

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

SEVEN NETWORKS, LLC,
Patent Owner.

IPR2020-00507
Patent 10,243,962 B1

Before THU A. DANG, KARL D. EASTHOM, and
JONI Y. CHANG, *Administrative Patent Judges*.

EASTHOM, *Administrative Patent Judge*.

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

Apple Inc. (“Petitioner”) filed a Petition (Paper 2, “Pet.”) requesting an *inter partes* review of claims 1–44 (the “challenged claims”) of U.S. Patent No. 10,243,962 B1 (Ex. 1001, “the ’962 patent”). Petitioner filed a Declaration of Craig E. Wills, Ph.D. (Ex. 1003) with its Petition. SEVEN Networks, LLC (“Patent Owner”) filed a Preliminary Response (Paper 7, “Prelim. Resp.”).

The Board’s authority to determine whether to institute an *inter partes* review stems from 35 U.S.C. § 314(b) and 37 C.F.R. § 42.4(a). Under 35 U.S.C. § 314(a), the Board can not authorize an *inter partes* review unless the information in the Petition and the Preliminary Response “shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” For the reasons that follow, we deny institution of an *inter partes* review as to the challenged claims of the ’962 patent on the grounds of unpatentability presented in the Petition.

I. BACKGROUND

A. *Real Parties-in-Interest*

Petitioner identifies Apple Inc. as the real party-in-interest. Pet. 66. Patent Owner identifies SEVEN Networks, LLC, and CF SVN LLC as the real parties-in-interest. Paper 4, 1.

B. *Related Proceedings*

The parties identify *SEVEN Networks, LLC v. Apple Inc.*, No. 2:19-cv-00115 (E.D. Tex.) as a related matter involving the ’962 patent. Pet. 66; Paper 4, 1.

C. The '962 patent

The '962 patent is titled “Multiple Data Store Authentication.” Ex. 1001, code (54). The '962 patent describes “[s]ystems and methods for authentication access to multiple data stores substantially in real time.” *Id.* code (57). A “server may authenticate access to the data stores and forward information from those stores to the client device.” *Id.*

Figure 1 illustrates an “exemplary environment 100 for providing simplified provisioning, including authentication of data store access.” *Id.* at 6:11–13.

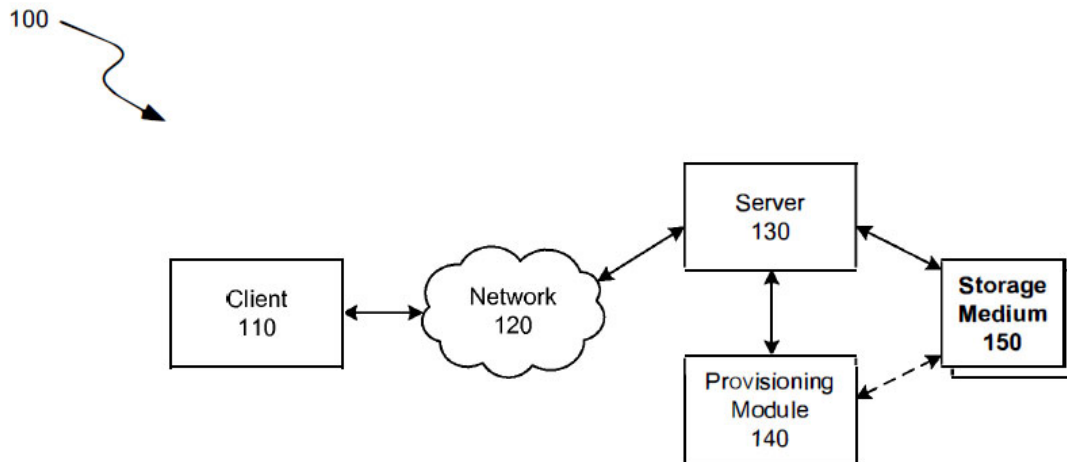


FIG. 1

As shown in Figure 1, “[a] client communicates with a server 130 via a network 120,” where “client 110 may be a data-enabled device that can, for example, send and receive electronic-mail, receive and send short message service (SMS) messages, access the Internet and so forth.” *Id.* at 6:14–21. Provisioning module 140, coupled to server 130, provides “provisioning event related services, which may include various forms of authentication.” *Id.* at 6:46–48. Server 130 may have access one or more storage mediums

150, which “may include internal mail servers at an enterprise or that may be offered by any variety of service providers,” “databases for storage of contact and Personal Information Management (PIM) data as well as calendar, notes, and task data,” or “data stores for documents (e.g., file servers).” *Id.* at 6:59–7:7.

