

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

NETSKOPE, INC.,
Petitioner,

v.

BITGLASS, INC.,
Patent Owner.

IPR2021-01045
Patent 10,757,090 B2

Before JAMES J. MAYBERRY, KEVIN C. TROCK, and
SHEILA F. McSHANE, *Administrative Patent Judges*.

TROCK, *Administrative Patent Judge*.

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

ORDER
Dismissing Petitioner's Motion to Strike
37 C.F.R. § 42.23(b)
Dismissing Patent Owner's Motion to Strike
37 C.F.R. § 42.23(b)
Dismissing Petitioner's Motion to Exclude
37 C.F.R. § 42.64(c)

I. INTRODUCTION

We have authority to hear this *inter partes* review under 35 U.S.C. § 6. This Final Written Decision issues pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73. For the reasons discussed below, we determine that Netskope, Inc. (“Petitioner”) has proven by a preponderance of the evidence that claims 1–5, 8–13, and 16 (the “challenged claims”) of U.S. Patent No. 10,757,090 B2 (Ex. 1001, “the ’090 patent”) are unpatentable. *See* 35 U.S.C. § 316(e) (2018); 37 C.F.R. § 42.1(d) (2022).

A. Procedural History

Petitioner filed a Petition (Paper 2, “Pet.” or “Petition”) to institute an *inter partes* review of the challenged claims of the ’090 patent. Bitglass, Inc. (“Patent Owner”) filed a Preliminary Response. Paper 6 (“Prelim. Resp.”). We instituted *inter partes* review on all challenged claims on the grounds presented in the Petition. Paper 11 (“Institution Decision” or “Dec.”).

After institution, Patent Owner filed a Response to the Petition. Paper 15 (“PO Resp.”). Petitioner thereafter filed a Reply (Paper 17, “Pet. Reply”) and Patent Owner filed a Sur-reply (Paper 18, “PO Sur-reply”).

With our authorization (Ex. 3001), Petitioner filed a Motion to Strike. Paper 20 (“Mot. to Strike”). Patent Owner filed an “Opposition to Motion to Strike and Counter Motion to Strike Petitioner’s Reply.” Paper 23 (“Mot. to Strike Opp.”). Petitioner filed a Motion to Exclude Evidence. Paper 25 (“Mot. to Exclude”). Patent Owner filed an Opposition to the Motion to Exclude (Paper 26, “Mot. to Exclude Opp.”), and Petitioner filed a Reply to the Opposition (Paper 27, “Mot. to Exclude Reply”).

An oral hearing was held on September 19, 2022. A transcript of the hearing is included in the record. Paper 29 (“Tr.”).

B. Related Matters

According to the parties, the '090 patent is the subject of the following action: *Netskope, Inc. v. Bitglass, Inc.*, No. 3:21-cv-00916 (N.D. Cal.). Pet. 2; Paper 4, 2.

The parties also acknowledge that Petitioner has filed another petition (IPR2021-01046) challenging claims 17–21 and 24 of the '090 patent. Pet. 2; Paper 4, 2.

Further, the parties identify a continuation of the '090 patent (U.S. Patent No. 10,855,671 B2, “the '671 patent”), and further acknowledge that Petitioner has filed two petitions (PGR2021-00091 and PGR2021-00092) challenging claims of the '671 patent. Pet. 2; Paper 4, 2.

C. The '090 Patent (Ex. 1001)

The '090 patent relates, in relevant part, to providing secure user access to applications which are hosted by a remote server, e.g., “cloud applications.” Ex. 1001, 2:28–29, 5:61–62, 6:23–24; *see id.* at 3:5–9. In particular, the '090 patent describes using network proxies to route user access requests and provide secure access. *See id.* at 5:60–6:22. Figure 3b of the '090 patent is reproduced below.

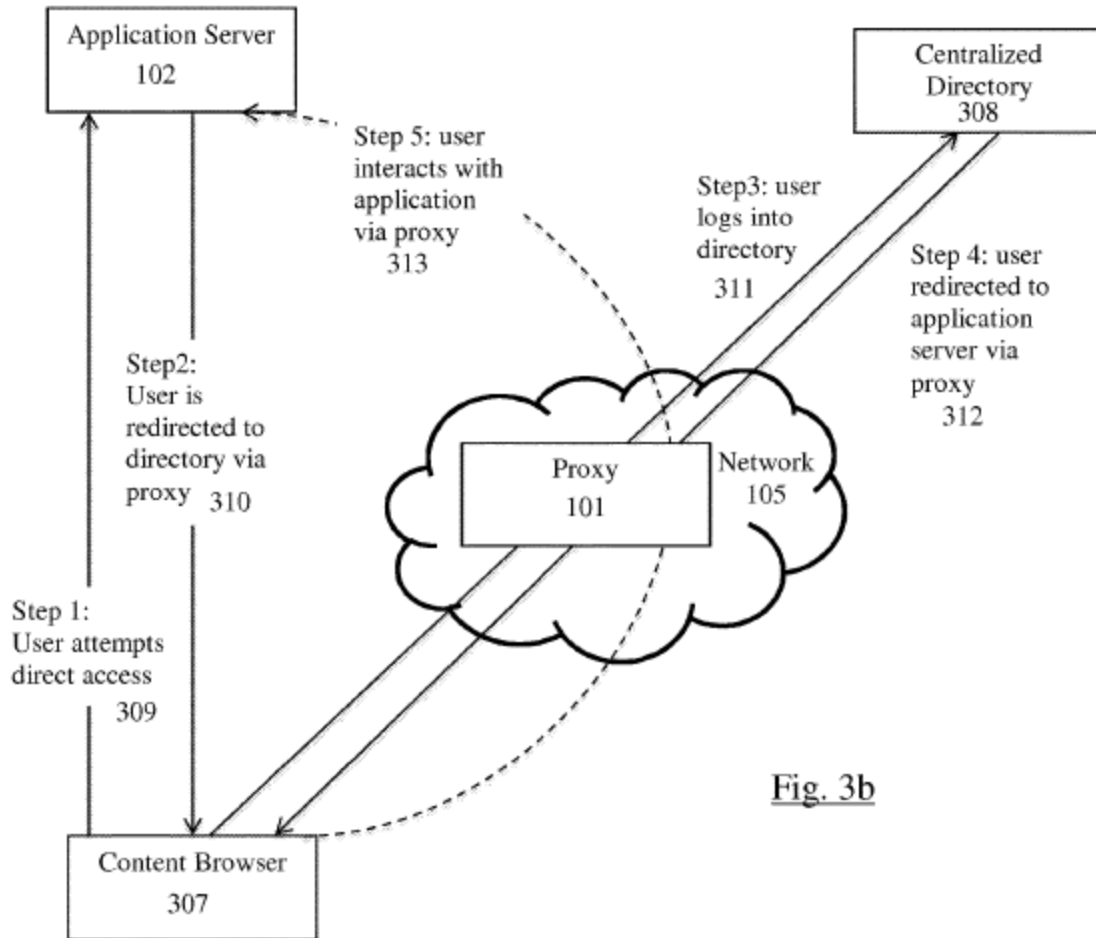


Fig. 3b

Figure 3b, above, shows a network having a proxy that enables a user's content browser access to an application hosted on an application server. *Id.* at 2:5–6, 6:23–24. In order to access an application hosted on an application server, a user must first login. *Id.* at 6:4–5, 6:23–24. As shown in Figure 3b, in step 1, “a user attempts access 309 to the application [hosted on the application server] 102 via a content browser 307.” *Id.* at 6:23–24. In step 2, “application server 102 may redirect 310 the [access] request to point to the centralized directory 308 via the proxy 101.” *Id.* at 6:25–26. In step 3, centralized directory 308 receives the user's login credentials and performs a login process. *Id.* at 6:12–17, 6:26–28. After a successful login, the user's content browser 307 is directed to the application server 102 by the proxy 101 and the user's content browser 307 then interacts with the

application hosted on application server 102. *Id.* at 6:28–39. As described above, proxy 101 “broker[s] all authentication requests and manipulat[es] the requests and responses” to provide access to resources. *Id.* at 6:39–41.

In another embodiment in which a proxy helps manage user content requests and security, a Security Assertion Markup Language (SAML) proxy is used to provide a user secure access to an application provided by an application provider. *Id.* at 2:23–24, 6:44–51. Figure 11 of the ’090 patent is reproduced below.

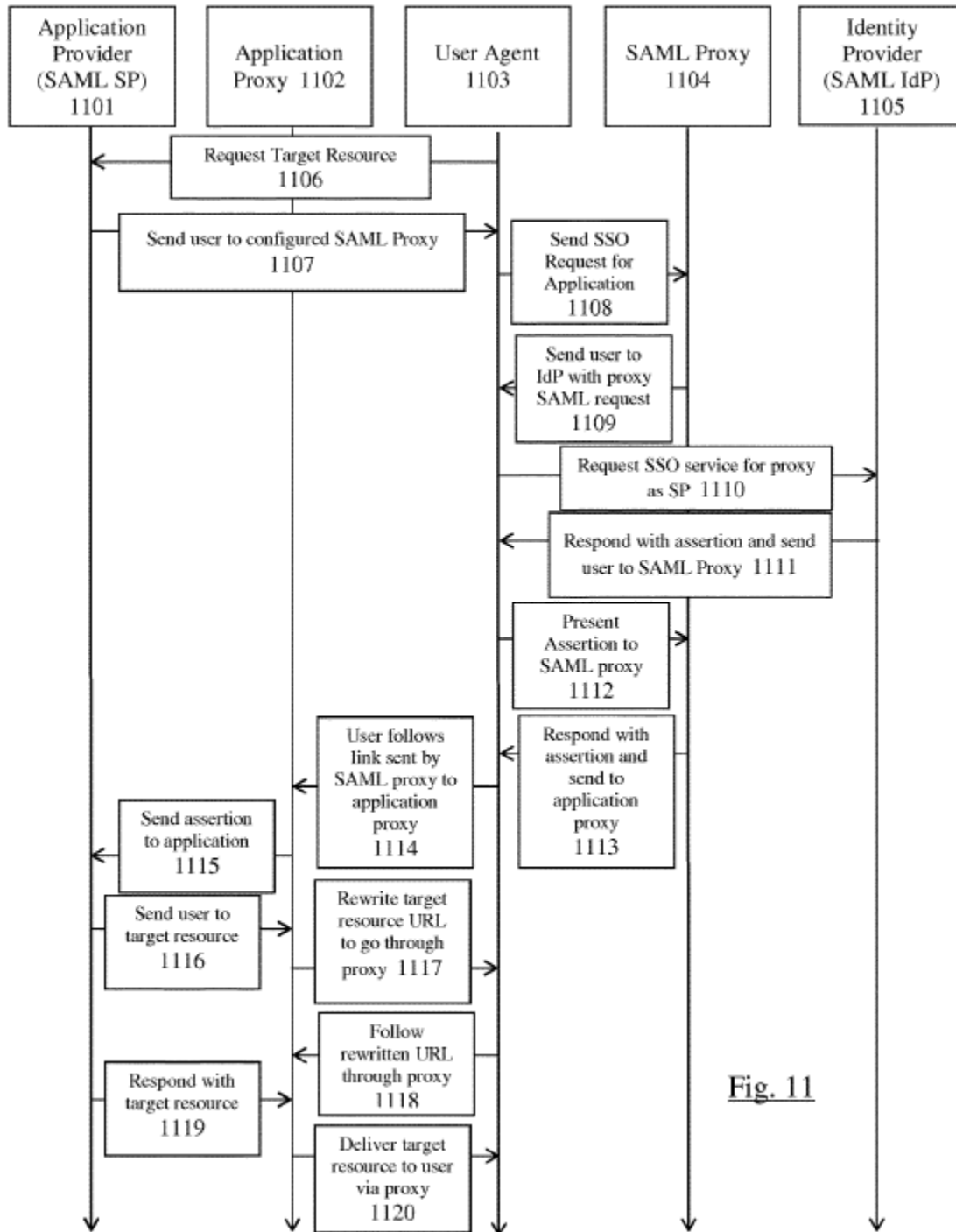


Fig. 11

Figure 11, above, depicts a flow diagram showing communication sequences and data exchanges between a SAML proxy and various “entities.” *Id.* at 2:23–24, 6:44–49. As shown in Figure 11, in order to provide users access to resources, a series of communication sequences and

