

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

KAYAK SOFTWARE CORP., OPENTABLE, INC.,
PRICELINE.COM LLC, and THE PRICELINE GROUP INC.,
Petitioner,

v.

INTERNATIONAL BUSINESS MACHINES CORP.,
Patent Owner.

Case IPR2016-00609
Patent 7,631,346 B2

Before DAVID C. McKONE, BEVERLY M. BUNTING, and
MICHELLE N. WORMMEESTER, *Administrative Patent Judges*.

WORMMEESTER, *Administrative Patent Judge*.

FINAL WRITTEN DECISION
35 U.S.C. § 318(a) and 37 C.F.R. § 42.73

I. INTRODUCTION

KAYAK Software Corp., OpenTable, Inc., Priceline.com LLC, and The Priceline Group Inc. (collectively, “Petitioner”) filed a Petition (Paper 1, “Pet.”) requesting *inter partes* review of claims 1–20 of U.S. Patent No. 7,631,346 B2 (Ex. 1001, “the ’346 patent”). Pursuant to 37 C.F.R. § 314, we instituted an *inter partes* review of claims 1, 3, 12, 13, 15, and 18 on one ground of unpatentability. Paper 12 (“Inst. Dec.”); see 35 U.S.C. § 314(a).

After institution of trial, International Business Machines Corporation (“Patent Owner”) filed a Patent Owner Response (Paper 23, “PO Resp.”), and Petitioner filed a Reply (Paper 27, “Pet. Reply”). On April 27, 2017, we conducted an oral hearing. A copy of the transcript is included in the record. Paper 41 (“Tr.”).

We have jurisdiction under 35 U.S.C. § 6(b). For the reasons that follow, we determine that Petitioner has shown by a preponderance of the evidence that claims 1, 3, 12, 13, 15, and 18 of the ’346 patent are unpatentable. This final written decision is issued pursuant to 35 U.S.C. § 318(a).

II. BACKGROUND

A. *Related Proceedings*

The parties identify the following related federal district court cases: (1) *International Business Machines Corporation v. The Priceline Group Inc.*, Civil Action No. 1:15-cv-00137 (D. Del. Feb. 9, 2015); and (2) *International Business Machines Corporation v. Groupon, Inc.*, Civil Action No. 1:16-cv-00122 (D. Del. Mar. 2, 2016). Pet. 2; Paper 11, 1. The parties

also identify several related requests for *inter partes* review and covered business method patent review. Pet. 2; Paper 11, 2; Paper 32, 1.

B. The '346 Patent

The '346 patent is titled “Method and System for a Runtime User Account Creation Operation within a Single-Sign-On Process in a Federated Computing Environment.” Ex. 1001, at [54]. According to the '346 patent, when a user navigates domains within the Internet by accessing resources at the different domains, the user may be subjected to multiple user authentication requests, which can slow the user's navigation. *Id.* at 8:1–6. The '346 patent describes a federated computing environment in which entities may provide a user with a single-sign-on (SSO) experience, doing away with the frustration of having to authenticate to multiple domains for a single transaction. *Id.* at 10:14–16, 24–26.

An SSO process, according to one embodiment of the '346 patent, starts with an identity provider sending to a user an offer to provide access to federated resources. *Id.* at 31:21–23. In this case, the user already has been authenticated by the identity provider, meaning that the user currently has a valid session with the identity provider. *Id.* at 31:6–10. The user then selects a federated resource, which is provided at a service provider. *Id.* at 31:29–31. If the user does not yet have a federated identity for use with a federated SSO operation, then the identity provider creates an alias (information that authenticates a user identity) for the user. *Id.* at 31:34–36. The identity provider sends to the service provider a message that requests access to the selected resource and includes the alias information for the user. *Id.* at 31:36–47, 31:58–32:3. Upon receipt of the message, the service

provider retrieves the alias information. *Id.* at 32:4–7. In the event that the service provider determines that it does not have a local account for the user that links with a user account at the identity provider, the service provider creates a new account for the user based on the alias information, so that the user has an active session at the service provider. *Id.* at 32:16–19, 41–46. After creating the linked user account, the service provider performs the requested resource access. *Id.* at 33:4–5.

C. Illustrative Claim

Claims 1, 15, and 18 are independent. Claims 3, 12, and 13 depend from claim 1. Claim 1 is illustrative of the subject matter at issue:

1. A method for managing user authentication within a distributed data processing system, wherein a first system and a second system interact within a federated computing environment and support single-sign-on operations in order to provide access to protected resources, at least one of the first system and the second system comprising a processor, the method comprising;
triggering a single-sign-on operation on behalf of the user in order to obtain access to a protected resource that is hosted by the second system, wherein the second system requires a user account for the user to complete the single-sign-on operation prior to providing access to the protected resource;
receiving from the first system at the second system an identifier associated with the user; and
creating a user account for the user at the second system based at least in part on the received identifier associated with the user after triggering the single-sign-on operation but before generating at the second system a response for accessing the protected resource, wherein the created user account supports single-sign-on operations between the first system and the second system on behalf of the user.

D. The Instituted Ground

Petitioner asserts in its Petition various grounds that include anticipation under 35 U.S.C. § 102 and obviousness under 35 U.S.C. § 103. Pet. 3–4. We instituted *inter partes* review on one ground of unpatentability: anticipation of claims 1, 3, 12, 13, 15, and 18 by Mellmer.¹ In support of the instituted ground, Petitioner proffers the declaration of James Olivier (Ex. 1011).² With its Response, Patent Owner submits the Declaration of Susan Spielman (Ex. 2103). The transcripts of the depositions of Mr. Olivier and Ms. Spielman are entered in the record as Exhibits 2102 and 1014, respectively.

III. ANALYSIS

A. Claim Construction

For an *inter partes* review, we construe claims in an unexpired patent by applying the broadest reasonable interpretation in light of the specification of the patent in which they appear. *See* 37 C.F.R. § 42.100(b); *Cuozzo Speed Techs. LLC v. Lee*, 136 S. Ct. 2131, 2144–46 (2016) (upholding the use of the broadest reasonable interpretation standard).

¹ Mellmer, U.S. Patent No. 7,680,819 B1, issued Mar. 16, 2010 (Ex. 1008).

² Petitioner originally submitted the declaration of Ray Larson (Ex. 1002) in support of the instituted ground. With our authorization, Petitioner subsequently submitted the substitute declaration of James Olivier (Ex. 1011). *See* Paper 15, 1. Petitioner states that Mr. Olivier “has reviewed and concurs with the original declaration” and that “[t]he substitute declaration is identical to the original declaration except for an introductory paragraph, the CV, the Education and Professional Experience Section, and several omitted paragraphs.” *Id.* Petitioner also states that “Patent Owner has reviewed the substitute declaration and has indicated to Petitioner that Patent Owner has no objections to the substitute declaration.” *Id.*

Under this standard, claim terms generally are given their ordinary and customary meaning, as would be understood by one of ordinary skill in the art in the context of the entire disclosure. *See In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007). A “claim term will not receive its ordinary meaning if the patentee acted as his own lexicographer,” however, and clearly set forth a definition of the claim term in the specification. *CCS Fitness, Inc. v. Brunswick Corp.*, 288 F.3d 1359, 1366 (Fed. Cir. 2002).

