

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS CO., LTD., and
SAMSUNG ELECTRONICS AMERICA, INC.,
Petitioner,

v.

RIGHTQUESTION, LLC,
Patent Owner.

IPR2022-00251
Patent 10,929,512 B1

Before JAMESON LEE, CHARLES J. BOUDREAU, and
STEPHEN E. BELISLE, *Administrative Patent Judges*.

BELISLE, *Administrative Patent Judge*.

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

I. INTRODUCTION

A. Case Posture

Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc. (collectively, “Petitioner”) filed a Petition (Paper 1, “Pet.”) requesting an *inter partes* review of claims 1–4, 6–15, and 17–21 (“Challenged Claims”) of U.S. Patent No. 10,929,512 B1 (Ex. 1001, “the ’512 patent”). Petitioner identifies itself as a real party in interest. Pet. 2. RightQuestion, LLC (“Patent Owner”) identifies itself as a real party in interest (Paper 6, 2), and timely filed a Preliminary Response to the Petition (Paper 11, “Prelim. Resp.”). In addition, with prior authorization from the Board, the parties filed supplemental briefing concerning the Preliminary Response. Paper 13 (“Reply”); Paper 14 (“Sur-Reply”).

We have authority to determine whether to institute an *inter partes* review. 35 U.S.C. § 314(b) (2018); 37 C.F.R. § 42.4(a) (2021). We may not institute an *inter partes* review “unless . . . there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” 35 U.S.C. § 314(a).

Applying those standards, and upon consideration of the information presented in the Petition and Preliminary Response, we determine that Petitioner has not demonstrated a reasonable likelihood of prevailing with respect to any of challenged claims 1–4, 6–15, and 17–21 of the ’512 patent. *See* 35 U.S.C. § 314; 37 C.F.R. § 42.4(a). Accordingly, constrained by the record before us, we deny institution of an *inter partes* review of the ’512 patent.

B. Related Matters

The parties indicate that the '512 patent is involved in one U.S. district court action, namely, *RightQuestion, LLC v. Samsung Elecs. Co.*, No. 2:21-cv-00238-JRG (E.D. Tex.) (“District Court Case”). Pet. 2; Paper 6, 2.

Patent Owner also indicates that Petitioner requested an *inter partes* review of a patent that issued from a parent application of the '512 patent, namely, U.S. Patent No. 10,824,696 B1 (“the '696 patent”). Prelim. Resp. 1 n.1 (citing IPR2022-00244).

Although not identified by either party under the mandatory notices of 37 C.F.R. § 42.8(b), we note that both the '512 and '696 patents are part of a larger family of continuing applications and patents, including three pending applications. *See, e.g.*, Ex. 1001, code (63).

C. The '512 Patent

The '512 patent is titled “Authentication Translation,” and issued on February 23, 2021, from U.S. Patent Application No. 16/773,767, filed January 27, 2020, and claims priority through a series of continuing applications to U.S. Provisional Patent Applications Nos. 61/587,387, filed January 17, 2012, and 61/569,112, filed December 9, 2011. Ex. 1001, codes (21), (22), (45), (54), (60), (63).

The '512 patent relates generally to authentication techniques to provide credentials to a service. Ex. 1001, 1:35–44. The goal is to reduce user practices such as password re-use and/or selection of poor quality passwords. *Id.* Specifically, the '512 patent pertains to authentication translation and states:

Authentication translation is disclosed. A request to access a resource is received at an authentication translator, as is an authentication input. The authentication input corresponds to at least one stored record. The stored record is associated at least with the resource. In response to the receiving, a previously stored credential associated with the resource is accessed. The credential is provided to the resource.

Id. at code (57). Figure 1 of the '512 patent is reproduced below:

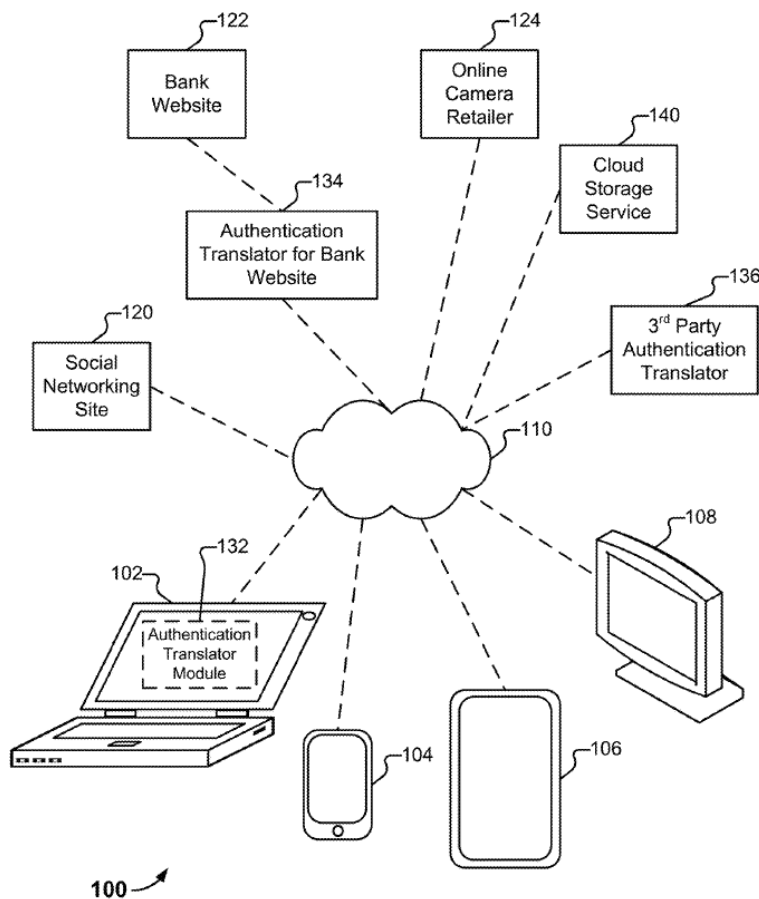


FIG. 1

Figure 1 depicts an embodiment of an environment in which authentication translation is provided.

Id. at 1:51–52, 2:37–38, Fig. 1. As shown in Figure 1 above, various client devices 102–108 are connected through one or more networks (represented

as single network cloud 110) to various services 120–124, which are also referred to as sites. *Id.* at 2:38–42.

In an exemplary embodiment, client device 102 is a notebook computer owned by user “Alice” and includes a camera, a microphone, and a fingerprint sensor. Ex. 1001, 2:42–45. Client device 104 is a smartphone also owned by user Alice and includes a camera. *Id.* at 2:45–46. Client device 106 is a tablet owned by user “Bob” and includes a camera and a fingerprint sensor, and device 106 is sometimes used by Bob’s son “Charlie.” *Id.* at 2:47–49. Client device 108 is a kiosk located in the lobby of a hotel and it includes a camera and a microphone. *Id.* at 2:49–51.

Service 120 is a social networking site; service 122 is a website of a bank; service 124 is the online store of a boutique camera retailer; and each service 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. Ex. 1001, 2:57–62. A user need not type such usernames and passwords into the devices whenever required by a service, but can authenticate to an “authentication translator” which will provide the appropriate credentials to the service on the user’s behalf. *Id.* at 2:62–3:1.

For example, notebook computer 102 includes authentication translator module 132 that provides authentication translation services. Ex. 1001, 3:4–6. Devices 104–108 can also include, but need not include, their own respective authentication translator modules. *Id.* at 3:6–8. The owner of bank website 122 operates authentication translator 134 associated with the bank. *Id.* at 3:8–10. Authentication translator 136 provides authentication services to a variety of businesses, including online camera retailer 124. *Id.* at 3:10–12.