data exchanges occur between SAML proxy 1104, application provider/application 1101, application proxy 1102, user agent 1103, and identity provider (IdP) 1105. *Id.* at 6:49–52. First, in block 1106, user agent 1103 sends a request to application provider 1101 for a target resource provided by application provider 1101. *Id.* at 7:4–5. In response, in block 1107, application provider 1101 directs user agent 1103 to SAML proxy 1104, and, in block 1108, “user agent 1103 sends a single sign on (SSO) request for the application” to SAML proxy 1104. *Id.* at 7:5–9. In block 1109, SAML proxy 1104 receives the SSO request and directs user agent 1103 to IdP 1105 so that, in block 1110, user agent 1103 sends an SSO request to IdP 1105. *Id.* at 7:9–13. Next, in block 1111, IdP 1105 validates and authenticates the SSO request and provides user agent 1103 “an assertion of a valid SSO . . . for the SAML proxy.” *Id.* at 6:58–59, 7:13–15. Following that, in block 1112, user agent 1103 sends the assertion to SAML proxy 1104 so that, in block 1113, SAML proxy 1104 creates an assertion for application proxy 1102 and sends that assertion and the location of application proxy 1102 (e.g., an IP address) to user agent 1103. *Id.* at 7:15–19. Having the assertion and location of application proxy 1102, user agent 1103 receives the target resource via application proxy 1102. *See id.* at 7:20–38.

In the embodiment of Figure 11, as shown in blocks 1114–1120, user agent 1103 accesses the resources of application provider 1101 using application proxy 1102 as an intermediary. *See id.* However, user agent 1103 may also access application provider 1101 directly. In the case that “application proxy 1102 goes down or its functionality deteriorates . . . SAML proxy 1104 routes the user directly to the application 1101,

bypassing the application proxy 1102” in order to provide “failover” protection. *Id.* at 6:64–7:1.

D. Challenged Claims

Petitioner challenges claims 1–5, 8–13, and 16 of the ’090 patent. Pet. 1. Claims 1 and 9 are independent and recite similar limitations. Claim 1, however, is directed to a method for improving secure access to application programs, whereas claim 9 is directed to a non-transitory computer readable medium. Claim 1 is representative and is reproduced below.

- 1[pre] A method for improving secure access to application programs, comprising:
 - 1[a][i] receiving, by a proxy server, a single-sign-on request from a device for access to an application program,
 - 1[a][ii] the device directed by an application server to a cloud network location of the proxy server,
 - 1[a][iii] the proxy server configured to authenticate computer security validation requests for the application program;
 - 1[b][i] directing, by the proxy server, the device to an identity provider by sending the device a network location of the identity provider,
 - 1[b][ii] the identity provider configured to authenticate computer security validation requests for the proxy server,
 - 1[b][iii] the device communicates directly with the identity provider using the network location of the identity provider,
 - 1[b][iv] the identity provider redirects the device to the cloud network location of the proxy server with a single-sign-on validation after validation of the single-sign-on request;

- 1[c] receiving, at the proxy server, the single-sign-on validation from the device;
- 1[d] creating, by the proxy server, a valid identification assertion;
- 1[e][i] directing, by the proxy server, the device to the application server by sending the device a network location of the application server and the valid identification assertion,
- 1[e][ii] the device communicates directly with the application server using the network location of the application server and the valid identification assertion,
- 1[e][iii] the device thereafter communicates directly with the application server for subsequent accesses to the application program.

Ex. 1001, 13:56–14:19 (bracketed labeling designated by Petitioner; *see* Pet. 20–39).

E. Evidence

Petitioner relies upon the following evidence:

(1) U.S. Patent Application Publication No. US 2015/0319156 A1, published November 5, 2015 (“Guccione”) (Ex. 1004);

(2) Jill Gemmill *et al.*, *Cross-domain Authorization for Federated Virtual Organizations Using the myVocs Collaboration Environment*, Concurrency and Computation: Practice and Experience (2008) (“Gemmill”) (Ex. 1005);

(3) U.S. Patent Application Publication No. US 2012/0278872 A1, published November 1, 2012 (“Woelfel”) (Ex. 1006);

(4) WIPO Publication No. WO 2005/069823 A2, published August 4, 2005 (“Song”) (Ex. 1007); and

(5) Declarations of Michael Franz, Ph.D. (Exs. 1002, 1017).

Patent Owner relies upon the Declaration of Seth James Nielson, Ph.D. (Ex. 2002).

F. Asserted Grounds of Unpatentability

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1–5, 9–13	103	Guccione, Woelfel
8, 16	103	Guccione, Woelfel, Song
1–5, 9–13	103	Gemmill, Woelfel
8, 16	103	Gemmill, Woelfel, Song

Pet. 4.

II. ANALYSIS

A. Principles of Law: Obviousness

Petitioner asserts that the challenged claims would have been obvious in view of the asserted prior art. Pet. 1. A claim is unpatentable as obvious 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) objective evidence of nonobviousness, i.e., secondary considerations.¹ *See Graham*, 383 U.S. at 17–18.

The Supreme Court has made clear that we apply “an expansive and flexible approach” to the question of obviousness. *KSR*, 550 U.S. at 415.

¹ The parties do not argue, nor direct us to, any objective evidence of nonobviousness.

Whether a patent claiming the combination of prior art elements would have been obvious is determined by whether the improvement is more than the predictable use of prior art elements according to their established functions. *Id.* at 417. Reaching this conclusion, however, requires more than a mere showing that the prior art includes separate references covering each separate limitation in a claim under examination. *Unigene Labs., Inc. v. Apotex, Inc.*, 655 F.3d 1352, 1360 (Fed. Cir. 2011). Rather, obviousness requires the additional showing that a person of ordinary skill at the time of the invention would have selected and combined those prior art elements in the normal course of research and development to yield the claimed invention. *Id.*

B. Level of Ordinary Skill

In determining whether an invention would have been obvious, we consider the level of ordinary skill in the pertinent art at the time of the invention. *Graham v. John Deere Co.*, 383 U.S. 1, 17 (1966). “The importance of resolving the level of ordinary skill in the art lies in the necessity of maintaining objectivity in the obviousness inquiry.” *Ryko Mfg. Co. v. Nu-Star, Inc.*, 950 F.2d 714, 718 (Fed. Cir. 1991).

Petitioner describes a person of ordinary skill in the art as a person having “a bachelor’s degree in computer science, computer engineering, or electrical engineering (or equivalent experience) and [having] at least two years of experience with applying web-based service computing technologies, including the then-current technologies such as HTML, XML, Java, and JavaScript.” Pet. 12 (citing Ex. 1002 ¶¶ 24–28). In the Institution Decision, we adopted Petitioner’s assessment of the level of ordinary skill. Dec. 9–10.

In its Response, Patent Owner states that it “does not dispute the Board’s definition of a person of ordinary skill in the art.” PO Resp. 11.

As we stated in the Institution Decision, Petitioner’s description of the level of ordinary skill is generally consistent with the subject matter of the ’090 patent. Paper 11, 10. For purposes of this Final Decision, we continue to use Petitioner’s assessment of the level of ordinary skill.

C. Claim Construction

In this proceeding, a claim shall be construed 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 (2021). We therefore apply the claim construction standard as set forth in *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc).

Under *Phillips*, claim terms are generally given their ordinary and customary meaning as would be understood by one with ordinary skill in the art in the context of the specification, the prosecution history, other claims, and even extrinsic evidence including expert and inventor testimony, dictionaries, and learned treatises, although extrinsic evidence is less significant than the intrinsic record. *Phillips*, 415 F.3d at 1312–17. Usually, the specification is dispositive, and it is the single best guide to the meaning of a disputed term. *Id.* at 1315.

Only terms that are in controversy need to be construed, and then only to the extent necessary to resolve the controversy. *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co. Matal*, 868 F.3d 1013, 1017 (Fed. Cir.

2017) (in the context of an *inter partes* review, applying *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

In the Institution Decision, we determined that no claim term required express construction at that stage of the proceeding. Dec. 10–11. In its Response, Patent Owner states that it “does not believe that the Board needs to address any claim construction issue.” PO Resp. 11. In this Final Decision, we do not construe expressly any claim terms, and use a term’s ordinary and customary meaning as explained in *Phillips*.

D. Relevant Prior Art

1. Guccione (Ex. 1004)

Guccione is a U.S. Patent Publication that published November 5, 2015, and claims priority to two provisional applications filed on December 12, 2012, and February 15, 2013 (Ex. 1004, code (60)), before the earliest priority date of the ’090 Patent (Ex. 1001, code (63)). Petitioner asserts that Guccione is prior art under 35 U.S.C. § 102(a)(2). Pet. 4.

Guccione describes techniques for “authenticating a user and/or a user equipment (UE)” when the user or UE “request[s] access to a service controlled by a service provider (SP).” Ex. 1004, code (57). Guccione further explains that authentication can be provided by single sign-on (SSO) services. *Id.* ¶ 28. “An entity that offers an SSO service may be referred to” in Guccione “as an Identity Provider (IdP).” *Id.* ¶ 28. As such, “a mobile network operator (MNO) that offers an SSO service and an independent entity,” i.e., a third party, “that offers an SSO service may both be referred to as an IdP.” *Id.* Figure 4 of Guccione is reproduced below.