The parties separately argue proposed constructions for various limitations of the claims. *See* Pet. 17–20; PO Resp. 20–29; Pet. Reply 2–8. In light of the parties’ arguments and evidence developed during trial, we address two claim terms: (1) “federated computing environment;” and (2) “single-sign-on operation.” *See Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999) (“only those terms need be construed that are in controversy, and only to the extent necessary to resolve the controversy”).

1. “*federated computing environment*”

This term appears in the preambles of independent claims 1, 15, and 18. Relying on the specification of the ’346 patent, Petitioner proposes in its Petition that a “federated computing environment” means a “loosely coupled affiliation of enterprises which adhere to certain standards of interoperability; the federation provides a mechanism for trust among those enterprises with respect to certain computational operations for the users within the federation.” Pet. 18 (quoting Ex. 1001, 1:64–2:1). In its Response, Patent Owner proposes the same construction, adding that the term “federated computing environment” is limiting. PO Resp. 23–24.

Petitioner counters, arguing that “federated computing environment” is not limiting “because that term only appears in the preamble, which the patentee used merely to state an intended use for the claimed subject matter,” the invention of the ’346 patent “is not limited to operating in a federated computing environment,” and “[t]he claim body of each independent claim defines a structurally complete invention.” Pet. Reply 2–3. According to Petitioner, that “the applicant argued that the preamble was limiting during prosecution” is not “categorically determinative,” but, rather, should be treated as a “guidepost[.]” in “deciding whether a preamble is limiting.”

Id. at 4.

Petitioner raises the argument as to whether the preamble is limiting for the first time in its Reply, even though it had an opportunity to brief this issue in its Petition. We therefore find Petitioner’s new argument in this regard waived. *See Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1369–70 (Fed. Cir. 2016).

Even if we were to consider Petitioner’s argument, however, we would still find it to be unpersuasive. “[C]lear reliance on the preamble during prosecution to distinguish the claimed invention from the prior art transforms the preamble into a claim limitation because such reliance indicates use of the preamble to define, in part, the claimed invention.” *Catalina Mktg. Int’l, Inc. v. Coolsavings.com, Inc.*, 289 F.3d 801, 808 (Fed. Cir. 2002) (cited at PO Resp. 25). In this case, as Patent Owner points out, “the inventors stated that the preambles of [c]laims 1, 15, and 18 limit those claims,” and they “also used the term ‘federated computing environment’ to distinguish their claims over a reference cited during prosecution.” PO Resp. 24–25; *see also* Ex. 1003, 14–15 (“the subject disclosure provides for

a ‘runtime user account creation operation within a single-sign-on process’ within the context of a ‘federated computing environment’” and “[t]he ‘federated’ context of the subject disclosure is evident from the preamble in each independent claim”); *id.* at 16 (“the ‘federated computing environment’ limitations of the preamble[s] are limiting”); *id.* at 17 (“Ting, the alleged anticipatory prior art, is not a ‘federated’ teaching. For that reason alone, the reference cannot and does not anticipate any pending claim.”). Based on the record before us, we conclude that the term “federated computing environment” is limiting.

We do not conclude, however, that the scope of the term is limited to an affiliation of *enterprises*, as both parties urge. Pet. 18; PO Resp. 23. Indeed, the specification of the ’346 patent teaches that, “[i]n the context of the present invention, a federation is a set of distinct *entities*, such as enterprises, organizations, institutions, etc., that cooperate to provide a single-sign-on, ease-of-use experience to a user.” Ex. 1001, 10:62–64 (emphasis added). According to the specification of the ’346 patent, an entity “generally refers to an organization, an individual, or a system that operates on behalf of an organization, an individual, or another system.” *Id.* at 8:31–33. We recognize that the portion of the ’346 patent that the parties cite specifies *enterprises*, but, in light of the specification of the patent as a whole, we find this instance of “enterprises” to illustrate an example of the types of entities that may make up a federation. *Compare id.* at 10:62–64 (“[i]n the context of the present invention, a federation is a set of distinct entities, such as enterprises”), *with id.* at 1:64–2:1 (“[a] federation is a loosely coupled affiliation of enterprises”).

Accordingly, we determine that, under a broadest reasonable interpretation in light of the specification of the '346 patent, the term “federated computing environment” refers to “an environment having a loosely coupled affiliation of entities that adhere to certain standards of interoperability; the federation provides a mechanism for trust among those entities with respect to certain computational operations for the users within the federation.”

2. “*single-sign-on operation*”

The '346 patent teaches that users may “be forced to reckon with multiple authentication processes that stymie user access across a set of domains.” Ex. 1001, 1:48–50. The '346 patent further teaches that single-sign-on processes, which address authentication burdens, “have a common purpose: after a user has completed a sign-on operation, i.e. been authenticated, the user is subsequently not required to perform another authentication operation” during a given user session. *Id.* at 1:53–61. Based on these teachings, Petitioner proposes in its Petition that the term “single-sign-on operation” means “a process by which a user is authenticated on a first *domain* and subsequently not required to perform another authentication before accessing a protected resource on a second *domain*.” Pet. 18 (emphases added) (citing Ex. 1001, 1:47–61).

By contrast, Patent Owner proposes in its Response that the term “single-sign-on operation” means “a process by which a user is authenticated on a first *enterprise* and subsequently not required to perform another authentication before accessing a protected resource at a second *enterprise*.” PO Resp. 28 (emphases added). As Patent Owner points out,

its proposed construction is, for the most part, “word-for word the same” as Petitioner’s proposed construction, except that Patent Owner’s construction uses “enterprise” instead of “domain.” *Id.* at 29. In support of its construction, Patent Owner directs us to where the ’346 patent teaches that “[t]he present invention is supported within a federation model that allows enterprises to provide a single-sign-on experience to a user.” *Id.* at 28–29 (quoting Ex. 1001, 10:24–26).

Petitioner counters, pointing out that the ’346 patent teaches that “a user can request a protected resource at one of many domains.” Pet. Reply 8; Ex. 1001, 7:3–4. Petitioner explains that Patent Owner “attempts to restrict the phrase ‘single-sign-on operation’ . . . to only single-sign-on operations that occur ***within a federated computing*** environment by reading in the words ‘first enterprise and ‘second enterprise.’” Pet. Reply 7. According to Petitioner, we “should reject [Patent Owner’s] attempt to indirectly read the preamble into the body of the claims.” *Id.* at 7–8.

Although we agree with Petitioner that the scope of the term “single-sign-on operation” is not limited to enterprises, we disagree that the term should be read outside the context of a federated computing environment. As discussed above, we conclude that the term “federated computing environment” is limiting. We also conclude that the scope of that term is limited to entities, which encompass enterprises. *See* Ex. 1001, 10:62–64 (“[i]n the context of the present invention, a federation is a set of distinct entities, such as enterprises”).