In an embodiment, client 110 may contact server 130 to request services provided by a service provider associated with server 130. *Id.* at 7:8–11. “[S]erver 130 requests information about the user at the client 110 or about the client 110 itself before allowing the user to access services (i.e., authenticating access to the services and/or data). *Id.* at 7:13–16. “[S]erver 130 utilizes the provisioning module 140 to provide specified services and configurations for those services to the user at the client 110,” and “provisioning module 140 may verify information associated with the client 110 in one embodiment (e.g., authentication).” *Id.* at 7:66–8:3.

D. Illustrative Claim 1

Of the challenged claims, claims 1 (“[a] server”) and 23 (“[a] method”) are independent. Claims 1 and 23 recite materially similar limitations. *See* Ex. 1001, 19:45–20:10, 21:15–45. Remaining challenged claims 2–22 and 24–44 depend from claim 1 and claim 23, respectively.

Claim 1 illustrates the challenged claims at issue:

1. [1.pre] A server, comprising:
 - [1.1a] a memory and a processor, [1.1b] the server communicatively coupled to a network and a plurality of data stores, [1.2] wherein the server is configured to:
 - send a first identifier to a client device upon the client device communicating with the server over a connection;
 - [1.3] receive registration information from the client device;
 - [1.4] send a second identifier to the client device in response to the received registration information;
 - [1.5] configure a service to receive data from a first data store on behalf of the client device, wherein the service is based on the second identifier;
 - [1.6] receive a communication from the client device to receive data from the plurality of data stores, [1.7] wherein the communication includes the first identifier;
 - [1.8] receive a first message from the first data store, wherein the first message is indicative of new data at the first data store;
 - [1.9a] transmit a second message to the client device in response to receipt of the first message and authentication of the client device, [1.9b] wherein the second message is transmitted over a subsequent connection, and [1.9c] wherein the authentication of the client device is based on the first identifier, [1.10] wherein the subsequent connection is an IP connection between the client device and the server; and
 - [1.11] receive a keep-alive message from the client device for maintenance of the subsequent connection, [1.12] wherein additional information associated with the first message is sent from the

first data store to the client device upon receipt of the second message by the client device.

Id. at 19:45–20:10; *see* Pet. 17–33 (quoting Ex. 1001, 19:45–20:10 (bracketed information by Petitioner)).

E. The Asserted Grounds

Petitioner challenges claims 1–44 of the '962 patent on the following grounds (Pet. 6):

Claims Challenged	35 U.S.C. §	References
1–8, 10–30, 32–44	103	Yared ¹ , Wills ² , Dunk ³
9, 31	103	Yared, Wills, Dunk, Cook ⁴

II. ANALYSIS

Petitioner challenges claims 1–44 as obvious based on the grounds listed above. Patent Owner disagrees.

A. Legal Standards

35 U.S.C. § 103(a) renders a claim unpatentable 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. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). Tribunals resolve obviousness on the basis of underlying factual

¹ Yared et al., US 2003/0149781 A1, published Aug. 7, 2003 (Ex. 1005).

² Wills et al., US 2005/0169285 A1, published Aug. 4, 2005 (Ex. 1008).

³ Dunk, US 2005/0188098 A1, published Aug. 25, 2005 (Ex. 1009).

⁴ Cook et al., US 7,783,281 B1, issued Aug. 24, 2010 (Ex. 1007).

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) where in evidence, so-called secondary considerations. *See Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). Prior art references must be “considered together with the knowledge of one of ordinary skill in the pertinent art.” *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994) (citing *In re Samour*, 571 F.2d 559, 562 (CCPA 1978)).

