Trials@uspto.gov
571.272.7822

Paper 56
Entered: October 11, 2023

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

EBATES PERFORMANCE MARKETING, INC. DBA RAKUTEN REWARDS, ZILLOW GROUP, INC., and ZILLO, INC.,
Petitioner,

v.

INTERNATIONAL BUSINESS MACHINES CORP.,
Patent Owner.

IPR2022-00646
Patent 7,631,346 B2

Before DAVID C. MCKONE, MICHELLE N. WORMMEESTER, and ARTHUR M. PESLAK, *Administrative Patent Judges*.

MCKONE, *Administrative Patent Judge*.

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

I. INTRODUCTION

Ebates Performance Marketing, Inc., dba Rakuten Rewards filed a Petition (Paper 2, "Pet.") requesting *inter partes* review of claims 1–20 of U.S. Patent No. 7,631,346 B2 (Ex. 1001, "the '346 patent"). International Business Machines Corp. ("Patent Owner") filed a Preliminary Response to the Petition. Paper 6 ("Prelim. Resp."). Rakuten Rewards filed a Preliminary Reply to the Preliminary Response (Paper 7, Prelim. Reply) and Patent Owner filed a Preliminary Sur-reply to the Preliminary Reply (Paper 8, Prelim. Sur-reply).

The Board instituted an *inter partes* review of the challenged claims pursuant to 35 U.S.C. § 314. Paper 10 ("Inst. Dec."). We subsequently denied Patent Owner's Request for Rehearing of the Institution Decision (Paper 13). Paper 33 ("Reh'g Dec.").

After institution, Patent Owner filed a Patent Owner Response (Paper 35, "PO Resp."). We joined Zillow Group, Inc., and Zillow, Inc., as parties to the proceeding (collectively, with Rakuten Rewards, "Petitioner"). Paper 44. Petitioner filed a Reply (Paper 45) and Patent Owner filed a Sur-reply (Paper 47, "Sur-reply"). The PO Response and Reply were filed under seal. The parties also filed non-confidential versions of the PO Response (Paper 36) and Reply (Paper 46). The parties then presented oral arguments via a (video) Hearing (July 26, 2023), and the Board entered a Hearing transcript into the record. The non-confidential portion of the transcript is at Paper 54 ("Tr."). The confidential portion of the transcript is at Paper 55 ("Conf. Tr.").

For the reasons set forth in this Final Written Decision pursuant to 35 U.S.C. § 318(a), we determine that Petitioner demonstrates by a preponderance of the evidence that claims 1–4, 12–16, 18, and 19 are unpatentable, but does not demonstrate by a preponderance of the evidence that claims 5–11, 17, and 20 are unpatentable.

II. BACKGROUND

A. Related Proceedings

The parties identify the following related federal district court cases: (1) *International Business Machines Corp. v. Rakuten, Inc.*, Civil Action No. 1:21-cv-00461-LPS (D. Del.) ("related district court litigation"); (2) *International Business Machines Corp. v. Zillow Group Inc.*, Civil Action No. 2:20-cv-01130 (D. Del.); and (3) *International Business Machines Corp. v. Zillow Group Inc.*, Civil Action No. 2:20-cv-00851-TSZ (W.D. Wash.). Pet. 1; Paper 3, 1.

Petitioner also identifies several related requests for *inter partes* review, including *Kayak Software Corp. v. International Business Machines Corp.*, IPR2016-00608 ("the Kayak IPR"). Pet. 1. The Kayak IPR proceeded to a Final Written Decision (Ex. 1020 (IPR2021-00608, Paper 67 ("Kayak FWD"))) and was appealed to the United States Court of Appeals for the Federal Circuit, which vacated and remanded the decision (*International Business Machines Corp. v. Iancu*, 759 F. App'x 1002 (Fed. Cir. Apr. 1, 2019) (Ex. 1006, *IBM v. Iancu*)). While the appeal was pending, Kayak and Patent Owner settled, and the parties in that case moved to terminate the Kayak IPR after remand. Pet. 5; Kayak IPR, Paper 72.

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, [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, 10:24–26.

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 has already 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, 32:41–46. After creating the linked user account, the service provider performs the requested resource access. *Id.* at 33:4–5.

Claim 1, reproduced below (with bracketed numbering added to track the numbering used in the Petition) 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;
>
> [1.1] 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;
>
> [1.2] receiving from the first system at the second system an identifier associated with the user; and
>
> [1.3] 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.

C. Evidence

Petitioner relies on the references listed below.

Reference		Date	Exhibit No.
Sunada	Japanese Publ'n No. Tokkai 2004-302907A[1]	pub. Oct. 28, 2004	1005
OASIS[2]	Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1	Sept. 2, 2003	1013
	Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML) V1.1	Sept. 2, 2003	1014
	Conformance Program Specification for the OASIS Security Assertion Markup Language (SAML) V1.1	Sept. 2, 2003	1015
	Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V1.1	Sept. 2, 2003	1016
	Glossary for the OASIS Security Assertion Markup Language (SAML) V1.1	Sept. 2, 2003	1023
Dutcher	US 6,092,199	iss. July 18, 2000	1007

[1] We rely on a certified translation of the Japanese publication. Exhibit 2017 contains corrections to the translation of Sunada. Sur-reply 9 n.2.
[2] According to SAML Conformance Program Specification, Exhibits 1014–1016 and 1023 "comprise the Version 1.1 specification set for SAML." Ex. 1015, 6.

Petitioner also relies on the Declaration of Mark E. Crovella, Ph.D. (Ex. 1011).

Patent Owner relies on the Declaration of Michael I. Shamos, Ph.D. (Ex. 2028).

D. The Asserted Grounds of Unpatentability

Petitioner contends that claims 1–20 are unpatentable under the following grounds. Pet. 4.

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1, 3, 12, 14, 15, 18	102(a)[3]	Sunada
1, 3, 12, 14, 15, 18	103(a)	Sunada
1, 3, 12, 14, 15, 18	103(a)	Sunada, Applicant Admitted Prior Art (AAPA)
1–9, 11, 12, 14–20	103(a)	Sunada, OASIS
10, 13	103(a)	Sunada, OASIS, Dutcher

III. ANALYSIS

A. Collateral Estoppel

Petitioner argues that, due to collateral estoppel, it would be inappropriate to deviate from issues that the Board previously determined in the Kayak IPR. Pet. 15 (citing *Watermark Senior Living Retirement Communities, Inc. v. Morrison Management Specialists, Inc.*, 905 F.3d 421, 428 (6th Cir. 2018)). The Petition does not identify such issues with particularity, but argues generally that "Sunada discloses every limitation at

[3] The Leahy-Smith America Invents Act ("AIA"), Pub. L. No. 112-29, 125 Stat. 284, 287–88 (2011), amended 35 U.S.C. §§ 102 and 103. Because the '346 patent was filed before March 16, 2013, the effective date of the relevant amendment, the pre-AIA versions of §§ 102 and 103 apply.

issue in the Kayak IPR with the possible exception of a [federated computing environment]." *Id.* In the Reply, Petitioner contends that "Patentee is collaterally estopped from arguing that Sunada fails to disclose any limitation other than multiple distinct enterprises (i.e., a 'FCE') for the Ground 1 claims." Reply 1.

Petitioner seeks to collaterally estop Patent Owner from making certain arguments based on the Kayak FWD. Reply 1–5. Yet, the Federal Circuit vacated the Kayak FWD and remanded to the Board for further consideration. Ex. 1006, 2 ("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."), 8 ("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.").

"Collateral estoppel bars the relitigation of factual issues that were fully and fairly litigated and were the basis of final judgment in an action to which the person against whom the estoppel is sought was a party." *U.S. Philips Corp. v. Sears Roebuck & Co.*, 55 F.3d 592, 598 (Fed. Cir. 1995). However, "the general rule is that a judgment which is vacated, for whatever reason, is deprived of its conclusive effect as collateral estoppel." *Dodrill v. Ludt*, 764 F.2d 442, 444 (6th Cir. 1985); *accord Harris Tr. & Sav. Bank v. John Hancock Mut. Life Ins. Co.*, 970 F.2d 1138, 1146 (2d Cir. 1992) ("It is well-settled in [the Second Circuit] that a vacated order has no collateral estoppel effect."). *See also Rumsfeld v. Freedom NY, Inc.*, 329 F.3d 1320,

1332 (Fed. Cir. 2003) ("The law of the case thus does not apply because 'a vacated judgment 'has no preclusive force either as a matter of collateral or direct estoppel or as a matter of the law of the case.'"" (quoting *U.S. Philips*, 55 F.3d at 598)); *S-1 By & Through P-1 v. State Bd. of Educ. of N. Carolina*, 6 F.3d 160, 169 (4th Cir. 1993), reh'g en banc granted, opinion vacated (Oct. 21, 1993), on reh'g sub nom. *S-1 & S-2 By & Through P-1 & P-2 v. State Bd. of Educ. of N. Carolina*, 21 F.3d 49 (4th Cir. 1994) ("The judgment's vacatur on appeal renders it a legal nullity."); *Maryland Cas. Co. v. Armco, Inc.*, 822 F.2d 1348, 1355 (4th Cir. 1987) ("[T]he appellant argues that the action of the district court in Missouri, which assigned a special master to address the same issue but later vacated *nunc pro tunc* its order that adopted the master's recommendations, should have collateral estoppel or preferably res judicata effect in this case. The appellant argues that a defendant should not be able to manipulate the judicial system by entering into last-minute settlements in order to avoid the collateral estoppel effects of unfavorable judgments.[4] . . . We decline to hold that the recommendations of a special master, which have been vacated, rise to the level of a 'final judgment' in order to estop the present litigation." (internal

[4] This is not a case where Patent Owner seeks to avoid the preclusive effects of a decision by settling during appeal, with the underlying decision being vacated pursuant to settlement. Rather, the Federal Circuit made a merits determination, vacated the Kayak FWD pursuant to that determination, and remanded for further proceedings pursuant to its guidance on the merits. Ex. 1006, 2, 8. The parties settled after the Federal Circuit's decision vacating the Kayak FWD.

citations omitted)). Thus, the Kayak FWD, which the Federal Circuit vacated on the merits, is no basis for collateral estoppel in this proceeding.

Petitioner argues that "[w]hen parties settle *after* a sufficiently-final decision, as here, courts apply collateral estoppel." Reply 4 (citing *Sprint Communications Co. L.P. v. Cequel Communications, LLC*, 2020 WL 3048175 (D. Del. June 8, 2020)). In *Sprint*, "the prior district court case was completely adjudicated and Plaintiff was present and had a full and fair opportunity to litigate the case. The *Comcast* court issued a final judgment, and Plaintiff appealed that judgment before it settled." *Sprint*, 2020 WL 3048175 at *5. The *Sprint* court reasoned "[a] settlement during appeal when the *Comcast* court's order was final and appealable under [Federal] Rule [of Civil Procedure] 54 does not preclude a finding of collateral estoppel." *Id.* at *6. There is no indication, however, that the *Comcast* decision to which the *Sprint* court gave preclusive effect was vacated. Thus, Petitioner's argument, that a sufficiently final decision can be given preclusive effect notwithstanding settlement of the parties after filing a notice of appeal, is not persuasive because the Kayak FWD was vacated.

Additionally, applying collateral estoppel in light of the Kayak FWD is not appropriate because the Kayak FWD was decided under the broadest reasonable interpretation claim construction standard, while this proceeding is evaluating the '346 patent under the *Phillips* claim construction standard. *See SkyHawke Techs., LLC v. Deca Int'l Corp.*, 828 F.3d 1373, 1376 (Fed. Cir. 2016) ("Because the Board applies the broadest reasonable construction of the claims while the district courts apply a different standard of claim construction as explored in *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir.

2005) (en banc), the issue of claim construction under *Phillips* to be determined by the district court has not been actually litigated.").

For these reasons, we decline to give the Kayak FWD preclusive effect.

B. Claim Construction

For petitions filed after November 13, 2018, we construe claims "using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. 282(b), including construing the claim in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent." 37 C.F.R. § 42.100(b) (2019); *see also Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc).

1. "federated computing environment"

Petitioner contends that a "federated computing environment," in light of the Federal Circuit's decision in *IBM v. Iancu*, is a "loosely coupled affiliation of a plurality of distinct 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. 13; 759 F. App'x at 1008. Patent Owner agrees with this construction. Prelim. Resp. 23–24; PO Resp. 12. In light of the Federal Circuit's decision and the parties' agreement, we adopted Petitioner's proposed construction for purposes of our Institution Decision. Inst. Dec. 15. We maintain that construction.

2. "protected resource"

In the Institution Decision, we construed "protected resource" to mean "an application, an object, a document, a page, a file, executable code, or other computational resource, communication-type resource, etc., identified by a Uniform Resource Locator (URL), or more generally, a Uniform Resource Identifier (URI), that can only be accessed by an authenticated and/or authorized user." Inst. Dec. 15–16 (citing Prelim. Resp. 22–23; Ex. 1001, 5:60–67; Ex. 2003, 7; Ex. 2004, 6; Ex. 2005, 27; Ex. 2012, 11 (Petitioner agreeing to this construction in Joint Claim Construction statement in the related litigation)).

Patent Owner continues to assert that this is the correct construction. PO Resp. 12–14. Petitioner does not address the construction of "protected resource" in the Reply. Reply 1. We maintain our construction of "protected resource."

3. "identifier associated with the user"

Patent Owner contends that "identifier associated with the user," as recited in claim 1, means "information that uniquely identifies the user." PO Resp. 14. Patent Owner (*id.* at 14–15) cites to disclosure in the Specification that:

> [A] trust service can support the implementation of aliases as representatives of a user identity that uniquely identify a user without providing any addition information about the user's real world identity;

Ex. 1001, 16:48–52;

> A user is provided with a common unique user identifier across federation partners, which enables single-sign-on and the retrieval of attributes (if necessary) about a user as part of the fulfillment of a request at one federation partner;

Id. at 25:66–26:3;

> These accounts may be used independently because a unique user account is based on a unique user identifier; . . . Given that a linked user account is independent of any other user account that the user may have at the service provider, and given that a linked user account requires a unique user identifier to be associated with the linked user account, a linked user account is based on a user identifier that is independent and unique in comparison with any other user identifier that is known to the service provider;

Id. at 32:22–33.