As to the relationship between an entity and a domain, we note that the ’346 patent teaches that “[t]he term ‘domain’ connotes additional characteristics within a network environment, but the terms ‘entity’, ‘party’,

and ‘domain’ can be used interchangeably.” *Id.* at 8:33–36. Thus, in the context of the ’346 patent, entities encompass domains in addition to enterprises.

Accordingly, we determine that, under a broadest reasonable interpretation in light of the specification of the ’346 patent, the term “single sign-on operation” means “a process by which a user is authenticated at a first entity and subsequently not required to perform another authentication before accessing a protected resource at a second entity.”

B. Anticipation by Mellmer

Petitioner argues that Mellmer anticipates claims 1, 3, 12, 13, 15, and 18 of the ’346 patent under 35 U.S.C. § 102(e). Pet. 3–4, 20–36. For the reasons explained below, we are persuaded that Petitioner has demonstrated by a preponderance of the evidence that Mellmer anticipates these claims.

1. Mellmer

Mellmer describes a system for managing digital identity information in a network. Ex. 1008, at [57]. Mellmer’s description focuses primarily on Novell, Inc.’s DigitalMe system, which authenticates a partner’s users through a single-sign-on process. *Id.* at 4:27–29, 8:2–5, 24:13–15.

For a user, the login process starts when the user clicks on a “log in” button on a partner website. *Id.* at 24:23–25. The partner site presents the user with a link such as a DigitalMe login handprint. *Id.* at 24:26–32, Fig. 24 (handprint). When the user selects the link, the link captures the partner site’s URL and sends it to a web sign-on servlet at www.digitalme.com. *Id.* at 24:37–44.

Normally, the user would have a DigitalMe account as well as a DigitalMe accessCard representing the partner site. *Id.* at 24:46–48. If the user already is logged into the DigitalMe account, the partner site login happens automatically. *Id.* at 24:48–50. That is, the DigitalMe servlet sends a post to the partner site, adding accessCard attributes and a unique DigitalMe identifier for the user to the post buffer for the partner site’s login. *Id.* at 24:62–67. The identifier is included so that the partner site can use it to identify and consolidate the user’s accounts across that site. *Id.* at 24:32–36.

In some instances, however, a user may not have an accessCard for the partner site. Figure 34, which is reproduced below, illustrates such a scenario.

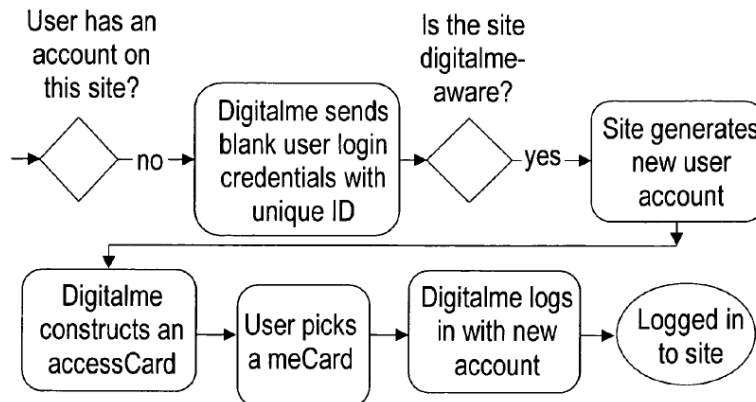


Fig. 34

Figure 34 is a flowchart illustrating a login process at a partner site. *Id.* at 5:60–62. In particular, Figure 34 illustrates a login process for a user without an account (let alone an accessCard) for the partner site. *Id.* In this scenario, the DigitalMe software sends a test post to the partner site by attempting a login with blank data, except for the unique DigitalMe identifier for the user. *Id.* at 25:60–63. The partner site keys off the

identifier and generates a new user account for the partner site. *Id.* at 25:63–66, Fig. 34. The DigitalMe servlet constructs an accessCard, prompts the user to associate a meCard (user profile), and reissues the post on behalf of the user. *Id.* at 25:66–26:1. The user is then logged into the partner site. *Id.* at 26:2.

2. Claims 1, 15, and 18

Petitioner explains in its Petition how Mellmer discloses each element of independent claims 1, 15, and 18. *See* Pet. 22–29 (discussing claim 1); *id.* at 32–36 (referring to discussion of claim 1 for claims 15 and 18). For example, the claims recite “a first system and a second system interact within a federated computing environment.” For this limitation, Petitioner identifies Mellmer’s DigitalMe as a “first system” and Mellmer’s partner site as a “second system.” *See id.* at 23 (citing Ex. 1008, 24:16–23, 29:9–13). We agree with Petitioner and find that Mellmer’s DigitalMe discloses a “first system” and Mellmer’s partner system discloses a “second system.” Below, we address the parties’ dispute as to whether Mellmer’s DigitalMe and partner system interact within a “federated computing environment.”

The claims also recite the steps of (1) triggering a single-sign-on operation to access a protected resource at the second system, which requires a user account to complete the operation; (2) receiving from the first system at the second system an identifier associated with the user; and (3) creating a user account at the second system based on the received identifier after triggering the single-sign-on operation but before generating a response for accessing the protected resource.

For the “triggering step,” Petitioner directs us to where Mellmer discloses that “the login process starts when the user goes to the partner’s web site,” where “the user 1002 is presented with a login dialog that asks for the user’s name and password but also includes a link such as a DigitalMe™ login handprint.” *Id.* at 24 (citing Ex. 1008, 24:24–32). Petitioner further directs us to where Mellmer discloses creating a user account for the partner site in the event that the user does not already have such an account. *Id.* at 26 (citing Ex. 1008, Fig. 34). We find that Mellmer discloses the recited step of “triggering a single-sign-on operation.” Namely, we note Mellmer’s disclosure of generating a new user account at the partner site before logging the user into the partner site. Ex. 1008, Fig. 34. This disclosure refers to “A No Account On This Site Scenario,” which occurs “[i]f the user selects the DigitalMe™ login.” *Id.* at 24:39–44, 25:60–61. Below, we further address the parties’ dispute as to whether Mellmer discloses “triggering a single-sign-on operation on behalf of the user in order to obtain access to a protected resource that is hosted by the second system.”

For the “receiving step,” Petitioner directs us to where Mellmer discloses that the “DigitalMe™ software attempts a login [at the partner site] with blank login data, except for a globally unique identity for the DigitalMe™ user.” Pet. 26 (citing Ex. 1008, 25:61–63, Fig. 34). Petitioner identifies the globally unique identity in Mellmer as an “identifier associated with the user.” *Id.* Mellmer further discloses that “a partner’s site can use this unique identifier to consolidate and identify user 1002 accounts across that site and other sites.” Ex. 1008, 24:35–37. We find that Mellmer’s globally unique identity corresponds to the recited “identifier associated with the user.”

Lastly, for the “creating” step, Petitioner directs us to where Mellmer discloses that the partner site “will key off the DigitalMe™ unique ID” and create a user account. Pet. 28–29 (citing Ex. 1008, 25:63–66, Fig. 34). The account creation in Mellmer occurs after the user has attempted to log into the partner site but before the user is logged into the partner site. See Ex. 1008, Fig. 34. We find that Mellmer’s account creation corresponds to the recited step of “creating a user account.”

