S.C. § 318(a)

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 ("Pet."). Petitioner filed a Declaration of Dr. Patrick McDaniel in support of the Petition. Ex. 1003. Carbyne Biometrics, LLC ("Patent Owner") filed a Preliminary Response. Paper 7 ("Prelim. Resp."). On July 16, 2024, we instituted this *inter partes* review as to all challenged claims and all grounds presented in the Petition. Paper 10 ("Dec.").

After institution, Patent Owner filed a Response to the Petition (Paper 13, "PO Resp.") supported by a Declaration of Dr. Michael T. Goodrich. Ex. 2037. Petitioner filed a Reply ("Pet. Reply"). Paper 16. Petitioner filed a Supplemental Declaration of Patrick McDaniel with the Petitioner Reply. Ex. 1030. Patent Owner filed a Sur-reply ("Sur-reply"). Paper 17. An oral hearing was held on April 16, 2025, and the transcript is entered into the record. Paper 25 ("Tr.").

We have jurisdiction under 35 U.S.C. § 6. This is a Final Written Decision under 35 U.S.C. § 318(a) as to the patentability of the challenged claims of the '512 patent. For the reasons discussed below, we determine Petitioner establishes by a preponderance of the evidence that all challenged claims are unpatentable.

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.

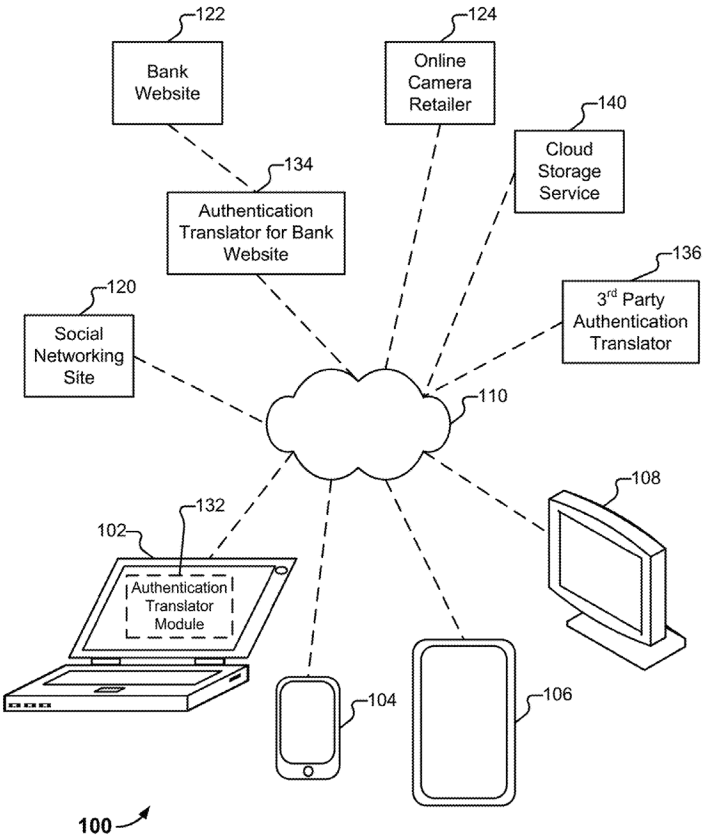


FIG. 1

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.

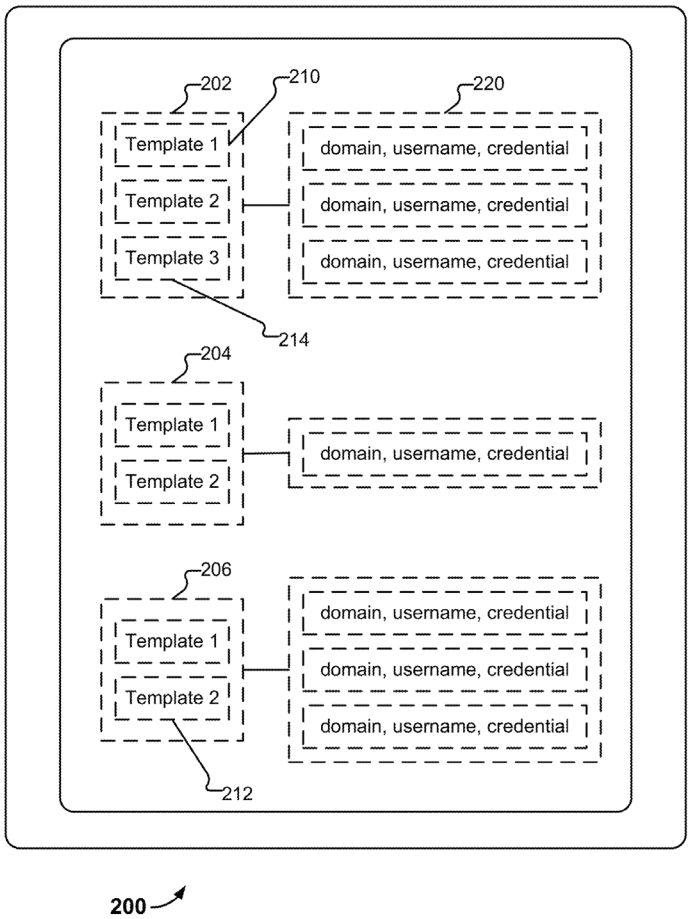


FIG. 2

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.

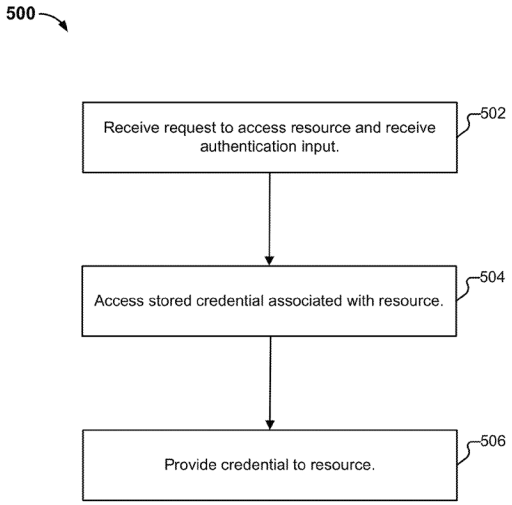


FIG. 5

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. Overview

Petitioner bears the burden of establishing the unpatentability of the challenged claims by a preponderance of the evidence. 35 U.S.C. § 316(e) (2024); 37 C.F.R. § 42.1(d) (2024). This burden of persuasion never shifts to Patent Owner. *Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015).

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

[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").

(i.e., secondary considerations).[5] *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

The Supreme Court explained in *KSR* 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). "[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)).

B. Level of Ordinary Skill in the Art

Petitioner contends that:

[5] No evidence of secondary considerations has been presented.

> 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 has applied Petitioner's definition of the level of skill of a person of ordinary skill in the art. PO Resp. 13.

We apply Petitioner's undisputed level of skill in the art with the exception of the phrase "at least" which injects potential ambiguity into the level of skill, because Petitioner's proposed level of skill appears consistent with the problems addressed in the '512 patent and the prior art.

C. 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 Phillips*, 415 F.3d 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 Intell. 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" because the Patent Owner Response "does not depend on this definition." PO Resp. 13.

Upon review of the complete record before us, we determine that it is not necessary for us to expressly construe any 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)).

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

Petitioner contends claims 1–6, 10–16, 20, and 21 would have been obvious over Kesanupalli, Challener, and Cheng. Pet. 10–72. Petitioner supports its contentions with the Declaration of Dr. Patrick McDaniel. Ex. 1003.

We begin with brief summaries of Kesanupalli, Challener, 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, 3:32–38. 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.

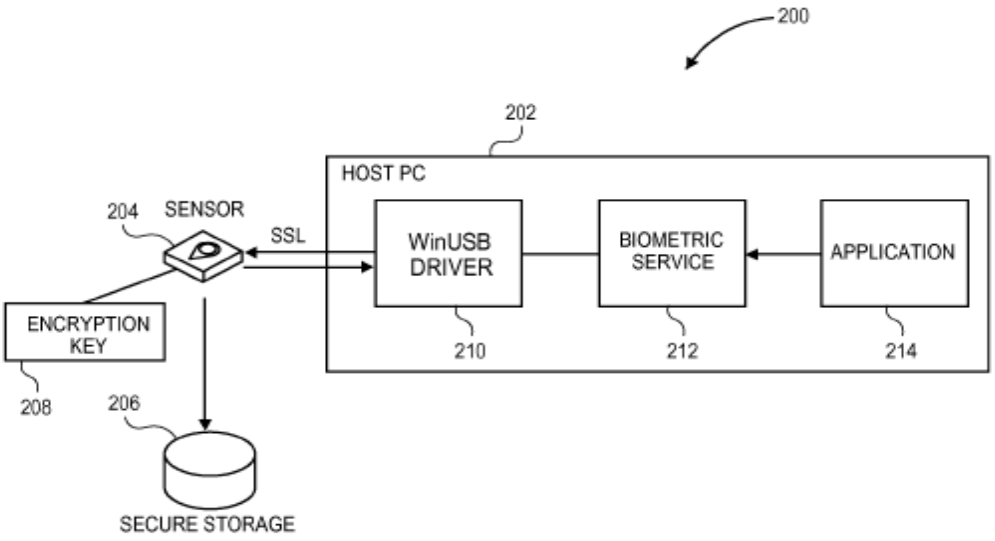


FIG. 2

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. Challener (Ex. 1007)

Challener is titled "Apparatus and Method for Enabling Applications on a Security Processor." Ex. 1007, code (54). Challener'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, Challener 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 Challener is reproduced below.

