NOTE: This disposition is nonprecedential.

United States Court of Appeals for the Federal Circuit

INTERNATIONAL BUSINESS MACHINES CORPORATION,
Appellant

v.

ANDREI IANCU, UNDER SECRETARY OF COMMERCE FOR INTELLECTUAL PROPERTY AND DIRECTOR OF THE UNITED STATES PATENT AND TRADEMARK OFFICE,
Intervenor

2018-1065, 2018-1066

Appeals from the United States Patent and Trademark Office, Patent Trial and Appeal Board in Nos. IPR2016-00608, IPR2016-00609.

Decided: April 1, 2019

KARIM ZEDDAM OUSSAYEF, Desmarais LLP, New York, NY, argued for appellant. Also represented by JOHN M. DESMARAIS, KEVIN KENT MCNISH.

MONICA BARNES LATEEF, Office of the Solicitor, United

States Patent and Trademark Office, Alexandria, VA, argued for intervenor. Also represented by THOMAS W. KRAUSE, MOLLY R. SILFEN.

Before MOORE, TARANTO, and CHEN, *Circuit Judges.*

TARANTO, *Circuit Judge.*

International Business Machines Corporation (IBM) owns U.S. Patent No. 7,631,346, entitled "Method and System for a Runtime User Account Creation Operation Within a Single-Sign-On Process in a Federated Computing Environment." At the behest of several private companies (who have settled and are not parties here), the Patent Trial and Appeal Board of the Patent and Trademark Office, acting as delegee of the PTO Director, 37 C.F.R. §§ 42.4, 42.108, instituted two related inter partes reviews (IPRs) of various claims of the '346 patent under 35 U.S.C. §§ 311−319. In IPR2016-00608, the Board found that claims 1, 3, 12, 14, 15, and 18 are unpatentable because they are anticipated by Japanese Publication No. Tokkai 2004-302907A (Sunada). In IPR2016-00609, the Board found that claims 1, 3, 12, 13, 15, and 18 are unpatentable because they are anticipated by U.S. Patent No. 7,680,819 (Mellmer).

We have jurisdiction to review the Board's final written decisions under 35 U.S.C. §§ 141(c), 319 and 28 U.S.C. § 1295(a)(4). We vacate the Sunada IPR decision because it rests on an incorrect claim construction of the "federated computing environment" limitation of all claims at issue, and we remand for further consideration under the correct construction. In the Mellmer IPR decision, the same claim-construction error is present, but it does not affect our result. We reverse the Board's decision in the Mellmer IPR because we have been pointed to no substantial evidence to support the Board's finding that Mellmer discloses the separate "single-sign-on" limitation of all claims at issue.

I

The specification gives the background to the invention described and claimed. It explains that "[e]nterprises" try to give their users the benefit of being able to gain access to multiple applications "without regard to authentication barriers that protect each particular system supporting those applications." '346 patent, col. 1, lines 14−24. Users had come to expect reduction of authentication burdens: "A user might assume that once he or she has been authenticated by some computer system, the authentication should be valid throughout the user's working session, or at least for a particular period of time, without regard to the various computer architecture boundaries that are almost invisible to the user." *Id.*, lines 25–33. "Enterprises generally try to fulfill these expectations in the operational characteristics of their deployed systems . . . ." *Id.*, lines 33–35. Among the techniques used to do so are "'single-sign-on' (SSO) processes," which aim to require of a user "only one authentication process during a particular user session." *Id.*, lines 53–61.

The specification explains that user expectations about ease of access are coming to extend beyond the systems within an enterprise to Internet domains of different enterprises: "users are coming to expect the ability to jump from interacting with an application on one Internet domain to another application on another domain without regard to the authentication barriers that protect each particular domain." *Id.*, lines 43–46. "To reduce the costs of user management and to improve interoperability *among* enterprises, *federated* computing spaces have been created." *Id.*, lines 62–64 (emphasis added). The specification then defines the term "federated" as based on a cooperative relationship among enterprises that falls short of the unitary control available within an enterprise:

> A federation is *a loosely coupled affiliation of enterprises* which adhere to certain standards of

> interoperability; the federation provides a mechanism of trust among those enterprises with respect to certain computational operations for the users within the federation.