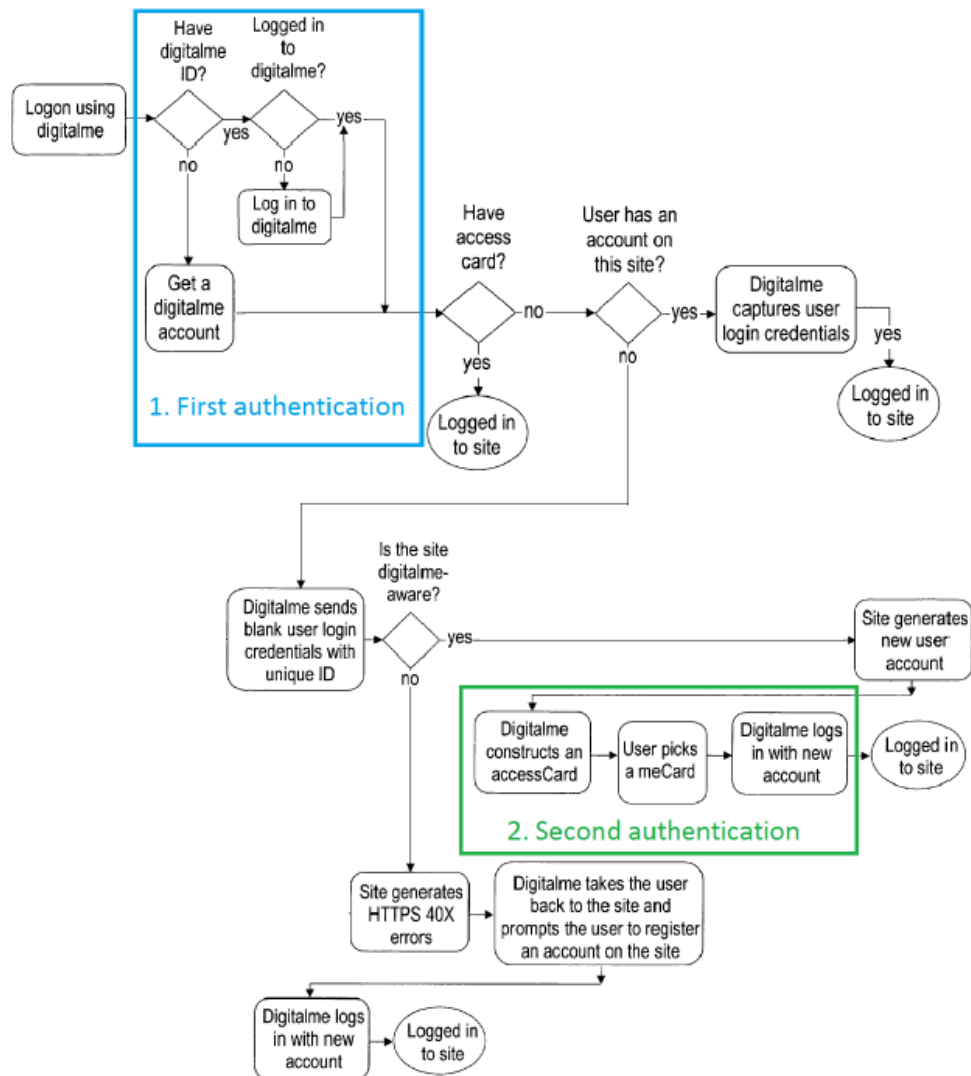
We note that Patent Owner does not dispute that Mellmer discloses most elements recited in claims 1, 15, and 18. See Paper 13, 3 (“arguments for patentability not raised in the response will be deemed waived”). Patent Owner contends, however, that “Mellmer does not disclose either ‘triggering a single-sign-on operation on behalf of the user in order to obtain access to a protected resource that is hosted by the second system’ or a ‘federated computing environment.’” PO Resp. 30 (discussing claim 1); *id.* at 44–45 (referring to discussion of claim 1 for claims 15 and 18). We address the disputed limitations in turn.

- a. “triggering a single-sign-on operation on behalf of the user in order to obtain access to a protected resource that is hosted by the second system”*

For this limitation, Petitioner identifies the partner site in Mellmer as a “second system.” Pet. 23. In addition, Petitioner directs us to where Mellmer discloses that “the login process starts when the user goes to the partner’s web site,” where “the user 1002 is presented with a login dialog that asks for the user’s name and password but also includes a link such as a DigitalMe™ login handprint.” *Id.* at 24 (citing Ex. 1008, 24:24–32). In a “Normal Scenario,” if the user already is logged into DigitalMe, “the partner

site login happens automatically without any intervention when the DigitalMe™ login image (e.g., a handprint) is clicked.” *Id.* at 24–25 (citing Ex. 1008, 24:46–54). If the user is not already logged into DigitalMe, “the user is prompted to login and the user is then logged into the partner site.” *Id.* at 26 (citing Ex. 1008, 24:52–54, Fig. 31). In a “No Account On This Site Scenario,” however, Mellmer discloses creating a user account for the partner site in the event the user does not already have such an account. *Id.* (citing Ex. 1008, Fig. 34). Petitioner relies on this latter scenario for disclosing the disputed limitation. *See id.*

In response, Patent Owner argues that “Mellmer requires two authentications before the user is logged into a DigitalMe partner site.” PO Resp. 31. As support, Patent Owner relies on its expert’s declaration testimony and directs us to a figure that was created based on Mellmer’s teachings, which is reproduced below. *See id.* at 35 (citing Ex. 2103 ¶ 84).



The figure shows Mellmer's "fully assembled 'Logon using DigitalMe' flow." *Id.* at 35; *see also* Tr. 15:11–13 (Petitioner stating that "what [Patent Owner] and its expert did in their papers was take those scenarios in Figures 31 through 35 [in Mellmer] and combine them into a contiguous flow"), 16:8–10 (Petitioner stating that it "do[es]n't dispute that they've accurately pieced the flows together to make their combined graphic"). Patent Owner explains,

[T]he user [in Mellmer] must authenticate with the DigitalMe service before the DigitalMe service sends blank user log-in credentials to the DigitalMe partner site, which is the first step in

the “No Account on this Site” Scenario after the “User has account on this site?” decision block With the blank user login credentials, the DigitalMe service also submits a globally unique ID for the DigitalMe user. DigitalMe refers to the submission of the blank user login credentials and globally unique ID as a “test post.” If the DigitalMe partner site is “DigitalMe-aware,” it generates an account. Next, a DigitalMe servlet will generate an accessCard for that account. DigitalMe then prompts the user to associate a meCard with the created accessCard in order for the DigitalMe service to re-issue the post on behalf of the user.

PO Resp. 33–34 (internal citations omitted); *see also* Ex. 1008, 25:60–26:2 (describing “A No Account On This Site Scenario”), Fig. 34 (illustrating “A No Account On This Site Scenario”).