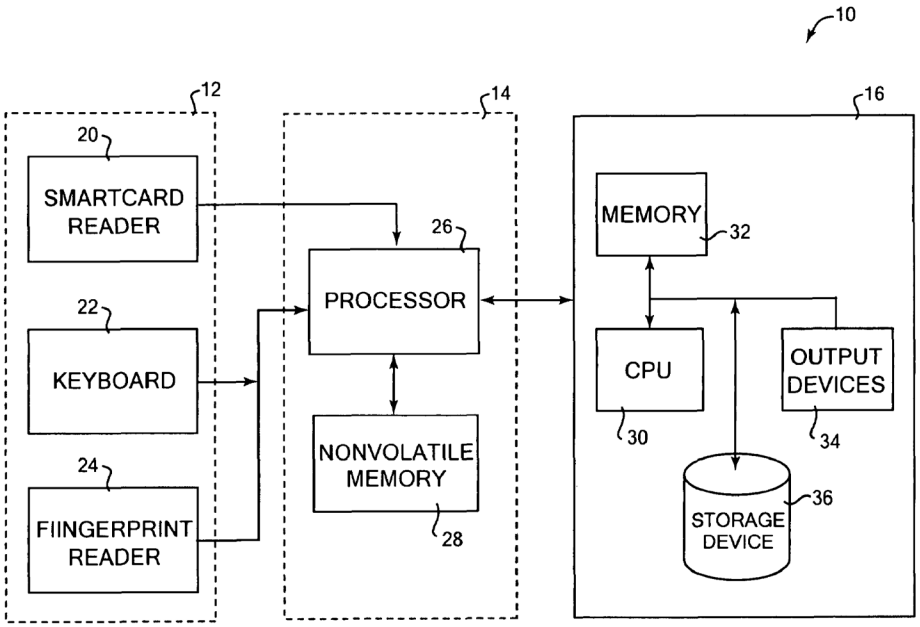


FIG. 1

Figure 1 of Challener 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. Challener 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.

Challener 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.

Challener 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. Challener also describes a "nonvolatile memory 28 . . . included in security portion 14 and . . . connected to the processor 26." *Id.* at 4:57–58. According to Challener, "memory 28 is a secure memory which cannot be easily tampered with to read its data contents." *Id.* at 4:61–63.

Challener'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:

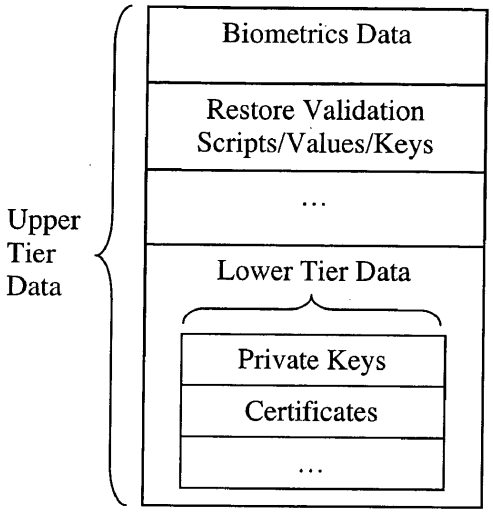


FIG. 1

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." Ex. 1008 ¶ 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, reasons to combine Kesanupalli, Challener, and Cheng, and a reasonable expectation of success in the combination. *Id.* at 21–27.

Patent Owner contends that an ordinarily skilled artisan would not have combined Kesanupalli and Challener to arrive at the claimed two-processor system (PO Resp. 14–16), Kesanupalli is directed to curbing social engineering attacks and would not have benefited from Challener's TPM (*id.* at 16–29), Challener's TPM had drawbacks (*id.* at 29–31), the

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

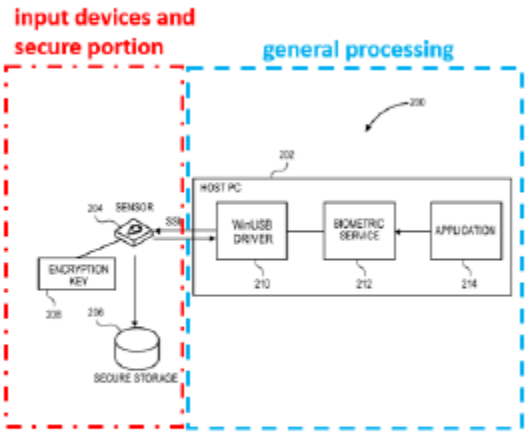
combination of Cheng with Kesanupalli-Challener does not disclose a second processor configured to perform a secure backup (*id.* at 31–35), and an ordinarily skilled artisan would not have reasonably expected the Cheng backup to work with the TPM architecture of the Kesanupalli-Challener combination (*id.* at 35–38).

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

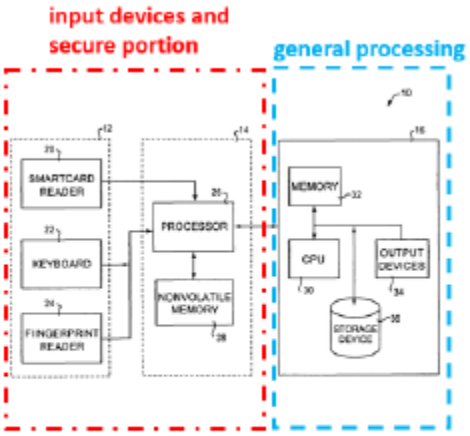
Motivation to Combine Kesanupalli and Challener

Petitioner argues that "Kesanupalli discloses the authentication techniques espoused by the '512 patent." Pet. 18. In particular, Petitioner argues that Kesanupalli's "sensor 204 is capable of receiving and authenticating biometric information and communicating with its secure storage 206, which stores the user credentials and biometric templates, and on successful authentication, releases the user credential." *Id.* (citing Ex. 1006, 6:26–49, Fig. 2). 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 provides the following side-by-side comparison of Figure 2 of Kesanupalli and Figure 1 of Challener with annotations by Petitioner:



Kesanupalli, FIG. 2, Annotated



Challenger, FIG. 1, Annotated

Pet. 20. Figure 2 of Kesanupalli, on the left, is a block diagram illustrating an "example system capable of performing biometric user enrollment and authentication." Ex. 1006, 2:1–2. Figure 1 of Challener, on the right, "is a block diagram illustrating a computer system 10 suitable for use with the present invention." Ex. 1007, 3:7–8. Petitioner annotates each Figure with a broken line red rectangle surrounding certain components on the left with red text "Input devices and secure portions" and a broken line blue rectangle surrounding certain components on the right with blue text "general processing." Pet. 20.

Petitioner argues that both Kesanupalli and Challener involve a first portion, surrounded by the blue rectangles, that execute applications, perform general computing tasks and communicate with external resources. Pet. 20. Further, Petitioner argues that both Kesanupalli and Challener involve a second portion, surrounded by the red rectangles, that "execute function[s] for accepting biometric inputs, performing authentication, and securely storing associated data." *Id.* at 20–21. From this, Petitioner contends that an ordinarily skilled artisan

> would have been motivated to implement Kesanupalli's functionality on Challener's TPM architecture using a specialized security processor (*e.g.*, Challener's security processor 26 including its APIs) to isolate the secure functions of Kesanupalli's sensor 204 and secure storage 206, while hosting on a general processor (Challener's microprocessor 30) the applications and other functions of Kesanupalli's Host PC 202.

Id. (citing Ex. 1003 ¶ 79).

Petitioner argues that an ordinarily skilled artisan "would have been motivated to apply Challener'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." Pet. 21 (citing Ex. 1003 ¶¶ 80–84), 23–24 ("Challener'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 Challener 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).

Patent Owner argues that we are "presented with a unique opportunity to review a reference from a contemporary [person of ordinary skill in the art]—Ramesh Kesanupalli" who, according to Patent Owner, "was certainly aware of TPMs and made a conscious decision to not use them in his patented system." PO Resp. 15 (citing Ex. 2037 ¶ 37); *id.* at 16 (quoting Ex. 2037 ¶ 45).