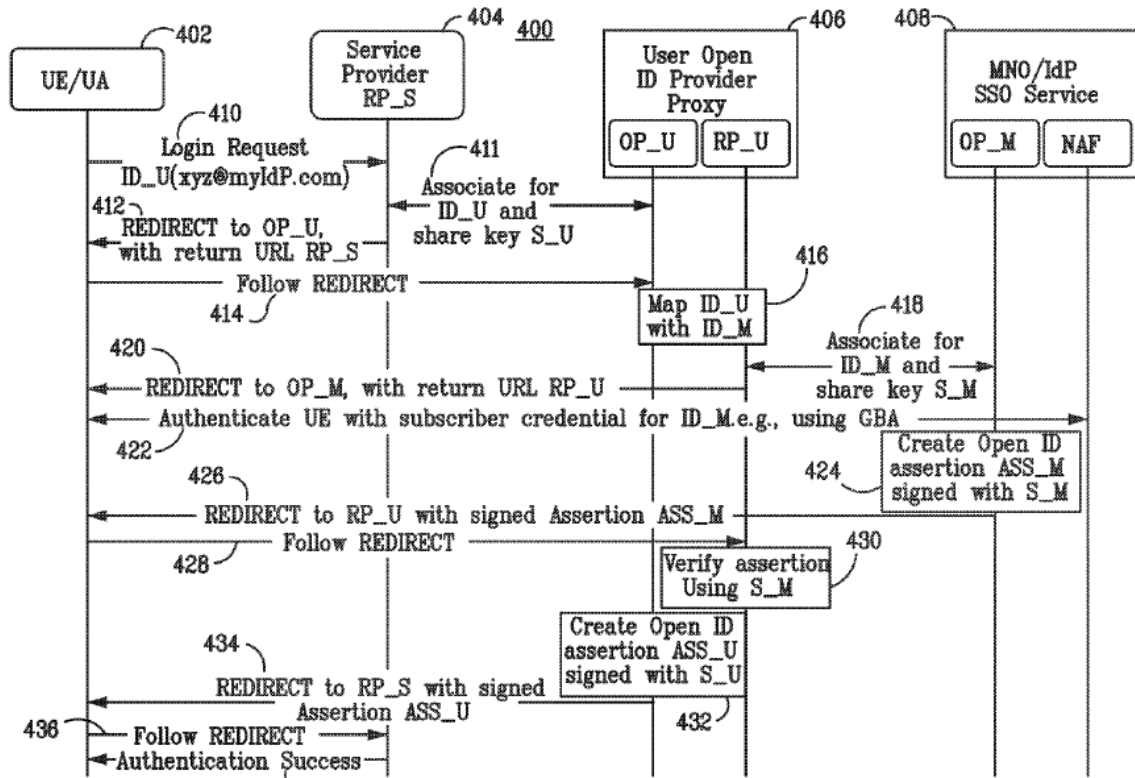


FIG. 4

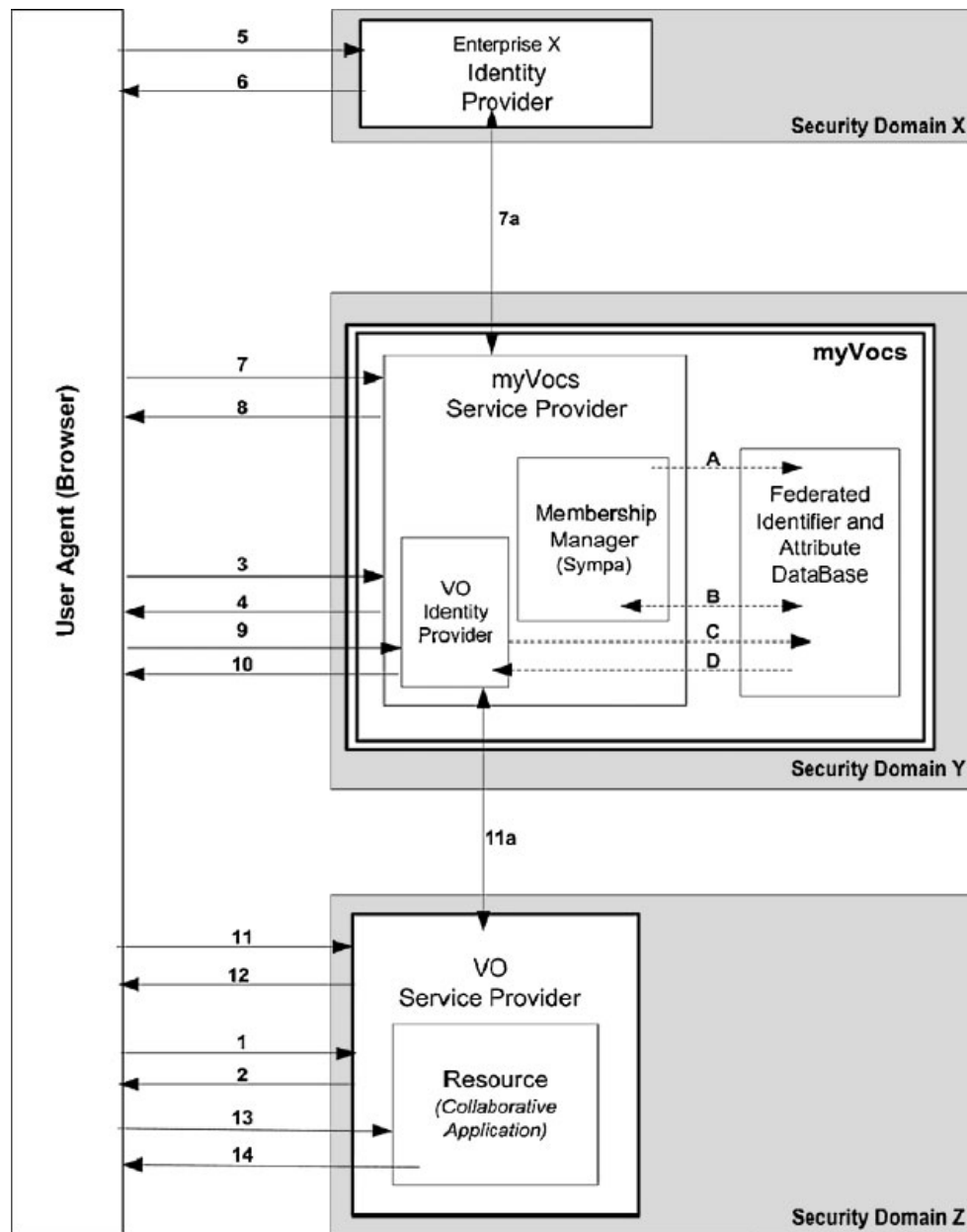
Figure 4, above, is a flow diagram illustrating a technique in which an MNO authenticates a UE for access to a service. *Id.* ¶¶ 10, 52. As shown in Figure 4, network 400 includes UE 402, service provider SP 404, user IdP proxy 406 and MNO 408 (which also functions as an IdP). *Id.* ¶ 52. The authentication process begins at flow 410, where “the user wants to login to a service, and thus requests access to the service provided by the SP 404 using an original user identity (ID_U).” *Id.* In flows 412 and 414, UE 402 is redirected to user IdP proxy 406. *Id.* In flow 416, the original user identity ID_U is mapped to, and associated with, identifier ID_M that is known by MNO 408. *Id.* ¶¶ 52–53. After the mapping and association of ID_M, UE 402 is redirected to MNO 408 in flow 420. *Id.* ¶ 53. MNO 408 authenticates UE 402 using UE 402’s “subscriber credentials” in flow 422 and further creates and signs an “authentication assertion” in flow 424, e.g.,

an Open ID assertion. *Id.* In flows 426 and 428, UE 402 is redirected to user IdP proxy 406, which, in flow 430, verifies the Open ID authentication assertion. *Id.* In turn, user IdP proxy 406 creates and signs a second Open ID authentication assertion in flow 432. *Id.* In flows 434–438, UE 402, along with the received second Open ID authentication assertion, is redirected to user IdP proxy 406 which receives the second Open ID authentication assertion, authenticates UE 402, and, so, grants UE 402 access to the service provided by the SP 404. *Id.* The procedure described in Figure 4 is “a one-factor authentication” where MNO 408 authenticates UE 402. *Id.* ¶ 54.

2. *Gemmill (Ex. 1005)*

Gemmill is a paper that published July 22, 2008 (Ex. 1005, 509), before the earliest priority date of the '090 Patent (Ex. 1001, code (63)). Petitioner asserts that Gemmill is prior art under 35 U.S.C. § 102(a)(1). Pet. 4.

Gemmill describes the implementation of myVocs (my Virtual Organization Collaboration System) and Shibboleth to provide security and authentication for access to resources across different domains (e.g., resource providers such as Yahoo or Google). Ex. 1005, 509–510. Figure 2 of Gemmill is reproduced below.



Gemmill’s Figure 2, above, illustrates the myVocs architecture components and further shows message flows between those components. *Id.* at 518–519. Regarding the components shown in Figure 2, the myVocs system (shown in double-lined box) within Security Domain Y includes “(1) a Shibboleth SP labeled ‘myVocs Service Provider’, (2) a Shibboleth [Identity Provider (IdP)] labeled ‘[virtual organization (VO)] Identity Provider’, (3) a VO membership management system labeled ‘Membership

Manager (Sympa)', and (4) a federated identifier and VO attribute data store labeled 'Federated Identifier and Attribute Database.'" *Id.* at 518. Further shown, in Security Domain Z, is "a Shibboleth [Service Provider (SP)], labeled 'VO Service Provider' protects some resource on one of many distributed web servers." *Id.* Still further shown, separately in Security Domain X, is a "Shibboleth IdP labeled 'Enterprise X Identity Provider.'" *Id.* Gemmill explains that a "Shibboleth IdP exposes an enterprise identity management system by leveraging a local authentication service," e.g., "a Shibboleth [single sign-on (SSO)] service." *Id.* at 515. Gemmill also explains that a Shibboleth SP provides web-based content and resources. *Id.*

Figure 2 also shows the message flows between components that provide authentication for a web browser client's, i.e., a User Agent, request for a resource from a VO Service Provider. *See id.* at 521–523. First, the "browser client requests a VO web resource protected by the VO SP" and is "redirected to the myVocs VO IdP component." *Id.* at 522. In flow 3, the "client makes a Shibboleth Authentication Request to the VO IdP." *Id.* The client is redirected to the appropriate IdP in flow 4 and, correspondingly, makes a Shibboleth Authentication Request to that IdP in flow 5 (i.e., to Enterprise X IdP). *Id.* In response to the Shibboleth Authentication Request, the IdP returns an authentication response to the client in flow 6. *Id.* Next, in flow 7, the client submits the authentication response to the SP at myVocs, where it is validated, and the client is redirected to the VO IdP in step 8. *Id.* The client again makes a Shibboleth Authentication Request to the VO IdP in flow 9; based on the previous authentication steps, a "security context" exists, and this time, the myVocs IdP authenticates the client based on the previous authentication response in flow 10. *Id.* With that authentication, next, in flows 11–14, the "client submits the authentication

response to the VO SP where the assertion is validated,” the client is directed to the VO resource, the client again requests the VO resource, and the resource is provided by the client. *Id.*

3. *Woelfel (Ex. 1006)*

Woelfel is a U.S. Patent Publication that published November 1, 2012, and claims priority to a provisional application filed on April 27, 2011 (Ex. 1006, codes (43), (60)), before the earliest priority date of the ’090 Patent (Ex. 1001, code (63)). Petitioner asserts that Woelfel is prior art under 35 U.S.C. § 102(a)(1). Pet. 4.

Woelfel describes client-server communicating in a network in which “user authentication . . . is mediated by a proxy.” Ex. 1006 ¶ 2. Woelfel explains that a server may provide “Software as a Service (SaaS),” i.e., “[c]loud applications.” *Id.* ¶ 6. Woelfel also explains that “a Single Sign-On infrastructure enables users to sign in once and have access to all authorized resources” and further describes a “federated SSO strategy” that “involves cooperation between independent network entities cooperating in SSO.” *Id.* ¶ 4.

4. *Song (Ex. 1007)*

Song is a World Intellectual Property Organization International Application that published August 4, 2005 (Ex. 1007, code (43)), before the earliest priority date of the ’090 Patent (Ex. 1001, code (63)). Petitioner asserts that Song is prior art under 35 U.S.C. § 102(a)(1). Pet. 4.

Song describes “centralized auditing of authentication, authorization and access control procedures for client computers to access networked servers and services.” Ex. 1007, 1:8–10. Song provides network access auditing when, e.g., the network “verifies the user’s identity, grants access rights to the identified user, [or] allows (or denies) the access request by the

access controller.” *Id.* at 4:18–24. Song does so by using a “transaction id, audit-request object and audit-response object” to “identify the transaction and log the events during the request process and response process.” *Id.* at 5:1–5. In particular, “the audit-response object can be just logged into a file.” *Id.* at 20:32–33.

E. Ground 1 - Obviousness over Guccione and Woelfel

For Ground 1, Petitioner contends that claims 1–5 and 9–13 would have been obvious under 35 U.S.C. § 103 over the teachings of Guccione and Woelfel. Pet. 13–46. Because we determine that all the challenged claims in the Petition are unpatentable on other asserted grounds (see Sections II.G and H, below) we need not reach ground 1. *See SAS Inst. Inc. v. Iancu*, 138 S. Ct. 1348, 1359 (2018); *see also Boston Sci. Scimed, Inc. v. Cook Grp. Inc.*, 809 F. App’x 984, 990 (Fed. Cir. 2020).