According to Patent Owner, “before Mellmer’s ‘Logon using DigitalMe’ flow reaches the ‘No Account on this Site Scenario’ in Fig. 34 of Mellmer, the user must have performed a first authentication with the DigitalMe service.” PO Resp. 32; *see also* Ex. 1008, Fig. 34. In addition, according to Patent Owner, the “re-issued post constitutes a second authentication at the DigitalMe partner site.” PO Resp. 34. This is shown in Patent Owner’s assembled figure as three steps: DigitalMe constructing an accessCard, the user picking a meCard, and DigitalMe logging in with the new account. *See id.* at 35. Patent Owner explains that, “[w]hen the DigitalMe service re-issues the post on behalf of the user, the DigitalMe service is sending to the DigitalMe partner site the user’s newly created accessCard for that partner site,” which “includes the user’s login credentials for the DigitalMe partner site.” *Id.* at 34. Patent Owner further explains that, “[i]n order for the DigitalMe service to re-issue the post to the DigitalMe partner site, the user must associate a meCard with an accessCard

for the partner site,” meaning that “the user has to actively participate in the authentication to the DigitalMe partner site, *i.e.*, perform that second authentication.” *Id.*

In its Reply, Petitioner argues that “Mellmer does not require a second authentication, much less a second authentication that is performed **by the user.**” Pet. Reply 8. First, Petitioner explains, an authentication refers to a “process of validating a set of credentials that are provided by a user or on behalf of a user.” *Id.* Petitioner points out that “[t]he only step performed by the user during the alleged ‘second authentication’ in Mellmer is that the user picks a meCard, which is a user profile, to associate with the newly-created accessCard.” *Id.* at 10. Petitioner further points out that “meCards do not contain credentials” and that “[s]electing a meCard is not an authentication.” *Id.* at 10–11. According to Petitioner, “simply because there is an intermediate step that is performed by the user (which itself is not an authentication) does not make all of the surrounding steps attributable to the user, much less a second authentication performed by the user.” *Id.* at 11.

Second, Petitioner explains, “Mellmer discloses various different scenarios and configurations in which DigitalMe could be implemented by different systems, but none of those scenarios includes the set of ‘second authentication’ steps that [Patent Owner] describes.” *Id.* at 12. According to Petitioner, Patent Owner “assumes that a user’s credentials will be included in the accessCard, sent to the partner site, and verified by the partner site upon the reissued post to perform the second authentication.” *Id.* at 11. Petitioner points out that Patent Owner relies on portions of Mellmer that do not relate to the “No Account On This Site Scenario,” however, which

Petitioner alleges is the scenario that anticipates the challenged claims of the '346 patent. *Id.* at 12. Petitioner acknowledges that Patent Owner also relies on a portion in Mellmer related to the “No Account On This Site Scenario,” but explains that this portion in Mellmer “is silent as to what information is included in the accessCard or what, if any, authentication process is performed by the partner site.” *Id.*

Based on the record before us, we agree with Petitioner. As discussed above in the “Claim Construction” section, we construe the term “single sign-on operation” to mean “a process by which a user is authenticated at a first entity and subsequently not required to perform another authentication before accessing a protected resource at a second entity.” An authentication, as explained by Petitioner, refers to a “process of validating a set of credentials that are provided by a user or on behalf of a user.” Pet. Reply 8. This is supported by the '346 patent. *See* Ex. 1001, 9:50–51 (providing the same definition); *see also* Tr. 27:24–28:2 (Patent Owner stating that there is “no real dispute on the meaning of authentication”).

While we recognize that DigitalMe “will construct an accessCard, prompt the user to associate a meCard, and re-issue the post” *before* the user is logged into the partner site in Mellmer, (*see* Ex. 1008, 25:66–26:2, Fig. 34), we do not find this disclosure to be indicative of a second authentication, as Patent Owner urges, (*see* PO Resp. 34). For instance, we note that an accessCard in Mellmer “represent[s] the partner site.” Ex. 1008, 24:48. As Petitioner points out, Mellmer “is silent as to what information is included in the accessCard” described in the “No Account On This Site Scenario” section. Pet. Reply 12. That is, Mellmer does not teach that the accessCard in a “No Account On This Site Scenario” includes a set of

credentials. *See id.*; *see also* PO Resp. 34 (citing Ex. 1008, 24:62–25:4 (describing “A Normal Scenario”), 25:9–13 (describing “A Normal Scenario”), 25:38–43 (describing “A No Access Card Scenario”), 25:63–26:2 (describing an accessCard in “A No Account On This Site Scenario,” without describing the contents of the accessCard), 26:32–35 (describing “A Site that is not DigitalMe™—Aware Scenario”)). Thus, based on the arguments and evidence presented, we find that constructing an accessCard representing the partner site does not constitute providing or validating a set of credentials.

With respect to the step of associating a meCard, we also note that a meCard in Mellmer represents a user’s profile, such as business profile with a professional picture, a personal profile with a sound file, or an anonymous profile with no picture. Ex. 1008, 4:8–13 (cited at Pet. Reply 10). Mellmer discloses that each accessCard in the DigitalMe architecture is associated with a user’s meCard structure. *Id.* at 27:66–67. Mellmer further discloses that online merchants may “collect information profiles on their customers so they can improve their sales.” *Id.* at 8:13–15 (cited at Pet. Reply 11). As Petitioner points out, Mellmer does not teach that a meCard includes a set of credentials. *See* Pet. Reply 10–11. Thus, we find that associating a meCard representing a user profile with an accessCard representing the partner site does not constitute providing or validating a set of credentials.

Lastly, we also find that the step of reissuing the post in the “No Account On This Site Scenario” does not constitute providing or validating a set of credentials. As discussed above, Mellmer discloses specifically that DigitalMe initially attempts a login with “*blank* login data” in the “No Account On This Site Scenario.” *Id.* at 25:60–63 (emphasis added) (cited at

PO Resp. 33–34). This disclosure indicates that the original test post does not include a set of credentials. Mellmer does not further disclose adding a set of credentials to the post before DigitalMe reissues it or before the user is logged into the partner site.

Having considered the arguments and evidence developed during trial, we find that Mellmer’s login procedure for a “No Account On This Site Scenario” discloses “triggering a single-sign-on operation on behalf of the user in order to obtain access to a protected resource that is hosted by the second system,” as required by claims 1, 15, and 18. Namely, we note the cited disclosures in Mellmer that the user logs into DigitalMe, and that the partner site then creates a user account for the partner site where the user does not already have such an account. *See* Ex. 1008, Figs. 31, 34 (cited at Pet. 25–26). We also note the absence of sufficient evidence showing the provision or validation of a set of credentials at the partner site in the “No Account On This Site Scenario.” Accordingly, we find that Mellmer discloses the recited triggering step.

b. “federated computing environment”

The preambles of claims 1, 15, and 18 recite that “a first system and a second system interact within a federated computing environment.” As discussed above in the “Claim Construction” section, we construe a “federated computing environment” to mean “an environment having a loosely coupled affiliation of entities that adhere to certain standards of interoperability; the federation provides a mechanism for trust among those entities with respect to certain computational operations for the users within the federation.” For this limitation, Petitioner identifies DigitalMe in

Mellmer as a “first system” and the partner site in Mellmer as a “second system.” See Pet. 23 (“a partner site, which is a website that hosts protected resources . . . and, in this example, is federated with DigitalMe”). Petitioner also directs us to where Mellmer discloses that “DigitalMe™ technology offers a way to securely authenticate a partner’s users and encourage them to come back to the partner’s site.” *Id.* (quoting Ex. 1008, 24:14–16). In particular, “[t]he user receives relatively quick and simple access to the partner site via a trusted DigitalMe™ interface.” Ex. 1008, 24:21–23 (cited at Pet. 23).