B. Level of Ordinary Skill in the Art

Dr. Wills testifies that a person having ordinary skill in the art (“POSITA”) “would have had a bachelor’s degree in electrical engineering, computer engineering, computer science, or the equivalent and 2-3 years of work experience with computer networks, or the equivalent.” Ex. 1003 ¶ 14.

Patent Owner does not present a proposed level of ordinary skill. For purposes of this Decision, we adopt Petitioner’s proposed level of ordinary skill in the art, which comports with the teachings of the ’962 patent and the asserted prior art.

C. Claim Construction

In an *inter partes* review, we construe each 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) (2019). Under the same standard applied by district courts, claim terms take their plain and ordinary meaning as would have been understood by a person of ordinary skill in the art at the time of the invention and in the context of the entire patent disclosure. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005) (en banc). “There are only two exceptions to this general rule: 1) when a patentee sets out a definition and

acts as his own lexicographer, or 2) when the patentee disavows the full scope of a claim term either in the specification or during prosecution.” *Thorner v. Sony Comput. Entm’t Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012).

Based on the current record, no terms require explicit construction. *See, e.g., Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (“[W]e need only construe terms ‘that are in controversy, and only to the extent necessary to resolve the controversy’” (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))).

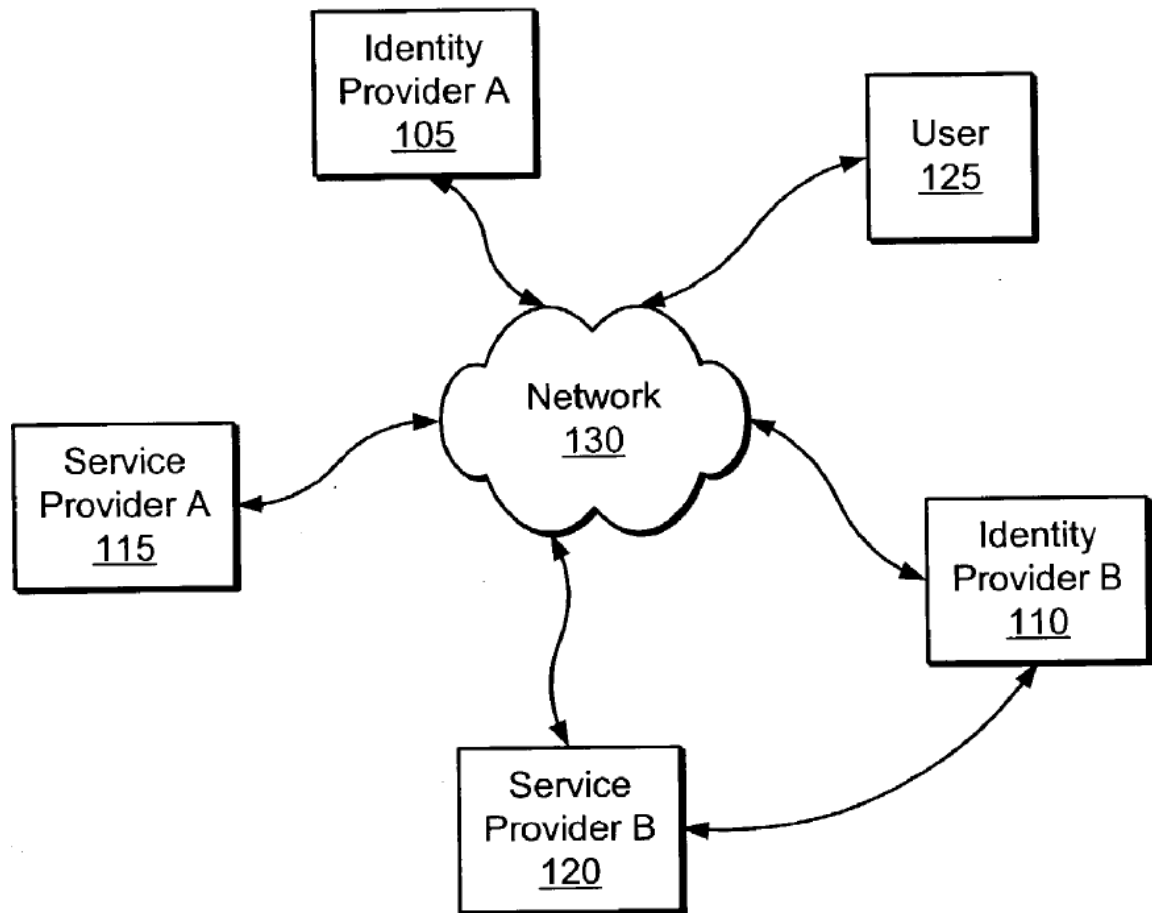
D. Obviousness, Yared, Wills, and Dunk

Petitioner contends the subject matter of claims 1–8, 10–30, and 32–44 would have been obvious over the combination of Yared, Wills, and Dunk. Pet. 8–59. Patent Owner disputes Petitioner’s contentions. Prelim. Resp. 9–40.

1. Yared

Yared, titled “Distributed Network Identity,” describes a “single sign-on architecture . . . where an identity provider is used to facilitate cross-domain authentication” among various service providers and “to enhance user convenience.” Ex. 1005, codes (54), (57). Yared’s system links identity providers and service providers “to enable information sharing and aggregation” and provides “[u]ser policies and privacy preferences . . . to control how information is shared.” *Id.*

Yared's Figure 1 follows, and illustrates a distributed identity system:



Yared's Figure 1 shows identity providers 105 and 110, service providers 115, 120, and user 125, all connected via network 130. *Id.* ¶ 42. To facilitate authentication, Yared's system employs "cookies" and other data. "The cookie is a mechanism of storing information on an Internet browser that can be presented in websites. An identity provider can write a cookie [to a user] that a service provider is able to recognize and thereby authenticate the user." *Id.* ¶ 52.

Yared's system also employs HTTP "redirection" as part of its authentication and access scheme:

Redirection causes a browser to access a different resource identified by a uniform resource identifier (URI) or uniform

resource locator (URL). A uniform resource identifier (URI) is a string of characters used for identifying an abstract or physical resource. A URI or URL can contain additional information, such as a query parameter, to send to the destination website. In an embodiment, an identity provider embeds a secure credential as an HTTP parameter for a service provider. A credential is data that is transferred or presented to establish either a claimed identity or the authorizations of a system entity. Credentials generally include the data necessary to prove an assertion. By embedding a credential, an identity provider can communicate the necessary authentication information to a service provider. Therefore, HTTP redirect enables a single sign-on framework within the existing HTTP infrastructure.

Id. ¶ 54.

By way of a redirect example, Yared's system "embed[s]" the following "[p]arameter[s] within a [r]edirect":

"http://www.foobar.com/auth . . . [r]edirects to foobar.com"; and

"http://www.foobar.com/auth?id=1234 . . . [r]edirects to

foobar.com and also passes an HTTP parameter 'ID' with the value '1234.'" *Id.*

2. *Wills*

Wills, titled "Stateful Push Notifications," describes methods for forming and processing push notifications and client state information for a client device. *See* Ex. 1008, codes (54), (57). Wills further describes "embedding validation metadata and intelligent filtering metadata with the client state information." *Id.* ¶ 12.

3. *Dunk*

Dunk, titled "System and Method for Maintaining a Network Connection," describes a system that maintains a persistent connection between a client and a web server via a physical link that "includes at least

one network address translation (‘NAT’) router . . . configured to terminate idle connections.” Ex. 1009, codes (54), (57). Dunk’s client “send[s] keep-alive packets to the web-server in order to reduce the likelihood of the NAT router terminating the connection.” *Id.* at code (57).

4. *Claims 1–8, 10–30, and 32–44*

Petitioner contends that Yared teaches “**“a server can host . . . [the] identity provider”**” and the identity provider can include various computing devices, including ‘enterprise *servers*’ as well as ‘application *servers*.’” Pet. 17 (quoting Ex. 1005 ¶¶ 43, 45) (citing Ex. 1003 ¶ 27) (emphases by Petitioner).