Figure 2 of the '512 patent is reproduced below:

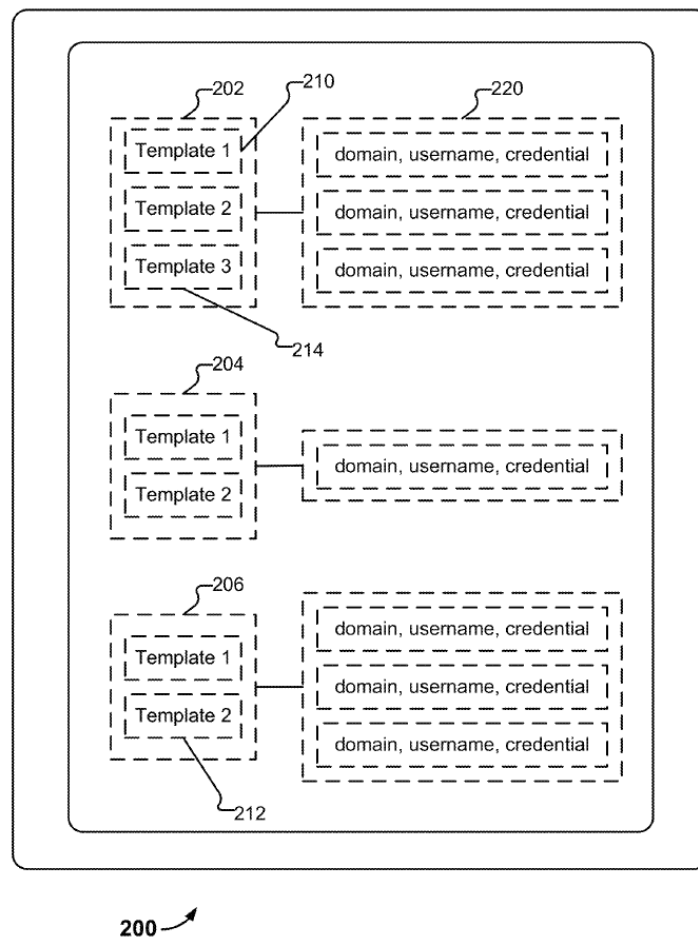


FIG. 2

Figure 2 depicts an embodiment of credential information stored on a device.

Ex. 1001, 1:53–54, 3:13–14, Fig. 2. As shown in Figure 2 above, device 200 stores three user profiles 202–206, each of which contains a username and one or more templates associated with the user. *Id.* at 3:14–17. A template is a collection of biometric features, where a fingerprint is an example of a biometric feature. *Id.* at 3:17–19. A representation of a single fingerprint may be included in multiple templates, such as in different

resolutions in accordance with different protocols, e.g., warm or cold conditions and/or by itself or in combination with multiple fingerprints. *Id.* at 3:18–28. When other biometrics are employed, for example facial recognition, voice print, or retina scan, corresponding features are included in the template. *Id.* at 3:28–31.

Policies can be included in a profile that govern how matches are to be performed. Ex. 1001, 3:45–47. Policies can specify thresholds or tolerances for what constitutes a match, and can specify that different levels of matches can result in different levels of access to different resources. *Id.* at 3:47–50. A profile is associated with a vault, for example vault 220. *Id.* at 3:51. A vault, in turn, contains triples specifying a service provider/domain, a username, and a credential. *Id.* at 3:51–53. The credential for a service provider or domain can be a password or a cryptographic key. *Id.* at 3:56–59. The '512 patent describes that profiles, templates, and vaults are collectively referred to as “authentication information” and that in some embodiments secure storage techniques are used to store at least a portion of the authentication information. *Id.* at 3:60–65. Profiles and vaults can be updated while in secure storage, and if that occurs, they are encrypted before being written back to insecure storage, which may in turn propagate them to external backup storage. *Id.* at 4:19–23.

Figure 3 of the '512 patent is reproduced below:

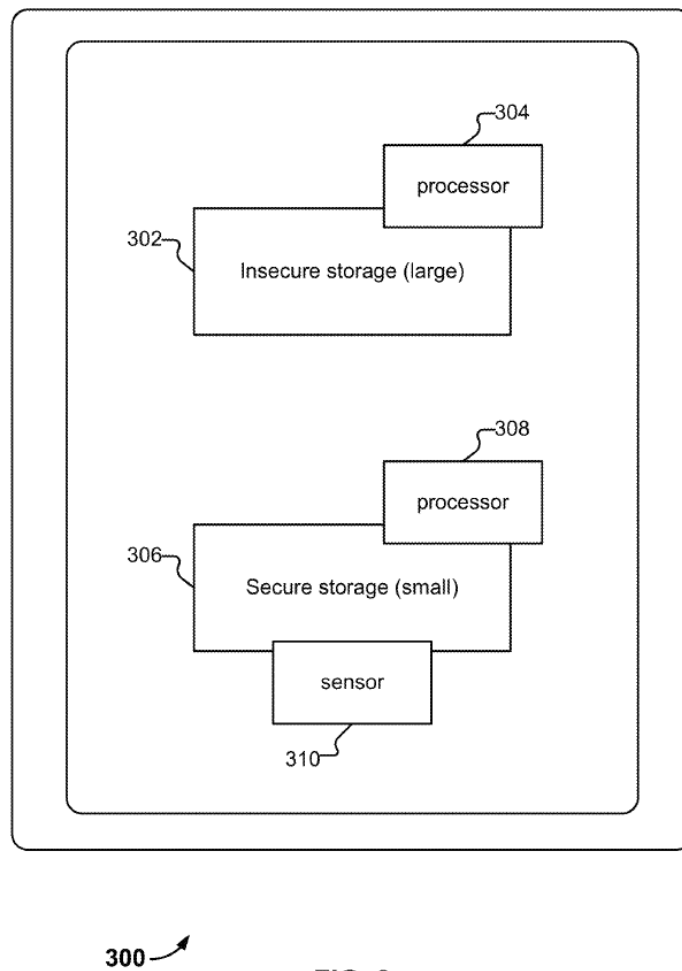


FIG. 3

Figure 3 depicts an embodiment of a device with secure storage to hold authentication information.

Ex. 1001, 1:55–56, 3:66–67, Fig. 3. As shown in Figure 3 above, mobile phone 300 includes large and insecure storage 302 attached to fast processor 304, and smaller but secure storage 306 is attached to dedicated processor 308 and sensor 310, which can be a camera or a fingerprint reader. *Id.* at 3:67–4:4. “Users (and applications) can read from and write to the insecure storage area. However, users cannot access the secure storage area,

and the fast processor can only communicate with the dedicated processor/sensor via a restricted API.” *Id.* at 4:5–8.

D. Illustrative Claim

The ’512 patent includes twenty-one claims, of which claims 1–4, 6–15, and 17–21 are challenged. Claims 1, 11, and 21 are the challenged independent claims. Claim 1 is illustrative and 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. Applied References

Petitioner relies upon the following references:

Johansson, U.S. Patent No. 8,776,214 B1 (Ex. 1005, “Johansson”), filed August 12, 2009, issued July 8, 2014.

Owen et al., U.S. Patent No. 7,780,080 B2 (Ex. 1006, “Owen”), filed April 23, 2007, issued August 24, 2010.

Shah et al., U.S. Patent Publication No. 2008/0059804 A1 (Ex. 1008, “Shah”), filed August 22, 2007, published March 6, 2008.

Kesanupalli et al., U.S. Patent Publication No. 2011/0138450 A1 (Ex. 1010, “Kesanupalli”), filed June 3, 2010, published June 9, 2011.

Pet. 3–4.

F. Asserted Grounds of Unpatentability

Petitioner challenges the patentability of claims 1–4, 6–15, and 17–21 of the ’512 patent based on the following grounds.

Claims Challenged	35 U.S.C. §	Reference(s)/Basis
1–4, 6–15, 17–21	103 ¹	Johansson, Kesanupalli
1–4, 6–15, 17–21	103	Shah, Owen

¹ The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112–29, 125 Stat. 284, 287–88 (2011), amended 35 U.S.C. § 103. Because the ’512 patent claims priority through a series of continuation applications to an application that was filed before March 16, 2013, the effective date of the relevant amendment, the pre-AIA version of § 103 applies.

Pet. 3–4. Petitioner also relies upon the Declaration of Dr. Mark E. Crovella (Ex. 1002).

II. ANALYSIS

A. Applicable Law

Petitioner challenges the patentability of claims 1–4, 6–15, and 17–21 of the ’512 patent on grounds that the claims would have been obvious under 35 U.S.C. § 103 in light of various references, namely Johansson, Kesanupalli, Shah, and Owen. “In an [*inter partes* review], the petitioner has the burden from the onset to show *with particularity* why the patent it challenges is unpatentable.” *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016) (citing 35 U.S.C. § 312(a)(3) (requiring *inter partes* review petitions to identify “with particularity . . . the evidence that supports the grounds for the challenge to each claim”)) (emphasis added). This burden never shifts to Patent Owner. *See Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015) (citing *Tech. Licensing Corp. v. Videotek, Inc.*, 545 F.3d 1316, 1326–27 (Fed. Cir. 2008)) (discussing the burden of proof in *inter partes* review).