Id., col. 1, line 64 through col. 2, line 1 (emphasis added). The specification underscores the inter-enterprise nature of being "federated" by stating that "[a]s enterprises move to support federated business interactions, these enterprises should provide a user experience that reflects the increased cooperation between *two businesses*." *Id.*, col. 2, lines 9–11 (emphasis added). In particular, "a user may authenticate to one party that acts as an identity provider and then single-sign-on to a federated business partner." *Id.*, lines 12–14.

The specification discusses the special challenges of providing single-sign-on capabilities in a "federated" environment. *Id.*, lines 19–42. The Background of the Invention section ends by asserting: "it would be advantageous to have methods and systems in which enterprises can provide comprehensive single-sign-on experiences to users in a federated computing environment in a lightweight manner that does not require an extensive amount of a priori processing." *Id.*, lines 44–48.

The one-paragraph Summary of the Invention immediately follows. It begins by stating that "[a] method, system, apparatus, and computer program product are presented to support computing systems of different enterprises that interact within a federated computing environment." *Id.*, lines 53−56. The Summary then describes the contemplated process of users getting access to multiple federation partners through a "single-sign-on": "Federated single-sign-on operations can be initiated at the computing systems of federation partners on behalf of a user even though the user has not established a user account at a federation partner prior to the initiation of the single-sign-on operation." *Id.*, lines 59–60. The Summary refers to "an identity provider" as an example of initiating such a single-sign-on user access to resources of a service provider: "For example, an identity provider can initiate a single-sign-on operation at a service provider while attempting to obtain access to a controlled resource on behalf of a user." *Id.*, lines 60–63. It then says what happens "[w]hen the service provider recognizes that it does not have a linked user account for the user that allows a single-sign-on operation from the identity provider," *i.e.*, "the service provider creates a local user account based at least in part on information from the identity provider." *Id.*, lines 63–67. It concludes: "The service provider can also pull user attributes from the identity provider as necessary to perform the user account creation operation." *Id.*, col. 2, line 67 through col. 3, line 2.

The independent claims at issue are 1, 15, and 18. We follow the parties in focusing on claim 1, which recites:

> 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 use*r 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.

Id., col. 44, lines 38–61 (emphasis added). No separate arguments are presented as to the other claims at issue.

II

The disputes before us focus on the "federated computing environment" and "single-sign-on" claim limitations. The Board and the parties agree that both phrases are limiting, even though the first appears only in the preamble. *See* J.A. 8, 52–53. IBM challenges, and the Director of the Patent and Trademark Office defends, the Board's construction of "federated computing environment." Separately, IBM challenges, and the Director defends, the Board's finding that Mellmer teaches the "single-sign-on" claim limitation.

These inter partes reviews of an unexpired patent are subject to the PTO regulation (since changed) providing that the Board should give the claims their broadest reasonable interpretation in light of the specification. *See* 37 C.F.R. § 42.100(b); *Cuozzo Speed Techs. LLC v. Lee*, 136 S. Ct. 2131, 2144–46 (2016). We review the Board's claim construction de novo here, because the Board relied exclusively on intrinsic evidence to construe the claims. *See Teva Pharms. USA, Inc. v. Sandoz, Inc.*, 135 S. Ct. 831, 841 (2015); *In re Cuozzo Speed Techs., LLC*, 793 F.3d 1268, 1279–80 (Fed. Cir. 2015), *aff'd*, 136 S. Ct. 2131 (2016).

"To anticipate a claim, a prior art reference must disclose every limitation of the claimed invention, either explicitly or inherently." *In re Schreiber*, 128 F.3d 1473, 1477 (Fed. Cir. 1997). What a reference discloses and therefore whether it anticipates a claim (as properly construed) present fact questions. *Id.*; *see Idemitsu Kosan Co. v. SFC Co.*, 870 F.3d 1376, 1379 (Fed. Cir. 2017). We review the Board's factual findings for substantial evidence. *In re Chudik*, 851 F.3d 1365, 1371 (Fed. Cir. 2017).

A

We turn first to the Board's construction of the term "federated computing environment," which, though it appears in both IPRs before us, we will discuss only with reference to IPR2016-00608, the Sunada IPR. The Board recognized that both IBM and the private companies that requested the IPRs ("Petitioner") agreed about what 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.'" J.A. 6−7 (emphasis added) (quoting Petition).[1] Under that agreed-on construction, a "federated computer environment" must involve a plurality of "enterprises."