Patent Owner contends that "Kesanupalli was concerned with addressing social engineering attacks like phishing and spoofed websites" and these attacks do not depend on how securely information is stored on the actual device (such as securing data with a TPM) and instead depend on tricking a user to release their credentials to imposters or bad actors." PO Resp. 16–17 (citing Ex. 1006, 1:35–37; Ex. 2037 ¶ 46); *id.* at 17 ("Tricking the user to release their credentials is typically done through email or text messages containing a link to a fake website that looks legitimate to convince the victim to enter their sensitive information." (citing Ex. 2037 ¶¶ 47–50)); *id.* at 19 ("Bad password practices, such as the ones that Kesanupalli wants to discourage, are more vulnerable to phishing attacks/social engineering attacks." (citing Ex. 1006, 1:37–39; Ex. 2037 ¶ 51)).

Patent Owner next contends that Kesanupalli addressed social engineering attacks by "promot[ing] the use of stronger passwords and it does this by binding credentials on the correct website" so that "a user can store their login information in the safe environment (the fingerprint sensor) and easily use it with a single biometric scan." PO Resp. 19 (citing Ex. 2037 ¶ 52). According to Patent Owner, "a TPM would not have helped avoid social engineering attacks" because such "attacks are not about breaching

the user device and accessing the credentials—presumably protected by a TPM; rather, these attacks are about tricking users to provide their credentials to bad actors or using common techniques . . . which exploit human psychology to gain access to a user's account." *Id.* at 20 (citing Ex. 2037 ¶ 60).

Patent Owner next contends that "the basic architecture of Kesanupalli demonstrates that Kesanupalli is only concerned with social engineering and not breaches to the actual device." PO Resp. 25 (citing Ex. 2037 ¶¶ 46–60). Pointing to Kesanupalli's Figure 11, Patent Owner contends that "the user's *biometrics* are being provided to the browser extension." *Id.* (citing Ex. 1006, Fig. 11; Ex. 2037 ¶ 56). Based on this, Patent Owner contends that an ordinarily skilled artisan would understand that "malware on the device would be able to access the biometrics" indicating that "Kesanupalli was not concerned with bad actors ***breaching the device***" but about "bad actors ***tricking users*** for their credentials." *Id.* at 26 (citing Ex. 2037 ¶ 60).

Patent Owner next contends that Kesanupalli communicates a cryptographic key to a recipient website. PO Resp. 27 (citing Ex. 1006, 3:41–44, 4:3–11; Ex. 2037 ¶ 59). According to Patent Owner, because Kesanupalli's Figure 12 shows that the biometric extension sends the credential to the web server, this also supports its contention that Kesanupalli was not concerned with a breach of the device by a bad actor. *Id.* at 27–28 (citing Ex. 2037 ¶ 59).

Patent Owner next contends that there were drawbacks with using a TPM. PO Resp. 29–31. First, Patent Owner argues that "utilizing a TPM would have introduced compatibility issues with existing systems and

software that did not support TPMs and there were "[m]any security solutions that did not rely on TPMs." *Id.* at 30 (citing Ex. 2037 ¶ 62). Second, Patent Owner argues that because "TPMs were not turned on by default, utilizing TPMs would have required end users to make firmware changes to even enable the TPM to work" and an ordinarily skilled artisan "would not have wanted to further deter users from using the patented system by requiring them to set up and configure a TPM." *Id.* (citing Ex. 2037 ¶ 63).

Petitioner, in turn, argues that Patent Owner does not rebut the sufficiency of Petitioner's evidence concerning motivation to combine. Pet. Reply 2. Petitioner argues that Patent Owner "conjures reasons that Mr. Ramesh Kesanupalli—the individual—did not include a 'TPM' within the text of Kesanupalli—the patent—and argues that its conjured reasoning is determinative of non-obviousness." *Id.* According to Petitioner, "*why* Mr. Ramesh Kesanupalli chose not to include a discussion of TPM within a patent application is unknown" and Patent Owner provides "unsupported conjecture" in this regard. *Id.* at 4. Petitioner argues that the obviousness inquiry proceeds based on the perspective of the hypothetical person of ordinary skill in the art and "[t]he subjective decisions of Mr. Ramesh Kesanupalli . . . even if demonstrated unambiguously . . . are not a stand-in for the legal construct of a" person of ordinary skill in the art. *Id.* at 2–3.

Petitioner next argues that "Kesanupalli's teachings are not constrained to *only* mitigating social engineering attacks." Pet. Reply 6. In support of this contention, Petitioner argues that "two recognized risks—phishing and social engineering attacks—to which [Patent Owner] attempts to constrain <u>all</u> of Kesanupalli's teachings, appear once in the background

discussion." *Id.* Petitioner further contends that Kesanupalli is not limited to addressing social engineering attacks but "broadly discusses authentication systems and methods without constraining their purpose and claims these systems and method without such a limitation." *Id.* at 6–7 (citing Ex. 1006, 10:47–54, 11:5–38; Ex. 1030 ¶¶ 14–22). Petitioner argues that Kesanupalli "facilitates the use of secure, complex passwords by freeing a user from remembering complex passwords . . . by storing a copy of the passwords . . . and biometric information." *Id.* at 7. According to Petitioner, "another risk comes to the fore—breach of the device with the password biometric information store(s)." *Id.* (citing Ex. 1030 ¶ 15).

Petitioner next contends that Kesanupalli discloses "using secure socket layer (SSL) protocol for encrypted transmission of data including between its sensor and general processor, implementing strong cryptographic algorithms in its hardware and/or software, strengthening security by biometric sensor unique identifiers (ID), using cryptographic features of secure keys and hashes." Pet. Reply 8 (citing Ex. 1006, 1:28–30, 4:12–23, 6:39–42, 4:64–5:33; Ex. 1030 ¶¶ 14–22). Petitioner further contends that "Kesanupalli generally discusses providing 'secure transactions,' 'secure application,' and 'secure communication,' with no implication that these are 'secure' *only* with respect to social engineering attacks" as well as disclosing "storage for biometric data and credentials in 'a **secure** storage device.'" *Id.* (citing Ex. 1006, 3:46–51, 5:53–58, 6:6–10, 6:15–17, 6:39–42). According to Petitioner, "Kesanupalli is certainly concerned with breaches to its device—why else place the credentials in a '**secure** storage' of its architecture." *Id.* at 9 (citing PO Resp. 26).

For the following reasons, based on the evidence and arguments presented by Petitioner, we are persuaded that Petitioner establishes that an ordinarily skilled artisan would have been motivated to combine Kesanupalli and Challener with a reasonable expectation of success. Pet. 23–24; Ex. 1003 ¶¶ 48–51, 83.

First, Patent Owner's reliance on what Mr. Ramesh Kesanupalli, the individual, allegedly chose not to include in the disclosure of the Kesanupalli patent reference is unavailing. The question of obviousness is determined from the perspective of a *hypothetical* person of ordinary skill in the art not an actual person who may or may not have been a person of ordinary skill in the art. Ramesh Kesanupalli is one of five named co-inventors on Kesanupalli. Ex. 1006, code (75).[7] Patent Owner's argument, in essence, is an improper request to limit the Kesanupalli reference to just the explicit problems addressed, solutions proposed, and goals achieved by the Kesanupalli reference. However, "[t]he use of patents as references is not limited to what the patentees describe as their own inventions or to the problems with which they are concerned. They are part of the literature of the art, relevant for all they contain." *In re Heck*, 699 F.2d 1331, 1333 (Fed. Cir. 1983) (citing *In re Lemelson*, 397 F.2d 1006, 1009 (CCPA 1968)). We have reviewed all of the cases cited by Patent Owner regarding the determination of obviousness. None of them is at odds with the principle stated in *Heck*.

[7] Patent Owner has not provided evidence demonstrating that Mr. Kesanupalli or the other co-inventors meet the qualifications of a person of ordinary skill in the art as discussed above.

We agree with Petitioner that "[t]he subjective decisions of Mr. Ramesh Kesanupalli, even if demonstrated unambiguously (and they are not), are not a stand-in for the legal construct of a POSITA." Pet. Reply 3. However, even if the subjective intent of one co-inventor had any relevance, there is no record evidence why Mr. Kesanupalli and/or the other co-inventors of the Kesanupalli reference chose not to include a discussion of a TPM or other security issues in their patent application. The record contains no testimony from Mr. Kesanupalli or any of the other co-inventors.

Patent Owner's argument about Mr. Kesanupalli's subjective intent rests on Dr. Goodrich's testimony. PO Resp. 16 (citing Ex. 2037 ¶¶ 46–60). Dr. Goodrich, however, testified that he has "not . . . met [Mr. Kesanupalli] but is "familiar with his work, his achievements, his reputation." Ex. 1031, 68:8–20. His declaration testimony under the category titled "Ramesh Kesanupalli deliberately chose not to use a TPM" (Ex. 2037, 24) is mere speculation as to Mr. Kesanupalli's intent.