Although these passages are presented in terms of examples or embodiments, the Specification does ascribe importance to uniquely identifying a user through the use of an account or user identifier. Thus, the intrinsic evidence provides support for Patent Owner's proposed construction.

As Patent Owner argues (PO Resp. 15), Petitioner's expert witness, Dr. Crovella testified on cross-examination that an identifier, in the context of the ordinary meaning of identification, must "be[] able to designate a particular user," for example identifying a particular user among ten users. Ex. 2036, 142:13–143:8. Patent Owner also argues that technical dictionaries show that identifiers uniquely identify entities. PO Resp. 15 (citing Ex. 2053 (The Penguin Concise Dictionary of Computing, defining "identifier" as "[a] character string created to uniquely identify some entity used in a program."); Ex. 2054 (Dictionary of Information Security defining

"identification" as "process that enables recognition of an entity by a system, generally by the use of unique machine-readable usernames."); Ex. 2055; Ex. 2056). Thus, extrinsic evidence also supports Patent Owner's proposed construction.

Petitioner responds that "Patentee's construction is irrelevant because Sunada discloses 'information that uniquely identifies the user,' whether that be in the form of a user ID or other information unique to a user." Reply 1. At the oral argument, Petitioner argued that it did not agree or disagree with Patent Owner's proposed construction, but then argued that "if the Board is inclined to construe it, an identifier seems more particular than information," and that "information that uniquely identifies a user does not appear to be the correct construction." Tr. 15:16–16:14. Petitioner, however, did not argue for a different construction in the Petition or Reply, and, even at the oral argument, did not offer a specific alternative to Patent Owner's proposal or evidence in support of an alternative.

As Patent Owner's construction is consistent with the intrinsic and extrinsic evidence, and Petitioner has not meaningfully contested Patent Owner's proposal, we adopt Patent Owner's proposal. "[I]dentifier associated with the user," as recited in claim 1, means "information that uniquely identifies the user."

4. Remaining Terms

Petitioner proposes constructions for "single-sign-on operation," "alias identifier," "user attribute information," "front-channel information retrieval mechanism," "back-channel information retrieval mechanism,"

"identity provider," and "service provider." Pet. 14–15. Based on the record before us, we do not find it necessary to provide express claim constructions for these or any other terms. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (noting that "we need only construe terms 'that are in controversy, and only to the extent necessary to resolve the controversy'") (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

C. Anticipation by/Obviousness over Sunada, alone or in view of Applicant Admitted Prior Art (AAPA)

The Petition argues that Sunada anticipates or renders obvious claims 1, 3, 12, 14, 15, and 18 of the '346 patent, either alone or in view of Applicant Admitted Prior Art (AAPA). Pet. 4, 23–43.

"[A] prior art reference will anticipate if it 'disclose[s] each and every element of the claimed invention . . . arranged or combined in the same way as in the claim.'" *Blue Calypso, LLC v. Groupon, Inc.*, 815 F.3d 1331, 1341 (Fed. Cir. 2016) (quoting *In re Gleave*, 560 F.3d 1331, 1334 (Fed. Cir. 2009) (alteration by Federal Circuit)). "However, a reference can anticipate a claim even if it 'd[oes] not expressly spell out' all the limitations arranged or combined as in the claim, if a person of skill in the art, reading the reference, would 'at once envisage' the claimed arrangement or combination." *Id.* (quoting *Kennametal, Inc. v. Ingersoll Cutting Tool Co.*, 780 F.3d 1376, 1381 (Fed. Cir. 2015) (alteration by Federal Circuit); *In re Petering*, 301 F.2d 676, 681 (CCPA 1962)).

A claim is unpatentable under 35 U.S.C. § 103 "if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains." We resolve the question of obviousness 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. *See Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

Petitioner confirmed at the oral argument that, in light of our construction of "protected resource," it is no longer pursuing its allegations of anticipation and, instead, is proceeding on its grounds of obviousness:

> MR. BRIGGS: . . . So it's our position that Sunada discloses and suggests URLs and that is all that's required for this panel to find Sunada renders obvious the claims in view of the AAPA.
>
> JUDGE McKONE: It wouldn't be good enough for your anticipation ground.
>
> MR. BRIGGS: That's correct, Your Honor. Anticipation, we would have to have an express or an inherent disclosure here. . . .
>
> JUDGE McKONE: And you're no longer contending that Sunada expressly discloses or inherently discloses, correct?
>
> MR. BRIGGS: Correct. We're saying that Sunada discloses URLs in the context of web applications being accessed by users. And when they're doing that, a person of ordinary skill in the art would understand that URLs are commonly used to do that. . . .

> JUDGE McKONE: For streamlining purposes here, it sounds to me like you're conceding that we should rule against you on anticipation, but you're arguing that we should rule in your favor on obviousness. Am I incorrect about that?
>
> MR. BRIGGS: No, you're not incorrect on that, Your Honor.

Tr. 10:19–12:1.

Consistent with Petitioner's concession, we find that Petitioner has not shown that Sunada discloses "protected resources" under our claim construction of the term and, accordingly, Petitioner has not shown, by a preponderance of the evidence, that Sunada anticipates claims 1, 3, 12, 14, 15, and 18.

For the reasons given below, Petitioner has proved by a preponderance of the evidence that claims 1, 3, 12, 14, 15, and 18 would have been obvious over Sunada and AAPA.

1. Level of Skill in the Art

Petitioner, relying on the testimony of Dr. Crovella, contends that a person of ordinary skill in the art "was a person with a B.S. in electrical engineering or computer science or a master's degree in information science," and "should have 2–3 years of experience related to distributed systems and system administration in networked environments." Pet. 12 (citing Ex. 1011 ¶ 30). Patent Owner "applies Petitioner's definition." PO Resp. 11. Thus, the level of skill in the art is not contested. We adopt Petitioner's proposed level of skill.

2. Scope and Content of the Prior Art

a) Overview of Sunada

Sunada describes a single-sign-on (SSO) system through which a user may be authenticated only once in order to access services from different web applications that require separate authentications. Ex. 1005 ¶ 1. Sunada's system includes SSO server 1, web applications 2, 3, clients 5, 6, 7, and network 4, which allows the server, web applications, and clients to communicate with each other. *Id.* ¶ 13, Fig. 1. SSO server 1 authenticates users who log into the system, while the web applications manage user accounts and provide services to registered users. *Id.* ¶¶ 15–16.

If a user logs into the system through the SSO function and subsequently requests access to a service without being a registered user of the web application that provides the service, then the web application creates a registered local account for the user before providing the service to the user. *Id.* ¶ 16. This scenario is shown in Figure 3, which is reproduced below.

[Figure 3]

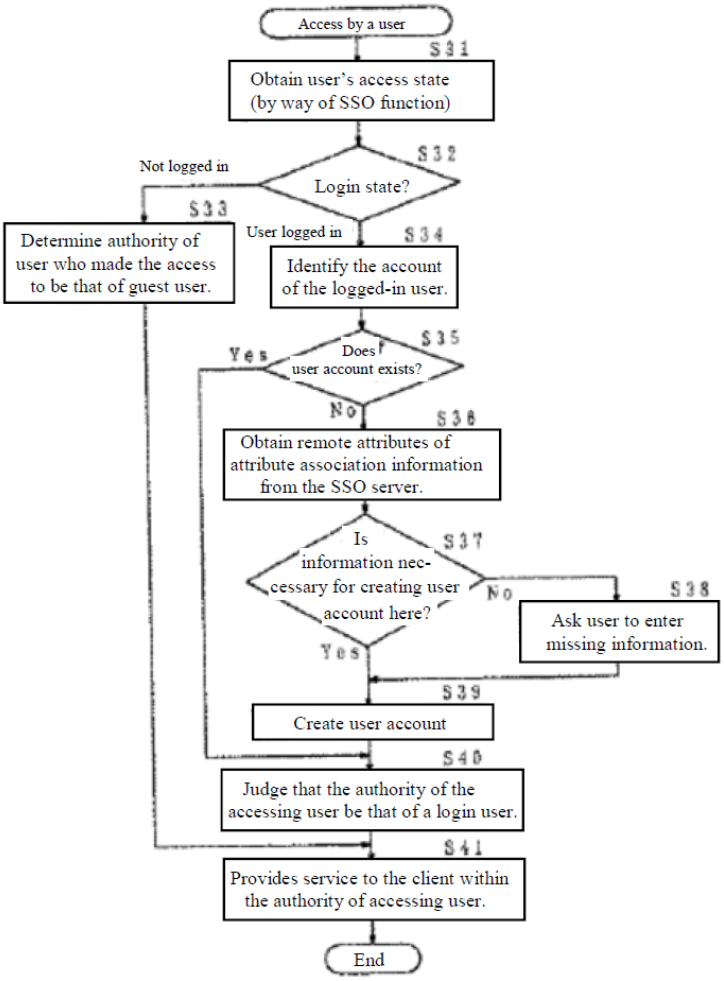


Figure 3 is an operational flowchart for a web application. *Id.* ¶ 26. When a user tries to access a service provided by the web application, the web application determines whether the user has logged into the system. *Id.* ¶ 27, Fig. 3 (S31, S32). Where the user has logged into the system through the SSO function (i.e., the SSO server has authenticated the user), the web application determines whether there is a registered local user account for accessing the web application. *Id.* ¶¶ 28, 30, Fig. 3 (S34, S35). If there is no such account, the web application obtains attribute information

from the SSO server. *Id.* ¶ 31, Fig. 3 (S36). Based on this information, the web application creates a registered local user account. *Id.* ¶ 35, Fig. 3 (S37, S39). The web application then provides the requested service to the user. *Id.* ¶ 36, Fig. 3 (S40, 41).

b) Overview of AAPA

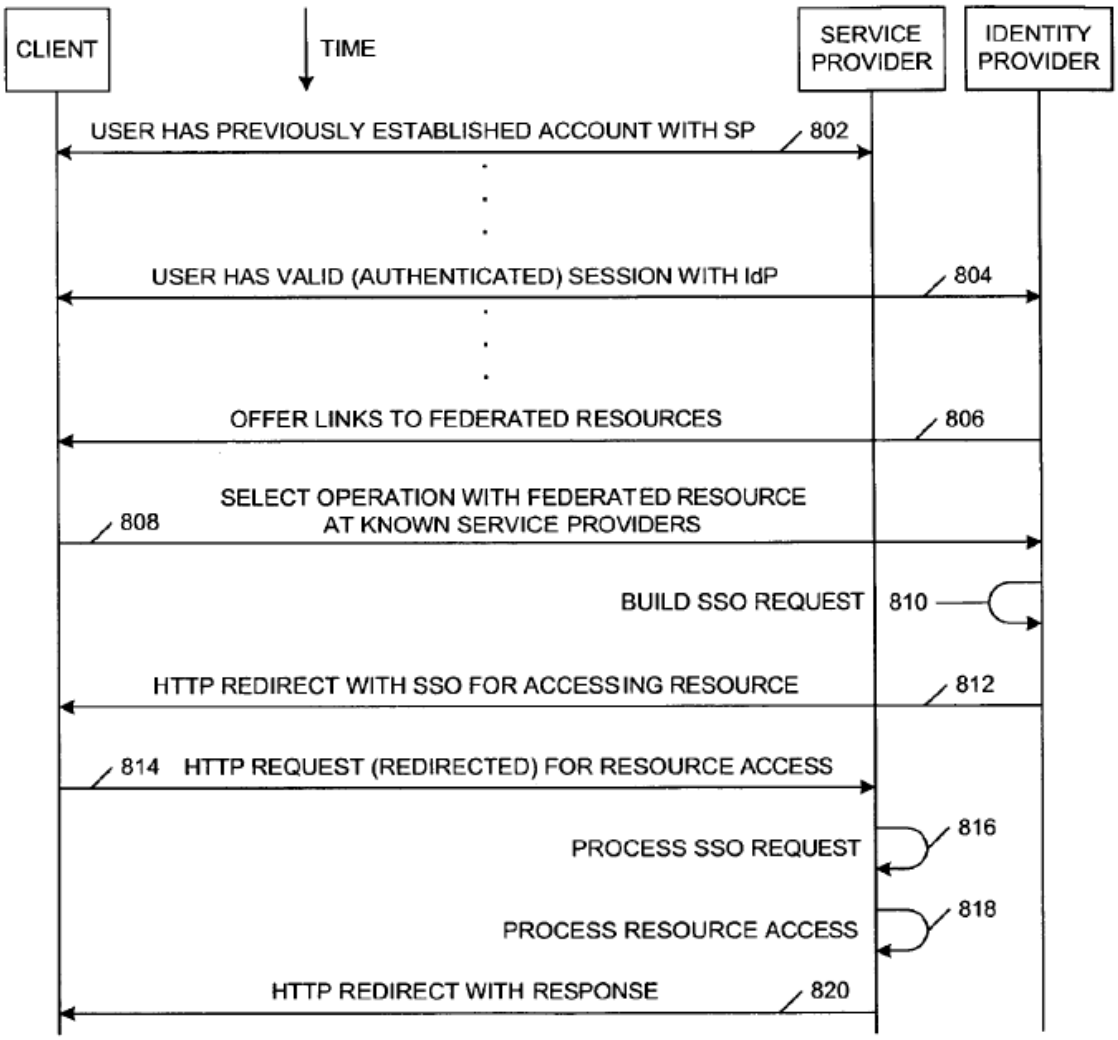
Petitioner relies on statements made in the Background of the Invention section of the Specification as well as the '346 patent's Figures 1A–1E and 8, which are labeled "PRIOR ART." Pet. 19–21. "Admissions are 'permissible evidence in an *inter partes* review for establishing the background knowledge possessed by a person of ordinary skill in the art' and 'provide a factual foundation as to what a skilled artisan would have known at the time of invention.'" Katherine K. Vidal, *Updated Guidance on the Treatment of Statements of the Applicant in the Challenged Patent in Inter Partes Reviews Under § 311* (June 9, 2022)[5], at 3 (quoting *Qualcomm Inc. v. Apple Inc.*, 24 F.4th 1367, 1376 (Fed. Cir. 2022)). "A patentee's admissions regarding the scope and content of the prior art under § 103 can be used, for example, to: (1) supply missing claim limitations that were generally known in the art prior to the invention . . . [or] (2) support a motivation to combine particular disclosures." *Id.* at 4. "Admissions may include statements in the specification of the challenged patent such as 'It is well known that . . . ,' 'It is well understood that . . . ,' or 'One of skill in the

[5] Available at https://www.uspto.gov/sites/default/files/documents/20220609updatedAAPAmemo.pdf.

art would readily understand that . . . ,' or may describe technology as 'prior art,' 'conventional,' or 'well-known.'" *Id.*

According to the Background of the Invention, various SSO techniques have been used to reduce authentication burdens on users and system administrators. Ex. 1001, 1:53–61. Specifically, federated computing spaces had been created to reduce management costs and improve interoperability among enterprises. *Id.* at 1:62–2:1. In an example, a federation partner acts as a user's home domain or identity provider and other partners within the same federation rely on the user's identity provider for primary management of the user's authentication credentials. *Id.* at 2:1–7.