F. Ground 2 - Obviousness over Guccione, Woelfel, and Song

For Ground 2, Petitioner contends that dependent claims 8 and 16 would have been obvious under 35 U.S.C. § 103 over the teachings of Guccione, Woelfel, and Song. *See* Pet. 46–50. Because we determine that all the challenged claims in the Petition are unpatentable on other asserted grounds (see Sections II.G and H, below) we need not reach ground 2. *See SAS Inst. Inc.*, 138 S. Ct. at 1359; *see also Boston Sci. Scimed, Inc.*, 809 F. App’x at 990.

G. Ground 3 - Obviousness over Gemmill and Woelfel

For Ground 3, Petitioner contends that claims 1–5 and 9–13 would have been obvious under 35 U.S.C. § 103 over the teachings of Gemmill and Woelfel. Pet. 52–84. Claims 1 and 9 are independent and substantially identical, except that claim 1 recites a method and claim 9 recites a non-transitory computer readable medium.

In support of its challenge to these claims, Petitioner provides the testimony of Dr. Franz (Ex. 1002 ¶¶ 252–338; Ex. 1017 ¶¶ 30–50).

Patent Owner contests Petitioner’s evidence and arguments with respect to two limitations of the independent claims, namely, limitations 1[a][ii] and 1[b][iv], and the corresponding limitations of claim 9. *See* PO Resp. 19–25. Patent Owner also contests Petitioner’s evidence and arguments with respect to Petitioner’s rationale to combine the teachings of Gemmill and Woelfel. *See id.* at 25–27. Patent Owner provides the testimony of Dr. Nielson in support of its position. *See* Ex. 2002. Patent Owner does not contest the remaining limitations of the independent claims.

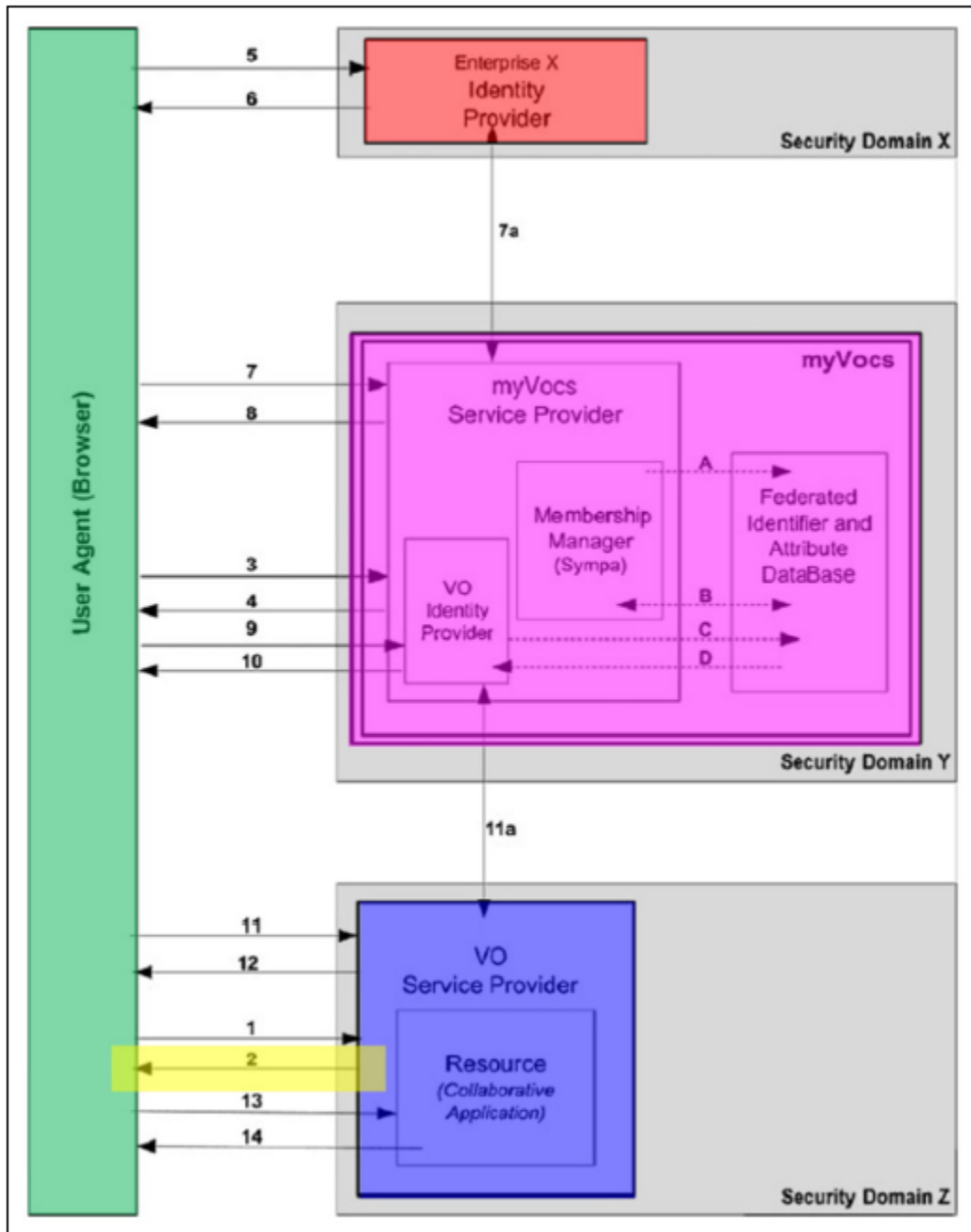
We address the disputed issues below. *In re NuVasive, Inc.*, 841 F.3d 966, 974 (Fed. Cir. 2016) (“The Board . . . [is] not required to address undisputed matters.”).

1. *Independent Claims 1 and 9*

a) *Limitation 1[a][ii]/9[a][ii] “the device directed by an application server to a cloud network location of the proxy server”*

Petitioner asserts that Gemmill teaches this limitation “because it disclosed that the user agent (device) is directed by an application server (server associated with VO SP) to a cloud network location of the myVocs proxy (proxy server).” Pet. 59 (citing Ex. 1002 ¶¶ 264–273). Petitioner argues that “[a]t step 2 of Figure 2, ‘the client is redirected to the myVocs VO IdP component (that is protected by the myVocs SP component).’” *Id.* (citing Ex. 1005, 522). Petitioner argues that “Gemmill disclosed that the VO SP at step 2 redirects the user agent to the ‘cloud network location’ of the myVocs proxy.” Pet. 59 (citing Ex. 1002 ¶¶ 264–273).

Petitioner provides an annotated version of Gemmill's Figure 2, shown below.



With respect to Gemmill's annotated Figure 2, shown above,
Petitioner explains that

[a] user agent, such as the browser of one of the members of the VO [virtual organization] (highlighted in green), attempts to

access the VO service provider (SP), which is “a VO web resource protected by the VO SP” (highlighted in blue). [Ex. 1005], 522–523. In order to authenticate the user agent, the VO SP redirects the user agent to the myVocs system (highlighted in pink). *Id.* The myVocs system then redirects the user agent to the enterprise X identity provider, such as the identity provider for the user’s home institution (highlighted in red). *Id.* The user authentication is passed from the enterprise identity provider to the myVocs system and then to the VO SP, in each case through the user agent. *Id.*

Pet. 52–53, 61 (font coloring omitted); Ex. 1002 ¶ 255.

Petitioner asserts that “[t]o the extent that Gemmill did not explicitly disclose the myVocs proxy and other entities were located at cloud network locations, this would have been obvious based on the disclosure of Woelfel.” Pet. 60. Petitioner argues that “Gemmill indicated that its system should be used in a federated authentication model,” and that “Woelfel disclosed that the federated authentication model was implemented by ‘cooperation between independent network entities.’” *Id.* (citing Ex. 1002 ¶¶ 264–273; Ex. 1006 ¶ 4). Petitioner notes that “Woelfel explains that these ‘independent network entities’ are present at cloud network locations.” *Id.* (citing Ex. 1006 ¶¶ 6, 8, Fig. 1; Ex. 1002 ¶¶ 264–273).

Patent Owner argues that “[n]either Gemmill nor Woelfel disclose ‘a **cloud** network location of the proxy server.’” PO Resp. 20. Patent Owner argues that the “[c]loud is not merely synonymous with ‘Internet.’” *Id.* (citing Ex. 2002 ¶ 126). According to Patent Owner, “[a] cloud system requires essential characteristics such as ‘on-demand self-service,’ ‘broad network access,’ ‘resource pooling,’ and ‘rapid elasticity.’” PO Resp. 27 (citing Ex. 2002 ¶ 123). Patent Owner points out that “[t]he ’090 patent refers to the cloud applications as ‘being hosted by third party vendors on

shared servers for multiple customers”’. PO Resp. 20–21 (citing Ex. 1001, 3:7–9).

Patent Owner also argues that “[t]he Woelfel reference actually teaches away from use of a proxy in the cloud.” PO Resp. 21 (citing Ex. 2002 ¶ 130).² Patent Owner argues that “[g]iven that [Woelfel’s] PRS Reverse Proxy is intended to control and monitor internal enterprise user access to cloud applications, a [person of ordinary skill in the art] would have understood the PRS Reverse Proxy to have a local URL on the private network and not a cloud-based location. Woelfel thus clearly teaches to give the proxy server a local URL not a cloud network location as required by the claims.” PO Resp. 23 (citing Ex. 2002 ¶¶ 130–131).

In its Reply, Petitioner asserts that Patent Owner’s argument with respect to the cloud, “depend[s] on an imaginary construction of ‘cloud,’ that ignores the specification, and that is based on an extrinsic definition of a different term ‘cloud *computing*,’ which is not even present in the ’090 patent.” Pet. Reply. 14. Petitioner argues that “[n]either Petitioner nor its expert makes an attempt to explain why ‘cloud’ and ‘cloud computing’ would have identical meanings. *Id.* at 17 (citing Ex. 2002 ¶ 126).

Petitioner points out that Figure 1 of the ’090 patent (shown below), “depicts a topology of a proxy system of the patent.” *Id.* at 14 (citing Ex. 1001, 3:45–46).

² We discuss Patent Owner’s “teaching away” argument in Section II.G.1.c, below.

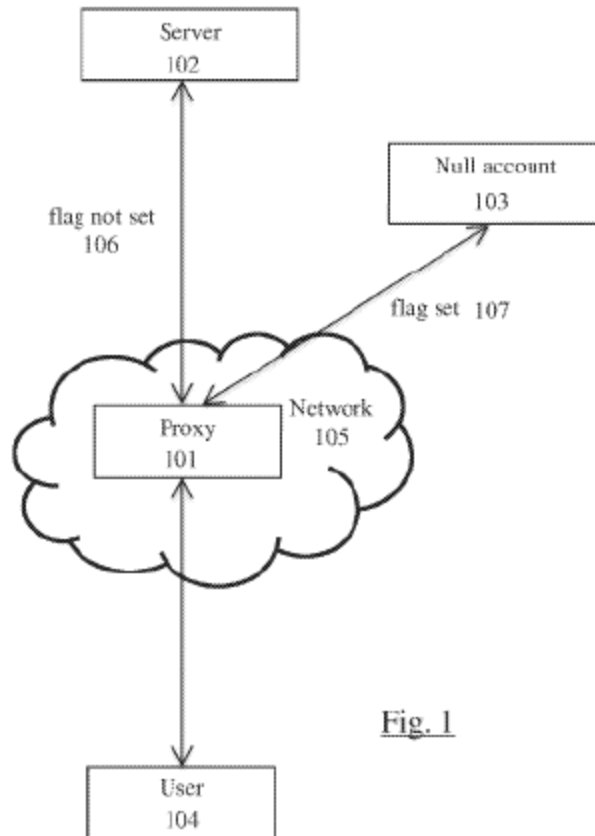


Fig. 1

According to Petitioner, the '090 patent

explains that “[p]roxy 101 may essentially be in the ‘cloud’” and communicate with a user device over network 105, which is depicted [in Figure 1 above] as a cloud. “Network 105 comprises, but is not limited to, any of: the Internet, intranet, local area networks (LANs), wide area networks (WANs), dedicated links, private computer networks, public computer networks, enterprise computer networks, etc.” Thus, the '090 patent provides several examples of networks over which a proxy could communicate with a client and still be in the “cloud.”