We now turn to Patent Owner's argument that "Kesanupalli was concerned with addressing social engineering attacks like phishing and spoofed websites" and such "concerns are not addressed by a TPM." PO Resp. 16 (citing Ex. 1006, 1:35–37; Ex. 2037 ¶¶ 46–60). Apart from the speculation concerning the subjective intent of Mr. Kesanupalli, Patent Owner directs us to a statement in the background of Kesanupalli that "[a]lthough passwords are commonly used to authenticate users, passwords are subject to various attacks, such as phishing attacks, social engineering attacks, dictionary attacks and the like." Ex. 1006, 1:35–38. However, similar to what is discussed above concerning Mr. Kesanupalli's intent, this

argument is an improper attempt to limit Kesanupalli to a problem explicitly addressed in the patent.

Contrary to Patent Owner's assertion that Kesanupalli is limited to addressing social engineering attacks, Kesanupalli reveals an interest and concern in areas outside of thwarting social engineering attacks, (1) by noting that "any person can access the user's Web-based accounts and information if they gain knowledge of the user's password and username" (Ex. 1006, 1:44–46), (2) by identifying malware attacks in the form of "Man in the Browser" as a potential threat associated with user passwords (*id.* at 1:47–58), and (3) by encrypting user credentials and storing the encrypted credentials in a secure storage (*id.* at 6:6–8).

We agree with Petitioner's reasoning as reproduced below:

> [Risk of device breach] is one reason Kesanupalli describes numerous specific security features that are not focused exclusively on social engineering attacks or on promoting stronger passwords. Rather, these security features focus on protecting passwords, other credentials such as cryptographic keys, and biometric information from compromise while held in its device and during communication. For example, Kesanupalli discusses using secure socket layer (SSL) protocol for encrypted transmission of data including between its sensor and general processor, implementing strong cryptographic algorithms in its hardware and/or software, strengthening security by biometric sensor unique identifiers (ID), using cryptography features of secure keys and hashes, and so on. APPL-1036, ¶¶17-18 (citing APPL-1006, 1:28-30, 6:39-42, 4:12-23, 4:64-5:33).[] In perhaps a plainest example, Kesanupalli provides that its storage for biometric data and credentials in "a **secure** storage device." APPL-1006, 3:46-51, 6:6-10. Thus, Kesanupalli is certainly concerned with breaches to its device—why else place the credentials in a "**secure** storage" of its architecture. *See* POR, p. 26. Any one of these features shows that Kesanupalli is concerned with security as a whole, including device security.

Reply 7–8 (footnote omitted).

Dr. McDaniel testifies:

> Kesanupalli is concerned with protection of user credentials (e.g., passwords and cryptographic keys) and biometric information in secure storage. For example, Kesanupalli describes that all user data is securely stored outside of the browser in a secure storage device: "The enrolled credentials of a user are encrypted with the encryption key and stored in a storage device. Such as secure storage 106."

Ex. 1030 ¶ 16.

> Kesanupalli addresses numerous security features not constrained to a social engineering purpose. Kesanupalli generally discusses providing "secure transactions," "secure application," and "secure communication," with no implication that these are "secure" *only* with respect to social engineering attacks. APPL-1006, 5:53-58, 6:15-17, 6:39-42. As one example, Kesanupalli discloses using secure socket layer (SSL) protocol for encrypted transmission of data including between its sensor and general processor. *See* APPL-1006, 1:28-30, 6:39-42. This addresses attacks in which the communication between process (programs) in an operating system can be compromised (addressing IPC eavesdropping attacks). Further, Kesanupalli discloses implementing strong cryptographic algorithms in its hardware and/or software which prevent compromise of data when stored (sometimes called offline or data-store attacks) or communicated between hosts and system components (eavesdropping attacks). *See* APPL-1006, 4:12-23. Further cryptography examples include using cryptography features of secure keys and hashes of the secure key, random challenge sensor ID, and the like. *See* APPL-1006, 4:64-5:33. These methods further strengthen communication and storage security . . . as well as providing data freshness . . . As another example, strengthening security by biometric sensor unique identifiers (ID), which makes bypassing biometric system authentication (often called masquerading attacks) very difficult. *See* APPL-1006, 4:23–30.

Id. ¶ 17.

> As . . . another example, Kesanupalli uses digitally signed code and runtime checks for protection against man-in-the-browser attacks and malware. This prevents adversaries from replacing or corrupting the authentication service of Kesanupalli either before or during use. APPL-1006, 8:23-28. These protections are essential in modern systems to prevent attacks against the storage and runtime of running services.

Id. ¶ 18.

We credit the above-quoted testimony of Dr. McDaniel as it is based on the disclosure of Kesanupalli when considered in its entirety. That in Kesanupalli's system, user biometrics and other credentials, such as a cryptographic key, may be sent to the browser extension in the general processor does not undermine Dr. McDaniel's testimony. Kesanupalli does not have to be free of all vulnerabilities to be regarded as having an interest in device security. Further, Dr. McDaniel testified that Kesanupalli "uses digitally signed code and runtime checks for protection against man-in-the-browser attacks and malware." Ex. 1030 ¶ 18 (citing Ex. 1006, 8:23–28). For these reasons, we credit Dr. McDaniel's testimony.

Second, even assuming that Kesanupalli's only goal and interest is to thwart social engineering attacks, Patent Owner incorrectly limits the usefulness of the Kesanupalli reference to just the problem addressed, solutions proposed, and the goals achieved by the reference's disclosures. Such a reading of Kesanupalli is misplaced and inappropriate. A prior art reference must be considered for everything it teaches by way of technology and is not limited to the particular invention it is describing and attempting to protect. *EWP Corp. v. Reliance Universal Inc.*, 755 F.2d 898, 907 (Fed. Cir. 1985).

Patent Owner's argument that "utilizing a TPM would have introduced compatibility issues with existing systems and software that did

not support TPMs" (PO Resp. 30) is not persuasive for the following reasons. Previous adoption in some commercial products of TPM is not a requirement for establishing obviousness of using TPMs, much less universal previous adoption of TPM in all commercial products. Dr. Goodrich, Patent Owner's expert, acknowledges that "TPMs were supported in Windows 7 and Windows 8. However, many features that used TPMs made TPMs optional as opposed to required." Ex. 2037 ¶ 63. These facts support and do not undercut Petitioner's facts and reasoning that one of ordinary skill in the art would have been motivated to incorporate Challener's TPM teachings in Kesanupalli's system.

We also have considered Patent Owner's argument that because preexisting systems provided TPM, not by default but by user activation, one of ordinary skill in the art who is "aiming to address the risk of social engineering" would not have wanted to further deter users by requiring them to set up and configure a TPM. PO Resp. 30. This argument is unavailing for four reasons. First, as we have explained above, one of ordinary skill in the art is a hypothetical person who reads Kesanupalli for all of its technical disclosures and is not limited solely to the problems addressed, solutions provided, and the express goals of Kesanupalli. Second, as we also explained above, Kesanupalli is not solely interested in defending against social engineering attacks but is also concerned with device security. Third, Petitioner has not proposed to add TPM to Kesanupalli only as an optional feature that requires user activation via some complicated procedure. Fourth, even if user activation is required to configure TPM for use, that inconvenience does not sufficiently undermine Petitioner's articulated reasons for incorporating into the disclosed system of Kesanupalli the

teachings of Challener regarding the use of a TPM. "[A] given course of action often has simultaneous advantages and disadvantages, and this does not necessarily obviate motivation to combine." *Medichem, S.A. v. Rolabo, S.L.*, 437 F.3d 1157, 1165 (Fed. Cir. 2006).

With respect to reasonable expectation of success, we note that Patent Owner does not address Petitioner's reasonable expectation of success arguments and evidence for the Kesanupalli-Challener combination. *See* PO Resp. 14–38. We have reviewed Petitioner's evidence and arguments and find that Petitioner establishes that an ordinarily skilled artisan would have had a reasonable expectation of success "implementing Kesanupalli's biometric authentication techniques in Challener's TPM-based architecture, as TPMs were well-known, standard and widely deployed in the industry." Pet. 24; Ex. 1003 ¶¶ 51, 84.

We have reviewed Petitioner's evidence and arguments in light of Patent Owner's evidence and argument and find that Petitioner establishes that an ordinarily skilled artisan would have been motivated to combine Kesanupalli and Challener with a reasonable expectation of success. Pet. 23–24; Ex. 1003 ¶¶ 48–51, 81–84.

Motivation to Combine Kesanupalli, Challener, 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 Ex. 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/Challener." 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) (second alteration in original). Petitioner further argues that "Cheng specifically teaches backing-up personal data related to biometric information and secret keys" that is "just like the data stored in Kesanupalli's device." *Id.* (citing Ex. 1006, 3:32–51; Ex. 1008 ¶¶ 7–9).

Patent Owner does not address Petitioner's reasons and evidence why an ordinarily skilled artisan would have been motivated to combine the teachings of Kesanupalli-Challener with Cheng. PO Resp. 14–38.

After reviewing Petitioner's evidence and explanation, we find that Petitioner establishes that an ordinarily skilled artisan would have been motivated to combine the teachings of Cheng with the Kesanupalli-Challener combination. Ex. 1003 ¶¶ 85–91.

iv. Reasonable Expectation of Success

Petitioner 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." Pet. 27 (citing Ex. 1003 ¶ 91).