Figure 8 of the '346 patent is reproduced below:



TYPICAL SINGLE-SIGN-ON OPERATION
(INITIATED BY IDENTITY PROVIDER -- USER PREVIOUSLY PROVISIONED AT SP)

FIG. 8
(PRIOR ART)

Figure 8 (labeled "PRIOR ART") is a dataflow diagram of a typical prior art HTTP-redirection-based single-sign-on operation that is initiated by a federated identity provider to obtain access to a protected resource at a federated service provider. *Id.* at 3:52–55; *see also id.* at 28:54–30:30 (providing detailed description of the operation of Figure 8).

3. Unpatentability of Claims 1, 15, and 18

The preamble of claim 1[6] 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 preambles of claims 15 and 18 include substantially similar recitations, except that claim 15 is directed to "[a] computer program product on a computer-readable medium for managing user authentication within a data processing system" and claim 18 is directed to "[a]n apparatus for managing user authentication within a data processing system."

Petitioner identifies Sunada's SSO server 1 as a "first system" and each of Sunada's web applications 2, 3[7] as a "second system," all operating in a networked environment. Pet. 29 (citing Ex. 1005 ¶¶ 8, 9, 13, 14, 24, Fig. 3). Petitioner argues that a web application 2, 3 is configured to create a user account for a user who attempts to log on using SSO server 1 but does

---

[6] The parties do not state expressly whether the preamble of claim 1 is limiting. However, both parties treat the preamble as limiting in their arguments. Pet. 29 ("Petitioner assumes without taking a position that this preamble is limiting."); PO Resp. 36–37. Also, the Board and the Federal Circuit treated the preamble as limiting in the Kayak IPR and its appeal, at least as to the term "federated computing environment." *See* Kayak FWD at 6–8; *IBM v. Iancu*, 759 F. App'x at 1005 ("The Board and the parties agree that both phrases [federated computing environment and single-sign on] are limiting, even though the first appears only in the preamble."). Consistent with these prior decisions, we treat the preamble of claim 1 as limiting.

[7] Petitioner refers to Sunada's web application as an "App Server" throughout the Petition.

not have an account with the web application. *Id.* We find that web applications 2, 3 include computers, which would comprise processors. Ex. 1005 ¶ 16; Pet. 30. Thus, Sunada teaches "[a] method for managing user authentication within a distributed data processing system, wherein a first system and a second system interact . . . and support single-sign-on operations in order to provide access to . . . resources, at least one of the first system and the second system comprising a processor," as recited in claim 1.

Regarding the preamble of claim 15, Petitioner argues that Sunada's SSO operations are performed on networked computers with databases and, thus, teaches that its method is performed by software, a computer program product on a computer readable medium. Pet. 40–41 (citing Ex. 1011 ¶¶ 136–138). We agree. As to the preamble of claim 18, Petitioner argues that Sunada's networked computers are apparatus. *Id.* at 42. Petitioner further argues that a skilled artisan would have understood that a networked computer in Sunada would have included "a processor" and "a computer memory holding computer program instructions, which when executed by the processor, perform" Sunada's method, as recited in claim limitations 18.1 and 18.2. *Id.* (citing Ex. 1005 ¶16; Ex. 1011 ¶¶ 148–154). We agree, and find that Sunada teaches such an apparatus with a processor and memory.

Patent Owner does not dispute these aspects of claims 1, 15, and 18.

Patent Owner argues that Sunada, alone or in light of AAPA, does not teach a federated computing environment or providing access to protected resources. PO Resp. 32–46. We address these aspects of the preambles of claims 1, 15, and 18 below.

a) "federated computing environment"

The preambles of claims 1, 15, and 18 each recite that "a first system and a second system interact within a *federated computing environment*." As discussed above in the "Claim Construction" section, a federated computing environment is a "loosely coupled affiliation of a plurality of distinct 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."

As to anticipation, Petitioner argues that the distinct services described by Sunada (web applications 2, 3) are multiple, distinct enterprises. Pet. 30–31. Patent Owner disputes that Sunada discloses a federated computing environment. PO Resp. 36–40. In reply, Petitioner argues that "Sunada discloses a FCE because it would not make any sense to limit Sunada to a single enterprise situation, especially in view of Sunada's Internet disclosures." Reply 11–12 (citing Pet. 26–27). At the oral argument, Petitioner acknowledged that it is no longer pursuing allegations of anticipation by Sunada. Tr. 10:19–12:1. Thus, we need not determine whether Sunada discloses a federated computing environment.[8]

As to obviousness, Petitioner argues that AAPA describes a federated computing environment and that Figure 8 of the '346 patent, labeled prior art, shows that federated computing environments were well-known and

[8] Our Institution Decision noted potential weaknesses in Petitioner's allegations as to anticipation reflected in the preliminary record. Inst. Dec. 28.

conventional. Pet. 27, 31–33.[9] Specifically, Figure 8 is "a dataflow diagram [that] depicts a *typical* prior art HTTP-redirection-based single-sign-on operation that is initiated by a federated identity provider to obtain access to a protected resource at a federated service provider." Ex. 1001, 28:54–58 (emphasis added). Figure 8 and its accompanying disclosure describe an SSO process to provide access to protected resources in the context of a federated computing environment. *Id.* at 29:25–29. In this example,

> [an] identity provider builds a message for requesting access to the selected federated resource on behalf of the user such that the message also includes a single-sign-on request (step 810), and the identity provider sends the resource request with the single-sign-on request to the client (step 812), e.g., in the form of an HTTP redirect message (HTTP Response message with status/reason code "302"). The redirect message redirects the client to the appropriate location, e.g., as identified by a URI within the "Location" header of the redirect message, that identifies the appropriate service at the service provider that controls access to the requested federated resource.
>
> . . .
>
> In response to receiving the redirect message from the identity provider, the client sends an HTTP Get message to the appropriate service at the service provider as indicated by the URI in the HTTP redirect message from the identity provider (step 814). In this manner, the client accesses the appropriate service at the service provider because the URI in the HTTP

[9] Petitioner also alleges that a federated computing environment would have been obvious over Sunada alone. Pet. 26, 31. Patent Owner disagrees. PO Resp. 40–42, 43–46. Because we find that Sunada and AAPA teach a federated computing environment, we do not reach whether Sunada alone provides such a teaching. Nevertheless, our Institution Decision noted potential weaknesses in Petitioner's allegations as to obviousness over Sunada alone reflected in the preliminary record. Inst. Dec. 28–30.

> Get message still contains the attached information that is required by the service at the service provider.

Id. at 29:38–49, 30:15–22, Fig. 8 (steps 810–814). As AAPA states, "the federation provides a mechanism for trust among those enterprises with respect to certain computational operations for the users within the federation." *Id.* at 1:66–2:1.

Petitioner argues that, in light of AAPA's teachings, skilled artisans would have known that many Internet websites required user registration to access services and that users expected a single login to work for multiple Internet sites. Pet. 26 (citing Ex. 1001, 1:14–52, 7:34–51). AAPA explains the benefits of federated computing environments, e.g., "[t]o reduce the costs of user management and to improve interoperability among enterprises." Ex. 1001, 1:62–64; Pet. 27. Dr. Crovella testifies that "Sunada motivates the combination by explaining benefits of allowing the user to access all services participating in the SSO irrespective of whether the user already has a registered account with various ones of the participating services." Ex. 1011 ¶ 95 (citing Ex. 1005 ¶ 38). Petitioner contends that Patent Owner

> admits Sunada discloses SSO functionality in the context of a single enterprise, and a [person of ordinary skill in the art] would have understood—including from Sunada's own teachings, as noted above—that SSO functionality was a predictable and known prior art technique that would benefit users in the context of a FCE featuring more than one enterprise.

Pet. 28–29.

Dr. Crovella further testifies that a skilled artisan

> would have recognized that Sunada's teachings provided predictable benefits to users and enterprises operating over the Internet—for example, users would have enjoyed the predictable benefit of logging in less often and being hassled for account authentication or creation requirements less frequently through the use of Sunada's SSO functionality. Likewise, enterprises would have predictably benefitted from larger userbases that were known to be trustworthy, as well as increased user participation and satisfaction due to the aforementioned lack of hassle experienced by users.

Ex. 1011 ¶ 102; Pet. 33. Dr. Crovella's testimony on the reasons to combine Sunada's teachings regarding SSO with typical and conventional federated computing environments, which admittedly used SSO, is credible and has rational underpinning. We find that a skilled artisan would have recognized that enterprises would have benefitted from the combination through increased user participation and satisfaction, and that users would have benefited by the convenience of logging in less often. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007) ("[I]f a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill.").

Patent Owner contends that "neither Petitioner nor its expert explains ***how*** a [person of ordinary skill in the art] would have achieved such alleged benefits beyond vague references to 'conventional' or 'corresponding' programming," and that "[m]erely reciting benefits of the proposed combination without sufficient explanations of ***how*** a [person of ordinary skill in the art] would have made the alleged combination is inadequate." PO Resp. 42–43 (citing Pet. 28; Ex. 1011 ¶ 96; *Pers. Web Techs., LLC v.*

Apple, Inc., 848 F.3d 987, 994 (Fed. Cir. 2017)). According to Patent Owner, "providing a service on various servers within the same enterprise is very different from providing a service across enterprises." *Id.* at 43 (citing Ex. 2028 ¶¶ 134–137, 140–141).

We are not persuaded by Patent Owner's argument. To the extent Patent Owner is arguing that Petitioner has not explained sufficiently how it would incorporate the disclosure of AAPA into the system described in Sunada, this is simply an argument that a skilled artisan would not bodily incorporate AAPA into Sunada. However, "[i]t is well-established that a determination of obviousness based on teachings from multiple references does not require an actual, physical substitution of elements." *In re Mouttet*, 686 F.3d 1322, 1332 (Fed. Cir. 2012); *accord MCM Portfolio LLC v. Hewlett-Packard Co.*, 812 F.3d 1284, 1294 (Fed. Cir. 2015) ("[T]he test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference.").

Moreover, Figure 8 of the '346 patent, a detailed flow chart showing conventional communications in a federated computing environment, and its accompanying description provide sufficient detail for a skilled artisan to implement a mechanism for trust among enterprises as it pertains to SSO. Sunada includes steps for implementing SSO similar to those of Figure 8, albeit with no express description of distinct enterprises. *Compare* Ex. 1005, Fig. 3 (steps S31, S32, S34, S35, S40, S41), *with* Ex. 1001, Fig. 8 (steps 802–820). Figure 8 "depicts a *typical* prior art HTTP-redirection-based single-sign-on operation that is initiated by a federated identity provider to obtain access to a protected resource at a federated service

provider." Ex. 1001, 28:54–58 (emphasis added). AAPA's description of SSO and a mechanism for trust within a federated computing environment, including that provided in Figure 8 and its accompanying description, would have been equally applicable to the teachings of Sunada. This improvement would have been no more than "the predictable use of prior art elements according to their established functions." *KSR*, 550 U.S. 398 at 417.

In the Sur-reply, Patent Owner changes its argument to a contention that Petitioner "failed to explain ***why*** a [person of ordinary skill in the art] would have combined Sunada with AAPA and ***how*** a [person of ordinary skill in the art] would have done so." Sur-reply 17. Patent Owner argues that it "is not suggesting that the AAPA as a whole must be physically combinable with Sunada. Instead, [Patent Owner] is pointing out that [Petitioner] failed to meet its burden to explain ***why*** and ***how*** a [person of ordinary skill in the art] would have combined Sunada and AAPA." *Id.* This argument is not persuasive. As explained above, we credit Dr. Crovella's testimony as to why a skilled artisan would have combined Sunada and AAPA, and Figure 8 of AAPA and its corresponding description provide sufficient teaching for how a skilled artisan would have made the combination (assuming Patent Owner's argument is more than a rebuttal of bodily incorporation).

Patent Owner also argues that "Petitioner fails to explain ***why*** a [person of ordinary skill in the art] would have found a single-enterprise SSO system operating over the Internet 'unusual,'" and that Sunada is more akin to the single domain systems described as prior art by the '346 patent. PO Resp. 43–45. Patent Owner further argues that "merely 'duplicating'

Sunada's single enterprise or placing Sunada's single enterprise into a FCE is not enough to render the claims obvious." *Id.* at 45–46. Although included under the PO Response's heading of "Petitioner Fails To Provide Sufficient Reasons For Modifying Sunada or Combining Sunada With AAPA," these arguments appear to be directed only to Petitioner's contention that a federated computing environment would have been obvious over Sunada alone, which we do not reach in this Decision. In any case, these arguments fail to take into account the teachings of AAPA and, thus, are unpersuasive.