In response, Patent Owner argues that “Mellmer does not have a ‘mechanism for trust’ and therefore does not disclose a ‘federated computing environment.’” PO Resp. 36. Patent Owner explains that “[a] DigitalMe partner site does not need to trust the DigitalMe service because the DigitalMe partner site always requires the DigitalMe user to present valid credentials for the partner site, consistent with DigitalMe’s ‘keychain’ function.” *Id.* at 37. As support, Patent Owner relies on Mellmer’s disclosure that “[u]sers also need only remember their DigitalMe™ user ID and password; the DigitalMe™ software caches and submits all other web login credentials.” *Id.* at 36–37 (citing Ex. 1008, 25:9–12); *see also id.* at 37 (“but for the presence of ‘additional DigitalMe attributes’ in the login post buffer, a DigitalMe partner site cannot even distinguish between a login through the ‘Logon using DigitalMe’ process and a login through the partner site’s own login form”); *accord id.* at 38. Patent Owner also relies on Ms. Spielman’s declaration testimony, which explains that “the DigitalMe service acts as a ‘keychain’ in that it stores the user’s credentials for DigitalMe partner sites and submits those credentials as accessCards to

DigitalMe partner sites at the user's request." PO Resp. 37 (citing Ex. 2103 ¶ 94); Ex. 2103 ¶ 94.

Petitioner counters, arguing in its Reply that "the Board should reject [Patent Owner's] attempt to read further limitations into the claim[s] via the phrase 'federated computing environment' to include a specific mechanism for trust." Pet. Reply 14. We are not persuaded by this argument. As discussed above in the "Claim Construction" section, we conclude that the term "federated computing environment" is limiting. Accordingly, based on our construction of that term, claims 1, 15, and 18 require a mechanism for trust among the entities.

Petitioner further argues that Mellmer nevertheless "does disclose a mechanism for trust." *Id.* As support, Petitioner directs us to where Mellmer discusses the "No Account On This Site Scenario" in which DigitalMe sends a "globally unique identity" to the partner site, and the partner site "key[s] off" the unique identity and generates a user account. *Id.* at 15 (citing Ex. 1008, 25:63–66, Fig. 34). Petitioner points out that "[t]his is precisely the type of 'trust relationship' that the '346 Patent describes—'shared secret keys and rules that define the expected and/or allowed token types and identifier translations.'" *Id.* at 15–16 (quoting Ex. 1001, 20:12–17).

Petitioner also directs us to where "Mellmer discloses using SSL connections and digital signatures to ensure security and authenticity." *Id.* at 14–15 (citing Ex. 1008, 27:39–43, 28:35–51); *see also* Ex. 1008, 28:24–26. With respect to communications between DigitalMe and a partner site in particular, Mellmer discloses:

When this post occurs over an SSL connection, the partner's site will be assured that the transmitted information is secure, but there is no assurance that the post, although apparently originating from the DigitalMe™ server, is indeed authentic. To provide this assurance of authenticity, the action post buffer will include two more attributes, which provide a digital signature of the post buffer.

Ex. 1008, 28:37–43.

According to Petitioner, Patent Owner's argument that Mellmer lacks a mechanism for trust "conflates different 'scenarios' and falsely assumes that the 'No Account On This Site Scenario' 'requires the DigitalMe user to present valid credentials for the partner site' when there is no support in Mellmer for that contention." Pet. Reply 16–17. Petitioner explains that "the portion [in Mellmer] that [Patent Owner] cites to support the conclusion that Mellmer will always require the partner site to verify a user's credentials again relates to the 'Normal Scenario,' not the 'No Account On This Site Scenario.'" *Id.* at 20. Petitioner also points out that Patent Owner's contention that, except for the DigitalMe attributes in the post buffer, the partner site cannot distinguish between a login through DigitalMe and a login through its own site ignores Mellmer's teaching that the DigitalMe attributes include "***two more attributes, which provide a digital signature of the post buffer***" in order to provide assurance of authenticity. *Id.* at 20 (citing Ex. 1008, 28:41–43).

Based on the record before us, we are persuaded by Petitioner's argument. The '346 patent teaches that "a fundamental notion of trust between the federation participants is required for business reasons in order to provide a level of assurance that the assertions (including tokens and attribute information) that are transferred between the participants are valid."

Ex. 1001, 20:22–28 (cited at Pet. Reply 14). According to the ’346 patent, “[i]f there is no trust relationship, then the service provider cannot depend upon the assertions received from the identity provider; they cannot be used by the service provider to determine how to interpret any information received from the identity provider.” *Id.* at 20:28–32 (cited at PO Resp. 38). We note that an assertion “will contain some sort of evidence of the user’s successful authentication to the issuing party together with an identifier for that user.” *Id.* at 22:19–21.

As discussed above, Mellmer discloses that the test post will succeed for a DigitalMe-aware partner site because such partner site “[is] expecting a DigitalMe™ login and will key off the DigitalMe™ unique ID.” Ex. 1008, 25:63–66. We consider Mellmer’s unique identity to represent a part of what the ’346 patent refers to as an “assertion,” which we note is distinguished from credentials. *Compare* Ex. 1001, 10:2–4 (“an authentication credential is presented by a user as part of an authentication protocol sequence with an authentication server or service”), *with id.* at 10:4–7 (“an authentication assertion is a statement about the successful presentation and validation of a user’s authentication credentials, subsequently transferred between entities when necessary”). As we mentioned above, an assertion “will contain some sort of evidence of the user’s successful authentication to the issuing party together with an *identifier for that user.*” *Id.* at 22:19–21 (emphasis added). Mellmer’s unique identity is analogous to such an identifier. Accordingly, that the partner site in Mellmer receives the unique identity from DigitalMe and then uses that unique identity to generate a local user account implies a trust relationship between DigitalMe and the partner site.

Moreover, we note that Mellmer also discloses that, “[w]henver DigitalMe™ software is used to login to a site, a DigitalMe™ globally unique id will preferably be added to the post buffer.” Ex. 1008, 26:53–55. As discussed above, Petitioner directs us to where Mellmer discloses that the partner site may “verify a DigitalMe™ digital signature of the post buffer” (which includes the unique identity) so that it can “be assured of the security and authenticity of the login from the DigitalMe™ service.” Pet. Reply 15 (citing Ex. 1008, 27:39–43). This verification allows for a trust relationship between DigitalMe and the partner site.