A claim is unpatentable under 35 U.S.C. § 103 if “the differences between the subject matter sought to be patented 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 of record, objective evidence of

obviousness or non-obviousness, i.e., secondary considerations. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). Secondary considerations may include the following: “commercial success, long felt but unsolved needs, failure of others, etc.”² *Id.* The totality of the evidence submitted may show that the challenged claims would not have been obvious to one of ordinary skill in the art. *In re Piasecki*, 745 F.2d 1468, 1471–72 (Fed. Cir. 1984). When evaluating a combination of teachings, we must also “determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.” *KSR*, 550 U.S. at 418 (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)).

We analyze the challenges presented in the Petition in accordance with the above-stated principles.

B. Level of Ordinary Skill in the Art

Petitioner contends that a person of ordinary skill in the art, at the time of the invention of the ’512 patent:

would have had a bachelor’s degree in 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. 1002 ¶¶ 18, 24–26). Patent Owner states it “will apply the Petitioner’s definition of a [person of ordinary skill in the art] for the purposes of this response, but reserves the right to argue for a different definition should this Petition be instituted.” Prelim. Resp. 7.

² Patent Owner has not presented objective evidence of non-obviousness.

We regard Petitioner’s proposed definition as reasonable and consistent with the prior art before us. *See In re GPAC Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995) (determining that the Board of Patent Appeals and Interferences did not err in concluding that the level of ordinary skill in the art was best determined by the references of record). Accordingly, we apply the level of skill set forth above, which also is consistent with the testimony of Dr. Crovella (Ex. 1002 ¶¶ 18, 24–26).

C. Claim Construction – “Secure Backup Limitation”

We construe claims “using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. 282(b), including construing the claim in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.” 37 C.F.R. § 42.100(b); *see also Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc).

In this context, claim terms “are generally given their ordinary and customary meaning” as understood by a person of ordinary skill in the art in question at the time of the invention. *Phillips*, 415 F.3d at 1312–13; *see CCS Fitness, Inc. v. Brunswick Corp.*, 288 F.3d 1359, 1366 (Fed. Cir. 2002) (There is “a ‘heavy presumption’ that a claim term carries its ordinary and customary meaning.”). “In determining the meaning of the disputed claim limitation, we look principally to the intrinsic evidence of record, examining the claim language itself, the written description, and the prosecution history, if in evidence.” *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 469 F.3d 1005, 1014 (Fed. Cir. 2006) (citing *Phillips*, 415 F.3d at 1312–17). Extrinsic evidence is “less significant than the

intrinsic record in determining ‘the legally operative meaning of claim language.’” *Phillips*, 415 F.3d at 1317.

Only those claim terms that are in controversy need to be construed, and only to the extent necessary to resolve the controversy. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (stating that “we need only construe terms ‘that are in controversy, and only to the extent necessary to resolve the controversy’” (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))).

In this case, “Petitioner does not believe that any term requires explicit construction to resolve the issues presented in this Petition.” Pet. 7. Patent Owner also does not provide any express constructions for any claim terms. *See generally* Prelim. Resp. However, in the District Court Case, the parties proposed constructions for certain limitations, including “perform a *secure backup* of the record to a storage service,” as recited for example in independent claim 1, which is relevant to this Decision. Ex. 2020, 13–15, 19. Hereinafter, we refer to this limitation as the “Secure Backup Limitation.”

In the District Court Case, Petitioner argued the Secure Backup Limitation is indefinite. Ex. 2020, 13. Patent Owner argued the limitation should be given its “[p]lain and ordinary meaning; no construction necessary.” *Id.* After the filing of the Petition and Preliminary Response, the district court in the District Court Case entered a *Markman* order construing the Secure Backup Limitation, among others. *Id.* at 13–15, 19. The district court construed the Secure Backup Limitation to mean “create a backup of the record that is protected from unauthorized access and transmit

it to a storage service.” *Id.* at 15. In adopting this construction, the district court found “[t]he words of this disputed phrase have well-understood meanings:”

Generally, a “backup” may be either (1) the act of backing up, or (2) a backup copy of data. *See, e.g.,* <https://www.yourdictionary.com/backup> (last visited Mar. 29, 2022) (defining “backup” as “the act or an instance of backing up computer data, files, etc.” and, alternatively, as “[a] backup copy of data, a file, etc.”). Here, the claims recite “performing a . . . backup,” which aligns only with the former—performing the *act* of backing up. The limitation is silent as to whether the storage is secure or insecure, but requires the *act* be “secure.” “Secure” in this context, as already determined with respect to “secure storage,” means “protected from unauthorized access.”

Ex. 2020, 14–15.

We have reviewed the district court’s reasoning, as well as the ’512 patent and other evidence of record before us, and agree that, for reasons given by the district court, the Secure Backup Limitation should be given the same construction as determined by the district court.

We therefore adopt the district court’s construction for that limitation.

Ex. 2020, 13–15, 19. Accordingly, we construe the Secure Backup Limitation to mean “create a backup of the record that is protected from unauthorized access and transmit it to a storage service.” *See id.*

We do not find that the express construction of any other limitation is necessary for this decision. *See Vivid Techs.*, 200 F.3d at 803.

D. Obviousness of Claims 1–4, 6–15, and 17–21 over Johansson and Kesanupalli

Petitioner contends claims 1–4, 6–15, and 17–21 are unpatentable under 35 U.S.C. § 103 as obvious over the combination of Johansson

(Ex. 1005) and Kesanupalli (Ex. 1010). Pet. 21–44. Patent Owner opposes Petitioner’s contentions. Prelim. Resp. 24–43. Based on our review of the Petition and Preliminary Response, we determine that Petitioner has not demonstrated a reasonable likelihood that it would prevail in showing that any of claims 1–4, 6–15, and 17–21 is unpatentable as obvious over the combination of Johansson and Kesanupalli, as discussed below. We begin with an overview of Johansson and Kesanupalli.

1. Overview of Johansson

Johansson discloses an authentication manager that generates a security credential based at least in part on a security credential specification associated with a network site. Ex. 1005, code (57). Johansson describes that many problems associated with using passwords as a security credential are caused by humans not being able to process the type of data that passwords represent. *Id.* at 1:54–56. Johansson states that passwords are often not a single chunk of information and can stretch the limits of human working memory, and that the system it discloses “largely separates the user from the password, thereby resolving many of the issues.” *Id.* at 1:58–61.

Figure 1 of Johansson is reproduced below:

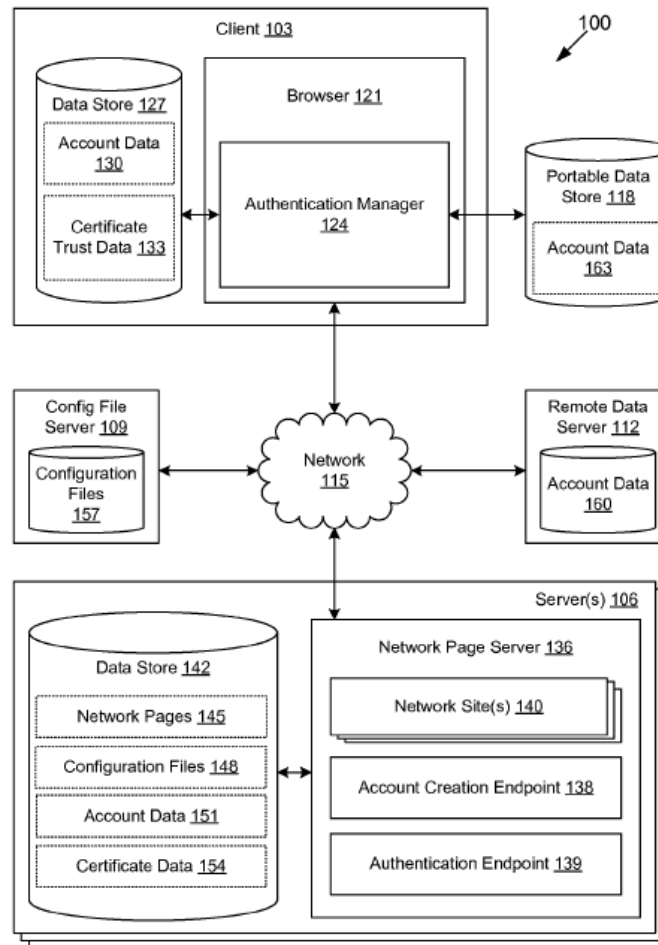


FIG. 1

Figure 1 depicts a network environment of an embodiment disclosed by Johansson.