As to reasonable expectation of success, Dr. Crovella testifies that "[a]ll that would have been required was conventional programming to implement Sunada's teachings across multiple distinct enterprises." Ex. 1011 ¶ 96. We agree. AAPA, including the detailed flowchart of Figure 8 and its corresponding description, provide detailed steps for communication in a federated computing environment that could be implemented with conventional programming. Patent Owner responds that "neither Petitioner nor its expert explain why a [person of ordinary skill in the art] would have been able to use the same approach to restricting access to resources in both a single-enterprise and multi-enterprise environment," and that "exposing a single enterprise to accesses from multiple enterprises creates security concerns different from a single enterprise environment." PO Resp. 46 (citing Ex. 2028 ¶ 142). This argument is unpersuasive, as the '346 patent admits that the procedure for communicating in a federated computing environment is typical and, therefore, conventional. Ex. 1001, 28:54–30:30, Fig. 8; *see also id.* at 3:12–25 (Figs. 1A–1E illustrate "typical"

networks, data flows, and transaction on which the invention may be implemented).

Accordingly, on the complete record, we find that Sunada and AAPA teach "a first system and a second system interact within a federated computing environment," as recited in claims 1, 15, and 18, and that a skilled artisan would have had reasons, with rational underpinnings, to combine the teachings of Sunada and AAPA, with a reasonable expectation of success.

b) "protected resource"

Petitioner contends that "Sunada discloses that a user may gain access to a protected service on a web application that requires an account by using a SSO function." Pet. 34 (citing Ex. 1005 ¶ 18, Fig. 3 (steps S35–S40); Ex. 1011 ¶ 108). In describing web application 2, Sunada explains:

> the communications control part accepts an access from a client; examines the user account information which is held by the user account information database 23; and judges whether or not to provide the service. For instance, in a case where a user logs in as a local user by way of his/her user account information which is registered in advance, or in a case where a user has received an authentication at the time of utilizations of another service by way of the SSO function and further the user account information exists in the user account information database 12 [sic], the communications control part instructs the processing part 22 to provide the processes.

Ex. 1005 ¶ 18 (alteration in original); *see also id.* ¶ 36 ("S40 judges that the authority of the user attempting to access is that of a login user; and S41 provides a service to the client within the authority of the accessing user. In

other words, in this case, S41 provides a service for the user with the authority of a 'login user.'").

As noted in the Claim Construction section above, "protected resource" means "an application, an object, a document, a page, a file, executable code, or other computational resource, communication-type resource, etc., identified by a Uniform Resource Locator (URL), or more generally, a Uniform Resource Identifier (URI), that can only be accessed by an authenticated and/or authorized user." Patent Owner contends that "Petitioner does not even attempt to apply the agreed-upon construction of protected resources in its analysis of Sunada, in violation of" 37 C.F.R. § 42.104(b)(4). PO Resp. 33.[10]

As we explained in the Institution Decision, Sunada's services are provided by web applications, Ex. 1005 ¶ 18, which suggests that Sunada's services are identified by URLs or URIs. Inst. Dec. 34. We further explained (*id.*) that AAPA shows that it was known to provide access to federated resources at federated web sites using URLs or URIs, and that under Petitioner's proposed combination of Sunada and AAPA, "[t]he

[10] Patent Owner also argues that Sunada "does not mention URLs or URIs at all" and that Petitioner did not present or prove an inherency theory. PO Resp. 33–35 (citing Ex. 2036, 93:12–94:7, 94:10–95:9; Ex. 1028 ¶¶ 97–106); *see also* Sur-reply 16 ("Rakuten's argument is predicated on inherency which cannot be supported even if the use of the URLs were 'conventional' or 'ubiquitous.'"). As noted above, Petitioner concedes that Sunada does not expressly describe URLs or URIs, and no longer contends that Sunada anticipates any claim of the '346 patent. Tr. 10:19–12:1. Nor is Petitioner's obviousness challenge based on inherency. Thus, we need not reach whether Sunada inherently discloses URLs or URIs.

identity provider . . . offers links ***to federated resources*** (806)," and "'the offer may be in the form of hyperlinks to resources ***at federated web sites*** or, more generally, ***federated domains***.'" Pet. 32 (quoting Ex. 1001, 29:25–29[11]); *see also* Ex. 1001, 29:20–30:30, Fig. 8.

Patent Owner contends that "Petitioner relies solely on the theory that Sunada 'discloses' the claimed protected resources," and that we should "limit[] [our] review to the theory that Petitioner presented in the Petition." PO Resp. 35. However, we explained in the Rehearing Decision that "in Petitioner's combination, in a federated computing environment (supplied by AAPA), the SSO server 1 Petitioner identifies in Sunada would offer hyperlinks to services on web applications 2, 3," and that "[s]uch communication using hyperlinks and HTTP redirects implies that the federated resources are identified by URLs or URIs." Reh'g Dec. 7–8 (citing Pet. 32–33, Ex. 1001, Fig. 8). We further explained that "although the Petition did not expressly state that AAPA teaches that federated resources are identified by URLs or URIs, the preliminary record shows that Petitioner's combination of Sunada and AAPA in fact had that feature." *Id.* at 8. We continued, "Petitioner cited AAPA to show that an identity provider offers hyperlinks to federated resources," and that "Petitioner's proposed combination includes federated resources that are identified by URLs or URIs, even if Petitioner did not state expressly in the Petition that

[11] The Petition purports to cite column 30, lines 25–29, of the '346 patent but the material Petitioner reproduces appears at column 29, lines 25–29.

AAPA teaches identifying resources using URLs or URIs." *Id.* at 8–9 (citing Inst. Dec. 34; Pet. 32; Ex. 1001, 30:25–29).

In the Reply, Petitioner argues that "Sunada discloses the combined use of the Internet, servers (e.g., the SSO server) and web applications (App Servers 2, 3) for provision of protected resources using SSO," and that a skilled artisan "would have known that such an arrangement conventionally used URLs." Reply 10–11 (citing Pet. 26–29; Ex. 1005 ¶¶ 13–18; Ex. 1036, 54:19–57:19, 58:22–74:16). Dr. Shamos acknowledges that, prior to the '346 patent, it was conventional to use URLs in Internet communications such as web pages (although, as Patent Owner points out (Sur-reply 16), he would not have considered them conventional for videos). Ex. 1036, 56:19–57:17.

Patent Owner argues that "[a]lthough web pages might have been 'usually' 'transmitted using URLs,' that is irrelevant because Sunada does not disclose that its 'services' are 'web pages.'" Sur-reply 16–17 (quoting Ex. 1036, 57:14–17). We disagree that this is irrelevant. We find that Sunada, by specifically referring to its applications as "web applications," strongly suggests that web pages are among the services it provides. We further find that, in those instances where Sunada's web applications provide access to web pages, it would provide them using admittedly conventional URLs or URIs. Moreover, we find that AAPA expressly describes providing access to resources using URIs. Ex. 1001, 29:25–30:30, Fig. 8.

On the complete record, we find that both Sunada and AAPA teach providing access to protected resources at federated web sites using URLs or URIs.

c) Claim limitations 1.1, 15.1, and 18.3

Claim limitation 1.1 recites "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." Claim limitations 15.1 and 18.3 include the same limitation.

Petitioner directs us to Figure 3 of Sunada, explaining that Sunada's SSO operation begins when the user attempts to access web application 3. Pet. 34 (citing Ex. 1005, Fig. 3). Petitioner argues that Sunada discloses that web application 3 will not provide its services to the user unless the user has a registered local account. *Id.* at 33–34 (citing Ex. 1005 ¶ 16). According to Petitioner, the user gains access to the protected resource on web application 3 that requires an account by using the SSO function. *Id.* at 34 (citing Ex. 1005 ¶ 18, Fig. 3 (steps S35–S40)).

Patent Owner does not contest these allegations (other than to contest whether Sunada's resources are "protected resources," which we address above).

We find that Sunada discloses "triggering a single-sign-on operation," as recited in claims 1, 15, and 18. For example, Sunada discloses that "the communications control part 21 [of web application 2] accepts an access from a client; examines the user account information . . . ; and judges whether or not to provide the service." Ex. 1005 ¶ 18. Sunada further discloses that,

> where a user has received an authentication at the time of utilizations of another service by way of the SSO function, because it is desirable for the user to be able to utilize the service even though the user is one for whom a user registration has not been conducted, his/her user account information is automatically generated and registered.

Id.

d) Claim limitations 1.2, 15.2, and 18.4

Claim limitation 1.2 recites "receiving from the first system at the second system an identifier associated with the user." Claim limitations 15.2 and 18.4 include the same limitation.

Petitioner (Pet. 34–35) directs us to where Sunada discloses that "the communications part 21 [of web application 2] conducts an inquiry of the SSO server 1 and obtains information regarding the user." Ex. 1005 ¶ 19. Petitioner argues that the response from SSO server 1 received by web application 2 includes a "user ID or other identifying information." Pet. 34 (citing Ex. 1005 ¶ 15). Sunada describes the following:

> The SSO server 1 is constituted by including the authentication part 11, the user information database 12, the user information providing part 13, and the like. In the user information database 12, there registered are *authentication information for each of respective users, e.g., information such as the user ID and password*; and *various pieces of information regarding users such as other personal information*. In lieu of the web applications, the authentication part 11 conducts user authentication processes by using information registered in the user information database 12. Moreover, in response to inquiries from the web applications 2 and 3, it conducts sending back user authentication results, and the like. Thereby, it provides SSO functions. In response to inquiries from the web

> applications 2 and 3, the user information providing part 13 conducts provision of the *information regarding users* which is registered in the user information database 12.

Ex. 1005 ¶ 15 (emphases added).[12] Sunada further provides: "In order to automatically generate user account information, the communications control part 21 collects *information regarding the user* for whom the registration is being conducted. For instance, the communications control part conducts an inquiry of the SSO server 1 and obtains *information regarding the user*." *Id.* ¶ 19 (emphases added).[13]

Patent Owner argues that Sunada does not state that the "information regarding the user" obtained by communications control part 21 of web application 2 from SSO Server 1, described in Sunada's paragraph 19, includes the "user ID" discussed in paragraph 15. PO Resp. 23–24. Patent Owner argues that a user's ID at a web application need not be the same as the user's ID at the SSO server, thus, "there is no reason for the web application to receive any user ID or any identifying information from the SSO server." *Id.* at 24 (citing Ex. 2036, 48:14–23).

Patent Owner also argues that Sunada's Figure 3 does not show the web application receiving a user ID from the SSO server. *Id.* at 24–29. Patent Owner argues that the web application receives an access state at step S31 and remote attribute information at step S36, and that neither includes a user ID. *Id.* at 26–27 (citing Ex. 1005 ¶¶ 27, 31). Patent Owner argues, citing to Figures 2(A) and 2 (B) of Sunada, that "the remote attribute

[12] Exhibit 2017 contains corrections to the translation of paragraph 15.
[13] Exhibit 2017 contains corrections to the translation of paragraph 19.

information received from the SSO server is limited to values for local attributes (e.g., attributes X and Y in Figure 2A), and the local attributes do not include, and are distinct from, a user ID (e.g., the User ID in Figure 2A)." *Id.* at 28 (color emphasis omitted). Patent Owner argues that Dr. Crovella admitted that the web application does not necessarily receive a user identifier as part of the attributes obtained from the SSO server in step S36. *Id.* (citing Ex. 2036, 170:18–171:2).

Patent Owner further argues that Sunada "consistently distinguishes the 'information regarding the user' (*i.e.*, attributes) from user IDs." *Id.* at 28. In particular, Patent Owner argues that both paragraphs 15 and 21 of Sunada distinguish between "user IDs" and "information regarding the users." *Id.* at 28–29; *see also* Sur-reply 9 ("[N]owhere does Sunada teach that 'information regarding users'—which is received by a web application—includes a user ID."). According to Patent Owner, of the two, only information regarding the user, which it equates to the "attributes" discussed for step S36 of Figure 3, is received by web application 2. PO Resp. 29 (citing Ex. 2028 ¶ 88). Dr. Shamos repeats this argument in his testimony. Ex. 2028 ¶ 88.

First, we find that Sunada teaches a web application receiving a user ID from the SSO server. For example, Sunada states that user information database 12 includes "authentication information for each of respective users, e.g., information such as the user ID and password." Ex. 1005 ¶ 15.[14] The database can also include "various pieces of information regarding users

[14] Exhibit 2017 provides corrections to the translation of paragraph 15.

such as other personal information." *Id.* When a web application inquires, the SSO server provides "the information regarding users which is registered in the user information database 12." *Id.* Paragraph 15 is clear that "the information regarding users which is registered in the user information database 12" includes "information such as the user ID and password." *Id.* In paragraph 19, Sunada explains, "[i]n order to automatically generate user account information, the communications control part 21 collects information regarding the user for whom the registration is being conducted. For instance, the communications control part conducts an inquiry of the SSO server 1 and obtains information regarding the user." Here, Sunada does not purport to exclude user IDs and passwords from the information regarding the user obtained from the SSO server 1.

Sunada's discussion of Figures 2(A) and 2(B) is not to the contrary. Figures 2(A) and 2(B) of Sunada are reproduced below:

[Figure 2]

(A)

User ID	Attribute X	Attribute Y	...
user-A	nameA	addrA	...
user-B	nameB	addrB	...
...	...	...	...

(B)

Local Attribute	Remote Attribute
X	RX
Y	RY
...	...

Figure 2 is an explanation figure of an example of user account information and attribute association information. *Id.* ¶21.

According to Sunada:

> The user account information, as shown in Figure 2 (A) as an example, associates user IDs identifying users with various pieces of information regarding the users. Here, the figure shows an example in which an attribute X and an attribute Y are associated with user IDs. Respective attributes may include any attribute including personal information such as address and name and a password for conducting authentication. . . .
>
> The attribute association information, as shown in Figure 2 (B) as an example, is the information which associates local attributes which indicate respective attributes of the user account information with remote attributes which indicate attributes of respective pieces of information when information regarding users is externally obtained. This example shows that the information for the attribute X within the user account information is associated with the information for the attribute RX within the externally obtained information related to users.