Regarding “[1.1a] a memory and processor,” Petitioner contends that Yared teaches “the identity provider [server] ‘can be implemented by **program instructions that execute in an appropriate computing device.**’” *Id.* at 18 (quoting Ex. 1005 ¶ 43) (emphasis by Petitioner). Petitioner relies on Yared’s disclosure of a number of examples of computing devices that could be used as the identity provider and contends that “[a] POSITA would have understood these ‘computing devices’ to include a memory (e.g., a hard drive or random access memory (RAM)) and a processor (e.g., a general purpose central processing unit (CPU) or an application specific integrated circuit (ASIC)).” *Id.* at 18–19 (citing Ex. 1003 ¶ 30; Ex. 1005 ¶ 43; Ex. 1008 ¶¶ 4, 57, Fig. 7).

Regarding “[1.1b] the server communicatively coupled to a network and a plurality of data stores,” Petitioner contends that Yared teaches “an identity provider (server) and service providers (data stores) ‘can be linked to enable information sharing and aggregation.’” *Id.* at 19 (quoting Ex. 1005, Abstract) (citing Ex. 1003 ¶¶ 31–33).

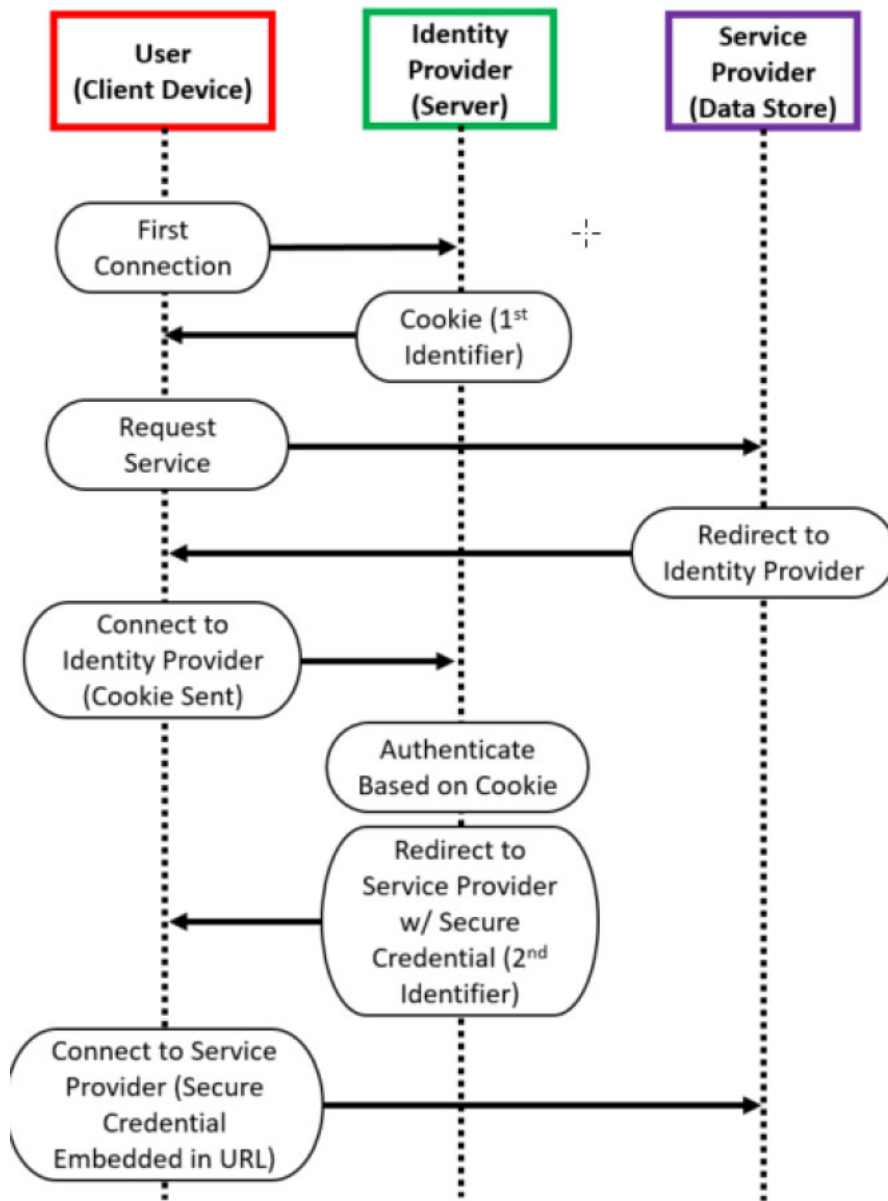
Regarding “[1.2] wherein the server is configured to: send a first identifier to a client device upon the client device communicating with the server over a connection,” Petitioner contends that Yared teaches a “‘user 125’ (client device) is coupled to the ‘network 130,’ along with the identity provider 105 (server) and the service providers 115 and 120 (data stores).” *Id.* at 22 (quoting Ex. 1005 ¶42). Petitioner further contends that Yared teaches “the ‘user 125’ (client device) can authenticate with and ‘**obtain an assertion from identity provider A 105**’ (server), such as a ‘**session cookie**’ (first identifier).” *Id.* at 23 (quoting Ex. 1005 ¶¶ 46, 66) (citing Ex. 1003 ¶ 35) (emphases by Petitioner). Moreover, Petitioner contends, “Yared teaches that the identity provider can ‘**write[] a session cookie** the first time a user logs in’ (e.g., by utilizing functionality in a browser executed by user 125) in order to store session information for subsequent authentication.” *Id.* (quoting Ex. 1005 ¶ 66) (citing Ex. 1003 ¶ 35) (emphasis by Petitioner).