Pet. Reply 15 (citing Ex. 1001, 3:50–56).

Petitioner also argues that “Gemmill’s myVocs proxy was at a cloud network location at least because it was ‘a server accessible in a remote network,’ it was ‘accessible over the Internet,’ it allowed users ‘access to resources anywhere on the Internet,’ it was ‘not on the same network’ as the

user, and its entire purpose was to be ‘accessible by different organizations.’” Pet. Reply 16 (citing Pet. 59; Ex. 1002 ¶¶ 265–268).

In its Sur-Reply, Patent Owner argues that “Petitioner does not point to any disclosure in Gemmill that myVocs has a cloud network location other than to state that this system is accessible on the Internet.” PO Sur-reply 10. Patent Owner argues that during prosecution of the ’090 patent, it “distinguished the ‘cloud’ claim term from prior art that included a self-contained (local) web server,” even though the “web server was accessible on the Internet.” *Id.* at 11.

Patent Owner also argues that Petitioner’s interpretation of Figure 1 from the ’090 patent is misleading. *Id.* Patent Owner argues that “[t]he exemplary embodiments relate to the network 105, not the proxy 101,” and that “[t]hese examples are provided as potential systems for the network 105, not network locations of the proxy 101.” *Id.* at 12.

We disagree with Patent Owner. In its Response, Patent Owner states that “Patent Owner does not believe that the Board needs to address any claim construction issue.” PO Resp. 11. Yet, with respect to Petitioner’s showing that the asserted prior art satisfies the limitation “cloud network location of the proxy server,” Patent Owner argues that “[a] cloud system requires essential characteristics such as ‘on-demand self[-]service,’ ‘broad network access,’ ‘resource pooling,’ and ‘rapid elasticity.’” *Id.* at 27 (citing Ex. 2002 ¶ 123). These “essential characteristics” of a “cloud system” are proffered by Patent Owner’s expert, Dr. Nielson, who obtains them from a definition of “cloud computing” published by the United States National Institute of Standards and Technology (NIST). Ex. 2002 ¶ 126. But neither Patent Owner nor Dr. Neilson explains why NIST’s definition for the term “cloud computing” would be synonymous with the claim term “cloud” as

that term is used in the '090 patent. *See* PO Resp. 20–23, 25–27; Ex. 2002 ¶¶ 124–128; PO Sur-reply 9–13.

Petitioner points out, and we agree, that the '090 patent's discussion of the “cloud” is materially different from the definition of “cloud computing” offered by Patent Owner. The '090 patent does not describe “the cloud” as requiring “on-demand self[-]service,” “broad network access,” “resource pooling,” or “rapid elasticity” that Patent Owner's proffered definition of “cloud computing” encompasses.

For example, with respect to the '090 patent's Figure 1, a topology of a proxy system, the patent explains that

[p]roxy 101 may essentially be in the “cloud.” Communication between proxy 101, server 102, and user device 104 may occur across network 105. Network 105 comprises, but is not limited to, any of: the Internet, intranet, local area networks (LAN s), wide area networks (WANs), dedicated links, private computer networks, public computer networks, enterprise computer networks, etc.

Ex. 1001, 3:50–56.

Dr. Franz testifies, and we agree, that this passage in the '090 patent provides examples of “[t]he networks over which the proxy [101] could communicate with the user device [104],” such that proxy 101 would be considered “in the cloud” relative to the user device. Ex. 1017 ¶¶ 33; *see also* Ex. 1002 ¶ 268 (Explaining that “whether a server is in the ‘cloud’ is relative, e.g., relative to the other computer that is trying to access it. If a server is not on the same network (e.g., local area network, intranet, etc.) as the other computer, then from the perspective of the computer, the server is in the ‘cloud.’”).

Patent Owner, however, points to another section of the '090 patent, which states that the “'090 patent refers to . . . cloud applications as “being

hosted by third party vendors on shared servers for multiple customers,” arguing that “[t]he Petition has not established that Gemmill discloses cloud locations as that term would be understood to a [person of ordinary skill in the art].” PO Resp. 20–21. But Dr. Franz points out that this description from the ’090 patent “is entirely consistent with Gemmill which teaches myVocs as a shared proxy server for numerous academic institutions.” Ex. 1017 ¶ 32. Dr. Franz testifies, and we agree, that “because myVocs is accessed over the Internet, a [person of ordinary skill in the art] would understand it as being at a cloud network location. I also explained that from the perspective of the user device, because the myVocs was provided from outside of the enterprise infrastructure of some entity, it was in the ‘cloud.’” Ex. 1017 ¶ 31.

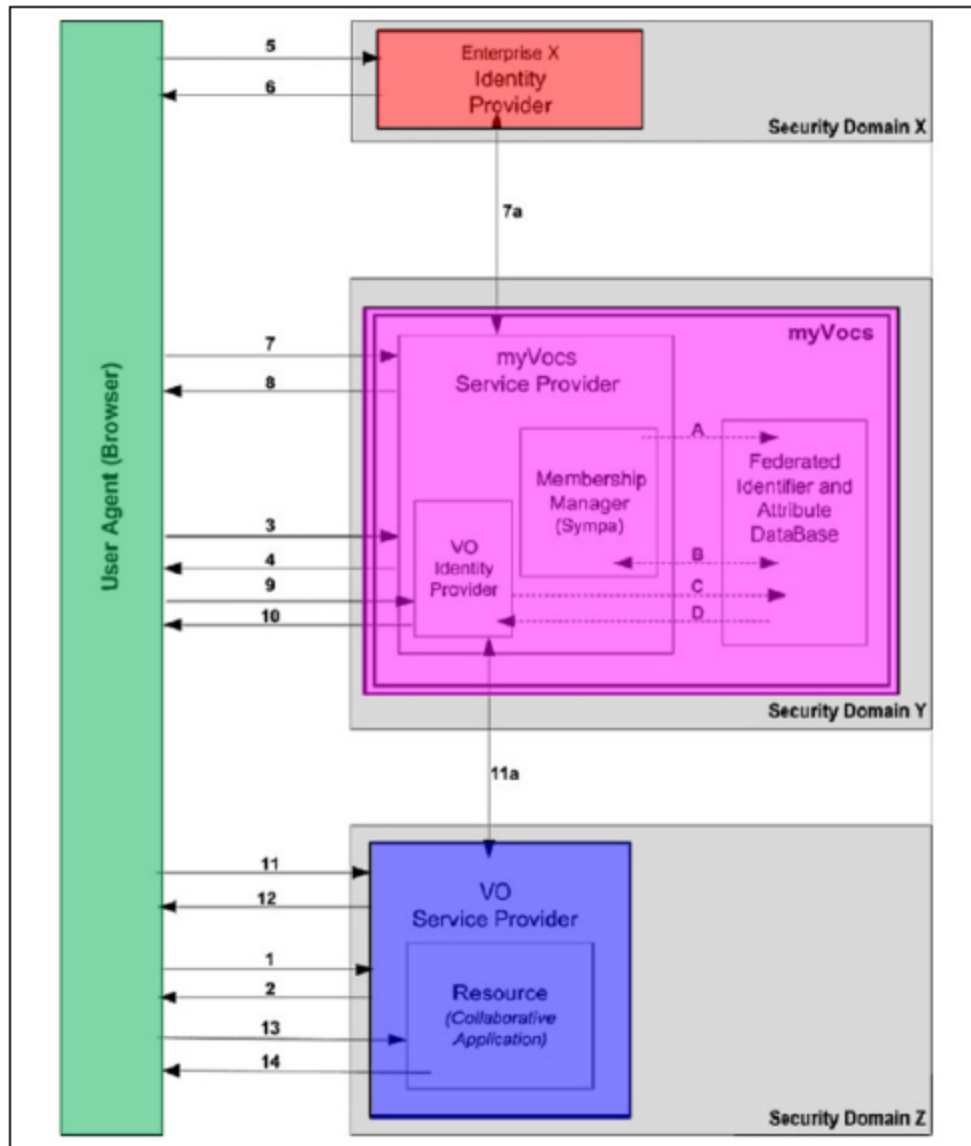
Petitioner provides persuasive evidence that Gemmill and Woelfel describe proxy servers with cloud network locations consistent with the ’090 patent’s use of the term “cloud” as a person of ordinary skill in the art would understand that term. For example, Gemmill describes how a user agent (device) is directed by an application server (server associated with VO SP) to a network location of the myVocs proxy (proxy server).

Dr. Franz explains that

Gemmill discloses a new system called my Virtual Organization Collaboration System (“myVocs”). [Ex. 1005], 509. That system provides federated identity management for multiple, unrelated virtual organizations (“VO”). [*Id.*] The myVocs system “provides a flexible environment for exploring new approaches to security, application development, and access control built from Internet services.”

Ex. 1002 ¶ 252.

Gemmill’s Figure 2, annotated by Petitioner, is shown below.



As Petitioner explains, in Gemmill’s Figure 2 above, a user agent (device, highlighted in green) at step 1 attempts to access the VO service provider (application server, highlighted in blue). Pet. 52–54, 59 (citing Ex. 1005, 522–523; Ex. 1002 ¶¶ 255–256, 264–273). In order to authenticate the user agent, at step 2, “the client is redirected to the myVocs VO IdP component (that is protected by the myVocs SP component)” (proxy server, highlighted in pink). Pet. 59 (citing Ex. 1005, 522; *see also* Ex. 1002 ¶¶ 264–265).

Dr. Franz testifies that the myVocs system in Gemmill “can interact with multiple enterprise identity providers, thereby allowing VO members from different institutions to authenticate with their home identity provider.” Ex. 1002 ¶ 256 (citing Ex. 1005, 522–523). According to Dr. Franz, “the myVocs system acts as a proxy identity provider and provides the VO SP a federated identity management system.” *Id.*

Dr. Franz testifies that a person of ordinary skill in the art would have understood that a server accessible in a remote network, such as the one described in Gemmill, which is accessible over the Internet, would be located in “the cloud.” Ex. 1002 ¶ 266 (citing Ex. 1005, 509). “Gemmill explains,” Dr. Franz testifies, “that the system provides user access to ‘resources located anywhere on the Internet.’” Ex. 1002 ¶ 266 (citing Ex. 1005, 512).

Dr. Franz also testifies that a person of ordinary skill in the art “would have recognized based on Gemmill’s disclosure of using SAML would have indicated that it would be used in a system distributed over multiple networks of independent organizations,” indicating that Gemmill’s myVocs proxy “would have been provided at a cloud network location.” Ex. 1002 ¶ 267.

To the extent that Gemmill does not expressly describe that its myVocs proxy is located at a “cloud” network location, Petitioner also provides persuasive evidence that it would have been obvious to a person of ordinary skill in the art to locate Gemmill’s myVocs proxy at a “cloud” network location based upon the relevant teachings of Woelfel. We discuss Petitioner’s application of the teachings of Gemmill and Woelfel in greater detail in Section II.G.1.c below.