With respect to Patent Owner’s argument that “the DigitalMe partner site always requires the DigitalMe user to present valid credentials for the partner site,” we agree with Petitioner that Patent Owner relies on disclosures in Mellmer that do not relate to the “No Account On This Site Scenario.” See PO Resp. 37–38 (citing Ex. 1008, 24:62–25:4 (describing “A Normal Scenario”), 25:5–13 (describing “A Normal Scenario”), 25:38–43 (describing “A No Access Card Scenario”), 25:55–59 (describing “A No Access Card Scenario”), 26:32–35 (describing “A Site that is not DigitalMe™—Aware Scenario”)); see also Pet. Reply 16 (“[Patent Owner] conflates different ‘scenarios’”).

Although we recognize that Patent Owner also relies on disclosures in Mellmer that do relate to the “No Account On This Site Scenario,” we note that Patent Owner’s argument appears to be inconsistent with these disclosures. See PO Resp. 37 (citing 25:63–26:2). For instance, Mellmer discloses that “DigitalMe™ software attempts a login with *blank login data*, except for a globally unique identity for the DigitalMe™ user.” Ex. 1008, 25:60–63 (emphasis added). This disclosure indicates that credentials are

not presented to the partner site. *See also* Pet. Reply 16–17 (“[Patent Owner] . . . falsely assumes that the ‘No Account On This Site Scenario’ ‘requires the DigitalMe user to present valid credentials for the partner site’”). Mellmer also discloses that DigitalMe “will construct an accessCard, prompt the user to associate a meCard, and re-issue the post” before the user is logged into the partner site. Ex. 1008, 25:66–26:2, Fig. 34. As discussed above with respect to the recited “single-sign-on operation,” however, neither the accessCard, the meCard, nor the reissue of the post includes a set of credentials in the context of a “No Account On This Site Scenario.” Thus, the cited disclosures in Mellmer do not support Patent Owner’s argument that the partner site always requires the user to present valid credentials for the partner site in the context of a “No Account On This Site Scenario.”

Patent Owner additionally points to what it considers to be “[o]ther evidence in Mellmer confirm[ing] that [Mellmer] does not disclose a mechanism for trust.” PO Resp. 37. For example, Patent Owner notes that “Mellmer lacks the hallmarks of a mechanism for trust as described in the ’346 patent.” *Id.* According to Patent Owner, such hallmarks would include trust proxies at the DigitalMe service and partner site, a bootstrapping process for establishing initial trust between those trust proxies, and business or liability agreements between the DigitalMe service and partner site. *Id.* at 37–38.

As discussed above, we find that Mellmer’s exchange of the unique identity between DigitalMe and the partner site as well as Mellmer’s security and authenticity features sufficiently disclose a trust relationship. Patent Owner’s evidence is not sufficient to rebut Petitioner’s showing that

Mellmer discloses a mechanism for trust. Claims 1, 15, and 18 do not recite any “hallmark” of a mechanism for trust.

Patent Owner further notes “the partner site can rely on its own authentication mechanisms to validate the user’s credentials for the partner site contained in a DigitalMe accessCard.” PO Resp. 38. This evidence also is not sufficient to rebut Petitioner’s showing that Mellmer discloses a mechanism for trust. As discussed above, Patent Owner does not produce sufficient evidence showing an exchange of *credentials* at the partner site in the context of a “No Account On This Site Scenario.” Moreover, we find that Mellmer’s exchange of the unique identity (which we consider to be an assertion, not a credential) as well as Mellmer’s security and authenticity features sufficiently disclose a trust relationship.

Lastly, Patent Owner notes that “[a]ll that a DigitalMe partner site has to do to incorporate ‘Logon using DigitalMe’ functionality is to code a link to www.digitalme.com onto the partner site’s login page.” *Id.* at 37. According to Patent Owner, “[n]o trust relationship between the DigitalMe service and the DigitalMe partner site is necessary for that; just a few lines of HTML code at the partner site.” *Id.* Even if this were true, we note again that we find that Mellmer’s exchange of the unique identity as well as Mellmer’s security and authenticity features sufficiently disclose a trust relationship. Patent Owner’s evidence is not sufficient to show that Mellmer lacks a mechanism for trust.

In sum, having considered the arguments and evidence developed during trial, we find that Mellmer’s exchange of the unique identity between DigitalMe and the partner site as well as Mellmer’s security and authenticity features disclose a trust relationship. Specifically, we note the cited teaching

in the '346 patent that the service provider cannot depend on assertions from the identity provider where there is no trust relationship. *See* Ex. 1001, 20:28–32. We also note the cited disclosures in Mellmer that the partner site “key[s] off” the unique identity from DigitalMe to generate a user account, (*see* Ex. 1008, 25:63–66, Fig. 34), and that the partner site verifies the DigitalMe signature of the post buffer (which includes the unique identity) to ensure security and authenticity of the login from DigitalMe, (*see id.* at 27:39–43). Accordingly, we find that Mellmer discloses a mechanism for trust.

In view of the foregoing, we determine that Petitioner has demonstrated by a preponderance of the evidence that Mellmer anticipates claims 1, 15, and 18.

3. *Claim 3*

Claim 3 depends from claim 1 and additionally recites “sending a message from the second system to the first system to pull authentication information for the user from the first system to the second system in order to trigger the single-sign-on operation for the user at the second system.” For this limitation, Petitioner directs us to where Mellmer discloses that, “[i]f the user selects the DigitalMe™ login (e.g., by clicking on a ‘login using DigitalMe™’ GIF), the Novell-provided link captures and wraps the site’s URL . . . , which is sent to a web sign-on servlet 508.” Pet. 30 (quoting Ex. 1008, 24:39–44). Petitioner also directs us to where Mellmer discloses that, “[i]n response, the ‘DigitalMe™ software attempts a login with blank login data, except for a globally unique identity for the DigitalMe™ user.’” *Id.* (quoting Ex. 1008, 25:61–63). Petitioner explains

that “the initial message from the partner site may be considered a request, in response to which, the DigitalMe server sends a unique identifier for the user to trigger the single-sign-on operation at the partner site.” *Id.* at 31. In other words, Petitioner explains, “the partner site pulls user ID information to begin the single-sign-on operation disclosed in Fig. 34 [of Mellmer].” *Id.*

In response, Patent Owner argues that “[t]he partner site [in Mellmer] does not send a message to the DigitalMe service to pull authentication information when the user clicks the ‘login using DigitalMe’ link on the DigitalMe partner site.” PO Resp. 40. Relying on the declaration testimony of Ms. Spielman, Patent Owner explains that, “when the user clicks the ‘login using DigitalMe’ link on the partner site, **‘without receiving a message from the DigitalMe partner site**, the DigitalMe service executes JavaScript on the DigitalMe server . . . to identify, capture, and wrap the URL of the DigitalMe partner site.’” *Id.*; Ex. 2103 ¶ 103 (citing Ex. 1008, 29:14–27, 30:25–57). According to Patent Owner, once the “Logon using DigitalMe” flow reaches the “No Account On This Site Scenario,” “the DigitalMe service sends the user’s globally unique ID to the DigitalMe partner site—without having received a message from the DigitalMe partner site to pull that globally unique ID.” PO Resp. 40–41.