The Board rejected the parties' agreed-on construction "that the scope of the term is limited to an affiliation of *enterprises*." J.A. 8 (emphasis in original). The Board did so even while recognizing the specification passage, quoted above, stating that "[a] federation is a loosely coupled affiliation of enterprises . . . ." *See* J.A. 8–9. Despite that passage, the Board concluded that a federated computing environment "is not limited to enterprises." J.A. 9.

[1] Petitioner argued that the phrase, being in the preamble, was not limiting, but the Board rejected that contention, explaining that IBM clearly relied on the term as limiting during prosecution. J.A. 7−8. The parties now before us (IBM and the Director) agree with the Board. We do not question the Board's conclusion.

The Board relied for that conclusion entirely on two specification passages and their use of the word "entity." One passage, from column 10, states 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." '346 patent, col. 10, lines 62–64. The other passage, from column 8, states that "[t]he terms 'entity' or 'party' generally refers to an organization, an individual, or a system that operates on behalf of an organization, an individual, or another system." *Id.*, col. 8, lines 31−33; *see* J.A. 8.

On those bases, the Board construed "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.

J.A. 9 (emphasis added). That construction uses the specification's definitional passage but replaces "enterprises" with "entities." As the Board explained when finding this claim element met in Sunada, the key significance of that replacement is that, under the Board's construction, "two computer *systems* (or entities) *within a single enterprise* could disclose a 'federated computer environment.'" J.A. 30 (emphasis added); *see* J.A. 25, 27.

We conclude that the Board's construction is not reasonable in light of the specification. In the key specification passage quoted above, which is on its face definitional, the patent states that a "federation" is "a loosely coupled affiliation of enterprises." '346 patent, col. 1, lines 64–65. That passage demands that the phrase "federated computing environment" be construed to require a plurality of enterprises unless something else in the specification contradicts the passage's plain meaning. Nothing does.

In fact, the passage is reinforced by two key passages in the specification. The Summary of the Invention states that the invention is addressed to "computing systems *of different enterprises* that interact within a federal computing environment." *Id.*, col. 2, lines 54–56 (emphasis added). And the Background of the Invention confirms the point. As discussed above, the Background makes clear that the problem addressed by the patent is to ease user authentications, through single-sign-on techniques, when the resources to which a user seeks access are not within the unitary control of a single enterprise but, instead, are controlled by a plurality of enterprises, who must make cooperative arrangements to establish trust mechanisms to meet the greater challenges of simplifying user access when unitary control is missing. *See id.*, col. 1, line 14 through col. 2, line 48. Being "federated," these passages make clear, presupposes the absence of the unitary control that a single enterprise could exercise over its own resources.

The two passages that the Board relied on do not reasonably support a contrary claim construction. The column 10 passage states: "In 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." *Id.*, col. 10, lines 62–64. At least when understood in light of the specification language already discussed, the column 10 passage is not reasonably read as an open-ended sweeping in of all "entities," including mere "systems" in the sense of physical equipment. The column 10 passage refers to entities "such as" the ones listed and includes "etc."—both of which, in this context, indicate that only things of a type similar to the itemized ones are covered, namely, other establishments or ventures or firms or the like. We have recognized that "such as" and "etc." sometimes have just that meaning. *See Archer Daniels Midland Co. v. United States*, 561 F.3d 1308, 1313 (Fed. Cir. 2009) (holding that the "rule of *ejusdem generis* . . . limits the additional [things] included by the general phrase 'etc.' to others of the types listed"); *United States v. Nichols Copper Co.*, 29 C.C.P.A. 186, 191 (1941) (holding that "by the use of the words 'such as' in the paragraph we are required to determine whether a substance not specifically named in the paragraph is like or similar to, or belongs to the same class as, the substances therein named"). That understanding is the only reasonable one for the passage, given the plain meaning of the definitional and other language we have already discussed. And it is confirmed by the patent's statement that "[a] federated environment includes federated enterprises *or similar entities* that provide a variety of services for users." '346 patent, col. 15, lines 55–57 (emphasis added).

A "system," referring to just the physical equipment and not who controls it or deals with customers in providing access to it, is not of the same type as "enterprises, organizations, institutions." And those words themselves may be summarized by the term "enterprise" itself, as the definitional passage does. The column 10 sentence just conveys that a variety of very similar words can be used to refer to the same thing. Indeed, the quoted passage ends with a semicolon, and what immediately follows the semicolon confirms that "two enterprises" are needed. *Id.*, col. 10, line 65–col. 11, line 1 ("[A] federated environment differs from a typical single-sign-on environment in that two enterprises need not have a direct, pre-established, relationship defining how and what information to transfer about a user.").