Patent Owner contends that Petitioner does not prove that a person of ordinary skill in the art would have had a reasonable expectation of success. PO Resp. 37. According to Patent Owner, Petitioner's reason for the combination, i.e., adding a backup feature would merely have been applying a known technique to a known device ready for improvement to yield predictable results, is insufficient because "the point of a TPM is to restrict access to its contents and Petitioner is attempting to open up access to that TPM." *Id.* at 37–38.

For the following reasons, Patent Owner's contention is unavailing.

"[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) (alteration in original). 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).

Patent Owner does not address 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"). We credit Dr. McDaniel's testimony on this point because it is supported by Exhibit 1017 and Exhibit 1018. *Id.* This evidence shows that an ordinarily skilled artisan would have had knowledge of the techniques described in Exhibits 1017 and 1018 and, thus, had a reasonable expectation of success, i.e., the combination of Cheng with Kesanupalli and Challener would have worked for its intended purpose of performing a secure backup of a record to a storage service.

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 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.

Claim 1

[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.* at 27–28):

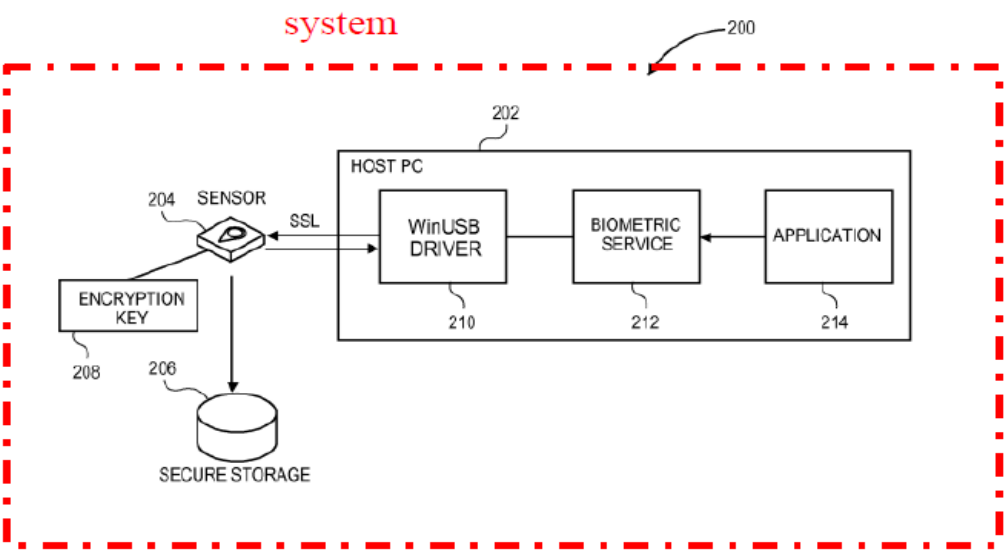


Figure 2 is a block diagram of an "example system." Ex. 1006, 2:1–2. Petitioner adds a red broken-line rectangle around Figure 2 with the word "system." According to Petitioner, an ordinarily skilled artisan would have applied Challener's "known architecture . . . to Kesanupalli . . . to form the *system*." *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* PO Resp.

We reviewed Petitioner's evidence and explanations for the preamble and find that the combination of Kesanupalli and Challener teaches 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 Challener 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 webservers." 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 Challener" 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 Challener 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. *See generally* PO Resp.

We reviewed Petitioner's evidence and explanations for this limitation and find that the combination of Kesanupalli and Challener teaches this limitation.

[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 Challener 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 provides the following annotated version of Kesanupalli's Figure 12 (Pet. 33):

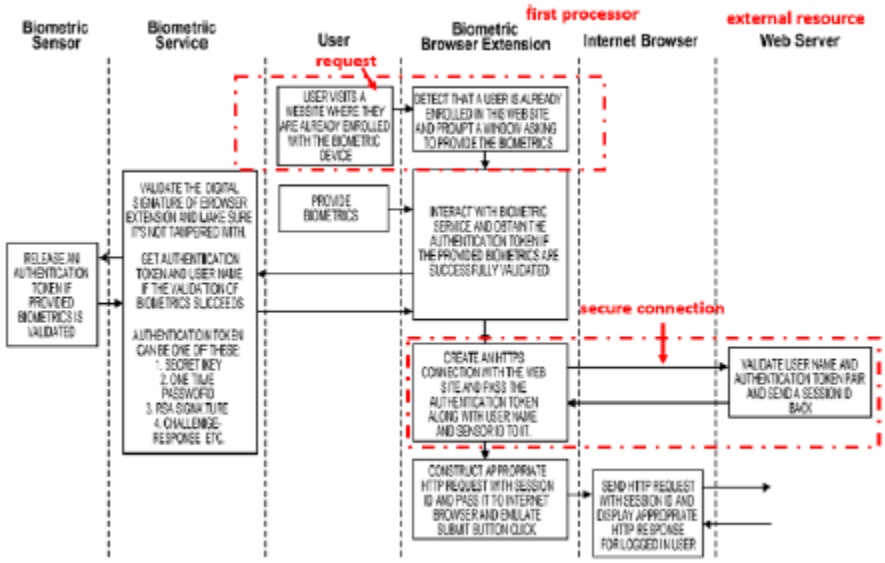


Figure 12 is a block diagram illustrating "a procedure for identifying and authenticating a user of a biometric authentication system." Ex. 1006, 2:22–24. Petitioner adds red rectangles in broken lines with associated text identifying where it contends Figure 12 shows a "request," a "first processor," 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* PO Resp.

We reviewed Petitioner's evidence and explanations for this limitation and find that the combination of Kesanupalli and Challener teaches this limitation.

[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 API[8] 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

[8] As used herein, "API" refers to an application programming interface.

TPM standard for access to the security portion of the system." *Id.* at 37 (citing Ex. 1003 ¶¶ 51, 117–119).

Petitioner next contends that using Challener'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* PO Resp.

We reviewed Petitioner's evidence and explanations for this limitation and find that the combination of Kesanupalli and Challener teaches this limitation.

[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 Challener 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) (emphasis omitted).

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

We reviewed Petitioner's evidence and explanations for this limitation and find that the combination of Kesanupalli and Challener teaches this limitation.

[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 an 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* PO Resp.

We reviewed Petitioner's evidence and explanations for this limitation and find that the combination of Kesanupalli and Challener teaches this limitation.

[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 Challener 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* PO Resp.

We reviewed Petitioner's evidence and explanations for this limitation and find that the combination of Kesanupalli and Challener teaches this limitation.

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

Petitioner contends that the combination of Kesanupalli and Challener 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 an ordinarily skilled artisan "would have implemented the sensor 204 functions using a *second processor* according to the TPM-based architecture of Challener," 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* PO Resp.

We reviewed Petitioner's evidence and explanations for this limitation and find that the combination of Kesanupalli and Challener teaches this limitation.

[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 Challener 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) (alteration in original). 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 TSL) 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 53–54 (citing Ex. 1003 ¶¶ 154–155; Ex. 1006, 5:22–24, Fig. 12).

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

We reviewed Petitioner's evidence and explanations for these limitations and find that the combination of Kesanupalli and Challener teaches these limitations.

[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, Challener, 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 "it would have been obvious for the *second processor* (sensor 204 functionality implemented on Challener's secure processor 26 in its TPM-based system) to be configured to implement Cheng's technique and thus, for the second processor to perform a secure backup." Pet. 54–55 (citing Ex. 1003 ¶¶ 158–164). Petitioner further contends that an ordinarily skilled artisan "would have been motivated to configure the *second processor* to perform the backup process of Cheng because the secure backup is directed to the kind of data (user authentication information, electronic identity, etc.) that underlie security functions of the device" which, according to Petitioner, an ordinarily skilled artisan "would want to isolate from insecure processes and potential attacks, and the relevant records for backup are disposed in the secure storage accessible only by the second processor." *Id.* at 55 (citing Ex. 1003 ¶¶ 158–164). According to Petitioner, "[t]his was a common arrangement prior to the '512 patent, and would have been straightforward for a [person of ordinary skill in the art] to implement including widely practiced porting of code to a TPM environment." *Id.* (citing Ex. 1003 ¶¶ 158–164; Ex. 1017; Ex. 1019).

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.'" *Id.* at 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 the Kesanupalli-Challener combination with 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).

Patent Owner contends that the combination of Kesanupalli, Challener, and Cheng "does not disclose a 'second processor configured to' . . . 'perform a secure backup of the record to a storage service." PO Resp. 32. Patent Owner further contends that "there is no disclosure that the TPM/Sensor of Kesanupalli/Challener is the processor *performing* the secure backup *to* a storage service." *Id.* at 33. Patent Owner argues that "one of the main reasons Petitioner believes that a [person of ordinary skill in the art] would have combined Kesanupalli/Challener is because the TPM of Challener is isolated so as to keep its contents secure." *Id.* (citing Pet. 21; Ex. 2037 ¶ 67). But, according to Patent Owner, "[t]he TPM/Sensor is isolated and it is not connected to any external storage service—the only thing it can do is communicate with the 'general' processor, which would then be the processor 'performing' any secure backup '*to* a storage service.'" *Id.* (citing Ex. 2037 ¶ 66).