Id. ¶¶ 21–22. We do not read Sunada as differentiating between user IDs and other information about a user (e.g., name and address), and assigning only the latter to "attributes." When we read it in the context of paragraph 15, which lists user ID and password as examples of authentication information, paragraph 21 suggests that authentication information can be part of such attributes, as paragraph 21 expressly lists "a password for conducting authentication" as an example of an attribute.

Paragraphs 31–33 of Sunada are consistent with a web application receiving the information it requires from the SSO server, including authentication information such as a user ID. According to Sunada:

> In a case where S35 determines that the user account does not exist, S36 inquires of the SSO server 1 for remote attribute information in the attribute association information which is housed in an attribute association database 24, like the one shown in Figure 2 for instance, and obtains the information.

> Here, as for the processes regarding the SSO server 1, no illustration is made; but for an inquiry from the web application 2, the user information providing part 13 of the SSO server 1 searches the user information database 12, extracts the information for which the inquiry has been received, and returns the information to the inquiring web application 2.
>
> Furthermore, rather than inquiring of the SSO server 1 for the remote attribute information as described above, S36 may obtain from the SSO server 1 various pieces of information regarding the user which the SSO server 1 has, and pick and choose the information associated with the remote attributes from the pieces of information.

Id. ¶¶ 31–33. Here, Sunada discloses alternatives of a web application receiving the particular user information it requests of the SSO server or receiving various pieces of information from the SSO server and picking what it needs from that information. As Petitioner observes, "Sunada's FIG. 3 disclosures confirm that *any* appropriate user information may be sent from the SSO to the web applications." Reply 8. Contrary to Patent Owner's arguments (Sur-reply 10–11), Sunada does not distinguish and exclude user IDs from this information.

Patent Owner's inherency arguments (Sur-reply 7–8) are also misplaced. We do not understand Petitioner to argue, nor do we find, that Sunada's web application necessarily receives a user ID in all cases. Rather, we find that Sunada teaches a web application requesting and receiving from the SSO server the information about the user that it needs to create an account, which can, in appropriate circumstances, include authentication information such as a user ID and password for the user. Ex. 1005 ¶¶ 15, 19, 21, 31–33. Sunada teaches that a web application receives from the SSO

server a user identifier that "uniquely identifies the user," and, thus, Sunada teaches "receiving from the first system at the second system an identifier associated with the user," as recited in claim limitations 1.2, 15.2, and 18.4.

As noted above, Petitioner contends that the response from the SSO server to a web application includes "a user identifier such as a user ID *or other identifying information*." Pet. 34 (citing Ex. 1005 ¶ 15) (emphasis added). Petitioner argues that, even if Sunada's SSO server only sends information other than a user ID to web applications, what Patent Owner identifies as "user attribute" information is information that uniquely identifies a user. Reply 5–9. As Petitioner points out (Reply 9), Dr. Shamos admits that "for example, if I have many people with the same name living in an apartment house, the name alone will not uniquely identify them, but it's possible that the name plus the apartment number they live in would identify them." Ex. 1036, 46:5–10; *see also id.* at 49:6–9 ("Q. So, can multiple pieces of information be used to uniquely identify a user? A. Yes, they can."). As noted above, the "various pieces of information regarding users such as other personal information" described in Sunada can include "any attribute including personal information such as address and name and a password for conducting authentication." Ex. 1005 ¶¶ 15, 21. As Dr. Shamos admits, this information could uniquely identify a user and constitute "an identifier associated with the user," under our construction. Ex. 1036, 46:5–10, 49:6–9.

Patent Owner argues that Sunada does not state that its user attributes uniquely identify a user. Sur-reply 12. However, Patent Owner's argument

is unpersuasive because Dr. Shamos admits that such information could uniquely identify a user. Ex. 1036, 46:5–10, 49:6–9.

As to Dr. Shamos's testimony, Patent Owner argues that he testified that Sunada's user attributes cannot show the claimed identifier because "'an identifier is usually a contiguous string of characters,' *i.e.*, 'a single piece of information." Sur-reply 12–13 (quoting Ex. 1036, 48:17–49:12). Patent Owner argues that Dr. Shamos testified that Sunada does not teach concatenating user attributes to transform the attributes into an "identifier." *Id.* at 13 (citing Ex. 1036, 84:17–23). We are not persuaded. As explained above, we adopt Patent Owner's proposed construction of "identifier associated with the user," as recited in claim 1, namely "information that uniquely identifies the user." This construction does not require that the information be packaged or concatenated into a single entity or piece of information.

Patent Owner offers no persuasive evidence or argument that we should further construe "identifier associated with the user" to include a concatenation or single piece requirement. Instead, Dr. Shamos contradicted this construction on cross examination, testifying that, although he "didn't consider" whether the term is "limited to a single piece of information," "an identifier is usually a continuous string of characters." Ex. 1036, 48:17–49:5. This suggests that an identifier need not always be a single piece of information.

Patent Owner argues that claim 5 of the '346 patent separately recites "user attribute information," which, according to Patent Owner, must mean something other than the "identifier associated with the user" recited in

claim 1. Sur-reply 13–14. Whether user attribute information is separate from an identifier associated with the user is beside the point. Petitioner points to information sent by Sunada's SSO server to a web application that Dr. Shamos admits could uniquely identifier a user. Pet. 34–35 (citing Ex. 1005 ¶¶ 15, 19, 21); Reply 9–10 (citing Ex. 1036, 48:17–49:5). Under the construction proposed by Patent Owner (which does not include a single piece requirement) and adopted by us, this information is an "identifier associated with the user," as recited in claim limitations 1.2, 15.2, and 18.4. Thus, even if Sunada only teaches the SSO server transmitting a name and address to a web application, Sunada still teaches claim limitations 1.2, 15.2, and 18.4.

e) Claim limitations 1.3, 15.3, and 18.5

Claim limitation 1.3 recites

> 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.

Claim limitations 15.3 and 18.5 include the same limitation.

Petitioner argues that Sunada discloses that, if user account information does not exist at web application 2 (the second system) after SSO is triggered, web application 2 automatically creates an account for the user with the user ID received from SSO server 1, and the user is given access to the resource only after the account is created. Pet. 35–38 (citing

Ex. 1005 ¶¶ 19, 35–37, Fig. 2, Fig. 3 (steps S35, S36, S39, S41)). According to Petitioner, the account that Sunada discloses creating for the user supports SSO operations between the web application and the SSO server. *Id.* at 37 (citing Ex. 1011 ¶ 118).

For the reasons given for claim limitation 1.2, above, Sunada's web application receives a user ID from the SSO server, e.g., in step S36. Ex. 1005 ¶¶ 15, 19, 21, 31–33. "Upon putting together information necessary for creating the user account in this manner, S39 creates the user account information and registers it with the user account information database 23." *Id.* ¶ 35. Thus, Sunada teaches "creating a user account for the user at the second system based at least in part on the received identifier associated with the user," as recited in claim limitation 1.3. Following this, "S40 judges that the authority of the user attempting to access is that of a login user; and S41 provides a service to the client within the authority of the accessing user. In other words, in this case, S41 provides a service for the user with the authority of a 'login user.'" *Id.* ¶ 36. Thus, the account is created "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," as recited in claim limitation 1.3.

Patent Owner argues that Petitioner relies on the user information attributes referenced in step S36 of Figure 3 of Sunada and that those attributes do not include an identifier associated with the user. PO Resp. 31 (citing Pet. 35–38, 52; Ex. 2028 ¶¶ 92–93). Patent Owner refers to its

argument for claim limitation 1.2, stating that "remote attributes received in step S36 are values for local attributes in Figure 2A and do not include any User ID (e.g., user-A) in Figure 2A." *Id.* Patent Owner argues that Dr. Crovella admitted that it is not necessarily the case that the user ID is part of the information received at the web application from the SSO server in step S36 (instead, it could be received in step S34). *Id.* at 31–32 (citing Ex. 2036, 170:18–171:2). Patent Owner further argues that "the received attributes, such as nameA, cannot show the 'received identifier' because they do not uniquely identify the user." *Id.* at 32 (citing Ex. 2028 ¶¶ 94–95). As explained above, the arguments Patent Owner presents for claim limitation 1.2 (including those directed to inherency) are unpersuasive.

In sum, we find that Sunada teaches claim limitations 1.3, 15.3, and 18.5.

4. Claims 3, 12, and 14

As to claim 3, Sunada discloses that communications control part 21 of web application 2 (the second system) "conducts an inquiry of the SSO server 1 and obtains information regarding the user." Ex. 1005 ¶ 19; Pet. 38; Ex. 1011 ¶¶ 121–123. This results in subsequent account creation at web application 2. Ex. 1005 ¶ 36, Fig. 3 (steps S40, S41); Pet. 38; Ex. 1011 ¶ 124. We find that this teaches "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," as recited in claim 3.

As to claim 12, Sunada's SSO server provides identity information for the reasons given for claim limitation 1.2, above. Sunada's Web applications provide services to a client. Ex. 1005 ¶ 36. Thus, Sunada teaches "wherein the first system supports an identity provider and the second system supports a service provider," as recited in claim 12.

As to claim 14, Petitioner argues that Sunada's Web application sends a request to the user's computer (a fourth system) if it does not have sufficient user attribute information to create a user account, and the Web application receives the information from the user and completes creation of the user's account. Pet. 39–40 (citing Ex. 1005 ¶¶ 30, 34–35, Fig. 3 (steps S34, S37–39); Ex. 1011 ¶¶ 130–131, 133–135). We agree, and find that Sunada teaches the additional limitations of claim 14.

Patent Owner does not argue claims 3, 12, and 14 separately.

5. Objective Indicia of Nonobviousness

Patent Owner argues that a long-felt but unmet need, industry praise, and the commercial success of the invention of the challenged claims evidence nonobviousness. PO Resp. 58–68. For the reasons given below, Patent Owner's evidence is unpersuasive and entitled to little weight.

"[E]vidence of secondary considerations may often be the most probative and cogent evidence in the record." *Stratoflex, Inc. v. Aeroquip Corp.*, 713 F.2d 1530, 1538 (Fed. Cir. 1983). "[T]o be accorded substantial weight in the obviousness analysis, the evidence of secondary considerations must have a 'nexus' to the claims, *i.e.*, there must be 'a legally and factually sufficient connection' between the evidence and the patented invention."

Henny Penny Corp. v. Frymaster LLC, 938 F.3d 1324, 1332 (Fed. Cir. 2019) (quoting *Demaco Corp. v. F. Von Langsdorff Licensing Ltd.*, 851 F.2d 1387, 1392 (Fed. Cir. 1988)). "The patentee bears the burden of showing that a nexus exists." *WMS Gaming Inc. v. Int'l Game Tech.*, 184 F.3d 1339, 1359 (Fed. Cir. 1999). Patent Owner may "prove nexus by showing that the evidence of secondary considerations is the 'direct result of the unique characteristics of the claimed invention.'" *Fox Factory, Inc. v. SRAM, LLC*, 944 F.3d 1366, 1373–74 (Fed. Cir. 2019) (quoting *In re Huang*, 100 F.3d 135, 140 (Fed. Cir. 1996)).

a) Long-felt Need

"Evidence of a long-felt but unresolved need can weigh in favor of the non-obviousness of an invention because it is reasonable to infer the need would not have persisted had the solution been obvious." *Apple Inc. v. Samsung Elecs. Co.*, 839 F.3d 1034, 1056 (Fed. Cir. 2016). "Evidence is particularly probative of obviousness when it demonstrates both that a demand existed for the patented invention, and that others tried but failed to satisfy that demand." *In re Cyclobenzaprine Hydrochloride Extended-Release Capsule Pat. Litig.*, 676 F.3d 1063, 1082 (Fed. Cir. 2012). "[L]ong-felt need is analyzed as of the date of an articulated identified problem and evidence of efforts to solve that problem." *Texas Instruments Inc. v. U.S. Int'l Trade Comm'n*, 988 F.2d 1165, 1178 (Fed. Cir. 1993). "Absent a showing of long-felt need or the failure of others, the mere passage of time without the claimed invention is not evidence of nonobviousness." *Iron Grip Barbell Co. v. USA Sports, Inc.*, 392 F.3d 1317, 1325 (Fed. Cir. 2004).

Patent Owner argues that work it performed for a telecommunications customer evidences a long-felt need for the invention of the '346 patent. PO Resp. 58–60. Specifically, Patent Owner points to a January 8, 2004, requirements design document for the customer for implementing Tivoli Federated Identity Management (TFIM). *Id.* at 59 (citing Ex. 2030, 19, 21, 50). Patent Owner argues that, when the customer approached Patent Owner, each of its mobile content operators (MCOs) was responsible for authenticating its own users and that Patent Owner proposed that the customer adopt a federated SSO solution in which the customer would act as an identity provider to third-party service providers. *Id.* (citing Ex. 2030, 19, 21). According to Patent Owner, the customer "suggested addressing that requirement by providing a user with an option to manually 'create a new account with a federated partner' when the user attempts to access the federated partner at which the user does not have a user account linked to" the customer. *Id.* (quoting Ex. 2030, 50). Patent Owner argues that it "questioned whether asking the user to 'create a new account with a federated partner' was 'really a viable [customer] option,'" and eventually developed an alternative with "an inventive a [sic] runtime provisioning solution that was incorporated into a product called Tivoli Federated Identity Manager, or 'TFIM.'" *Id.* at 59–60 (quoting Ex. 2030, 50; citing Ex. 2070).

Petitioner responds that Patent Owner "offers no evidence that others tried and failed to satisfy a demand for the patented invention," and that "Patentee's evidence suggests a one-year gap (at most) between the identification of an alleged problem and the [April 2005] filing of the '346 patent application." Reply 22.

We agree with Petitioner. Patent Owner's evidence of long-felt need shows, at most, that Patent Owner was in discussions with a customer, roughly a year before the '346 patent was filed, on a feature that might correspond to the claimed invention. There is little evidence to suggest that demand for the invention existed prior to, or even during the discussions with the customer. Nor does Patent Owner's evidence show that artisans articulated a problem and made efforts to solve that problem, but failed. Given a reading most favorable to Patent Owner, this evidence at most shows that Patent Owner suggested implementing for a customer a system corresponding to the invention of the '346 patent and later implemented it. Ex. 2030; Ex. 2070.