Based on the record before us, we agree with Petitioner. Mellmer discloses that clicking on the “login using DigitalMe” link (which is provided at the partner site) will cause the link to capture and wrap the partner site’s URL, “which is *sent* to a web sign-on servlet 508 at www.digitalme.com,” and “[t]hen one or more of the following scenarios will happen.” Ex. 1008, 24:39–44 (emphasis added); *see also id.* at 30:25–29 (“incorporating the HTML . . . into a partner site’s login page will start

the process of leveraging DigitalMe™ web sign-on capabilities for that site”) (cited at Ex. 2103 ¶ 103). Mellmer further discloses that, in the context of “A No Account On This Site Scenario,” DigitalMe will “attempt[] a login with blank login data, except for a globally unique identity.” *Id.* at 25:60–63. These disclosures indicate a communication from the partner site to DigitalMe, which results in DigitalMe providing the partner site with a globally unique identity. We consider such communication to imply a message to pull authentication information. Accordingly, we find that Mellmer discloses “sending a message from the second system to the first system to pull authentication information for the user from the first system to the second system in order to trigger the single-sign-on operation for the user at the second system.”

In view of the foregoing, we determine that Petitioner has demonstrated by a preponderance of the evidence that Mellmer anticipates claim 3.

4. Claim 12

Claim 12 depends from claim 1 and additionally recites that “the first system supports an identity provider and the second system supports a service provider.” For this limitation, Petitioner directs us to where Mellmer describes DigitalMe as including an “identity server” that “holds a user’s data.” Pet. 31 (quoting Ex. 1008, 9:23–25). Petitioner also directs us to where Mellmer describes fidelity.com as an example of a partner site. *Id.* (citing Ex. 1008, Fig. 30). We note that Petitioner, relying on its expert’s declaration testimony, explains with respect to the preamble of claim 1 that

fidelity.com hosts protected resources, namely “user investment accounts.” *Id.* at 23 (citing Ex. 1002 ¶ 73³).

In response, Patent Owner argues that Mellmer does not disclose an “identity provider” or a “service provider” because Mellmer does not disclose a “federated computing environment.” PO Resp. 41. As discussed above with respect to claims 1, 15, and 18, however, we find that Mellmer discloses a “federated computing environment.”

Based on the record before us, we find that Mellmer’s DigitalMe and partner site disclose an “identity provider” and a “service provider,” respectively. Accordingly, we determine that Petitioner has demonstrated by a preponderance of the evidence that Mellmer anticipates claim 12.

5. Claim 13

Claim 13 depends from claim 1 and additionally recites “prompting the user by the service provider to provide or to select an identifier for the identity provider prior to receiving an identifier associated with the user.” For this limitation, Petitioner again directs us to where Mellmer discloses that, “[if] the user selects the DigitalMe™ login (e.g., by clicking on a ‘login using DigitalMe™’ GIF), the Novell-provided link captures and wraps the site’s URL . . . , which is sent to a web sign-on servlet 508 at www.digitalme.com.” Pet. 32 (quoting Ex. 1008, 24:39–44). Petitioner explains that “Mellmer discloses that the user is prompted by the partner site to select DigitalMe as the identity provider prior to receiving a user

³ Although Petitioner cites Ex. 1002 ¶ 73 (original expert declaration) in its Petition, we refer to Ex. 1011 ¶ 73 (substitute expert declaration). We note that both paragraphs are identical.

identifier.” *Id.* Petitioner further explains that, “[a]fter the user clicks on the DigitalMe handprint and if the user does not yet have an account at the partner site, DigitalMe sends the partner site a unique identifier for the DigitalMe user.” *Id.*; *see also* Ex. 1008, 25:60–63.

In response, Patent Owner argues that “the disclosure [in Mellmer] on which Petitioner relies does not meet the limitations of [c]laim 13.” PO Resp. 43. According to Patent Owner, “[c]laim 13 requires prompting the user to provide or select an **identifier** for the identity provider, not to provide or select an **identity provider**.” *Id.* Patent Owner also points out that “the user [in Mellmer] is not prompted to provide or select th[e] unique identifier,” and that, “[i]nstead, DigitalMe—not the user—provides the globally unique identifier without the user selecting or providing it.” *Id.*

In its Reply, Petitioner points out that claim 13 does not require the user to be prompted to provide or select the unique identifier provided by DigitalMe. Pet. Reply 24. According to Petitioner, claim 13 instead “requires that the user is prompted to select an identifier **for the identity provider**—that is, to identify the preferred identity provider.” *Id.* As support, Petitioner relies on teachings in the ’346 patent. *See id.* 24–25 (citing Ex. 1001, 40:83–67⁴); *see also* Ex. 1001, 40:62–41:2. Petitioner explains that Mellmer discloses prompting the user to select an identifier for the identity provider because “the user is prompted by the partner site to select the handprint, which is an identifier for DigitalMe.” Pet. Reply 24.

⁴ Although Petitioner cites Ex. 1001, 40:83–67, we believe Petitioner intended to cite Ex. 1001, 40:62–41:2, which includes the language quoted in Petitioner’s Reply.

Based on the record before us, we agree with Petitioner. As Petitioner points out, claim 13 requires the service provider to prompt the user to provide or select an *identifier for the identity provider* before the service provider receives an *identifier associated with the user*. Mellmer discloses that the partner site presents the user with a handprint or link that the user may click on, thereby disclosing the step of prompting the user to select an *identifier for the identity provider*, namely DigitalMe. Ex. 1008, 24:39–44; *see also id.* at 24:27–33 (“At the partner site, the user 1002 is presented with a login dialog that asks for the user’s name and password but also includes a link such as a DigitalMe™ login handprint Alternately, the partner site may use only the DigitalMe™ login process.”). Mellmer also discloses that, after the user selects the handprint or link, the partner site receives from DigitalMe a globally unique identity for the user, thereby disclosing the subsequent step of receiving an *identifier associated with the user*. *Id.* at 25:60–66. Having considered the arguments and evidence developed during trial, we find that Mellmer discloses “prompting the user by the service provider to provide or to select an identifier for the identity provider prior to receiving an identifier associated with the user.”

In view of the foregoing, we determine that Petitioner has demonstrated by a preponderance of the evidence that Mellmer anticipates claim 13.

IV. CONCLUSION

For the foregoing reasons, we determine that Petitioner has demonstrated by a preponderance of the evidence that claims 1, 3, 12, 13,

IPR2016-00609
Patent 7,631,346 B2

15, and 18 of the '346 patent are unpatentable under 35 U.S.C. § 102 as anticipated by Mellmer.

V. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that claims 1, 3, 12, 13, 15, and 18 of the '346 patent are held to be *unpatentable*; and

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

PETITIONER:

Richard S. Zembek
Bert Greene
Daniel Prati
NORTON ROSE FULBRIGHT US LLP
richard.zembek@nortonrosefulbright.com
bert.greene@nortonrosefulbright.com
dan.prati@nortonrosefulbright.com

PATENT OWNER:

Kevin K. McNish
Andrew G. Heinz
DESMARAIS LLP
kmcnish@desmaraisllp.com
aheinz@desmaraisllp.com