Regarding “wherein the server is configured to . . . [1.3] receive registration information from the client device,” Petitioner contends that Yared teaches “a user can log into the identity provider and ‘update’ their account by entering information into editable fields.” *Id.* at 24 (citing Ex. 1005 ¶ 87). In particular, Petitioner contends that “user information that is sent to the identity provider and made available to the service providers is registration information. *Id.* at 25–26 (citing Ex. 1003 ¶ 37).

Regarding “wherein the server is configured to . . . [1.4] send a second identifier to the client device in response to the received registration information,” Petitioner contends that “[a]n example of the claimed second identifier is the secure credential embedded in the HTTP redirect URL by the identity provider and sent to the client device.” *Id.* at 26 (citing Ex. 1003

¶ 41; Ex. 1005 ¶ 54). Petitioner explains that in Yared “a ‘user that desires identity authentication with service provider 310’ (data store) can ‘go[] to service provider 310 and select[] an identity provider,’” and “[o]nce identity provider 305 authenticates the user, the identity provider 305 ‘redirects the user’s browser back to service provider 310 *passing a transient, encrypted authenticated credential 335 embedded within the URI.*’” *Id.* (quoting Ex. 1005 ¶ 65) (emphasis by Petitioner). Petitioner contends “the embedded credential is associated with the user’s account information (registration information) because the identity provider generates the embedded credential after authenticating the user . . . and receiving the user’s account information.” *Id.* at 27 (citing Ex. 1003 ¶ 44; Ex. 1005 ¶ 65).

Petitioner provides an “exemplary process exemplary process flow illustrating the above-described redirect process, as prepared by Dr. Wills based on Yared’s disclosure,” as reproduced here (Pet. 27–28):



Id. at 28 (citing Ex. 1005 ¶¶ 46, 52, 54, 65, 66; Ex. 1003 ¶¶ 42, 44). The process flow diagram above shows a user/client device receiving an embedded secure second credential (second identifier) so that the user/client device can send the embedded credential to a data store. *See* Ex. 1005 ¶¶ 46, 52, 54, 65, 66; Ex. 1003 ¶¶ 42–44.

Patent Owner contends that Yared does not teach “wherein the server is configured to . . . [1.4] send a second identifier to the client device *in response to the received registration information*.” See Prelim. Resp. 31 (emphasis by Patent Owner). According to Patent Owner, “[e]ven if Yared did teach its embedded credential being sent to the user, the Petition fails to even argue, let alone prove, that Yared does so ‘in response to the received registration information.’” *Id.* at 31. Quoting Petitioner, Patent Owner contends that “the only thing the Petition says about Yared’s user account information in this limitation is that ‘the embedded credential is *associated* with the user’s account information (registration information) because the identity provider generates the embedded credential after authenticating the user . . . and receiving the user’s account information.’” *Id.* at 33–34 (quoting Pet. 27) (emphasis by Patent Owner).