The Board's claim construction finds no better support in the one other basis the Board cited—the column 8 statement that "[t]he terms 'entity' or 'party' generally refers to an organization, an individual, or a system that operates on behalf of an organization, an individual, or another system." *Id.*, col. 8, lines 31−33. That sentence is part of a general section, headed "Terminology," that indicates how certain words may be used anywhere in the patent. The sentence just declares that the highly general word "entity" can refer to quite different things—an establishment, an individual, physical things. That declaration does not focus on defining "federated," and it does not say which of the types of things that can be an "entity" are the types relevant to "federation" or "federated computing environment." The column 10 passage does that, and as explained, it must be understood as referring only to the type of entity that is properly summarized by the term "enterprise."

For those reasons, we conclude that a "federated computing environment" requires a plurality of distinct enterprises. In light of that conclusion, we vacate the Board's final written decision in IPR2016-00608 and remand for the Board to determine in the first instance whether, under the correct claim construction, Sunada anticipates the claims at issue in that IPR.

B

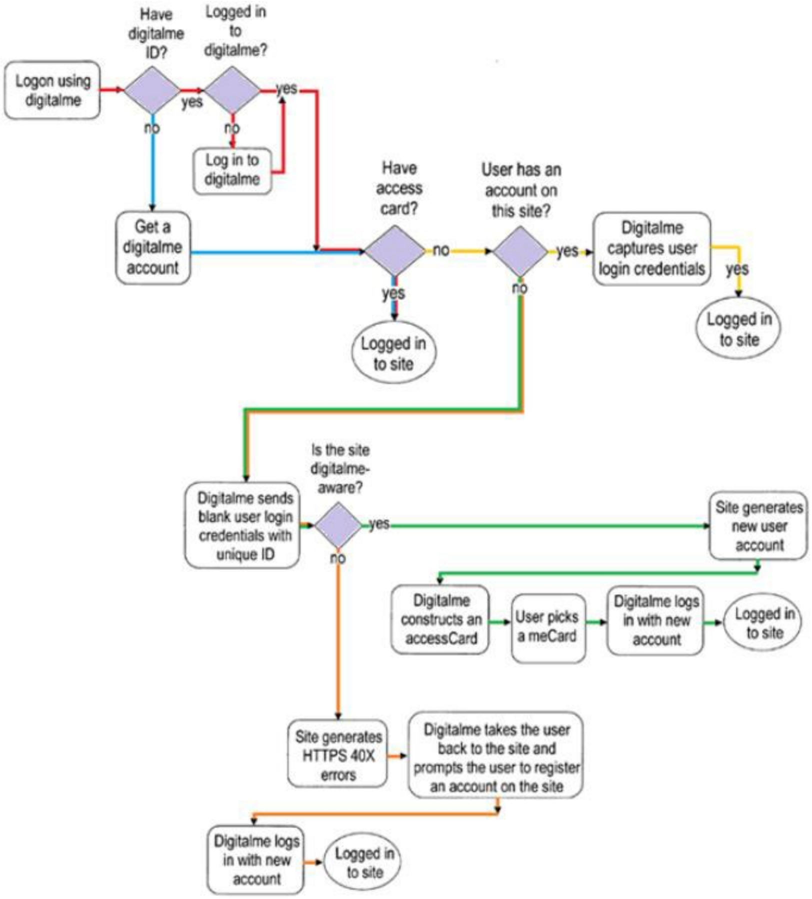
In its decision in IPR2016-00609, the Board found that Mellmer anticipates the claims at issue there. IBM seeks reversal on the ground that Mellmer does not teach the single-sign-on limitation. We have been shown no substantial evidence to support the Board's finding that Mellmer teaches that claim limitation, and we therefore reverse the finding of anticipation in the Mellmer IPR.

The relevant claim limitation of the '346 patent requires "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." *Id.*, col. 44, lines 45–47. The Board construed "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." J.A. 56. And it adopted the specification definition of "authentication" as meaning "the process of validating a set of credentials that are provided by a user or on behalf of a user." '346 patent, col. 9, lines 50–51; J.A. 56. It is undisputed before us that, under those definitions, a user "perform[s]" an authentication when the user takes an action that provides credentials, or that plays a role in launching a provision of credentials on the user's behalf, to obtain access to resources. A "single-sign-on operation" thus is one that does not require the user to take such action to gain access to a second entity's resources after the user has been authenticated with a first entity.