Based upon the complete record and for the reasons discussed, we are persuaded that Petitioner has demonstrated that Gemmill teaches a “device directed by an application server to a cloud network location of the proxy server” as recited in limitations 1[a][ii] and 9[a][ii].

b) Limitation 1[b][iv]/9[b][iv] “the identity provider redirects the device to the cloud network location of the proxy server with a single-sign-on validation after validation of the single-sign-on request”

With respect to this limitation, Petitioner argues that “Gemmill disclosed this element because it disclosed that the enterprise IdP (identity provider) redirects the user agent (device) to the cloud network location of the myVocs proxy (proxy server) with a single-sign-on validation after validation of the single-sign-on request.” Pet. 68 (citing Ex. 1002 ¶¶ 283–292). At step 6 of Gemmill’s Figure 2, Petitioner points out, the “IdP returns an authentication response to the client. The response may contain user attributes.” Pet. 68 (quoting Ex. 1005, 522). According to Petitioner, “Gemmill discloses that its systems can be used with services that ‘each use myVocs and the underlying Shibboleth mechanisms for SSO.’” Pet. 68 (citing Ex. 1005, 526). “In the standard Shibboleth mechanisms for SSO, depicted in Figure 1 of Gemmill,” Petitioner points out, “the IdP’s response to the SSO request is a ‘digitally signed SAML Response in HTML form.’” Pet. 68 (citing Ex. 1005, Fig. 1 (step 7)). According to Petitioner, a person of ordinary skill in the art “would have recognized that a ‘digitally signed SAML Response,’ made in the context of a Shibboleth single sign-on request, is a ‘single-sign-on validation.’” Pet. 68 (citing Ex. 1002 ¶¶ 283–292).

Petitioner argues that a person of ordinary skill in the art “would have recognized that the message sent from the enterprise IdP to the user agent at

step 6 included a redirect to the myVocs proxy, at least because, at step 7, ‘client submits the authentication response to the SP at myVocs.’” Pet. 68 (citing Ex. 1005, 522; Ex. 1002 ¶¶ 283–292).

Petitioner also argues that “[t]o the extent that Gemmill did not explicitly disclose that the message sent from the enterprise IdP to the user agent at step 6 included a redirect to the myVocs proxy, a [person of ordinary skill in the art] would have found it obvious to add this feature to Gemmill’s system.” Pet. 68–69 (citing Ex. 1002 ¶¶ 283–292). Petitioner argues that “Gemmill already disclosed the use of redirects between the myVocs system and other entities.” Pet. 69 (citing Ex. 1005, 520, 522, 527; Ex. 1002 ¶¶ 283–292). “In fact,” Petitioner notes, “in an exemplary user registration scenario, Gemmill disclosed a redirect from the enterprise IdP back to the myVocs proxy: the user is taken ‘on to the Shibboleth SSO service at his home institution. As [the user’s] browser is *redirected back to myVocs*.’” Pet. 69 (citing Ex. 1005, 520; Ex. 1002, ¶¶ 283–292).

Petitioner argues that a person of ordinary skill in the art

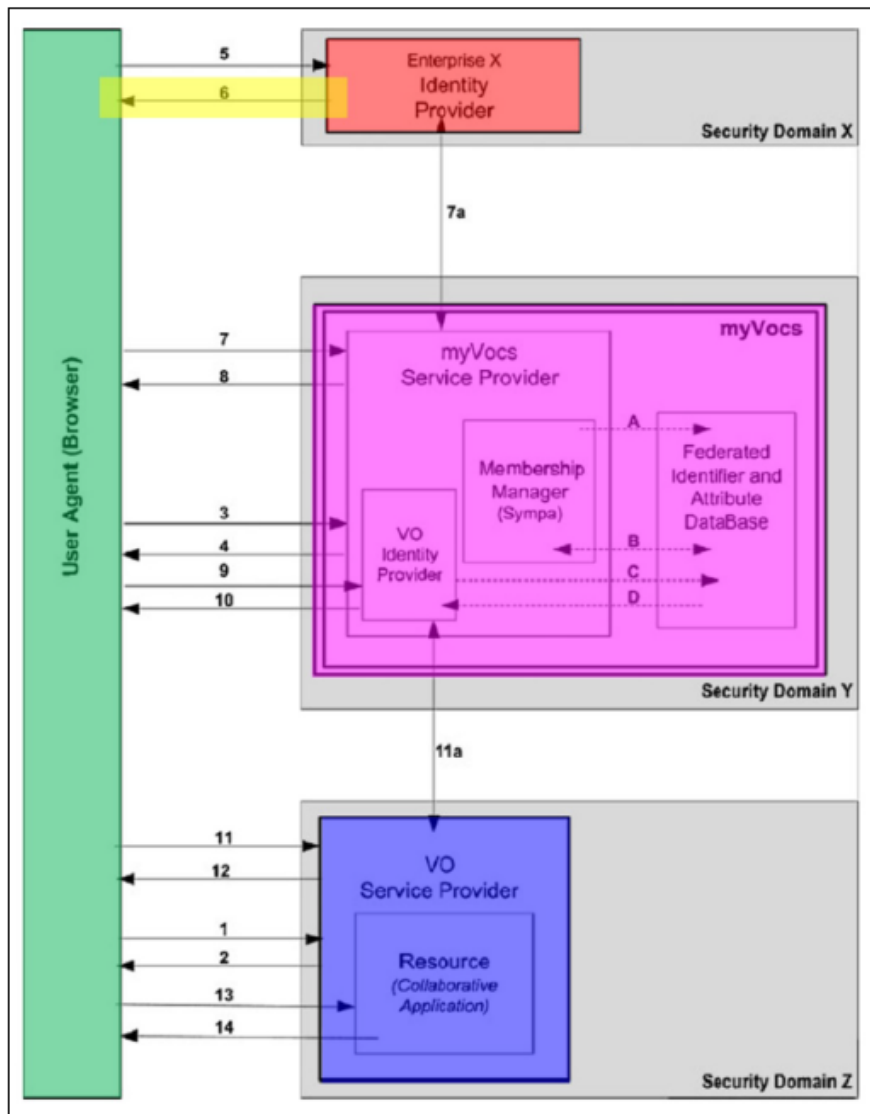
would have been motivated to use a redirect for various reasons. First, a [person of ordinary skill in the art] would have recognized that a redirect would have been one of a limited number of ways to cause the user agent to continue the authentication workflow and contact the myVocs proxy at step 7. [Ex. 1002] ¶¶ 283–292. Second, a [person of ordinary skill in the art] would have understood that, in the context of Internet-based communications, a redirect was a simple and effective technique for causing the user agent to continue the authentication workflow in the desired way. [*Id.*] ¶¶ 283–292. Third, Gemmill already disclosed the use of redirects to send the user agent to different entities in the myVocs system. [Ex. 1005], 522 (steps 2, 4, 8, 12), 527 (“path of redirects”). Hence, a redirect consistent with the other steps used in the authentication process. Therefore, a [person of ordinary skill in the art] would have found it obvious to modify step 6 to have the enterprise IdP

redirect the user agent to the myVocs proxy. [Ex. 1002] ¶¶ 283–292.

Pet. 69.

Petitioner also argues that a person of ordinary skill in the art “would have recognized that Gemmill disclosed that this redirect by the enterprise IdP of the user agent would be to the ‘cloud network location’ of the myVocs proxy, or alternatively that arrangement would have been obvious.” Pet. 70 (referencing Pet. Ground 3, element 1[a][ii]; Ex. 1002 ¶¶ 283–292).

Gemmill’s Figure 2, annotated by Petitioner, is shown below.



Gemmill's annotated Figure 2, above, illustrates the myVocs architecture components and message flow. The User Agent (Browser) in green; the VO Service Provider (in blue); the myVocs Service Provider (in pink); and the Enterprise X Identity Provider (in red). Pet. 70.

Patent Owner argues that "the IdP of Gemmill cited by the Petition is not validating the SSO but is merely providing an authentication response. It is the myVocs SP that is validating, not the IdP." PO Resp. 24 (citing Ex. 2002, XX).³ Patent Owner also argues that Petitioner improperly maps the VO IdP of Gemmill to the proxy server recited in limitations 1[a][i]/9[a][i], but maps the SP at myVocs as the proxy of limitations 1[b][iv]/9[b][iv]. PO Resp. 24. Patent Owner argues that "the plain language of the claims . . . require that the proxy receiving the SSO be the same proxy that the IdP redirects the device too." PO Resp. 24–25 (citing Ex. 2002 ¶ 122).

In its Reply, Petitioner asserts that Patent Owner is incorrect, and that "Gemmill's two-stage validation is . . . consistent with the arrangement recited in claim 1: validation of the single-sign-on request by the enterprise IdP (steps 5–6), that leads to a subsequent validation involved in creating the valid identification assertion by the myVocs proxy (steps 7-10)." Pet. Reply 20. "Further," Petitioner argues, a person of ordinary skill in the art "would have recognized that the generation of a 'SAML response' by the enterprise IdP indicated the validation of a single-sign-on request." *Id.* (citing Ex. 1002 ¶¶ 39–43).

³ Petitioner asserts that this citation by Patent Owner to Dr. Nielson's declaration (Ex. 2002, XX) cannot be located in the record, making this unsupported attorney argument. *See* Pet. Reply 19–20. We cannot locate the citation in Dr. Nielson's declaration and it does not appear that Patent Owner clarified the citation in its Sur-reply. *See* PO Sur-reply 7–13.

Petitioner also disputes Patent Owner’s other argument, that Gemmill’s enterprise IdP (identity provider) does not redirect the device to *the* cloud network location of the myVocs proxy (proxy server), i.e., the same cloud network location used for limitation 1[a][ii]. Pet. Reply 20–21 (citing PO Resp. 24–25). Petitioner points out that “the VO Identity Provider is a sub-component of the myVocs Service Provider,” and “[t]he claim does not preclude the possibility that the recited ‘proxy server’ could contain separate software sub-routines for different tasks.” Pet. Reply 22–23 (citing Ex. 1017 ¶¶ 44–46). Petitioner argues that a person of ordinary skill in the art “would have recognized that the subcomponents of the proxy server would be provided at the same cloud network location, absent a teaching otherwise.” Pet. Reply 23.

We agree with Petitioner. With respect to Patent Owner’s argument that “[i]t is the myVocs SP that is validating, not the IdP,” Dr. Franz testifies that Gemmill’s “IdP sends a ‘digitally signed SAML response in HTML form’ in response to the SSO request,” which is “sufficient to show that the IdP is validating the SSO request” and that a person of ordinary skill in the art “would have understood that the purpose of a ‘SAML response’ in the underlying protocol is the transport of an assertion with the identity of the user if the authentication was successful.” Ex. 1017 ¶ 40. Dr. Franz testifies that “[t]he fact that the communication from the IdP to the myVocs proxy can be separately validated does not change the fact that the IdP already validated the SSO request.” *Id.* ¶ 41.

With respect to Patent Owner’s argument that Gemmill’s IdP does not redirect the user device to the cloud network location of the proxy, Dr. Franz testifies, and we agree, that “Gemmill shows that the ‘VO Identity Provider’ is a component of the ‘myVocs Service Provider,’ and both are in turn

components of the myVocs proxy.” Ex. 1017 ¶ 45. Patent Owner has not explained why a proxy server having sub-components has any relevance to the claim language, whereas Dr. Franz testifies that a person of ordinary skill in the art “would have fully expected that the ‘proxy server’ could have distinct software components.” *Id.*

Based upon the complete record and for the reasons discussed, we are persuaded that Petitioner has demonstrated that Gemmill teaches “the identity provider redirects the device to the cloud network location of the proxy server with a single-sign-on validation after validation of the single-sign-on request” as recited in limitations 1[b][iv] and 9[b][iv].

c) Rationale to Combine the Teachings of Gemmill and Woelfel

Petitioner first argues that “to the extent that the Board finds that Gemmill only discloses a ‘network location’ and not necessarily a ‘cloud’ network location, a [person of ordinary skill in the art] would have found it obvious to provide the myVocs proxy at a cloud network location based on Woelfel’s teaching of such cloud implementations in the federated authentication model used in both references.” Pet. 55 (citing Ex. 1002 ¶¶ 258–260).