Patent Owner raises a valid point. Petitioner only alleges “the embedded credential is associated with the user’s account information” (Pet. 27) and fails to explain how merely associating the embedded credential with the user’s account information addresses how the second identifier is sent “in response to the received registration information” as limitation [1.4] requires. See Pet. 27–28 (citing Ex. 1005 ¶ 65; Ex. 1003 ¶ 44).

In turn, at the cited paragraph, Dr. Wills testifies that “the redirect message from the identity provider to the service provider, as illustrated above, would automatically include the registration information associated with the particular user so that the service provider will have the necessary account information of the user in performing the requested service.” Ex. 1003 ¶ 44. Although Petitioner cites to this testimony, the Petition does not advance Dr. Wills’ theory that underlies the testimony. See Pet. 27 (citing

1003 ¶ 44). Even if we deem the Petition to properly incorporate Dr. Wills’ theory that “the redirect message from the identity provider . . . would automatically include the registration information,” the record does not support the theory, as Patent Owner argues. *See* Prelim. Resp. 33–34.⁵ Dr. Wills’ testimony cites to Yared’s paragraph 87 for support (Ex. 1003 ¶ 44), but that paragraph neither mentions Yared’s redirect procedures nor otherwise suggests that the redirect message includes the registration relied-upon information. *See* Ex. 1005 ¶ 87. Also, Dr. Wills’ testimony does not explain sufficiently how something that Yared’s identity provider (server) renders “automatically available to service providers” (*see id.*) means that the identity provider transmits that information in Yared’s redirect message or why this transmission would have been obvious.

Petitioner relies on the same showing to address independent claim 23, which contains in material respects the same limitations as claim 1. *See* Pet. 54. Claims 2–8, 10–22, 24–30, and 32–44 depend from claim 1 or claim 23. Accordingly, based on the foregoing discussion, the Petition fails to show a reasonable likelihood of prevailing as to claims 1–8, 10–30, and 32–44.

E. Obviousness, Yared, Wills, Dunk, and Cook

Petitioner contends claims 9 and 31 would have been obvious over the combination of Yared, Wills, Dunk, and Cook. Pet. 59–63. Claims 9 and 31 depend respectively from claims 1 and 23. Petitioner relies on the same

⁵ Patent Owner also contends that considering the testimony as part of the Petition constitutes an improper incorporation by reference. Prelim. Resp. 33 (citing 37 C.F.R. § 42.6(a)(3) (“Arguments must not be incorporated by reference from one document into another document.”)).

showing addressed above to reach the above-discussed limitations of claims 1 and 23. *See id.*

Accordingly, based on the foregoing discussion, the Petition fails to show a reasonable likelihood of prevailing as to claims 9 and 31.

III. CONCLUSION

After considering the evidence and arguments presented in the Petition and the Preliminary Response, we determine that Petitioner has not demonstrated a reasonable likelihood that it would prevail with respect to its unpatentability challenges. Accordingly, we deny the request to institute an *inter partes* review of the challenged claims on the grounds in the Petition.

IV. ORDER

Accordingly, it is
In consideration of the foregoing, it is hereby

ORDERED that the Petition is *denied* as to claims 1–44 of the '962 patent; and

FURTHER ORDERED that no *inter partes* review is instituted.

PETITIONER:

Walter Renner
axf-ptab@fr.com
Stuart Nelson
snelson@fr.com
Dan Smith
dsmith@fr.com
Hyun Jin In
in@fr.com

PATENT OWNER:

Kenneth Weatherwax
weatherwax@lowensteinweatherwax.com
Bridget Smith
smith@lowensteinweatherwax.com
Patrick Maloney
maloney@lowensteinweatherwax.com
Flavio Rose
rose@lowensteinweatherwax.com
Parham Hendifar
hendifar@lowensteinweatherwax.com
Edward Hsieh
hsieh@lowensteinweatherwax.com
Jason Linger
linger@lowensteinweatherwax.com