Ex. 1005, 1:23–24, 2:5–6, Fig. 1. As shown in Figure 1 above, client device 103 is processor-based and, as such, includes a processor and a memory. *Id.* at 2:25–27. Client device 103 in networked environment 100 is in data communication with servers 106, configuration file server 109, and remote data server 112 by way of network 115. *Id.* at 2:5–10. Network 115 includes the Internet, intranets, extranets, wide area networks (WANs), local

area networks (LANs), wired networks, wireless networks, or other suitable networks, or any combination thereof. *Id.* at 2:10–14. Client device 103 may also communicate with portable data store 118 via a local interface. *Id.* at 2:14–17. Client device 103 can be a desktop computer, laptop computer, personal digital assistant, cellular telephone, set-top box, or other system with like ability. *Id.* at 2:18–22. Client device 103 includes data store 127, which may comprise data and applications configured to provide access to the data. *Id.* at 2:45–47. Data store 127 stores account data 130 which may include security credentials used to access various network sites or network pages, information regarding authentication endpoints, and/or other information. *Id.* at 2:49–52. Account data 130 may be stored in encrypted format. *Id.* at 2:52–54.

Regarding portable data store 118, Johansson describes:

The portable data store 118 may be configured to store account data 163. The account data 163 may include, for example, security credentials used to access various network sites 140 or network pages 145, information regarding authentication endpoints 139, and/or other information. In various embodiments, the account data 163 may be mirror of the account data 130. In other embodiments, the account data 163 may take the place of account data 130. The account data 163 may be stored in an encrypted format.

Ex. 1005, 4:59–67. Johansson further describes portable data store 118 as including a processor and a memory. *Id.* at 4:53–55.

Regarding servers 106, Johansson describes:

The server 106 is configured to execute various applications such as, for example, a network page server 136, an account creation endpoint 138, an authentication endpoint 139, and other applications. The network age server 136 is configured

to serve up network pages, such as web pages, and other files from the server 106 to various clients 103.

Ex. 1005, 3:3–8.

Account creation endpoint 138 may comprise a network page and/or software to facilitate creation of one or more accounts for one or more users at client device 103 for one or more network sites 140. Ex. 1005, 3:28–31. Authentication manager 124 communicates with account creation endpoint 138 through network page server 136. *Id.* at 3:31–33.

Configuration file server 109 includes a data store to store configuration files 157, which may include one or more security credential specifications and/or describe an interface of one or more account creation endpoints 138 and/or authentication endpoints 139. Ex. 1005, 4:18–23. Configuration file server 109 may be a system configured to provide configuration files 157 corresponding to plurality of servers 106. *Id.* at 4:23–25. Remote data server 112 includes a data store used to store account data 160 which may include security credentials used to access various network sites 140 or network pages 145. *Id.* at 4:40–43. Account data 160 may be stored in encrypted format. *Id.* at 4:46–48.

Figure 2 of Johansson is reproduced below:

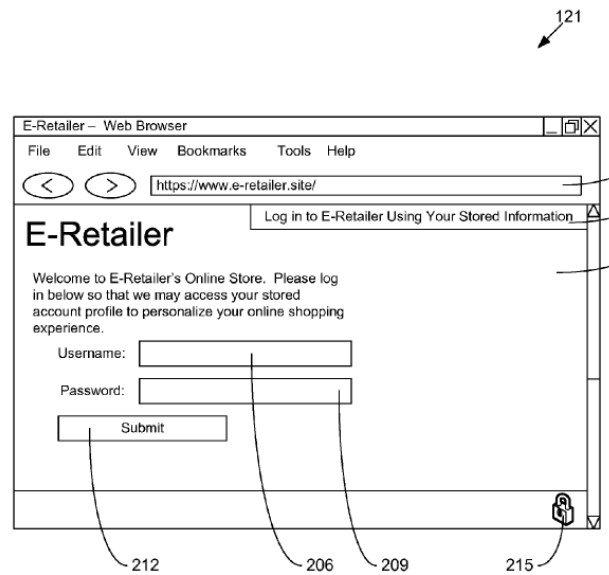


FIG. 2

Figure 2 shows an example of network pages rendered by a browser executed in a client device in the network environment of Figure 1.

Ex. 1005, 1:25–28, Fig. 2.

Johansson describes:

When a stored account exists for a network 140, the authentication manager 124 determines whether to provide the security credentials to the network site 140. As a preliminary matter, the authentication manager 124 may require that the user be authenticated to the authentication manager 124 by way of a master security credential such as a password, presence of the portable data store 118 at the client 103, biometric identification, native operating system identification, or some other authentication. Responsive to the authentication, the authentication manager 124 may decrypt the stored account data 130, 160, 163.

Ex. 1005, 8:21–31. In the example shown in Figure 2 above, network page 145 provided by network site 140 at the entered URL includes an

authentication form having username field 206, password field 209, and submit button 212. *Id.* at 9:48–54. Johansson further describes:

In FIG. 2, the authentication manager 124 (FIG. 1) has verified the identity of the network site 140 and is presenting an authentication button 218. The authentication button 218 indicates that account information associated with the network site 140 is stored in account data 130, 160, 163.

Once a user selects the authentication button 218, the authentication manager 124 may fill in the username field 206 and the password field 209. The authentication manager 124 may also automatically submit the logon request by programmatically pressing the submit button 212. In some embodiments, the username field 206 and password field 209 may be prefilled automatically with the security credential upon verification of the identity of the network site 140.

Id. at 9:58–10:4.

We further discuss below the disclosure of Johansson in connection with the parties' arguments.

2. Overview of Kesanupalli

Kesanupalli relates generally to “biometric authentication of users.” Ex. 1010 ¶ 24. Kesanupalli summarizes its secure transaction system using user authenticating biometric information as follows:

A user transaction request is received at a client device. A web browser plug-in communicates the user transaction request to a server that determines whether the user transaction request is a secure transaction. Transaction data is received from the server via the web browser plug-in. If the received transaction data indicates a secure transaction, the user is prompted to provide biometric data from a user using a biometric device and related security protocols. The web browser plug-in then communicates a transaction confirmation to the server.

Id. at codes (54), (57).

Figure 9 of Kesanupalli is reproduced below:

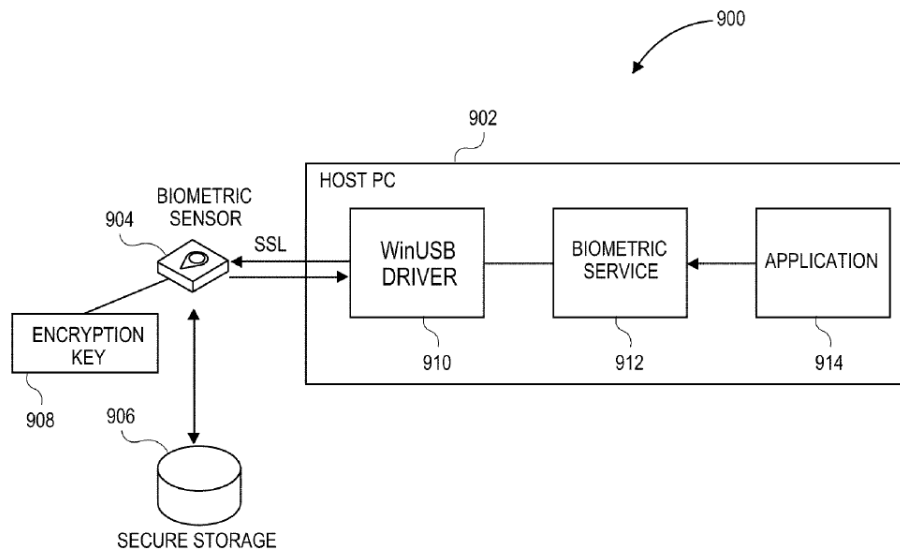


FIG. 9

Figure 9 depicts an exemplary system capable of performing biometric user authentication using biometric sensor 904.

Ex. 1010 ¶¶ 13, 57, Fig. 9. As shown in Figure 9 above, system 900 includes Host PC 902, WinUSB driver 910, biometric service 912, and application 914. *Id.* ¶ 57. Biometric sensor 904 decrypts user credentials only after a successful biometric reading, such as a fingerprint swipe or fingerprint scan (using a placement style fingerprint sensor). *Id.* In a successful fingerprint swipe, for example, the swiped fingerprint information matches a fingerprint template associated with the fingerprint sensor. *Id.* Biometric sensor 904 “creates a secure communication with Host PC 202 using SSL v3 protocol or other secure communication technique.” *Id.* In an exemplary embodiment, biometric sensor 904 includes “a ‘match on chip’ functionality that releases a user’s credentials only upon a successful fingerprint swipe or other biometric reading.” *Id.*

Such user credentials and other information may be stored within biometric sensor 904, in secure storage 906, or any other storage mechanism. *Id.*

We further discuss below the disclosure of Kesanupalli in connection with the parties' arguments.