In particular, Petitioner argues that “Gemmill indicated that its system should be used in a federated authentication model.” Pet. 60 (citing Ex. 1002 ¶¶ 264–273). According to Petitioner, “Woelfel disclosed that the federated authentication model was implemented by ‘cooperation between independent network entities.’” Pet. 60 (citing Ex. 1006 ¶ 4). Petitioner points out that “Woelfel explains that these ‘independent network entities’ are present at cloud network locations.” Pet. 60 (citing Ex. 1006 ¶¶ 6, 8, Fig. 1; Ex. 1002 ¶¶ 264–273). “Thus,” Petitioner argues, a person of ordinary skill in the art “would have been motivated to provide the entities in

Gemmill [with] cloud network locations because that was the ordinary arrangement for such entities in the federated authentication model.” Pet. 60 (citing Ex. 1002 ¶¶ 264–273).

Petitioner next argues that “[t]o the extent that Gemmill did not explicitly disclose that the message sent from the enterprise IdP to the user agent at step 6 included a redirect to the myVocs proxy, a [person of ordinary skill in the art] would have found it obvious to add this feature to Gemmill’s system.” Pet. 68–69 (citing Ex. 1002 ¶¶ 283–292).

Petitioner argues that “Gemmill already disclosed the use of redirects between the myVocs system and other entities.” Pet. 69 (citing Ex. 1005, 520, 522, 527; Ex. 1002 ¶¶ 283–292). “In fact,” Petitioner argues, “in an exemplary user registration scenario, Gemmill disclosed a redirect from the enterprise IdP back to the myVocs proxy: the user is taken ‘on to the Shibboleth SSO service at his home institution. As [the user’s] browser is *redirected back to myVocs*.’” Pet. 69 (citing Ex. 1005 520; Ex. 1002 ¶¶ 283–292).

Petitioner argues that a person of ordinary skill in the art would have been motivated to use a redirect for various reasons. Petitioner argues that first, a person of ordinary skill in the art

would have recognized that a redirect would have been one of a limited number of ways to cause the user agent to continue the authentication workflow and contact the myVocs proxy at step 7. [Ex. 1002] ¶¶ 283–292. Second, a [person of ordinary skill in the art] would have understood that, in the context of Internet-based communications, a redirect was a simple and effective technique for causing the user agent to continue the authentication workflow in the desired way. [Ex. 1002] ¶¶ 283–292. Third, Gemmill already disclosed the use of redirects to send the user agent to different entities in the myVocs system. [Ex. 1005] 522 (steps 2, 4, 8, 12), 527 (“path of redirects”).

Hence, a redirect [is] consistent with the other steps used in the authentication process. Therefore, a [person of ordinary skill in the art] would have found it obvious to modify step 6 to have the enterprise IdP redirect the user agent to the myVocs proxy.

Pet. 69 (citing Ex. 1002 ¶¶ 283–292).

Petitioner also argues that a person of ordinary skill in the art “would have recognized that Gemmill disclosed that this redirect by the enterprise IdP of the user agent would be to the ‘cloud network location’ of the myVocs proxy, or alternatively that arrangement would have been obvious.” Pet. 70 (citing Pet. Ground 3, element 1[a][ii]; Ex. 1002 ¶¶ 283–292).

In its Response, Patent Owner argues that “there is a complete lack of explanation on how or why [a person of ordinary skill in the art] would be able to implement the teachings of ‘the cloud features’ from Woelfel in combination with Gemmill.” PO Resp. 26 (citing Ex. 2002 ¶¶ 132–137). Patent Owner also argues that “Woelfel’s network is within a given local network of an enterprise, whereas the . . . ’090 patent identifies [‘]cloud applications’ as being ‘hosted by third party vendors on shared servers for multiple customer.’” PO Resp. 27 (citing Ex 1001, 3:1–15). Patent Owner argues that “Petitioner has provided no analysis whatsoever to implement Woelfel’s local network features into a cloud network.” *Id.*

Patent Owner also argues that “Woelfel teaches the exact opposite. Woelfel teaches that its reverse proxy, PRS Proxy, is *enterprise specific*, connected to a private network, and is located behind the company firewall if one exists. A [person of ordinary skill in the art] would not have been motivated to combine Woelfel into Gemmill to meet the cloud network claim requirements.” PO Resp. 27 (citing Ex. 1006 ¶ [89]; Ex. 2002 ¶ 130).

Petitioner responds by pointing out that “the Petition uses Woelfel in Ground 3 as an alternative basis for finding the ‘*cloud*’ network location.”

Pet. Reply 23 (citing Pet. 55). “Thus,” Petitioner argues, “to the extent that the Board determines that Gemmill already discloses that its myVocs proxy is located at a ‘cloud network location,’ the combinability with Woelfel is irrelevant.” Pet. Reply 23 (citing Pet. Section II(C)). Petitioner also points out that “the Petition relies only on background state of the art discussion from Woelfel. Hence, Patent Owner’s arguments are misplaced in seeking to require an explanation of how to combine Woelfel’s specific proxy server with Gemmill’s system.” *Id.* at 23–24.

We agree with Petitioner. As we discussed above, Petitioner has provided persuasive evidence that Gemmill teaches the required “device directed by an application server to a cloud network location of the proxy server” as recited in limitations 1[a][ii] and 9[a][ii]. Moreover, we find that Petitioner has provided persuasive evidence that it would have been obvious to a person of ordinary skill in the art to apply Woelfel’s teaching of a federated authentication model implemented by cooperation between independent network entities present at cloud network locations to Gemmill’s myVocs collaboration system because Gemmill’s myVocs system already uses a federated identity management solution. Ex. 1005, 509, 516; *see also* Ex. 1002 ¶ 269 (A person of ordinary skill in the art “would have found it obvious to modify Gemmill to provide the myVocs proxy located at a ‘cloud’ network location based on the relevant teachings of Woelfel. Woelfel, like Gemmill, disclosed a federated authentication model, or ‘federated SSO strategy.’”). As Dr. Franz points out, such a solution was already well-known in the art. *See* Ex. 1017 ¶ 48; Ex. 1002 ¶ 269; Ex. 1006 ¶¶ 4, 6.

Moreover, we disagree with Patent Owner that Woelfel “teaches away” from using a proxy located in a cloud network location. To teach

away, a reference must actually “criticize, discredit, or otherwise discourage” investigation into the claimed solution. *In re Fulton*, 391 F.3d 1195, 1201 (Fed. Cir. 2004). A reference does not “teach away” if it merely expresses a general preference for an alternative invention from among options available to the ordinarily skilled artisan, and the reference does not discredit or discourage investigation into the claimed invention. *Id.*

Here, Woelfel clearly discloses a federated authentication model or federated SSO strategy, meaning that Woelfel acknowledges the value of an “SSO strategy that involves cooperation between independent network entities,” otherwise known as a “federated SSO strategy.” Ex. 1006 ¶ 4. Woelfel also recognizes that “[c]loud applications reside outside of the enterprise infrastructure, typically in a server providing ‘Software as a Service (SaaS).’” *Id.* ¶ 6. Woelfel’s recognition of “the need . . . for the development of an enhanced Reverse Proxy server” (*id.* ¶ 9) does not “criticize, discredit, or otherwise discourage” modifying Gemmill to provide the myVocs proxy located at a cloud network location as Patent Owner suggests.

For these reasons, we find that Petitioner has shown persuasively that one of ordinary skill in the art at the time of the claimed invention would have had sufficient reason to combine the teachings of Gemmill and Woelfel in the manner described by Petitioner.

d) Uncontested Limitations

Patent Owner does not contest Petitioner’s evidence and arguments with respect to the remaining portions of independent claim 1, namely 1[pre], 1[a][i], 1[a][iii], 1[b][i–iii], 1[c], 1[d], and 1[e][i–iii], as well as the corresponding portions of independent claim 9. *See* PO Resp. 20–25.

We have considered Petitioner’s evidence and arguments, as well as the testimonial evidence of Dr. Franz with respect to these uncontested portions of independent claims 1 and 9.⁴ We are persuaded that Petitioner has demonstrated that Gemmill and Woelfel teach the subject matter of the uncontested portions of independent claims 1 and 9.

e) Conclusion on Independent Claims

Based upon the complete record, and for the reasons discussed, we determine that Petitioner has demonstrated by a preponderance of the evidence that independent claims 1 and 9 are unpatentable under 35 U.S.C. § 103 as obvious over Gemmill and Woelfel.

2. Dependent Claims 2–5 and 10–13

Claims 2–5 and 10–13 depend from either independent claim 1 or independent claim 9. Petitioner contends that the combined teachings of Gemmill and Woelfel render these claims obvious. *See* Pet. 81–84. Petitioner provides the testimony of Dr. Franz in support of its positions on these claims. *See* Ex. 1002 ¶¶ 305–314, 330–338. Patent Owner does not dispute any of Petitioner’s arguments or evidence with respect to these dependent claims. *See* PO Resp. 19–27.

a) Dependent Claims 2 and 10

Claims 2 and 10 depend from independent claims 1 and 9, respectively. Claim 2 recites the following limitation: “[t]he method as recited in claim 1, wherein the device is a user device.” Ex. 1001, 14:20–21.

⁴ The issue of whether the preambles of claims 1 and 9 are limiting need not be resolved because, regardless of whether they are limiting, Petitioner shows sufficiently that the recitations in the preambles are satisfied by the prior art.

Claim 10 recites a similar limitation, but is directed to a non-transitory computer readable medium.

With respect to these claims, Petitioner argues that “Gemmill disclosed this element because it disclosed that the user agent (device) was a user device.” Pet. 81 (citing Ex. 1002 ¶ 305). Petitioner argues that “Gemmill discloses that a ‘user agent’ that is a ‘browser,’ which a [person of ordinary skill in the art] would recognize as a user device.” Pet. 81–82 (citing Ex. 1005, Fig. 2; *see also id.* at 510 (describing VO resources being accessed by “four scientists, their lab staff, and graduate students”); *id.* at 513 (describing downsides of non-Shibboleth solutions in “single user/multiple device scenarios”); 515 (Shibboleth “triggered by a user’s attempt to use a web browser to access some protected resource”); Fig. 4 (panel A); Ex. 1002 ¶ 305).

We are persuaded that Petitioner has demonstrated that Gemmill and Woelfel teach the subject matter of dependent claims 2 and 10.

b) Dependent Claims 3 and 11

Claims 3 and 11 depend from independent claims 1 and 9, respectively. Claim 3 recites the following limitation: “[t]he method as recited in claim 1, wherein the device is a user device, and wherein the user device sends a request for access to the application program to an application provider and receives a network location of the proxy server from the application provider.” Ex. 1001, 14:22–26. Claim 11 recites a similar limitation, but is directed to a non-transitory computer readable medium.

Petitioner argues that “Gemmill disclosed this element because it disclosed that the user agent (user device) sends a request for access to the VO SP-protected resource (application program) to the VO SP (application

provider) and receives a network location of the myVocs proxy (proxy server) from the VO SP (application provider).” Pet. 82 (citing Ex. 1002 ¶¶ 308–309). Petitioner explains that “[a]t step 1 of Figure 2, a ‘browser client requests a VO web resource protected by the VO SP,’” and “[t]hen at step 2, the ‘client is redirected to the myVocs VO IdP component.’” Pet. 82 (citing Ex. 1005, 522). Petitioner argues that a person of ordinary skill in the art “would have understood that the redirect at step 2 would have included the ‘network location’ of the myVocs proxy, so that the user agent would be able to identify where it should redirect to.” Pet. 82 (citing Ex. 1002 ¶¶ 308–309; *see also* Pet. Ground 3, claim 1[a][ii]).