Patent Owner next contends that because Kesanupalli's sensor 204 "connects *only* to the Host PC 202 via SSL connection . . . even if Cheng is added, the TPM/Sensor of Kesanupalli/Cheng is not the processor that will be backing up anything 'to' a storage service as it is only connected to the Host PC via the SSL connection." PO Resp. 34 (citing Ex. 2037 ¶ 67).

Patent Owner next contends that "[t]o the extent that Petitioner argues that the second processor does not need to be the processor doing the backup 'to' the storage service to 'perform the secure backup', Petitioner is incorrect." PO Resp. 34 (citing Ex. 2037 ¶ 68–69). Patent Owner contrasts limitation 1.6B, which "requires the second processor to '*facilitate* a login of the user to the external resource," with the "perform a secure backup of the record to a storage service" of limitation [1.7a]. *Id.* at 34–35 (citing Ex. 2037 ¶¶ 68–69). Patent Owner points to this differing language to support its argument that "the second processor needs to *perform* a secure backup of the record up 'to' a storage service." *Id.* at 35.

Petitioner, in turn, repeats its contention from the Petition that an ordinarily skilled artisan "would have been motivated to configure the *second processor* to perform the backup process of Cheng." Pet. Reply 18 (citing Pet. 54–47; Ex. 1003 ¶ 157). Petitioner directs us to Dr. McDaniel's testimony concerning "specific implementation details." *Id.* (citing Ex. 1003 ¶¶ 157–175). Petitioner points to specific testimony by Dr. McDaniel "that 'an import management function of TPM-based systems was commonly used for back up and recovery of TPM data" and notes Dr. McDaniel provides an example of a whitepaper discussing TPM back up. *Id.* at 18–19 (citing Ex. 1003 ¶ 160; Ex. 1018, 4). Petitioner also directs us to Dr. McDaniel's description of "the process for porting code to the TPM to provide the configuration of the second processor to perform the backup." *Id.* at 19 (citing Ex. 1003 ¶¶ 160–162).

Petitioner next contends that "Cheng states an onboard microprocessor of the biometric-based authentication device performs the backup." Pet. Reply 19 (citing Pet. 59; Ex. 1003 ¶ 173; Ex. 1008 ¶ 22).

According to Petitioner, this disclosure in Cheng suggests to an ordinarily skilled artisan "that the processor that authenticates against stored biometric information—i.e., the *second processor*—also performs the backup." *Id.* (citing Pet. 59; Ex. 1003 ¶ 173).

Petitioner next contends that "a desire to preclude unauthorized access or to restrict access to the data does not preclude a TPM or the secure processor of a TPM-based architecture from performing a secure backup," and according to Petitioner, "being restricted or preventing unauthorized access does not mean no interaction with the outside world." Pet. Reply 20 (citing Ex. 1030 ¶¶ 37–39). Petitioner further contends that restricted or unauthorized access "means that outside access is restricted to authorized access, and it would be obvious to perform Cheng's backup technique from within the restricted interface provided by the second processor as it includes security features." *Id.* (citing Pet. 54–58; Ex. 1003 ¶ 169).

Petitioner next contends that "the '512 patent describes that users can interact with an insecure storage, which is associated with the fast processor 304 (*first processor*) communicates with the dedicated processor/sensor (*second processor*) which controls access to the secure storage area 306." Pet. Reply 21 (citing Ex. 1001, 4:4–8). Petitioner further contends that "the '512 patent describes that the sensitive data is within 'an encrypted and authenticated container that can be stored on insecure storage, e.g., on the device, and also backed up (e.g., to a cloud storage service 140 or to an alternate form of external storage.) and "[t]he encryption is performed by the *second processor*." *Id.* at 21–22 (citing Ex. 1001, 3:60–4:26). According to Petitioner, "[t]his means that the backup process involves the record comprising sensitive data that, once encrypted by the *second processor*, is

sent to the insecure storage accessible by the *first processor*." *Id.* at 22 (citing Ex. 1030 ¶ 39); *see also id.* at 23–24 ("PO's attempt to characterize the second processor as performing the secure backup without any communication with the first processor is in conflict with its own patent disclosure." (citing Ex. 1030 ¶¶ 37–39)).

Petitioner contends that "the word 'facilitate' suggests making something easier and Cheng's secure backup technique implemented in the context of a second (secure) processor in the Kesanupalli-Challener combination does far more than simply making secure backup easier." Pet. Reply 25 (citing Pet. 54–57; Ex. 1030 ¶ 41). Petitioner further contends that "PO does not construe 'perform' to preclude involvement of downstream components along the path of the second processor's secure backup to a cloud storage service." *Id.*

In the Sur-reply, Patent Owner argues that Petitioner's arguments in the Petitioner Reply "(1) attempt to broaden the claims via embodiments in the specification; (2) conflate *performing* an action with *facilitating* an action; and (3) are late." Sur-reply 3–4.

For its first argument, Patent Owner contends that "Petitioner does not point to anything in the claims . . . permitting the first processor to be the processor that actually performs the secure backup to the storage service." Sur-reply 4 (emphasis omitted). According to Patent Owner, Petitioner's reliance on Figure 3 of the '512 patent and accompanying description in the specification is an improper attempt to "enlarge[] the scope of this claim and render[] the word perform largely superfluous." *Id.* at 5 (citing Pet. Reply 21). For its second argument, Patent Owner contends that Petitioner "read[s] 'perform' so broadly, the difference between perform and facilitate (used

earlier in the claim) is non-existent." *Id.* at 6. According to Patent Owner, "Petitioner's understanding of perform conveys the exact same idea—namely, that the second processor need not complete the backup, it just needs to start it and help bring about the backup." *Id.* at 7. For its third argument, Patent Owner argues that "[b]y failing to provide a construction for the term 'perform' or suggest its broad understanding in its Petition, Petitioner has waived any argument regarding its meaning." *Id.* at 7–8 (citing 37 C.F.R. § 42.104(b)(3)). Further, Patent Owner argues that it has consistently applied the plain and ordinary meaning of "perform" in this proceeding. *Id.* at 8.

For the following reasons, Petitioner persuades us that the combination of Kesanupalli, Challener, and Cheng teaches limitation 1.7A.

Cheng discloses a method "to securely backup and restore a user's authentication information, electronic identity and any data associated therewith" and using "biometrics, authentication, cryptography, and encryption/decryption." Ex. 1008 ¶ 7; *see also id.* ¶ 22 (portable device 200 includes "a data storage or memory means 204," an encryption/decryption engine 202, and "biometric processing means 201 for enrolling, processing, and comparing biometrics information.") Cheng further discloses "a two-tier backup encryption structure" wherein "lower tier data contain encrypted electronic identity such as private keys and associated certificates" and "upper tier data contain the encrypted lower tier data, restore validation script, and biometrics data." *Id.* ¶ 8. Lower tier data and upper tier data are encrypted using different encryption keys and a "multiple-encrypted backup file is then copied to a storage medium of user's choice." *Id.*

Patent Owner doesn't dispute that Cheng discloses a method of using a processor to securely back-up biometric authentication data like the data disclosed in Kesanupalli. *See* PO Resp. 31–35. Rather, Patent Owner argues that Petitioner has not shown how the combination's second processor is configured to "perform a secure backup of the record." *Id.* at 32–34. Patent Owner's contention is premised on Petitioner's combination of Kesanupalli and Challener alone because in that combination without Cheng, the general processing portion "communicates with external resources." Pet. 20. This contention, however, ignores Petitioner's modification of the Kesanupalli-Challener combination with the teachings of Cheng. *See id.* at 24–27. As discussed above in our motivation to combine analysis, Patent Owner does not dispute Petitioner's contentions that an ordinarily skilled artisan would have been motivated to modify the Kesanupalli-Challener combination with the teachings of Cheng.

As discussed above for limitation 1.1C, Petitioner's combination relies on Challener's security processor 26 as corresponding to the recited "second processor." Pet. 34. For limitation 1.7A, Petitioner contends that it would have been obvious for the "*second processor* ([Kesanupalli's] sensor 204 functionality implemented on Challener's secure processor 26 in its TPM-based system) to be configured to implement Cheng's technique and thus, for the second processor to perform a secure backup." *Id.* at 54–55 (citing Ex. 1003 ¶¶ 158–164). Petitioner supports this contention with the following testimony of Dr. McDaniel:

> POSITA would be motivated to configure the second processor with instructions to perform the backup process of Cheng because the secure backup is directed to the kind of data (user authentication information, electronic identity, etc.) that underlie security functions of the device and which a POSITA would want

> to isolate from insecure portions or processes in a Kesanupalli-Challener type device with backup. In addition, the relevant records for backup are disposed in the secure storage accessible only by the second processor. Thus, using the second (secure) processor to perform Cheng's backup would ensure that the information accessed in the course of the backup procedure (e.g., biometric data and user credentials) is isolated from insecure portions or processes of the device while the resulting backup is reliably available in the presence of failures, theft of devices etc.