3. *Independent Claim 1: “[a first processor configured to] communicate with a second processor using a restricted interface”*

Independent claim 1 requires, in relevant part, a first processor configured to “communicate with a second processor using *a restricted interface*.” Ex. 1001, 10:62–11:2 (emphasis added). The parties dispute, *inter alia*, whether Petitioner's cited evidence adequately supports Petitioner's contention that the combination of Johansson and Kesanupalli teaches a “restricted interface” in this context. *See, e.g.*, Prelim. Resp. 38–40; Pet. 28–29. Independent claims 11 and 21 also recite this limitation. Ex. 1001, 11:63–12:2, 12:61–13:2.

Petitioner contends “Johansson discloses that its first processor (i.e., of client 103) communicates with a second processor (i.e., of portable data store 118), *using a restricted interface*.” Pet. 28 (emphasis added). Petitioner's entire alleged support for this contention is that “Johansson discloses that client 103 connects with portable data store 118, which ‘may include a processor circuit comprising a processor and a memory,’ by way of, e.g., ‘*a local interface, data bus, or another network 115*.’” Pet. 28 (citing Ex. 1005, 2:15–17, 4:50–59) (emphasis added). Petitioner's declarant makes these same statements verbatim, without more, and with no additional citations to evidence. *See* Ex. 1002 ¶ 100.

Patent Owner argues “[n]one of [a local interface, data bus, and another network 115] are a ‘restricted interface’ and petitioner has not offer[ed] a single piece of evidence to the contrary.” Prelim. Resp. 38. Patent Owner argues “Petitioner’s ‘expert’ does not even opine on whether [the skilled artisan] would have viewed a local interface, data bus, or another network as a restricted interface.” *Id.* (citing Ex. 1002 ¶¶ 100–101); *see id.* at 40. Indeed, neither Petitioner nor its expert provides any express construction for what a “restricted interface” *is* in the context of the ’512 patent, and as argued by Patent Owner (*id.*), neither explains sufficiently, let alone with particularity, how or why Johansson’s “local interface, data bus, or another network 115” discloses or teaches the claimed “restricted interface.” *See* 35 U.S.C. § 312(a)(3) (“particularity”); 37 C.F.R. § 42.104(b)(3) (“How the challenged claim is to be construed.”).

Petitioner also contends “Kesanupalli discloses that a first processor (Host PC 202) communicates with biometric sensor [9]04 using *a restricted interface*.” Pet. 28 (emphasis added). Petitioner’s entire alleged support for this contention is that “Kesanupalli discloses that ‘biometric sensor 904 creates a secure communication with Host PC 202 using SSL v3 protocol or other secure communication technique.’” *Id.* But Petitioner’s argument here begs the question: Given Petitioner already argued Johansson itself “discloses” “a restricted interface” (Pet. 28), why turn to Kesanupalli for this feature (i.e., what is missing from Johansson)? We find Petitioner’s argument here reinforces our determination that Petitioner does not explain sufficiently how or why Johansson discloses or teaches the claimed “restricted interface.” *See* Prelim. Resp. 39 (“Essentially acknowledging

that Johansson does not disclose a restricted interface between the two processors, Petitioner turns to Kesanupalli to supply the missing link.”).

Patent Owner argues “Petitioner has failed to establish that . . . the SSL v3 protocol used in Kesanupalli [is a] restricted interface[] between the processors.” Prelim. Resp. 40. We agree. Again, neither Petitioner nor its expert provides any express construction for what a “restricted interface” *is* in the context of the ’512 patent. Despite claim 1 reciting features such as “a secure connection” (Ex. 1001, 10:66–67), “a secure storage” (*id.* at 11:9), and “a secure backup” (*id.* at 11:25), and doing so separate and distinct from “a restricted interface” (*id.* at 11:1–2), neither Petitioner nor its expert explains how or why “a secure communication” such as one using SSL v3 protocol is (or teaches) a “restricted interface” between processors. Thus, we agree with Patent Owner that Petitioner does not explain sufficiently, let alone with particularity, how or why Kesanupalli’s secure communication using SSL v3 protocol (alone or in combination with Johansson) discloses or teaches the claimed “restricted interface.”

Petitioner further contends “using a restricted interface in a biometrically-secured device would have been a logical and routine implementation choice for [the skilled artisan].” Pet. 29. Petitioner’s declarant also makes this same statement verbatim, without more, and with no further explanation or additional citations to evidence. *See* Ex. 1002 ¶ 101. We give such conclusory, unsupported assertions by Petitioner’s expert little or no weight. *See In re Am. Acad. of Sci. Tech Ctr.*, 367 F.3d 1359, 1368 (Fed. Cir. 2004) (“[T]he Board is entitled to weigh the declarations and conclude that the lack of factual corroboration warrants discounting the opinions expressed in the declarations.”); *Rohm and Haas*

Co. v. Brotech Corp., 127 F.3d 1089, 1092 (Fed. Cir. 1997) (noting that a fact finder is not required to “credit the unsupported assertions of an expert witness”); 37 C.F.R. § 42.65(a) (“Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight.”). Furthermore, the premise for this contention is Petitioner’s allegation that Johansson and Kesanupalli each disclose or teach the claimed “restricted interface” between processors, which Petitioner does not sufficiently support on the present record. Thus, we have no basis to credit Petitioner’s contention here.

For the foregoing reasons, and constrained by the Petition, we are not persuaded that the cited evidence adequately supports Petitioner’s contention that Johansson, Kesanupalli, or the combination thereof teaches a “restricted interface” between processors, as recited in independent claims 1, 11, and 21.

4. Summary

For the foregoing reasons, we determine that Petitioner has not demonstrated a reasonable likelihood of success in establishing the unpatentability of claims 1, 11, or 21, or claims 2–4, 6–10, 12–15, and 17–20 which depend therefrom, as obvious over the combination of Johansson and Kesanupalli.

E. Obviousness of Claims 1–4, 6–15, and 17–21 over Shah and Owen

Petitioner contends claims 1–4, 6–15, and 17–21 are unpatentable under 35 U.S.C. § 103 as obvious over the combination of Shah (Ex. 1008) and Owen (Ex. 1006). Pet. 44–67. Patent Owner opposes Petitioner’s contentions. Prelim. Resp. 43–47. Based on our review of the Petition and

Preliminary Response, we determine that Petitioner has not demonstrated a reasonable likelihood that it would prevail in showing that any of claims 1–4, 6–15, and 17–21 is unpatentable as obvious over the combination of Shah and Owen, as discussed below. We begin with an overview of Shah and Owen.

1. Overview of Shah

Shah discloses a method and apparatus for password management and single sign-on (SSO) access, which uses a trusted platform module (TPM) to interact with a proxy SSO unit and web-accessing applications to provide a secure, trusted mechanism to generate, store, and retrieve passwords and SSO credentials. Ex. 1008, code (57).

Figure 8 of Shah is reproduced below:

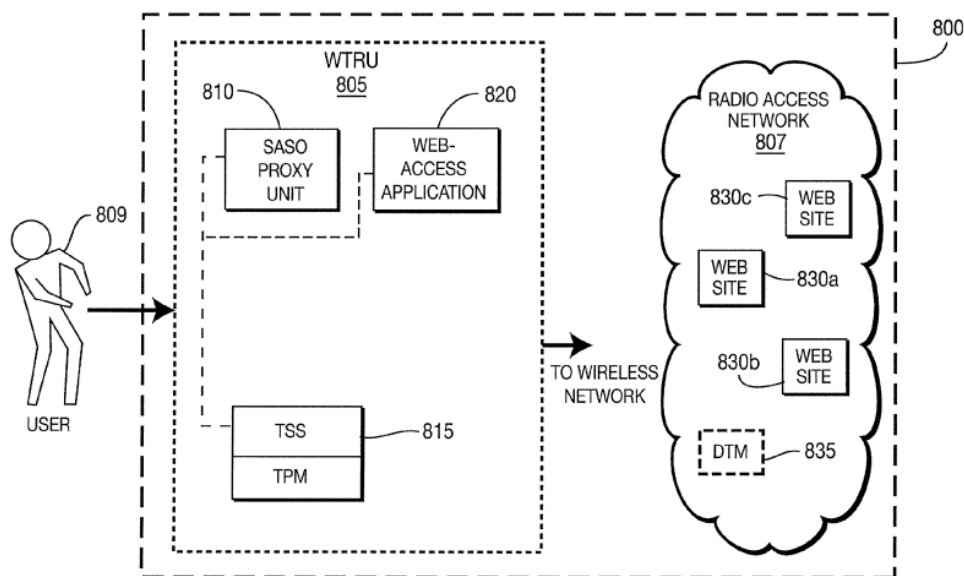


FIG. 8

Figure 8 depicts a wireless communication system.