The Mellmer patent is titled "Managing Digital Identity Information." In an effort to "provide better ways to manage personal information on the Internet," Mellmer, col. 2, lines 36–37, Mellmer describes a "basic architecture for managing digital identity information in a network," such as the Internet, *Id.*, Abstract. Mellmer teaches "[v]arious enhancements," among them, techniques for "securely logging in to multiple sites with a single password and doing so from any machine on the network." *Id.* More particularly, Mellmer describes a "DigitalMe" system that, for a user with a DigitalMe ID, eases access to various independent websites (DigitalMe partners) that participate in the system. *Id.*, col. 2, lines 21–35; *id.*, col. 8, lines 40–61. The issue before us is whether a particular part of the described system requires a second user authentication action to gain access to a DigitalMe partner's resources.

Among its many teachings, Mellmer discloses that users who have a DigitalMe identity can "view, create, edit, and delete Profiles" containing information they may use in their on-line activity. *Id.*, col. 4, lines 8–10. Mellmer calls graphical versions of that information "meCards." *Id.* Mellmer also describes "accessCards" that the DigitalMe system uses when a user seeks access to a partner website. *Id.*, col. 24, line 48.

Columns 25–28 describe a process for a user to gain access to a target site by first logging into a DigitalMe account. It is not disputed that the initial login to the DigitalMe site is a first authentication. What happens thereafter depends on whether the user has an accessCard for the target site or an account on the target site. The overall set of possibilities is shown in a flow chart, which was used by the Board, that combines Mellmer's Figures 31–35. J.A. 5375; J.A. 62; *see* Mellmer, Figs. 31–35.


Logon using digitalme
Have digitalme ID?
yes
no
Logged in to digitalme?
yes
no
Log in to digitalme
Get a digitalme account
Have access card?
no
yes
Logged in to site
User has an account on this site?
yes
no
Digitalme captures user login credentials
yes
Logged in to site
Digitalme sends blank user login credentials with unique ID
Is the site digitalme-aware?
yes
no
Site generates new user account
Digitalme constructs an accessCard
User picks a meCard
Digitalme logs in with new account
Logged in to site
Site generates HTTPS 40X errors
Digitalme takes the user back to the site and prompts the user to register an account on the site
Digitalme logs in with new account
Logged in to site

The steps shown in the upper left corner, involving logging into DigitalMe, involve a first authorization. The parties, the Board, and now the Director have all treated the issue of whether Mellmer teaches the single-sign-on limitation as reducing to the question whether a second user authentication action is involved in the steps taken when "no" is the answer to "User has an account on this site?" and the target site has a relationship with DigitalMe. We follow suit.

Mellmer calls that scenario the "No Account On This Site Scenario," Mellmer col. 25, line 60 through col. 26, line 25, and the Figure 34 illustration of that scenario is embedded just below the middle of the above combination flowchart. The steps are: "DigitalMe sends blank user login credential with unique ID" to the target site; "DigitalMe constructs an accessCard"; "User picks a meCard"; and "DigitalMe logs in with new account." Notably, the user's picking of a meCard for association with an accessCard is essential to the successful login to the target site in that scenario.

IBM argued that the user action of associating a meCard with an accessCard constitutes an action that launches provision of credentials to allow access to the target site, *i.e.*, constitutes a second user authentication action, which means that this scenario does *not* teach a "single-sign-on." The Board found otherwise. The Board recognized 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." J.A. 65 (quoting Mellmer, col. 25, line 66 through col. 26, line 2). But the Board agreed with Petitioner that "Mellmer 'is silent as to what information is included in the accessCard' described in the 'No Account On This Site Scenario,'" "[t]hat is, Mellmer does not teach that the accessCard in a 'No Account On This Site Scenario' includes a set of credentials." J.A. 65–66. The Board added that "Mellmer does not teach that a meCard includes a set of credentials." J.A. 66. Finally, the Board stated that "DigitalMe initially attempts a login with '*blank* login data'" in this scenario;[2] "the original test post does not include a set of credentials"; and "Mellmer does not further disclose adding a set of credentials to the post before DigitalMe reissues it or before the use is logged into the partner site." J.A. 66–67. For those reasons, the Board found that this scenario involved only one user authentication action, and thus practiced a single-sign-on operation within the relevant claim limitation of the '346 patent. *See* J.A. 67.