Ex. 1003 ¶ 159.

> Indeed, backing up signing data and keys of a TPM (such as the records in secure storage) was well known and widely deployed before the priority date—indeed an import management function of TPM-based systems was commonly used for backup and recovery of TPM data. For example, 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. (Infineon TPM Key Backup and Recovery for Trusted Platforms), [Ex. 1018], p. 3 (describing secure backup protocol elements created by TCG standardization group and implemented by Infineon Professional Package for its TPM implementation). As explained in the Infineon Whitepaper, *TPM Key Backup Recovery for Trusted Platforms*, to overcome the potential loss of keys and certificates in connection with system damage or loss,
>
> …an Emergency Recovery Mechanism is available together with the Infineon TPM professional SW package. This <u>backup</u> and migration capability is one of the cornerstones to allow the user a comfortable use of the applications without the total data loss due to system errors and missing backup support.
>
> …
>
> All these functions are implemented within the Infineon Professional Package which is available as an OEM product and is part of a PC package outfitted with Infineon TPM. This OEM package will be <u>delivered from nearly every PC manufacturers</u>, which integrates and sells trusted Computing (PC)-Platforms based on an Infineon Chip. [Ex. 1018], (p.4, emphasis added).

Ex. 1003 ¶ 160 (alterations in original).

> A POSITA would understand that implementing the backup function of Cheng on the second processor (secure processor 26 of Challener's TPM that also executes secure functions of sensor 204) would protect the process of securely backing up biometric data and user credentials from a myriad of potential attacks including the compromise of standard (insecure) portions of the operating system, main CPU, data in storage, etc. *See* (Challener) [Ex. 1007], 1:18–42. By executing the secure backup using the second processor, the backup procedure would be made substantially more secure, resistant, and in many cases, immune to the vast majority of attacks on computer systems.

Ex. 1003 ¶ 161.

> Providing the second processor (secure processor) configured to perform the secure backup would be straightforward for a POSITA to implement. To the extent that Cheng's techniques are directed to a general-purpose processor, a POSITA 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.

Ex. 1003 ¶ 162.

> To the extent that the Patent Owner argues that the second processor must solely be the performer of the backup procedure, Cheng states an onboard microprocessor of the biometric-based authentication device performs the backup. (Cheng APPL-1008, [0022]. This suggests to a POSITA that the processor performing the authentication method – i.e., the second processor – performs the backup. (Cheng) APPL-1008. A POSITA would also find using the *second processor* to perform the backup both predictable use of the processor and such an instruction would be executed by the processor with a reasonable expectation of success due to the processor's capabilities as discussed above in [1.3]. For example, the *second processor* has access to the records in secured storage and capability to perform the encryption taught by Cheng. (Challener) APPL-1007, FIG. 1, 4:24-36; (Kesanupalli) APPL-1006, 6:42–45. Further the TPM-based architecture provided by Challener provides a standardized interface (API) to implement secure (cryptographically supported) storage of data, e.g., sealed encryption.

Ex. 1003 ¶ 173.

We credit the foregoing testimony of Dr. McDaniel because it is supported by the cited evidence from Kesanupalli, Challener, Cheng, Exhibit 1017, and Exhibit 1018.

Patent Owner's argument that in Petitioner's proposed combination of Kesanupalli-Challener "[t]he TPM/Sensor is isolated and is not connected to any external storage service—the only thing it can do is communicate with the 'general' processor, which would then be the processor 'performing' any secure backup '*to* a storage service'" (PO Resp. 33) is a strawman argument. Petitioner provides evidence and argument, which we find persuasive and which Patent Owner does not dispute, that an ordinarily skilled artisan would have been motivated to modify Kesanupalli-Challener with Cheng so that the second processor is configured to perform the secure backup. Pet. 54–55. Petitioner's contentions and Dr. McDaniel's testimony are not limited to requiring the second processor to communicate the secure backup of a record to the "general processor" as Patent Owner posits. For example, Dr. McDaniel testifies that to the extent that Cheng utilizes a general processor for its backup procedure, in the combination, an ordinarily skilled artisan would have "implement[ed] the techniques in the secure processor by porting the code to the native TPM environment" and "the TPM-based architecture provided by Challener provides a standardized interface (API) to implement secure (cryptographically supported) storage of data, e.g., sealed encryption." Ex. 1003 ¶¶ 162, 173. Dr. McDaniel, thus, describes a scenario where an ordinarily skilled artisan would not involve the general processor in the backup process but would utilize the general processor only if desired. Although if, in fact, an ordinarily skilled artisan chose to involve the general processor, that would not conflict with the disclosure in the '512

patent. *See* Ex. 1001, 4:19–23 ("Profiles and vaults can be updated while in secure storage; if this occurs, they are encrypted and MACed before *being written back to the insecure storage, which may in turn propagate them to external backup storage*.") (emphasis added); *see also* Ex. 1030 ¶¶ 37–39 (Dr. McDaniel testifying to the '512 patent's communication of the backup record by communicating with the general processor.)

Patent Owner conceded at oral argument that:

> there are likely [an] endless amount of ways that you could implement the second processor performing the backup. The second processor, you could have a restricted interface directly to a server or something of that kind that bypasses, or a restricted interface from the second processor to a hard drive or something for storing the credentials.

Tr. 45:16–21. Patent Owner does not argue that any of the "endless amount of ways" or the specific ways stated by counsel for the second processor to "perform" the backup would be beyond the level of skill of an ordinarily skilled artisan to implement. Regardless of whether Petitioner's combination presumes the communication of the secure backup of a record to the general processor or not, Patent Owner's argument is unavailing for the foregoing reasons. Consequently, we need not address Patent Owner's argument that there is a claimed distinction between "performing" a backup as opposed to "initiating" a backup because we determine that Petitioner shows that the second processor is configured to "perform" that secure backup under Patent Owner's construction. Likewise, for the same reasons, we need not reach the question of whether Petitioner waived a claim construction argument by not raising it in the Petition (Sur-reply 7–8) but submitting it in the Reply.

Patent Owner's argument that "Petitioner does not show a *single* application of a TPM backing up it records to a storage service" (PO Resp.

31) overlooks Petitioner's evidence. Dr. McDaniel cites to Exhibit 1018, titled "TPM Key Backup and Recovery for Trusted Platforms," in support of his testimony that "backing up signing data and keys of a TPM (such as the records in secure storage) was well known and widely deployed before the priority date" and "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." Ex. 1003 ¶ 160 (citing Ex. 1018, 3–4). Dr. Goodrich does not dispute Dr. McDaniel's testimony that backing up TPM data was well known in 2006. *See* Ex. 2037 ¶¶ 65–68.

We have reviewed Petitioner's evidence and explanations for this limitation in light of Patent Owner's arguments and evidence and, for the foregoing reasons, find that the combination of Kesanupalli, Challener, and Cheng teaches limitation 1.7A.

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)).

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

We reviewed Petitioner's evidence and explanations for this limitation and find that the combination of Kesanupalli, Challener, and Cheng teaches this limitation.

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 this limitation. *See generally* PO Resp.

We reviewed Petitioner's evidence and explanations for this limitation and find that the combination of Kesanupalli, Challener, and Cheng teaches this limitation.

[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* PO Resp.

We reviewed Petitioner's evidence and explanations for this limitation and find that the combination of Kesanupalli and Challener teaches this limitation.

Summary of Claim 1

For all the foregoing reasons, Petitioner establishes a by a preponderance of the evidence that claim 1 would have been obvious over Kesanupalli, Challener, 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 Challener 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. PO Resp. 39.

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 establishes by a preponderance of the evidence that claim 11 and claim 21 would have been obvious over Kesanupalli, Challener, and Cheng.

5. Claims 2 and 12

Claim 2, depends from claim 1, and recites "wherein the storage service comprises a cloud storage service." Ex. 1001, 11:32–33. Claim 12, depends from claim 11, and contains the same recitation. *Id.* at 12:31–32.

Petitioner contends that the combination of Kesanupalli, Challener, and Cheng teaches claim 2. Pet. 60–61 (citing Ex. 1003 ¶¶ 181–183). Petitioner further contends that "Cheng describes its backup process in terms of a storage service implemented as an 'internet-based storage service'" and an ordinarily skilled artisan "would recognize that an internet-based storage service is a *cloud storage service*." *Id.* (citing Ex. 1003 ¶ 182; Ex. 1008 ¶ 29; Ex. 1021). For claim 12, Petitioner relies on its contentions and evidence for claim 2. *Id.* at 69.