Ex. 1008 ¶ 57, Fig. 8. As shown in Figure 8 above, wireless communication system 800 includes wireless transmit/receive unit (WTRU) 805 that

interacts with user 809. *Id.* ¶ 64. The WTRU includes single automatic sign-on (SASO) proxy unit 810, TPM/TSS (TPM software stack) 815, and web access application (WAA) 820. *Id.* TPM/TSS 815 interacts with both SASO proxy unit 810 and WAA 820 to provide a secure, trusted mechanism to generate, store, and retrieve passwords and SSO credentials. *Id.* Shah describes that TPM stands for “trusted platform module” and is a core platform module. *Id.* ¶ 37. Published U.S. Patent Application No. 11/745,697, incorporated by reference into the disclosure of Shah (*see id.* ¶ 73), states:

The TPM is a microcontroller that stores keys, passwords, performs ciphering and hashing functions and forms the basis of a root of trust mechanism. It potentially can be used in any computing device or platform that requires these functions, particularly a wireless transmit/receive unit (WTRU).

Ex. 1011 ¶ 5.

Figure 7 of Shah is reproduced below:

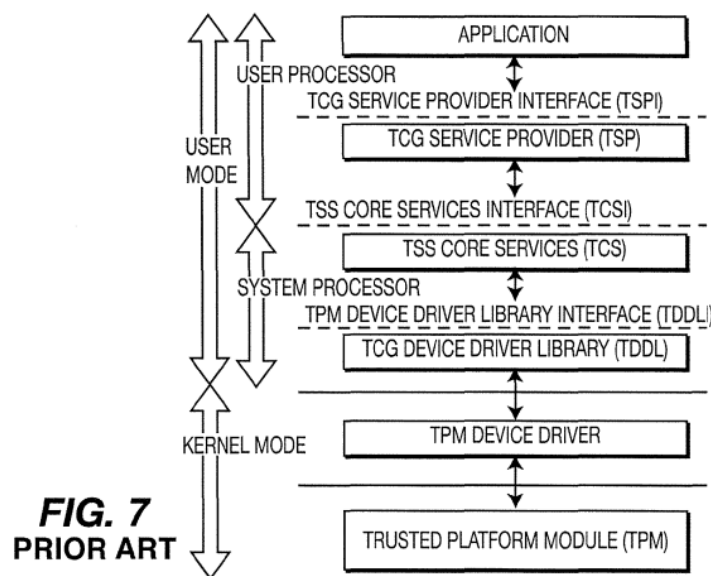


Figure 7 depicts a block diagram of the different layers within a TPM and TSS.

Ex. 1008 ¶ 56, Fig. 7. Figure 7 above shows the interface architecture of TPM and TSS layers between an application and a TPM. *Id.* ¶ 40. Shah describes:

TSS modules include the following components: 1) TSS device driver library interface (TDDLI) that interfaces to the standardized TPM device driver library (TDDL); 2) TSS core service interface (TCSI) that interfaces to the TPM's TCS commands (not shown); and 3) TCG service provider interface (TSPI) that interfaces with the TCG's TSP commands (not shown) and sits just below the application. On the TPM side, the TDDL sits on top of the vendor specific TPM device driver, which is in communication with the TPM.

Id.

Figure 11 of Shah is reproduced below:

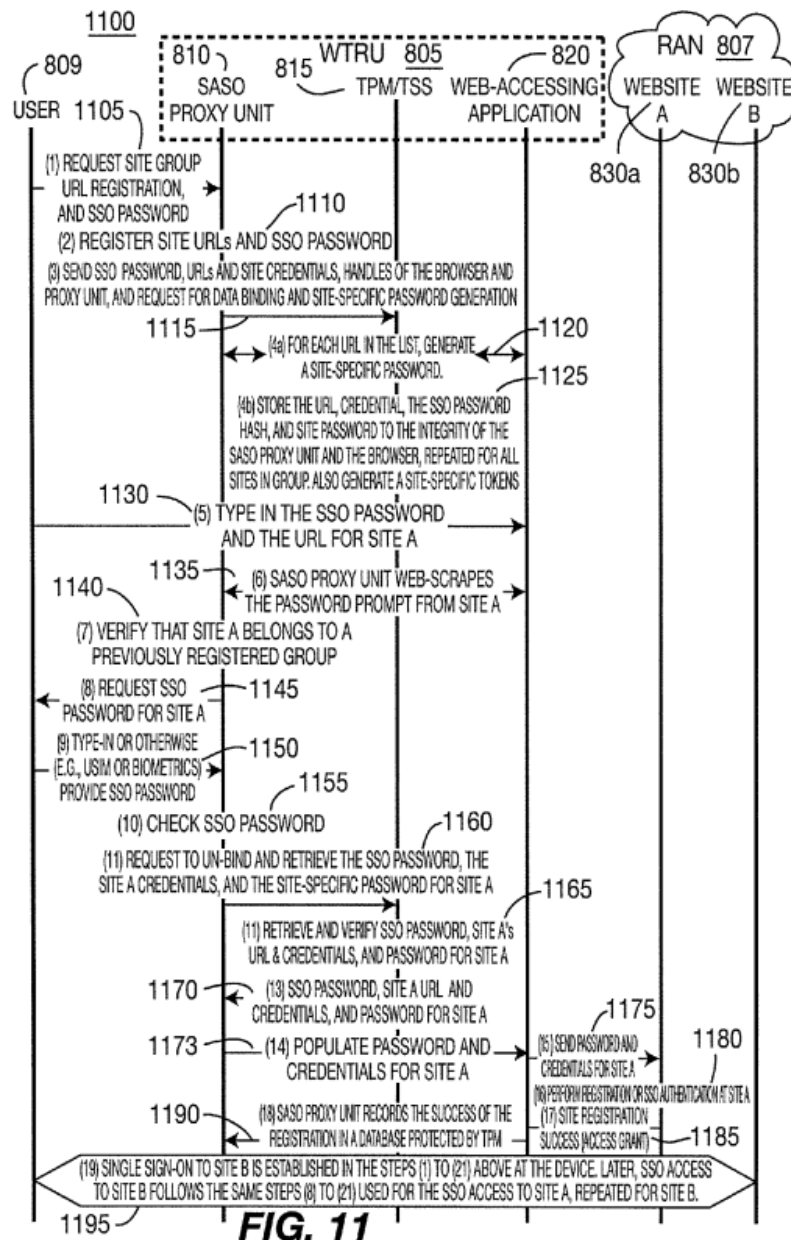


Figure 11 depicts a flow diagram of a SSO for web access using a TPM/TSS based on group-wise passwords using a TPM.

Ex. 1008 ¶ 60, Fig. 11. Shah explains that user 809 configures a group of sites, the access to each of which is controlled by the SASO proxy unit 810

and with a common, group-specific log-in/password furnished by the user 809. *Id.* at ¶ 88. By using such a procedure, user 809 can control the access to particular groups of websites using group-specific passwords. *Id.* Shah describes the procedure, in part, as follows:

The user 809 initiates the procedure 1100, possibly upon prompt by the SASO proxy unit 810, by sending to the SASO proxy unit 810 a request for establishment of a website group, at step 1105. The request may include website A 830a and website B 830b, and also a SSO password he has made for the website group, and the URLs of the websites belonging to the group. This step could be done in an incremental manner, whereby the user 809 starts the group by having only the website A 830a, and then later adding or deleting other websites. If such website list update is performed at any point, the SASO proxy unit 810 will need to request procedures for adding, deleting, or even un-binding and re-binding, certain data held by the TPM/TSS 815 (and some of them also by the SASO proxy unit 810).