The overall finding that this portion of Mellmer teaches a process involving only one user authentication action is not supported by substantial evidence. To begin with, even if the Board were correct that Mellmer is "silent" about the content of the accessCard, that characterization would not alone support a finding that there was *no* user authentication action in this scenario if, as appears, the Board meant that it simply could not tell one way or the other whether the accessCard contains credentials. Silence in that sense would not by itself suffice for the Petitioner to meet its burden to prove, by a preponderance of the evidence, that there was *no* user authentication action in this scenario. *See* 35 U.S.C. § 316(e). Nor would that burden be met merely by adding a finding that IBM did not prove the opposite, *i.e.*, a finding of "the absence of sufficient evidence showing the provision or validation of a set credentials at the partner site" in this scenario. J.A. 67.

In any event, the Board erred in its "silence" determination, and conclusion about the absence of evidence supporting IBM's position on this scenario, by taking too narrow a view of Mellmer. The Board unreasonably viewed

[2] Mellmer says of the test post: "DigitalMe software attempts a login with blank login data, *except for a globally unique identity for the DigitalMe user*." Mellmer, col. 25, lines 61–63 (emphasis added).

the No Account On This Site Scenario in isolation from its plain context in Mellmer. This particular scenario is part of a larger single flow chart with yes-no branching at various points. This scenario is the ending of one path through a process that, for the user, begins with the earlier common portions of the flow chart. Those earlier portions necessarily bear on the meaning of terms found throughout the overall flow chart.

Once the focus is properly widened to what columns 24–26 teach for the whole set of options and scenarios shown in the above flow chart, substantial evidence does not support a finding that there is no user action triggering an authentication at the target site in this particular scenario. The Board did not question that the user action in associating a meCard with an accessCard is necessary for the logon, as the evidence undisputedly showed. Nor did the Board question that DigitalMe then communicates with the target site to trigger the logon to that site. The flow chart and associated patent descriptions, together with expert testimony, establish those facts. *See* J.A. 6482 (Spielman), 6362 (Olivier).

Even as to the accessCard, the evidence is one-sided against the Board's finding. Consistent with the flow chart's indication that accessCards directly lead to login at the target site, Mellmer, in its descriptions of accessCards in the earlier parts of the overall flow chart, repeatedly indicates that accessCards contain authenticating information that is used for authorization at the target site. *See, e.g.*, Mellmer, col. 24, line 62 through col. 25, line 4; col. 25, lines 9–13 ("Users also need only remember their DigitalMe user ID and password; the DigitalMe software caches and submits all other web login credentials. Also, from the DigitalMe site, the user can list, maintain, and launch these accessCards directly." (emphasis added)); col. 25, lines 32–43 (at lines 40–42: "DigitalMe software will have captured this login data as an accessCard structure which can be applied to login automatically in the future.");

col. 25, line 63 through col. 26, line 2; col. 26, lines 32–35. IBM's expert, in her declaration, relied on this material to attest that, in the No Account On This Site Scenario, "when DigitalMe re-issues the post on behalf of the user" after the user associates a meCard with the accessCard, the DigitalMe service is sending the user's newly-created accessCard for the DigitalMe partner site—which accessCard includes the user's login information for the partner site." J.A. 6482.

The Board did not cite, and the Director in this court has not cited, anything in Mellmer that supports a contrary finding. Nor have we been shown any basis for discrediting the testimony of IBM's expert, which was grounded solidly in consideration of the full column 24–26 passages relevant to understanding what occurs in the No Account On This Site Scenario. And the Petitioner, in its Reply, answered IBM's evidence only by insisting, incorrectly, that the No Account On This Site Scenario be considered in isolation from the column 24–26 material involving the other scenarios that are part of the overall set of options shown in the combination flow chart. J.A. 5435–37. In these circumstances, we see no substantial evidence to support the Board's finding that Petitioner proved that Mellmer teaches the single-sign-on limitation of the claims at issue in this IPR.

III

The Board's decision in IPR2016-00608 is vacated because it rests on an incorrect claim construction, and the matter is remanded for further proceedings consistent with this opinion. The decision in IPR2016-00609 is reversed.

Costs awarded to IBM.

VACATED AND REMANDED in No. 18-1065
REVERSED in No. 18-1066