Patent Owner argues that "there is no per se rule that one year is not long enough." Sur-reply 25–26. Although there may be no per se rule, the short time period, when considered along with the other deficiencies noted above in Patent Owner's evidence, weighs against finding a long-felt but unmet need for the invention. *Cf. Adapt Pharma Operations Ltd. v. Teva Pharms. USA, Inc.*, 25 F.4th 1354, 1376 (Fed. Cir. 2022) ("At best, the asserted 'long-felt need' here . . . began just three years before the priority date of the patents-in-suit.").

Patent Owner argues that "[b]efore the '346 Patent, businesses—including IBM's own customers—were concerned about the shortcomings of then-existing identity-management systems and asked IBM to develop a solution to address them." PO Resp. 58–59 (citing Ex. 2079, 31, 37, 53, 61; Ex. 2040; Ex. 2041). In support of this argument, Patent Owner cites to what appears to be a 2003 Patent Owner internal document summarizing

discussions with customers (Ex. 2079) and two articles from 2002 and 2003 regarding identity management (Exs. 2040, 2041). Patent Owner does not explain the relevance of these documents and we, upon our review, find none.

In sum, Patent Owner's evidence of long-felt but unmet need is particularly weak and entitled to little weight.

b) Commercial Success and Industry Praise

According to the Federal Circuit,

> Commercial success is relevant because the law presumes an idea would successfully have been brought to market sooner, in response to market forces, had the idea been obvious to persons skilled in the art. Thus, the law deems evidence of (1) commercial success, and (2) some causal relation or "nexus" between an invention and commercial success of a product embodying that invention, probative of whether an invention was non-obvious.

Merck & Co. v. Teva Pharms. USA, Inc., 395 F.3d 1364, 1376 (Fed. Cir. 2005). "To establish a proper nexus between a claimed invention and the commercial success of a product, a patent owner must offer 'proof that the sales were a direct result of the unique characteristics of the claimed invention—as opposed to other economic and commercial factors unrelated to the quality of the patented subject matter.'" *SightSound Techs., LLC v. Apple Inc.*, 809 F.3d 1307, 1319 (Fed. Cir. 2015) (quoting *Huang*, 100 F.3d at 140).

"Evidence that the industry praised a claimed invention or a product that embodies the patent claims weighs against an assertion that the same claimed invention would have been obvious." *Apple*, 839 F.3d at 1053.

Patent Owner contends that "TFIM's account provisioning technique became a huge commercial success shortly after launching in 2005." PO Resp. 66. Patent Owner argues that Exhibit 2070, "Tivoli Access Manager: Federated Identity Management (FIM) System Design Document Level 0," shows that the "TFIM solution is described and claimed in the '346 Patent." *Id.* at 60–66 (citing Ex. 2070, 18, 27, 50, 64, 67, 89, 92, 99, Fig. 1). Patent Owner provides a claim chart mapping citations in Exhibit 2070 to limitations of the challenged claims, arguing that "TFIM embodied every single claim of the '346 Patent." *Id.* at 62–66. Patent Owner argues that "[t]here is a nexus between the '346 Patent claims and TFIM's commercial success and industry praise, given that TFIM implemented each of the '346 Patent claims and was commercially successful and praised for its identity management solution." *Id.* at 66.

Petitioner argues that Patent Owner "offers no testimony (expert or otherwise) that TFIM practices any claim of the '346 patent" and "does not explain how [Exhibit 2070] relates to the actual TFIM product and provides no analysis or explanation as to how the citations read on the claims." Reply 23. Exhibit 2070, on its face, appears to be a preliminary document and purports to be an "Approval Draft." Ex. 2070, 3. The document includes extensive redline edits and comments in the margins.

Petitioner's concerns are well-founded. Patent Owner does not offer any persuasive evidence that the product described in the preliminary

document of Exhibit 2070 corresponds to the product that Patent Owner alleges was commercially successful. Rather, all Patent Owner offers is the conclusory, and unpersuasive, attorney argument that Exhibit 2070's relationship to the TFIM product "is self-evident from EX2070 which is titled 'Federated Identity Management' and states that '[the document] contains high-level design and requirements for the Tivoli Federated Identity Management functionality.'" Sur-reply 24 (citing Ex. 2070, 1, 11) (alteration by Patent Owner). Thus, Patent Owner has not shown persuasive evidence of a nexus between the product alleged to be commercially successful and praised by the industry, and the claimed invention.

Patent Owner appears to point to the same evidence to show both commercial success and industry praise. First, Patent Owner points to its own software announcements (which appear to be akin to press releases) that tout TFIM. PO Resp. 66 (citing Ex. 2033); Sur-reply 24 ("IBM made a special announcement to tout TFIM's real-time provisioning technology, demonstrating that it was TFIM that was driving the industry praise." (citing Ex. 2033)). This appears to have little, if any, relevance to industry praise or commercial success. Patent Owner does not explain persuasively why a self-serving press release evidences commercial success.

Next, Patent Owner cites to a research report by the Burton Group (Ex. 2034, 30) stating that "IBM now claims that over 1,700 customers are licensed to use its IdM suite," and that "IBM is frequently mentioned by competitors as the 'one to beat' for IdM business"; an eWeek website article (Ex. 2091) stating that Patent Owner "is one of the leaders in the identity and access management market in terms of revenue"; and a Network Computing

website article (Ex. 2092) stating that "IDC has ranked IBM as the worldwide revenue share leader in the identity and access management software marketplace." PO Resp. 66. Patent Owner argues that these papers show success and praise "due to the 'strength' of TFIM." *Id.* Patent Owner argues that "TFIM was an integral part of a product suite that was identified as 'one to beat.'" Sur-reply 24 (citing Ex. 2034, 30).

Petitioner responds that Exhibit 2034 notes that TFIM is only one of at least nine Patent Owner product lines, and that Exhibit 2092 attributes Patent Owner's revenue share lead to several product lines, only one of which is TFIM. Reply 23. We agree with Petitioner. Although these papers provide evidence that Patent Owner's business as a whole was praised and commercially successful, Patent Owner's evidence is not sufficient to determine how much, if any, of that success and praise to attribute to TFIM. For example, Exhibit 2034, at 30, does not indicate that TFIM is any more or less important to Patent Owner's success than the eight other products listed. Thus, even if Patent Owner's evidence could establish a nexus between TFIM and the claimed invention, Patent Owner presents only weak evidence to show that TFIM was commercially successful or praised by the industry.

As additional evidence of commercial success, Patent Owner argues that "[t]he '346 Patent itself was widely licensed." PO Resp. 66. Patent Owner identifies several licenses following patent infringement lawsuits involving the '346 patent (Exs. 2047, 2048, 2058, 2080, 2081, 2087); a settlement with a party after Patent Owner notified it of alleged infringement (Exs. 2050, 2051, 2085); and an additional license where a party paid a substantial sum for a license listing the '346 patent at the top of its list of

several patents (Ex. 2052). PO Resp. 67. Patent Owner argues that "[e]ach of these companies have become commercially successful because of the '346 Patent's runtime account creation technology." *Id.* (citing Exs. 2071, 2072, 2073, 2074, 2075, 2086). Patent Owner further argues that a party purchased a license to the '346 patent after a jury verdict of infringement. *Id.* at 67–68 (citing Exs. 2058, 2059, 2060).

Here, as Petitioner observes, each license to which Patent Owner points was taken to resolve pending or threatened litigation. Reply 25. Petitioner further argues that "each license is to Patentee's worldwide patent portfolio, which includes numerous patents and applications." *Id.* Petitioner also argues that Patent Owner does not support its assertion that the licensees implemented the technology of the '346 patent. *Id.*

We agree with Petitioner.

> [Federal Circuit] cases specifically require affirmative evidence of nexus where the evidence of commercial success presented is a license, because it is often "cheaper to take licenses than to defend infringement suits." *EWP Corp. v. Reliance Universal Inc.*, 755 F.2d 898, 908 (Fed. Cir. 1985). Thus we held in *In re GPAC Inc.*, 57 F.3d 1573 [,1580] (Fed. Cir. 1995), that licenses "may constitute evidence of nonobviousness; however, only little weight can be attributed to such evidence if the patentee does not demonstrate a nexus between the merits of the invention and the licenses of record."

Iron Grip Barbell, 392 F.3d at 1324. *See also Merck & Cie v. Gnosis S.P.A.*, 808 F.3d 829, 838 (Fed. Cir. 2015) ("Merck's evidence of licensing is similarly unavailing. Although Merck successfully licensed the '040 patent to Pamlab, the licensing agreement also covered several other patents. . . . It is therefore difficult to determine the extent to which the

licensing agreement was a result of the novel features in the '040 patent, as opposed to the other patents involved. In light of this ambiguity, the Board's finding that the evidence of licensing should not be afforded much weight was reasonable."). Patent Owner's licenses are to its portfolio of patents, and there is no persuasive evidence from which to ascertain the relative value of the '346 patent in the licenses. Even in the case of a license after a jury verdict, the verdict was for infringement of several patents, including the '346 patent. Ex. 2059. Patent Owner's evidence is not sufficient to determine the extent, if any, to which the license was driven by the novel features of the '346 patent. As to whether licensees became commercially successful because of the '346 patent's "runtime account creation technology," PO Resp. 67, Patent Owner's evidence (frequently asked question responses and marketing materials from the licensees) is insufficient to determine whether the licensees practice the invention of the '346 patent. In short, Patent Owner has offered no persuasive evidence of a nexus between the novel features of the '346 patent and the licenses on which it relies.

We have considered Patent Owner's evidence of commercial success (including licensing) and industry praise, and find it particularly weak and entitled to little weight.

6. Conclusion of Obviousness

In sum, as detailed above, Petitioner's proposed combination of Sunada and AAPA teaches each limitation of claims 1, 3, 12, 14, 15, and 18. A skilled artisan would have had reasons, with rational underpinning, to

combine the teachings of Sunada and AAPA. Patent Owner's objective indicia of nonobviousness are unpersuasive and entitled to little weight. Upon consideration of all the evidence, we conclude that Petitioner has proved by a preponderance of the evidence that claims 1, 3, 12, 14, 15, and 18 would have been obvious over Sunada and AAPA.

D. Obviousness Over Sunada and OASIS

Petitioner contends that claims 1–9, 11, 12, and 14–20 would have been obvious over Sunada and OASIS. Pet. 43–65. For the reasons given below, Petitioner has proved by a preponderance of the evidence that claims 1–4, 12, 14–16, 18, and 19 would have been obvious over Sunada and OASIS, but has not proved, by a preponderance of the evidence, that claims 5–9, 11, 17, and 20 would have been obvious over Sunada and OASIS.

1. Scope and Content of the Prior Art – Overview of OASIS

As recognized by the '346 patent, the Organization for the Advancement of Structured Information Standards (OASIS) is a non-profit, global consortium. Ex. 1001, 9:1–3. The OASIS reference is a set of specification documents describing the OASIS Security Assertion Markup Language (SAML). Petitioner contends that a skilled artisan would have read this set of documents collectively, an assertion Patent Owner does not contest. Pet. 22. The Conformance Program Specification supports Petitioner's assertion. Ex. 1015, 6 (stating that Exs. 1013, 1014, 1015, 1016, and 1023 "comprise the Version 1.1 specification set for SAML.").

The Assertions and Protocol document "defines the syntax and semantics for XML-encoded [SAML] assertions, protocol requests, and protocol responses." Ex. 1013, 6. According to this document, "[SAML] is an XML-based framework for exchanging security information. This security information is expressed in the form of assertions about subjects, where a subject is an entity (either human or computer) that has an identity in some security domain." *Id.* at 8. "SAML defines a protocol by which clients can request assertions from SAML authorities and get a response from them." *Id.* Figure 1 of the Assertions and Protocol document (*id.* at 9) is reproduced below:

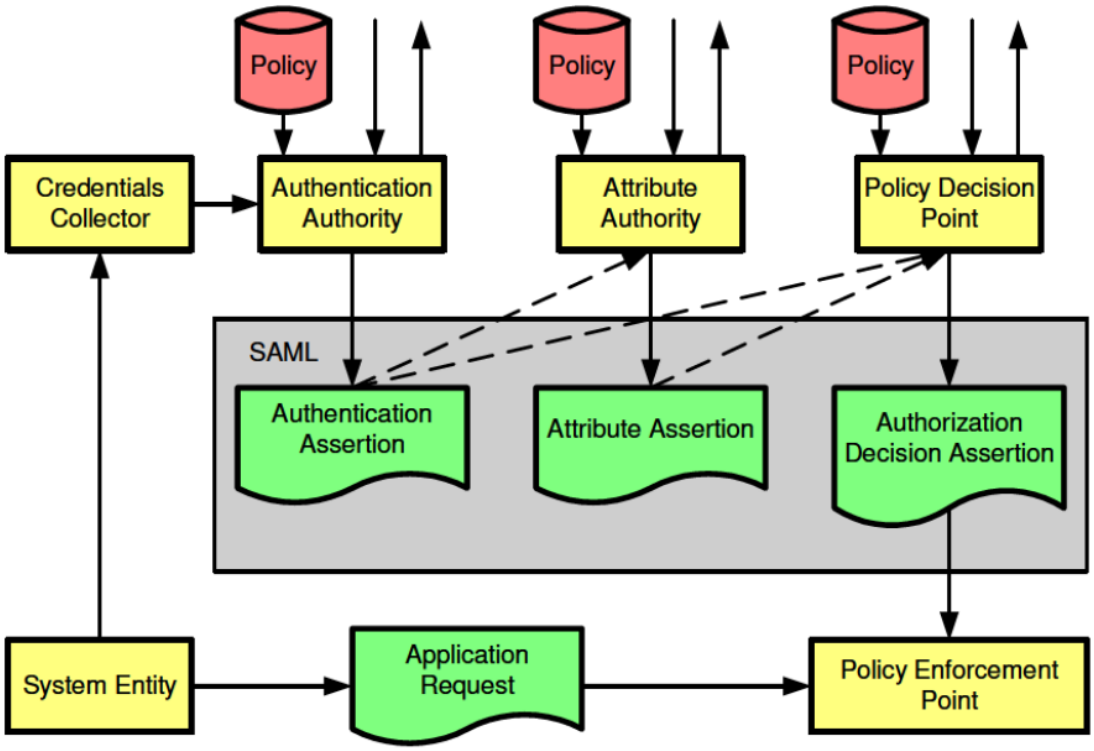
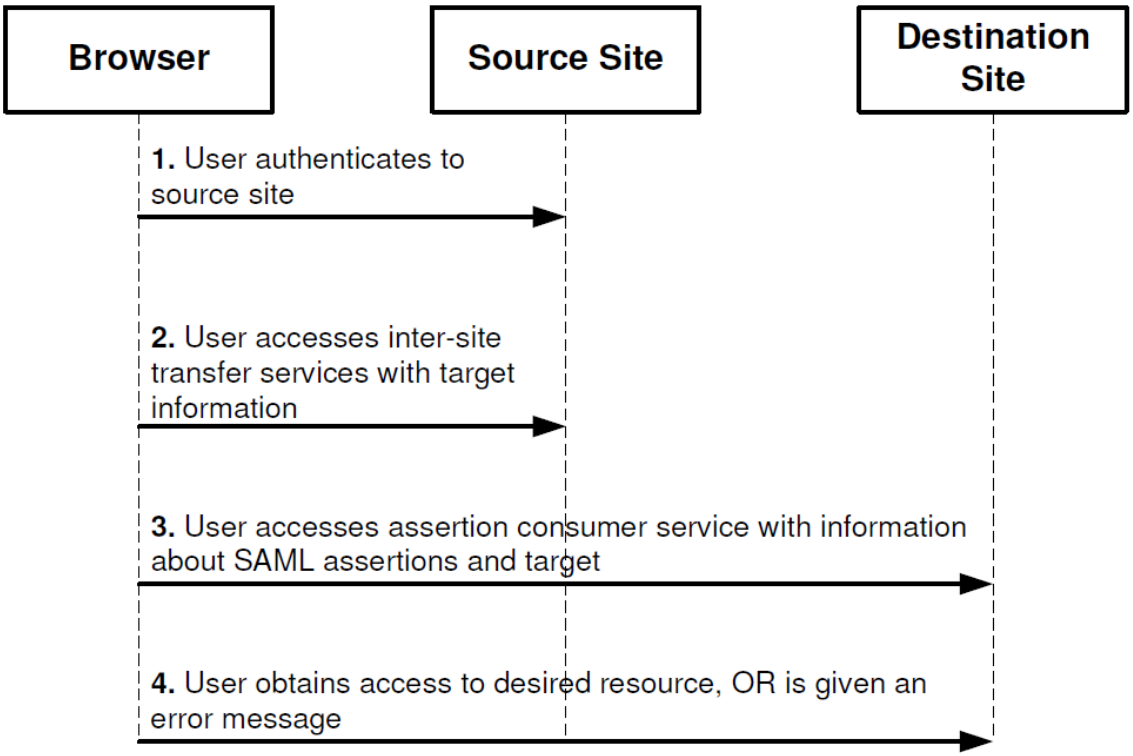


Figure 1 The SAML Domain Model

Figure 1 is a block diagram of the SAML Domain Model. Here, "SAML authorities can use various sources of information, such as external

policy stores and assertions that were received as input in requests, in creating their responses." *Id.* at 8. According to the document, "[o]ne major design goal for SAML is Single Sign-On (SSO), the ability of a user to authenticate in one domain and use resources in other domains without re-authenticating." *Id.* at 9.

The Bindings and Profiles document "specifies protocol bindings and profiles for the use of SAML assertions and request response messages in communications protocols and frameworks." Ex. 1014, 5. One example is in the context of web browser SSO profiles of SAML. *Id.* at 12–13. "In the scenario supported by the web browser SSO profiles, a web user authenticates to a *source site*. The web user then uses a secured resource at a destination site, without directly authenticating to the *destination site*." *Id.* at 12. A figure at page 13 of the document is reproduced below:



The above figure is an illustration of a basic template for achieving SSO. According to the document,

> At some point, the user attempts to access a *target* resource available from the destination site, and subsequently, through one or more steps (for example, redirection), arrives at an *inter-site transfer service* (which may be associated with one or more URIs) at the source site. Starting from this point, the web browser SSO profiles describe a canonical sequence of HTTP exchanges that transfer the user browser to an *assertion consumer service* at the destination site. Information about the SAML assertions provided by the source site and associated with the user, and the desired target, is conveyed from the source to the destination site by the protocol exchange.
>
> The assertion consumer service at the destination site can examine both the assertions and the target information and determine whether to allow access to the target resource, thereby achieving web SSO for authenticated users originating from a source site.

Id. at 12.

The Security and Privacy Considerations document "describes and analyzes the security and privacy properties of the OASIS [SAML] defined in the core SAML specification . . . and the SAML specification for bindings and profiles." Ex. 1016, 4. The Glossary document "defines terms used throughout the OASIS [SAML] specifications and related documents." Ex. 1023, 4.

Dr. Crovella testifies that "[t]he SAML standard . . . was the predominant industry standard for implementing cross-domain SSO." Ex. 1003 ¶ 82 (citing Ex. 1013, 8–9; Ex. 1001, 8:65–9:49).

2. Claims 1, 15, and 18

Petitioner argues that Sunada teaches most aspects of claims 1, 15, and 18, including the "triggering," "receiving," and "creating" limitations and aspects of the preamble other than a federated computing environment. Pet. 51–52. As explained above, we find that Sunada teaches these aspects of claims 1, 15, and 18.

The parties dispute whether Sunada and OASIS teach a federated computing environment and protected resources. Pet. 43–52; PO Resp. 35, 46–50.

a) Federated computing environment

Petitioner contends that OASIS teaches a federated computing environment "wherein different 'Source' and 'Destination' sites are part of separate domains (enterprises) and cooperate in a loosely affiliated fashion to achieve SSO functionality." Pet. 51 (citing Ex. 1013, 9; Ex. 1014, 12–13; Ex. 1023, 3, 8; Ex. 1016, 5, 8, 20; Ex. 1011 ¶¶ 161–171). Petitioner contends that Patent Owner has admitted to the Federal Circuit (in its reply brief in appealing the Kayak FWD) that separate "domains" are separate "enterprises." *Id.* at 45 (citing Ex. 1019, 1–2), 51 (same). Patent Owner does not contest that "domains" are "enterprises." Petitioner argues that the "basic template" shown in OASIS for achieving SSO is an example of a loosely coupled affiliation of different enterprises, with different domain name servers, that adhere to certain standards of interoperability. *Id.* at 45–47 (citing Ex. 1014, 12–13; Ex. 1023, 4; Ex. 1011 ¶¶ 163–166). Petitioner further contends that the "trust policies" of OASIS are trust mechanisms

implemented between enterprises. *Id.* at 47–48 (citing Ex. 1016, 5, 8, 20; Ex. 1011 ¶¶ 169–170). Petitioner argues that it would have been obvious to combine the teachings of Sunada and OASIS to provide SSO functionality in a federated computing environment. *Id.* at 43.

Petitioner contends that Sunada discloses SSO but does not describe conventional communications protocols for facilitating its SSO functionality. *Id.* at 44. Petitioner argues that the SAML standard described in OASIS is a conventional communication protocol, used in business-to-business scenarios, that would have facilitated Sunada's SSO functionality. *Id.* (citing Ex. 1011 ¶¶ 158–160). According to Petitioner, "OASIS teaches a [person of ordinary skill in the art] how to provide SSO functionality in a [federated computing environment] because OASIS defines how distinct enterprises 'adhere to certain standards of interoperability' for SSO." *Id.* at 47 (citing Ex. 1011 ¶¶ 167–168). Petitioner argues that OASIS provides "practical implementation details" that would have been useful in implementing Sunada's SSO functionality in a federated computing environment and would have provided "a well-documented and standardized system to which the enterprises could adhere," without wasting time, effort, and resources creating a new standard. *Id.* at 49–50 (citing Ex. 1011 ¶¶ 173–175).

Petitioner further argues that providing SSO functionality for a federated computing environment would have improved users' experiences and avoided the hassle associated with requiring individual authentications for each service a user wanted to access. *Id.* at 49 (citing Ex. 1011 ¶ 172 (a skilled artisan "would have done so to provide users with the convenience of

only needing to log in to one service in order to have access to a multitude of services that provide otherwise-protected resources, without the hassle of having to login multiple times or sign up for accounts for numerous services")). Patent Owner argues that "such conclusory references cannot demonstrate sufficient motivation to combine Sunada and OASIS." PO Resp. 50 (citing Ex. 2028 ¶ 152). We agree with Petitioner and credit Dr. Crovella's testimony that the combination would have provided "the convenience of only needing to log in to one service in order to have access to a multitude of services that provide otherwise-protected resources, without the hassle of having to login multiple times or sign up for accounts for numerous services." Ex. 1011 ¶ 172.

Petitioner argues that a skilled artisan would have had a reasonable expectation of success because the OASIS SAML standard "was the predominant standard for implementing SSO functionality" and it would have been routine and conventional to implement Sunada's SSO functionality across multiple distinct enterprises using this standard and conventional computer programming. Pet. 50–51 (citing Ex. 1015, 13–17; Ex. 1013, 6; Ex. 1014, 13; Ex. 1011 ¶¶ 176–177). According to Petitioner, the predictable result of this combination would have been

> SSO functionality pursuant to which a user could log in to a first enterprise service, then have access to a second enterprise even if the user did not have an account with the second enterprise, because the user's successful authentication at the first enterprise login would serve as sufficient authentication to allow access to the services of the second distinct enterprise.

Id. at 50. We find that employing the well-known standard protocols of OASIS for facilitating SSO would improve Sunada, a similar system, in the

same way. *See KSR*, 550 U.S. at 417 ("[I]f a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill."). We find that Petitioner's reasons to combine the teachings of Sunada and OASIS have rational underpinning and Petitioner's evidence supports a reasonable likelihood of success.

Patent Owner first argues that "[t]o the extent Petitioner incorporates by reference the arguments from Ground 1 and the AAPA, they fail for the same reasons as described above." PO Resp. 47. Patent Owner's argument is unpersuasive, however, because Patent Owner does not identify any specific argument of Petitioner's that it alleges should fail.

Patent Owner next argues that "Petitioner fails to show that OASIS teaches 'a mechanism for trust among those enterprises' as required by the construction of FCE because OASIS explicitly states that a 'trust model' is beyond the scope of OASIS." *Id.* As explained above, in our construction of "federated computing environment," "the federation provides a mechanism for trust among those enterprises with respect to certain computational operations for the users within the federation."

Patent Owner argues that OASIS expressly states that it does not teach a trust model. *Id.* OASIS identifies "issues [that] are important, but currently beyond the scope of SAML," including

> Trust Model: In many cases, the security of a SAML conversation will depend on the underlying trust model, which is typically based on a key management infrastructure (for example, PKI or secret key). For example, SOAP messages

> secured by means of XML Signature [XMLSig] are secured only insofar as the keys used in the exchange can be trusted. Undetected compromised keys or revoked certificates, for example, could allow a breach of security. Even failure to require a certificate opens the door for impersonation attacks. PKI setup is not trivial and must be implemented correctly in order for layers built on top of it (such as parts of SAML) to be secure.

Ex. 1016, 8. Patent Owner argues that "[t]he trust model and trust policies are merely aspirational features of an OASIS system." PO Resp. 48. According to Patent Owner, "[a person of ordinary skill in the art] would not have understood how such aspirational features would have been integrated into the combination of Sunada and OASIS espoused by Petitioner." *Id.* at 49.

Patent Owner further argues that the trust policies identified in OASIS (e.g., PKI or secret key) are not mechanisms of trust for facilitating SSO because "[p]roviding secure communication has no bearing on a mechanism of trust for SSO purposes." *Id.* at 49–50 (citing Ex. 2028 ¶ 151). Here, Patent Owner appears to construe "a mechanism of trust" as "[b]usiness agreements that specify contractual obligations and liabilities with respect to the trust relationships." *Id.* (quoting Ex. 1001, 21:38–40); *see also* Sur-reply 19 ("But 'secure communication' does not disclose a 'mechanism of trust' because it 'has no bearing on a mechanism of trust that is used for SSO purposes, such as business agreements that specify contractual obligations and liabilities with respect to the trust relationships.' . . . [Petitioner] fails to show that the 'agreements' between administrative domains implement a mechanism of trust because nothing in the record suggests that OASIS's

agreements 'specify contractual obligations and liabilities with respect to the trust relationships.'" (quoting Ex. 2028 ¶ 151; Ex. 1001, 21:38–42)).

According to the '346 patent,

> Business agreements that specify contractual obligations and liabilities with respect to the trust relationships between federated enterprises can be expressed in XML through the use of the ebXML (Electronic Business using XML) standards. For example, a direct trust relationship could be represented in an ebXML document; each federated domain that shares a direct trust relationship would have a copy of a contract that is expressed as an ebXML document.

Ex. 1001, 21:38–45. Here, contractual obligations and liabilities might be related to trust relationships, but they are not described as mechanisms. Rather, ebXML arguably could be the mechanism in this example. Neither Patent Owner nor Dr. Shamos, however, explains why business agreement and contractual obligations and liabilities are requirements of "mechanisms" of trust. PO Resp. 49–50; Sur-reply 18–19; Ex. 2028 ¶ 151.

Petitioner argues that the '346 patent describes reliance on authentication of authentication credentials by a user's home domain or identity provider as a trust mechanism. Reply 14 (citing Ex. 1001, 2:1–7, 11:8–14, 11:42–12:48)). According to Petitioner, the '346 patent describes "Public Key Infrastructure (PKI) certificates" as an example mechanism of trust. *Id.* at 14–15 (citing Ex. 1001, 9:61–10:7).