We are persuaded that Petitioner has demonstrated that Gemmill and Woelfel teach the subject matter of dependent claims 3 and 11.

c) Dependent Claims 4 and 12

Claims 4 and 12 depend from independent claims 1 and 9, respectively. Claim 4 recites the following limitation: “[t]he method as recited in claim 1, wherein the device is a user device, wherein the user device sends a request for access to the application program to an application provider and receives a network location of the proxy server from the application provider, and wherein the user device sends the single-sign-on request to the proxy server using the network location of the proxy server.” Ex. 1001, 14:27–33. Claim 12 recites a similar limitation, but is directed to a non-transitory computer readable medium.

Petitioner asserts that Gemmill discloses this limitation, citing as support Pet. Ground 3, claims 2 and 10, claims 3[b]/11[b], elements 1[a][i], and 1[a][ii]. Pet. 83–84.

We are persuaded that Petitioner has demonstrated that Gemmill and Woelfel teach the subject matter of dependent claims 4 and 12.

d) Dependent Claims 5 and 13

Claims 5 and 13 depend from independent claims 1 and 9, respectively. Claim 5 recites the following limitation: “[t]he method as recited in claim 1, wherein the proxy server and the identity provider exchange data using a Security Assertion Markup Language data format.” Ex. 1001, 14:34–36. Claim 13 recites a similar limitation, but is directed to a non-transitory computer readable medium.

Petitioner argues that “Gemmill disclosed this element because it disclosed that the myVocs proxy (proxy server) and the enterprise IdP (identity provider) exchange data using a SAML data format.” Pet. 84 (citing Ex. 1002 ¶ 314). “In particular,” Petitioner argues, “the enterprise IdP sends an authentication response to the myVocs proxy, by way of the user agent.” Pet. 84 (citing Ex. 1005, 522 (steps 6–7); Fig. 2; Ex. 1002 ¶ 314). Petitioner explains that the “authentication response is a ‘digital signed SAML response,’ i.e., a data object in the SAML data format.” Pet. 84 (citing Ex. 1005, 526 (system uses “the underlying Shibboleth mechanisms for SSO”), Fig. 1 (step 7 showing standard IdP response with Shibboleth as “digitally signed SAML Response in HTML form”); Ex. 1002 ¶ 314; *see also* Pet. Ground 3, element 1[b][iv]).

We are persuaded that Petitioner has demonstrated that Gemmill and Woelfel teach the subject matter of dependent claims 5 and 12.

e) Conclusion on Dependent Claims 2–5 and 10–13

We are persuaded that Petitioner has demonstrated that Gemmill and Woelfel teach the subject matter of dependent claims 2–5 and 10–13, and that a person of ordinary skill in the art at the time of the claimed invention would have had sufficient reason to combine the teachings of the asserted art in the manner described by Petitioner.

Based upon the complete record, and for the reasons discussed, we determine that Petitioner has demonstrated by a preponderance of the evidence that dependent claims 2–5 and 10–13 are unpatentable under 35 U.S.C. § 103 as obvious over Gemmill and Woelfel.

H. Ground 4 – Obviousness over Gemmill, Woelfel, and Song (Dependent Claims 8 and 16)

For Ground 4, Petitioner contends that dependent claims 8 and 16 are obvious under 35 U.S.C. § 103 over the teachings of Gemmill, Woelfel, and Song. Pet. 84–87. In support of its challenge to these claims, Petitioner provides the testimony of Dr. Franz (Ex. 1002 ¶¶ 387–400).

Patent Owner argues in its Response that “[f]or the reasons discussed above in Sections VI-VII, Petitioner fails to show how . . . Gemmill and Woelfel disclose or render obvious various limitations of independent claims 1 and 9. As such, the Petition’s Ground . . . 4 fail[s] for the reasons as discussed above.” PO Resp. 28.

Dependent claim 8 recites “[t]he method as recited in claim 1, further comprising: logging, by the proxy server, network requests from user devices to applications; creating a report relating to resource accesses based on the logged network requests.” Ex. 1001, 14:60–64.

Dependent claim 16 recites “[t]he non-transitory computer readable medium as recited in claim 9, wherein the software instructions when executed by the one or more processors further cause performance of: logging, by the proxy server, network requests from user devices to applications; creating a report relating to resource accesses based on the logged network requests.” Ex. 1001, 16:13–20.

For these claims, Petitioner argues that “Song disclosed a proxy server logging network requests from user devices to applications.” Pet. 86 (citing

(Ex. 1007 ¶¶ 29, 80–84, 119–138, Fig. 8; *id.* at 50 (system will “audit all the events happening during the transaction, either from downstream or upstream”); Ex. 1002 ¶¶ 392–394). Petitioner argues a person of ordinary skill in the art “would have recognized that when the myVocs proxy implemented the logging activities taught in Song, the myVocs proxy would log both the request received from the user agent (step 3 of Figure 2) and also the VO SP with which the request is associated, as indicated by the trust relationship previously established between the VO SP and the user myVocs proxy.” Pet. 86 (citing Ex. 1005, 522–523, 525–526, Fig. 2; Ex. 1002 ¶¶ 392–394; *see also* Ground 3, element 1[a][iii]). “At least by logging this information in the audit object,” Petitioner argues, “the myVocs proxy would log network requests from the user agent to the resources associated with the VO SP (applications).” Pet. 86 (citing Ex. 1002, 15 ¶¶ 392–394).

Petitioner also argues that “Song disclosed a proxy server creating a report relating to resource accesses based on the logged network requests, at least in the form of storing the final version of the audit object at the security proxy server.” Pet. 86 (citing Ex. 1007 ¶¶ 62–63, 80, 99, 102, 119–138, Fig. 8; Ex. 1002 ¶¶ 395–397). “In addition,” Petitioner argues, “because Song disclosed an auditor reviewing audit information ‘to trace a user’s activities,’ in a system that generates audit trails,” a person of ordinary skill in the art “would have recognized that Song disclosed the creation of a report based on the logged network accesses at least in the form of the generated audit trails.” Pet. 86–87 (citing Ex. 1002 ¶¶ 395–397).

Petitioner concedes that “[n]either Gemmill nor Woelfel discloses logging network requests from devices to applications, nor creating a report based on that logged information.” Pet. 84. “However,” Petitioner argues, “Song discloses these features, and [a person of ordinary skill in the art]

would have found it obvious to modify the system of Gemmill to include logging and reporting functionality in the myVocs proxy, such as described by Song.” *Id.* at 85. Petitioner argues that a person of ordinary skill in the art “would have been motivated to add the logging/reporting functionality to the IdP proxy (user IdP proxy in Guccione, myVocs proxy in Gemmill) at least because: logging and reporting was a well-known feature in computer systems, and in server systems in particular; the interest in logging and reporting was increasing due to the increasing complexity of networked computer systems; and Song explicitly teaches that the functionality should be performed by a proxy server.” *Id.* (citing Pet. Ground 2, Motivation to Combine; Ex. 1002 ¶¶ 388–390). A person of ordinary skill in the art, Petitioner argues, “would have been motivated to add the logging/reporting functionality to the myVocs proxy of Gemmill for the same reasons.” Pet. 85 (citing Ex. 1002 ¶¶ 388–390).

Petitioner argues that a person of ordinary skill in the art “would have had a reasonable expectation of success in adding Song’s functionality to Gemmill’s system, at least because that HTTP header-based approach would have been compatible with the SAML implementations of Gemmill and Woelfel.” Pet. 85 (citing Ex. 1002 ¶¶ 388–390).

We are persuaded that Petitioner has demonstrated that Gemmill, Woelfel, and Song teach the subject matter of dependent claims 8 and 16, and that a person of ordinary skill in the art at the time of the claimed invention would have had sufficient reason to combine the teachings of the asserted art in the manner described by Petitioner.

Based upon the complete record, and for the reasons discussed, we determine that Petitioner has demonstrated by a preponderance of the

evidence that dependent claims 8 and 16 are unpatentable under 35 U.S.C. § 103 as obvious over Gemmill, Woelfel, and Song.

III. MOTIONS

A. Petitioner's Motion to Strike

Petitioner moves to strike arguments it contends were made, for the first time, in Patent Owner's Sur-reply. Paper 20. Patent Owner opposes. Paper 23. Specifically, Petitioner argues that Patent Owner submitted a new exhibit (Ex. 2003) with its Sur-reply that it did not raise before and that it did not seek leave from the Board to submit. Paper 20, 2. Petitioner also argues that Patent Owner for the first time in this proceeding, presented an argument that the applicant allegedly disavowed the scope of "cloud network location" during prosecution to be something more specific than "accessible on the Internet." *Id.* at 2.

Although we acknowledge that Patent Owner made this prosecution history argument in its Sur-reply (*see* Section II.G.1.a, above) we do not rely on this argument, or Exhibit 2003, to make a ruling adverse to Petitioner. Accordingly, we dismiss Petitioner's motion as moot.

B. Patent Owner's Motion to Strike

In responding to Petitioner's Motion to Strike (Paper 20), Patent Owner filed an opposition, titled "Bitglass, Inc's Opposition to Motion to Strike and Counter Motion to Strike Petitioner's Reply." Paper 23. Patent Owner argues, in the context of the alleged new argument concerning the applicant disavowing a local proxy located in the cloud, that "[t]he Patent Owner's citation of the prosecution history should not be stricken. To the extent it is stricken, then . . . Patent Owner request[s] that Petitioner's citation of intrinsic evidence and accompanying argument be stricken from their Reply." *Id.* at 3.

Because we did not authorize a motion to strike from Patent Owner, this “motion” is dismissed. *See* 37 C.F.R. § 42.20(b).

C. Petitioner’s Motion to Exclude

Petitioner moves to exclude Exhibit 2003 under Federal Rules of Evidence 801 as inadmissible hearsay not subject to an exception to the hearsay rule, and Federal Rules of Evidence 403 because the probative value of Exhibit 2003 is substantially outweighed by prejudice the Petitioner would suffer if it were admitted into evidence. Paper 25, 1–2.

Because we do not rely on Exhibit 2003 for purposes of rendering our decision, we dismiss the motion as moot.

IV. CONCLUSION

For the foregoing reasons, we determine that Petitioner has demonstrated by a preponderance of the evidence that claims 1–5, 8–13, and 16 of the ’090 patent are unpatentable on the bases set forth in the following table.⁵

⁵ Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this Final 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 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).

Claims	35 U.S.C. §⁶	References	Claims Shown Unpatentable	Claims Not Shown Unpatentable
1–5, 9–13	103	Guccione, Woelfel		
8, 16	103	Guccione, Woelfel, Song		
1–5, 9–13	103	Gemmill, Woelfel	1–5, 9–13	
8, 16	103	Gemmill, Woelfel, Song	8, 16	
Overall Outcome			1–5, 8–13, 16	

V. ORDER

In consideration of the foregoing, it is hereby

ORDERED that Petitioner has demonstrated by a preponderance of the evidence that claims 1–5, 8–13, and 16 of U.S. Patent No. 10,757,090 B2 are unpatentable; and

FURTHER ORDERED that because this is a Final Written Decision, any party to the proceeding seeking judicial review of this Decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

⁶ Because each of the challenged claims is held unpatentable on grounds combining Gemmill and Woelfel, we do not reach the other asserted grounds in the Petition combining Guccione and Woelfel.

IPR2021-01045
Patent 10,757,090 B2

FOR PETITIONER:

Thomas Millikan
Babak Tehranchi
Kyle Canavera
Andrew Klein
PERKINS COIE LLP
millikan-ptab@perkinscoie.com
tehranchi-ptab@perkinscoie.com
canavera-ptab@perkinscoie.com
klein-ptab@perkinscoie.com

FOR PATENT OWNER:

Ben Yorks
Babak Redjaian
IRELL & MANELLA LLP
byorks@irell.com
bredjaian@irell.com