Patent Owner does not dispute Petitioner's contentions that Cheng discloses the recited "cloud storage service." PO Resp. 38–39. Rather, Patent Owner repackages its contentions for claim 1 by arguing that "[o]nly the general processing area of the Kesanupalli system on the host pc would be able to an internet-based storage service." *Id.* at 39 (citing Ex. 2037 ¶ 73). Patent Owner's contentions concerning claims 2 and 12 are unavailing for the same reasons discussed above for claim 1.

We have reviewed Petitioner's evidence and explanations for claims 2 and 12 and find that Cheng discloses the limitations of claims 2 and 12. Consequently, Petitioner establishes by a preponderance of the evidence that claims 2 and 12 would have been obvious over Kesanupalli, Challener, and Cheng.

6. Claims 3 and 13

Claim 3, depends from claim 1, and recites:

> wherein the second device is registered with the storage service at least in part by: connecting to the storage service; and providing at least one of a user identifier or a credential to the storage service, wherein the user identifier comprises at least one of a username or an account number.

Ex. 1001, 11:34–40. Claim 13 depends from claim 11 and contains the same recitation. *Id.* at 12:33–38.

Petitioner contends that the combination of Kesanupalli, Challener, and Cheng teaches claim 3. Pet. 61–63 (citing Ex. 1003 ¶¶ 184–188).

Petitioner reiterates its contentions for limitation 1.6 that "Cheng describes registering the second device . . . with the storage service (referred to as user service bureau) and in doing so the second device *connect[s] to the storage service*." Pet. 61 (citing Ex. 1008 ¶ 48, Fig. 4A) (second alteration in original). Petitioner further contends that Figure 4A "of Cheng shows a user providing the second device with 'user detail(s),' from which the device forms a registration record that it sends through 'Online registration verification' to the service bureau." *Id.* According to Petitioner, "[t]he service bureau then verifies the registration details" and an ordinarily skilled artisan "would understand that 'user details' that provide registration information are a *user identifier* and that a *username* or *account number* is a conventional and obvious example." *Id.* at 62 (citing Ex. 1003 ¶ 187; Ex. 1008 ¶ 32). For claim 13, Petitioner relies on its contentions and evidence for claim 3. *Id.* at 69.

Patent Owner does not address Petitioner's contentions. *See generally* PO Resp.

We have reviewed Petitioner's evidence and explanations for claims 3 and 13 and find that Cheng discloses the limitations of claims 3 and 13. Consequently, Petitioner establishes by a preponderance of the evidence that

claims 3 and 13 would have been obvious over Kesanupalli, Challener, and Cheng.

7. Claims 4 and 14

Claim 4 depends from claim 1 and recites "wherein the record downloaded by the second device is encrypted." Ex. 1001, 11:41–42. Claim 14 depends from claim 11 and contains the same recitation. *Id.* at 12:39–40.

Petitioner contends that the combination of Kesanupalli, Challener, and Cheng teaches claim 4. Pet. 63 (citing Ex. 1003 ¶¶ 189–191).

Petitioner reiterates its contentions for limitation 1.7 that "Cheng discloses a secure backup including a two-tier encryption of the record that is backed-up." Pet. 63. According to Petitioner, Cheng "describe[s] restoring, which is downloading, the record on the second device where the *encrypted* record is downloaded by the second device (*e.g.*, a new user device)." *Id.* (citing Ex. 1008 ¶ 9). For claim 14, Petitioner relies on its contentions and evidence for claim 4. *Id.* at 69.

Patent Owner does not address Petitioner's contentions. *See generally* PO Resp.

We have reviewed Petitioner's evidence and explanations for claims 4 and 14 and find that Cheng discloses the limitations of claims 4 and 14. Consequently, Petitioner establishes by a preponderance of the evidence that claims 4 and 14 would have been obvious over Kesanupalli, Challener, and Cheng.

8. Claims 5 and 16

Claim 5 depends from claim 4 and recites "wherein the encrypted record is stored to an insecure storage associated with the second device."

Ex. 1001, 11:43–45. Claim 16 depends from claim 14 and contains the same recitation. *Id.* at 12:45–47.

Petitioner contends that the combination of Kesanupalli, Challener, and Cheng teaches claim 5. Pet. 64 (citing Ex. 1003 ¶¶ 192–196).

Petitioner contends that "Cheng teaches downloading a record protected under Cheng's two-tier encryption structure" and an ordinarily skilled artisan "would have stored the received (an two-tier encrypted) record in an *insecure storage* of the second device." Pet. 64 (citing Ex. 1003 ¶¶ 193–195). Petitioner further contends that "Challener illustrates a general processing portion includes a storage portion for storing downloaded encrypted data" which, according to Petitioner, an ordinarily skilled artisan would understand "that storage device 36 is insecure storage at least because it is accessible by multiple components." *Id.* at 64–65 (citing Ex. 1003 ¶ 194; Ex. 1007, 5:26–40, Fig. 1). For claim 16, Petitioner relies on its contentions and evidence for claim 5. *Id.* at 69.

Patent Owner does not address Petitioner's contentions. *See generally* PO Resp.

We have reviewed Petitioner's evidence and explanations for claims 5 and 16 and find that Cheng discloses the limitations of claims 5 and 16. Consequently, Petitioner establishes by a preponderance of the evidence that claims 5 and 16 would have been obvious over Kesanupalli, Challener, and Cheng.

9. Claims 6 and 15

Claim 6 depends from claim 4 and recites "wherein the second device is configured to decrypt the downloaded record and store the decrypted record to a secure storage associated with the second device." Ex. 1001,

11:46–49. Claim 15 depends from claim 14 and contains the same recitation. *Id.* at 12:41–44.

Petitioner contends that the combination of Kesanupalli, Challener, and Cheng teaches claim 6. Pet. 65 (citing Ex. 1003 ¶¶ 197–200).

Petitioner contends that "Cheng discloses that the *second device is configured to decrypt the downloaded record*." Pet. 65 (citing Ex. 1009 ¶ 9). Petitioner next contends that both Kesanupalli and Challener "suggest storing personal data in a *secure storage*." *Id.* at 66 (citing Ex. 1006, 6:45–48; Ex. 1007, 4:57–5:9). According to Petitioner, an ordinarily skilled artisan "would have had reason to place data, decrypted with respect to the two-tiered encryption of Cheng, in a *secure storage* that is protected from unauthorized access to prevent 'identity theft and/or unwanted intruders.'" *Id.* (citing Ex. 1003 ¶ 199; Ex. 1008 ¶ 3). For claim 15, Petitioner relies on its contentions and evidence for claim 6. *Id.* at 69.

Patent Owner does not address Petitioner's contentions. *See generally* PO Resp.

We have reviewed Petitioner's evidence and explanations for claims 6 and 15 and find that Cheng discloses the limitations of claims 6 and 15. Consequently, Petitioner establishes by a preponderance of the evidence that claims 6 and 15 would have been obvious over Kesanupalli, Challener, and Cheng.

10. Claims 10 and 20

Claim 10 depends from claim 1 and recites "wherein the cryptographic operation comprises decrypting the record." Ex. 1001, 11:61–62. Claim 20 depends from claim 11 and contains the same recitation. *Id.* at 12:59–60.

Petitioner contends that the combination of Kesanupalli, Challener, and Cheng teaches claim 10. Pet. 66 (citing Ex. 1003 ¶¶ 201–203). Petitioner further contends that "Kesanupalli, as implemented on the architecture of Challener discloses a *second processor* configured to *perform a cryptographic operation*, as discussed above in limitation [1.5], which illustrates *cryptographic operation* is *decrypting* the record." *Id.* (citing Ex. 1003 ¶ 202; Ex. 1006, 6:31–49; Ex. 1007, 4:24–36). For claim 20, Petitioner relies on its contentions and evidence for claim 10. *Id.* at 69.

Patent Owner does not address Petitioner's contentions. *See generally* PO Resp.

We have reviewed Petitioner's evidence and explanations for claims 10 and 20 and find that Kesanupalli teaches the limitations of claims 10 and 20. Consequently, Petitioner establishes by a preponderance of the evidence that claims 10 and 20 would have been obvious over Kesanupalli, Challener, and Cheng.

III. CONCLUSION[9]

Weighing the competing evidence and testimony, we determine that Petitioner establishes by a preponderance of the evidence that claims 1–6, 10–16, 20, and 21 of the '512 patent are unpatentable.

---

[9] Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this decision, we draw Patent Owner's attention to the April 2019 *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding.* *See* 84 Fed. Reg. 16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we

In summary:

Claim(s)	35 U.S.C. §	Reference(s)/ Basis	Claim(s) Shown Unpatentable	Claim(s) Not Shown Unpatentable
1–6, 10–16, 20, and 21	103(a)	Kesanupalli, Challener, Cheng	1–6, 10–16, 20, 21	

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that claims 1–6, 10–16, 20, and 21 of the ’512 patent have been shown by a preponderance of the evidence to be unpatentable; and

FURTHER ORDERED that any party seeking judicial review must comply with the notice and service requirements of 37 C.F.R. § 90.2.

---

remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. *See* 37 C.F.R. § 42.8(a)(3), (b)(2).

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