Next, the SASO proxy unit 810 registers the website URLs and the single SSO password for each website in the website group, at step 1110. The SASO proxy unit 810 then sends the TPM/TSS 815 the SASO password, the URLs and the website credentials for all the websites belonging to the group, the address handle of the WAA 820 and the SSO proxy unit 810, and also a request for data binding and for website-specific password generation to the TPM/TSS 815, at step 1115. For each URL in the list of websites, the TPM/TSS 815 generates a cryptographically strong password, using the TPM random number generator (RNG), at step 1120. At step 1125, the TPM/TSS 815 then binds the website-specific URL, any credentials (including site certificates), the SSO password, and the site-specific password that it generated, in a data blob encrypted with a TPM storage key. Such a key is 'bound' to the platform (e.g. WTRU, or computer) that houses the TPM. If in step 1105 the user 809 has indicated an update (add, delete, or change) of the list of the group of websites with its associated information (URLs, credentials, etc.), there must be an indication

from the SASO proxy unit 810 and the TPM/TSS 815 to either add or delete the website-specific records for the affected websites.

Id. ¶¶ 89–90.

We further discuss below the disclosure of Shah in connection with the parties’ arguments.

2. Overview of Owen

Owen discloses a biometrically-secured device for facilitating various different types of in-person and online transactions. Ex. 1006, code (57). The in-person transactions can be credit card transactions, in which the user’s identity is biometrically authenticated. *Id.* The device also can be used to create a secure platform from which to make online transactions by loading a secure operating system from the device to a host computer’s volatile memory. *Id.* Biometrically secured online transactions can then be performed using the host computer. *Id.* Figure 1 of Owen is reproduced below:

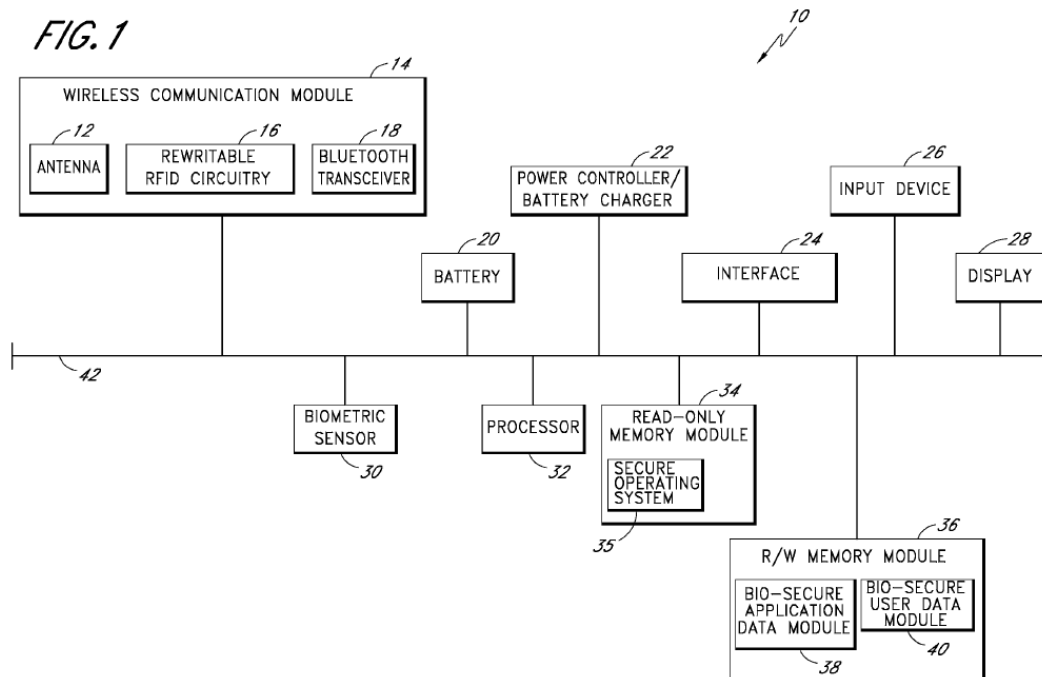


Figure 1 is a block diagram of portable biometrically-secured device 10 for facilitating biometrically-secured in-person or online transactions.

Id. at 6:62–65, 9:65–67, Fig. 1.

As shown in Figure 1 above, biometrically-secured device 10 includes biometric sensor 30 to biometrically authenticate the identity of a user. Ex. 1006, 13:20–23. It also includes two physically separate memory modules 34 and 36, both of which are biometrically secured so that access to them is at least partially restricted based on whether a user has biometrically authenticated his or her identity. *Id.* at 11:7–13. Biometrically-secured device 10 also includes interface 24 which couples device 10 to a host computer (not shown), and processor 32 which controls interface 24 and access to memory modules 34 and 36. *Id.* at 10:4–6, 10:63–11:2. Biometrically-secured device 10 further includes display 28, user input

device 26, battery 20, power controller/battery charger 22, and wireless communications module 14. *Id.* at 10:11–27.

Figure 13 of Owen is reproduced below:

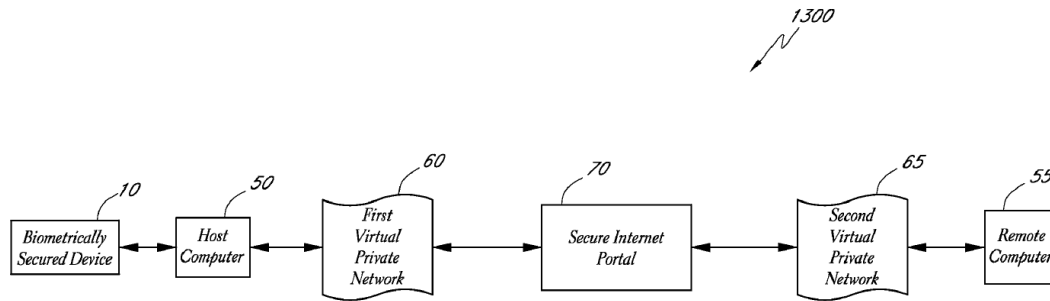


FIG. 13

Figure 13 depicts a dataflow chart of communications between the biometrically-secured device of Figure 1, a host computer, a secure internet portal, and a remote computer.

Ex. 1006, 7:39–41; 25:47–49, Fig. 13. As shown in Figure 13 above, remote access system 1300 includes biometrically-secured device 10, host computer 50, secure internet portal 70, and remote computer 55. *Id.* at 25:49–52. Device 10 is communicatively coupled to host computer 50 which is communicatively coupled to secure internet portal 70 through VPN 60, and secure internet portal 70 is communicatively coupled to remote computer 55. *Id.* at 27:52–58.

The remote computer is configured to accept access requests from the host computer that is in communication with a user's portable, biometrically-secured device 10 when the user is away from the remote computer. Ex. 1006, 26:12–17. The remote computer can be the user's home computer or a corporate file server, or some other network attached electronic data storage device. *Id.* at 25:59–63.

After being granted access to remote computer 55, a user is permitted “to access and modify electronic files stored by the remote computer 55.” Ex. 1006, 27:34–36. The electronic files can be downloaded to the user’s portable, biometrically-secured device for offline work. *Id.* at 27:49–51. Owen describes:

In the case where the remote computer 55 is, for example, a corporate file server, the company can be given the ability to change permission settings that control which files on the corporate file server are accessible by the user. If at any time the company removes access privileges to a file from a user after he has stored the file on his portable device 10, then, in certain embodiments, the secure internet portal 70 can be configured to send a command to the user’s portable device 10 to delete the file from the user’s device 10 once the device 10 is again used to establish a connection with the secure internet portal 70.

Id. at 27:56–66.

Additional security is provided to protect the secrecy of the user’s data on biometrically-secured device 10. For instance, an old device can be added to a “banned list.” Ex. 1006, 30:27–29. Specifically, Owen describes:

After being added to the banned list, the next time that the old device 10 is coupled to a host computer 50, the secure internet portal 70 can issue a “scorched earth” command to the old portable device 10, causing the processor 32 to erase the device’s memory modules and/or otherwise disable the old device 10.

Id. at 30:27–32.

We further discuss below the disclosure of Owen in connection with the parties’ arguments.

3. *Independent Claim 1: “perform a secure backup of the record to a storage service”*

Independent claim 1 requires, in relevant part, “perform[ing] a *secure backup* of the record to a storage service.” Ex. 1001, 11:25–26 (emphasis added). The parties dispute, *inter alia*, whether Petitioner’s cited evidence adequately supports Petitioner’s contention that the combination of Shah and Owen teaches a “secure backup” in this context. *See, e.g.*, Prelim. Resp. 43–47; Pet. 55–58. Independent claims 11 and 21 also recite this limitation. Ex. 1001, 12:26–27, 13:25–26.

Petitioner contends “Shah discloses that the second processor (i.e., of TPM/TSS 815 and/or SASO proxy unit 810, residing in the USIM) performs a *secure backup* of the record to a storage service (e.g., RAN 807 with a device trusted mirror DTM 835).” Pet. 55 (emphasis added). Petitioner submits the following as alleged support for this statement:

SASO proxy unit 810 sends the authentication data and list of desired services to DTM 835. Ex-1008, ¶80, FIG. 10 (step 1020).

Moreover, in one embodiment, Shah discloses that the function of SASO proxy 810 and TPM/TSS 815 may reside in a USIM, the structure of which is incorporated by reference to Shah ’256 (Ex-1011). Shah ’256 discloses a USIM 205, which includes a TPM microcontroller. Ex-1011, ¶38, FIG. 2. In the embodiment where SASO proxy 810 resides in the USIM, the USIM (second processor) sends the authentication data and list of desired services to DTM 835.

In particular, Shah discloses that SASO proxy unit 810 “sends the authentication data and the list of desired services to” TPM/TSS 815, which “seals the authentication data and the list of desired services to the integrity of the SASO proxy unit 810 and WAA 820.” Ex-1008, ¶80. SASO proxy unit 910 then sends the “integrity information (or, equivalently, attestation

information) for the WTRU 805, along with the authentication data and the list of applications and the desired services, to the DTM 835.” *Id.*; Ex-1002, ¶¶171-173.

Pet. 56–57 (Fig. 10 image omitted). Petitioner’s declarant makes these same statements verbatim, without more, and with no further explanation or additional citations to evidence. *See* Ex. 1002 ¶¶ 171–173.

Patent Owner argues “[Shah] does not disclose a secure backup,” and “[i]ndeed, [Shah] doesn’t even disclose a backup.” Prelim. Resp. 45. According to Patent Owner, “[w]hat [Shah] does disclose, and what Petitioner mistakenly label[s] as a ‘backup,’ is using a device trusted **mirror** (‘DTM’) to authenticate in the ‘secure automated sign-on’ process.” *Id.* (citing Ex. 1011 ¶ 59). Patent Owner argues “[t]his is not a backup; rather, as the name implies, the device trusted mirror (DTM), ‘provides services that “mirror[s]” the trustworthy service of the WTRU 805 and can attest to it to external requesters of such information.’” *Id.* (alteration in original).

Patent Owner submits:

Further evidencing the fact that this is not a backup, is that [Shah] does not disclose a second device that can download the record from the DTM—and Petitioner does not point to a second device downloading the backup from the DTM. Indeed, there is nothing that indicates that the DTM can do anything beyond attest the user in place of the WTRU.

Id. at 45–46. Patent Owner concludes, and we agree, “Petitioner does not explain how Shah discloses a secure backup.” *Id.* at 46 (“Petitioner does a lot of hand waving without any substantive analysis like adding a complicated figure [i.e., Figure 10] with no explanation as to how the figure is relevant.”). Patent Owner also concludes, and we agree, “[t]here is

nothing on the record that demonstrates that [the skilled artisan] would consider a ‘mirroring’ system to disclose a [secure] backup.” *Id.*

Neither Petitioner nor its expert provide any express construction for what a “secure backup” *is* in the context of the ’512 patent, and as argued by Patent Owner (*id.* at 45–46), neither explains sufficiently, let alone with particularity, how or why Shah’s “mirroring system” (e.g., DTM 835) discloses or teaches the claimed “secure backup.” *See* 35 U.S.C. § 312(a)(3); 37 C.F.R. § 42.104(b)(3). Although Petitioner does not construe “secure backup,” as noted above in Section II.C, for purposes of this decision we construe the term to mean “create a backup of the record that is protected from unauthorized access and transmit it to a storage service.” Under this construction, we still find Petitioner does not explain sufficiently (if at all) how or why Shah’s “mirroring system” discloses or teaches first creating a backup of a record that is protected from unauthorized access and then transmitting that protected backup to a storage service.

The burden of proof here lies with Petitioner, not Patent Owner, and we do not ourselves create and adopt unpatentability arguments on behalf of Petitioner as to whether or how Shah might teach a “secure backup.” *See Wasica Fin. GmbH v. Cont’l Auto. Sys., Inc.*, 853 F.3d 1272, 1286 (Fed. Cir. 2017) (“It is of the utmost importance that petitioners in the IPR proceedings adhere to the requirement that the initial petition identify with particularity the evidence that supports the grounds for the challenge to each claim.” (quoting *Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1369 (Fed. Cir. 2016))); *In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1381 (Fed. Cir. 2016) (“[W]e find no support for the PTO’s position

that the Board is free to adopt arguments on behalf of petitioners that could have been, but were not, raised by the petitioner during an IPR.”); *DeSilva v. DiLeonardi*, 181 F.3d 865, 866–67 (7th Cir. 1999) (“A brief must make all arguments accessible to the judges, rather than ask them to play archeologist with the record.”).

Petitioner also contends “Owen discloses that a user registers portable device 10 with secure internet portal 70, and creates a backup of the data stored in the portable device.” Pet. 57. Petitioner argues “Owen discloses that secure internet portal 70 can ‘include a registration’ (backup data) and ‘rebuild’ (download to a new device) service for the user should his/her old biometrically-secured device 10 become lost, stolen or damaged.” Pet. 57. Petitioner argues “Owen teaches that ‘[e]ven though the portable, biometrically-secured device 10 is a new one, the biometric sensor can be used to regenerate the user’s unique mathematical key pair so that his identity can be biometrically authenticated by the secure internet portal 70.” Pet. 57. Petitioner’s declarant makes these same statements verbatim, without more, and with no further explanation or additional citations to evidence. *See* Ex. 1002 ¶¶ 174–175. Petitioner does not explain whether it is relying on Owen to teach a “*secure* backup.”

Patent Owner argues, as with Shah, “Owen similarly does not disclose a secure backup.” Prelim. Resp. 46. “Rather, Owen discloses a system of registering and rebuilding a new device ‘[s]hould the user’s portable device 10 become lost, stolen, and/or damaged, [so that the user] can replace the old device 10 with a new one, and rebuild his private information to the new device.’” *Id.* (alterations in original). Patent Owner argues Owen “does not disclose how the data that [is] used for the registration and rebuilding

service is created and it certainly does not disclose a secure backup is made from a first device and then downloaded by a second device.” *Id.* at 46–47. “Rather, the disclosures that the Petitioner point to almost exclusively deal with the downloading by a second device.” *Id.* at 47. Patent Owner argues, “[n]otably, Petitioner points to the ‘initial registration’ of a device as a backup.” *Id.* Patent Owner concludes, and we agree, “it is unclear how or why [the skilled artisan] would understand device registration to be a backup—and . . . certainly not a *secure backup* as disclosed in the Patent.” *Id.* (emphasis added). We agree with Patent Owner that Petitioner does not explain sufficiently, let alone with particularity, how or why Owen’s secure internet portal 70 and device registration (alone or in combination with Shah) discloses or teaches the claimed “secure backup.”

For the foregoing reasons, and constrained by the Petition, we are not persuaded that the cited evidence adequately supports Petitioner’s contention that Shah, Owen, or the combination thereof teaches a “secure backup,” as recited in independent claims 1, 11, and 21.

4. *Summary*

For the foregoing reasons, we determine that Petitioner has not demonstrated a reasonable likelihood of success in establishing the unpatentability of claims 1, 11, or 21, or claims 2–4, 6–10, 12–15, and 17–20 which depend therefrom, as obvious over the combination of Shah and Owen.

III. DISCRETIONARY DENIAL UNDER 35 U.S.C. § 314(a)

Because we deny institution upon consideration of the merits of Petitioner's challenges, Patent Owner's arguments that we should exercise our discretion under 35 U.S.C. § 314(a) to deny institution are moot.

IV. CONCLUSION

Petitioner has not demonstrated a reasonable likelihood of prevailing with respect to any of claims 1–4, 6–15, and 17–21 of the '512 patent under either of its proffered Grounds 1 or 2 (Pet. 3–4).

V. ORDER

For the reasons given, it is:

ORDERED that, pursuant to 35 U.S.C. § 314(a), an *inter partes* review is not instituted for claims 1–4, 6–15, and 17–21 of U.S. Patent No. 10,929,512 B1.

IPR2022-00251
Patent 10,929,512 B1

For PETITIONER:

Marc J. Pensabene
Ryan Yagura
Nicholas J. Whilt
Caitlin P. Hogan
O'MELVENY & MYERS LLP
mpensabene@omm.com
ryagura@omm.com
nwhilt@omm.com
chogan@omm.com

For PATENT OWNER:

Richard A. Kamprath
George T. Fishback, Jr.
MCKOOL SMITH, P.C.
rkamprath@mckoolsmith.com
gfishback@mckoolsmith.com