We agree with Petitioner. The Specification states that:

> A federation is 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. For example, a federation

> partner may act as a user's home domain or identity provider. Other partners within the same federation may rely on the user's identity provider for primary management of the user's authentication credentials, e.g., accepting a single-sign-on token that is provided by the user's identity provider.

Ex. 1001, 1:64–2:7. Here, a federated partner relying on another partner's authentication of credentials is a mechanism of trust related to the computational operations of authentication.

In one example,

> The relying entity is an entity that receives an assertion from an issuing entity. The relying party is able to accept, trust, and understand an assertion that is issued by a third party on behalf of the user, i.e. the issuing entity; it is generally the relying entity's duty to use an appropriate authentication authority to interpret an authentication assertion. A relying party is an entity that relies on an assertion that is presented on behalf of a user or another entity. In this manner, a user can be given a single-sign-on experience at the relying entity instead of requiring the relying entity to prompt the user for the user's authentication credentials as part of an interactive session with the user.

Id. at 12:12–23. Here, a relying party trusts an assertion when it uses an appropriate authentication authority. According to the Specification,

> An authentication credential is a set of challenge/response information that is used in various authentication protocols. For example, a username and password combination is the most familiar form of authentication credentials. Other forms of authentication credential may include various forms of challenge/response information, Public Key Infrastructure (PKI) certificates, smartcards, biometrics, etc.

Id. at 9:61–67. Here, PKI certifications is one example of an authentication protocol to establish trust. Thus, we agree with Petitioner that "reliance on

authentication by a user's home domain or identity provider is a 'trust mechanism.'" Reply 14.

Like the examples in the '346 patent, entities in different domains in OASIS communicate authentication information via assertions. Ex. 1013, 8–9, 11; Ex. 1014, 13; Ex. 1016, 5; Ex. 1023, 5. As Petitioner argues, OASIS describes that "[a]ssertions can convey information about authentication acts that were previously performed by subjects, attributes of subjects, and authorization decisions about whether subjects are allowed to access certain resources." Ex. 1013, 8; Reply 15. Although not required by the SAML specification,

> In many cases, the security of a SAML conversation will depend on the underlying trust model, which is typically based on a key management infrastructure (for example, PKI or secret key). For example, SOAP messages secured by means of XML Signature **[XMLSig]** are secured only 246 insofar as the keys used in the exchange can be trusted. Undetected compromised keys or revoked certificates, for example, could allow a breach of security. Even failure to require a certificate opens the door for impersonation attacks. PKI setup is not trivial and must be implemented correctly in order for layers built on top of it (such as parts of SAML) to be secure.

Ex. 1016, 8. Here, OASIS contemplates (but does not require) communicating authentication credentials using the same mechanism, encrypted assertions, as described in the '346 patent. *Compare with* Ex. 1001, 9:61–67.

Patent Owner's arguments that "[t]he trust model and trust policies are merely aspirational features of an OASIS system," and that "[t]he aspirational trust features are not even part of the OASIS standard," PO

Resp. 48, are not persuasive. OASIS states that a "Trust Model" is "explicitly outside the scope of SAML." Ex. 1016, 8. We do not interpret this statement to mean that SAML-based systems do not have trust models, or that trust models are merely aspirational features not contemplated by OASIS. Rather, OASIS does not specify or require a particular trust model, leaving that decision to the system designer, although suggesting the same PKI or secret key trust model identified in the '346 patent. *Id.* Indeed, as Petitioner observes (Reply 16–17), OASIS identifies a trust model as an issue that is "important." Ex. 1016, 8.

Moreover, even if we were to agree with Patent Owner that mechanisms of trust are business agreements and contractual obligations and liabilities between parties, OASIS teaches that such policies should always be used. According to OASIS,

> When determining what issuers to trust, particularly in cases where the assertions will be used as inputs to authentication or authorization decisions, the risk of security compromises arising from the consumption of false but validly issued assertions is a large one. *Trust policies between asserting and relying parties should always be written to include significant consideration of liability* and implementations must be provide an audit trail.

Id. at 9 (emphasis added); *see also* Ex. 1023, 4 ("Administrative domains may interact and enter into agreements for providing and/or consuming services across administrative domain boundaries."). Here, OASIS does not require any particular trust policy or business agreement. However, the '346 patent does not specify any particular policy that would be required and, instead, refers generally to "[b]usiness agreements that specify contractual

obligations and liabilities with respect to the trust relationships between federated enterprises." Ex. 1001, 21:38–39.

Accordingly, on the complete record, we find that Sunada and OASIS teach "a federated computing environment," as recited in claims 1, 15, and 18.

b) Protected resources

As explained above, Sunada teaches providing access to protected resources. OASIS also teaches providing access to protected resources.

In Petitioner's combination, OASIS supplies "practical implementation details that would be useful when implementing Sunada's SSO functionality," Pet. 49, including "conventional communication protocols for facilitating . . . SSO functionality," *id.* at 44. According to Petitioner, "OASIS . . . describes how to facilitate Sunada's Internet-based SSO functionality through the use of a browser and HTTP to exchange user attribute information." *Id.* at 49 (citing Ex. 1014, 13; Ex. 1005 ¶¶ 13, 30–31, 34; Ex. 1011 ¶ 174). As explained in the Institution Decision (Inst. Dec. 42), OASIS describes assertions in the form of HTML exchanges in which the services described in OASIS are identified by URIs. Ex. 1014, 12–13; Ex. 1013, 8–10. Petitioner relies, in particular, upon OASIS's HTTP exchanges, including the use of URIs, to use a secured resource at a destination site without authenticating to the destination site directly. Pet. 47 (citing Ex. 1014, 12; Ex. 1011 ¶¶ 167–168). Thus, in Petitioner's combination of Sunada and OASIS, resources are identified by URIs.

Patent Owner argues that we "instituted the IPR trial based on findings that Sunada '***suggests*** that Sunada's services are identified by URLs or URIs'. . . , and 'in a ***combination of Sunada and OASIS***, protected resources would have been identified by URIs or URLs.'" PO Resp. 35 (citing Inst. Dec. 34, 42). Patent Owner contends that "Petitioner relies solely on the theory that Sunada 'discloses' the claimed protected resources," and that we should "limit[] [our] review to the theory that Petitioner presented in the Petition." PO Resp. 35. However, we explained in the Rehearing Decision that, in Petitioner's combination, with implementation details supplied by OASIS, the SSO server 1 Petitioner identifies in Sunada would offer URIs to services on web applications 2, 3. Reh'g Dec. 10 (citing Pet. 43–52). As we further explained, "[w]hen we consider the specific mapping Petitioner provided in its ground based on Sunada and OASIS, at least on the preliminary record, it is clear that Sunada and OASIS teach protected resources." *Id.* at 11.

On the complete record, we find that, in Petitioner's proposed combination of Sunada and OASIS, protected resources would have been identified by URIs or URLs. Inst. Dec. 42.

3. Claims 2–4, 12, 14, 16, and 19

Claim 2 depends from claim 1 and recites "creating an alias identifier for the user at the first system after triggering the single-sign-on operation." Petitioner contends that this limitation is taught by OASIS's descriptions of <NameIdentifier> elements, one-time-use identifiers, and one-time-use pseudonyms. Pet. 52–53 (citing Ex. 1013, 17–18; Ex. 1014, 13, 16;

Ex. 1016, 6–17; Ex. 1011 ¶¶ 184–185). We agree, and find that OASIS teaches the additional limitation of claim 2.

Claim 16 depends from claim 15 and claim 19 depends from claim 18. Both add limitations substantially similar to those of claim 2. Petitioner contends that claims 16 and 19 are taught by Sunada and OASIS for the reasons given for claim 2. Pet. 64–65. For the reasons given for claim 2, we find that OASIS teaches the additional limitations of claims 16 and 19.

Petitioner contends that claims 3, 12, and 14 are taught by Sunada for the reasons given in its ground based on Sunada alone or in light of AAPA. Pet. 53, 64. For the reasons given above, we find that Sunada teaches the additional limitations of claims 3, 12, and 14.

Claim 4 depends from claim 1 and recites "receiving a message from the first system at the second system to push 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." Petitioner contends that OASIS describes that an entity may "provide information to a system entity that did not actively request it" (Ex. 1023, 7), including authentication information (Ex. 1014, 20–22) and that this is an example of pushing authentication information from a first system to the second system. Pet. 54 (citing Ex. 1011 ¶ 191). We agree, and find that OASIS teaches the additional limitation of claim 4.

Patent Owner does not argue claims 2–4, 12, 14, 16, and 19 separately.

4. Claims 5–9, 11, 17, and 20

Claim 5 depends from claim 1 and claim limitation 5.0 recites:

> in response to a determination at the second system that the second system does not have sufficient user attribute information to complete creation of a user account for the user at the second system, sending a request message from the second system to the first system to retrieve user attribute information.

Petitioner contends that this is taught by Sunada, at paragraphs 30–31. Pet. 55. Here, Sunada states:

> Moreover, in a case where the user's access state is the login state, S34 searches the user account information database 23 and identifies the account of the user who has logged in. And S35 *determines whether or not the user account exists*. Even if the user's access state is the login state, in a case, for instance, where the SSO server 1 has conducted an authentication by way of the SSO function, the account of the user attempting to access does not necessarily exist. Accordingly, this *S35 judges whether or not user account information exists*; and *in a case where the user account does not exist*, S36 through S39 automatically create a user account anew. In a case where the user account already exists, it is not necessary to create a user account anew and hence, the operations proceed to S40.
>
> In a case *where S35 determines that the user account does not exist, S36 inquires of the SSO server 1 for remote attribute information* in the attribute association information which is housed in an attribute association database 24, like the one shown in Figure 2 for instance, and obtains the information.

Ex. 1005 ¶¶ 30–31 (emphases added).

Patent Owner argues that determining that a user account does not exist is not the same as, and does not teach, determining that the web application does not have sufficient user attribute information to complete

creation of a user account. PO Resp. 51. According to Patent Owner, "[i]n Sunada, the web application sends a request message for user attribute information ***regardless of*** whether the web application needs more user attributes to complete creation of a user account." *Id.* Thus, Patent Owner argues, "Sunada's web application requests attributes when a user account does not exist, not 'in response to a determination' that the web application 'does not have sufficient user attribute information to complete creation of a user account.'" *Id.*

Petitioner's Reply does not appear to address this argument, instead mischaracterizing Patent Owner's argument as an argument that "the 'determining' step of claim 5 must be completed separate from the 'creating' step of claim 1." Reply 17. Petitioner then points to disclosure in Sunada of web applications requesting and obtaining information from the SSO server, but without explaining why those examples are in response to a determination that the web application does not have sufficient user attribute information to complete creation of a user account. *Id.* at 18 (citing Ex. 1005 ¶¶ 18, 19, 30, 31).

We agree with Patent Owner. Sunada teaches that a web application requests information from the SSO server in response to a determination that a user account does not exist, not in response to a determination that the web application does not have sufficient user attribute information to create a user account. Ex. 1005 ¶¶ 30–31. Petitioner does not explain why a determination that a user account does not exist equates to a determination that the web application lacks sufficient information to create a user account. As Patent Owner observes, it is possible that Sunada's web application could

have sufficient information to create the user account but nevertheless request information from the SSO server because the Web application determines that the SSO server does not exist. PO Resp. 51. Thus, Petitioner has not shown that Sunada teaches claim limitation 5.0.

Petitioner further argues that "OASIS also discloses using multiple queries, including via <AuthenticationQuery> and <AttributeQuery> requests that may be used by the destination site *to request* ***additional*** *user attribute or authentication information*, which further confirms that OASIS discloses this limitation." Pet. 56 (citing Ex. 1013, 28–31); *see also* Reply 18. Here, as Patent Owner argues (PO Resp. 51–52), Petitioner points to queries for additional information, but does not explain why these queries are "in response to a determination at the second system that the second system does not have sufficient user attribute information to complete creation of a user account for the user at the second system." Thus, even if OASIS is combined with Sunada, Petitioner has not shown that OASIS cures the deficiency we find above with Sunada.

In sum, we find that Sunada and OASIS do not teach claim limitation 5.0 and, accordingly, Petitioner has not shown that Sunada and OASIS teach the additional limitations of claim 5.

Claims 6–9 and 11 depend, directly or indirectly, from claim 5. Petitioner's arguments and evidence for claims 6–9 and 11 (Pet. 57–63) do not cure the above-noted deficiencies in Petitioner's showing for claim 5. Accordingly, Petitioner has not shown that Sunada and OASIS teach claims 6–9 and 11.

Claim 17 depends from claim 15 and claim 20 depends from claim 18. Both add limitations substantially similar to those recited in claim 5. For example, claim 17 recites

> sending a request message from the second system to the first system to retrieve user attribute information in response to a determination at the second system that the second system does not have sufficient user attribute information to complete creation of a user account for the user at the second system,

which is substantially similar to claim limitation 5.0, which we find Petitioner has not shown to be taught by Sunada and OASIS. Thus, for the reasons given for claim 5, Petitioner has not shown that Sunada and OASIS teach the additional limitations of claims 17 and 20.[15]

5. Conclusion of Obviousness

In sum, as detailed above, Petitioner's proposed combination of Sunada and OASIS teaches each limitation of claims 1–4, 12, 14–16, 18, and 19, but not claims 5–9, 11, 17, and 20. A skilled artisan would have had reasons, with rational underpinning, to combine the teachings of Sunada and OASIS. Patent Owner's objective indicia of nonobviousness are

[15] Petitioner contends that claim 17 would have been obvious "for the reasons provided above relative to claim 14." Pet. 64. In the Reply, Petitioner states that "this was a clear typographical error because it is claims 5, 17, and 20 that have identical requirements. Accordingly, claims 17 and 20 are also disclosed by Sunada in view of OASIS as per the reasons provided for claim 5." Reply 20. Because we decide that Petitioner has not shown that claim 5 is taught by Sunada and OASIS, we need not reach Patent Owner's argument (Sur-reply 23) that it was improper for Petitioner to correct its argument in the Reply.

unpersuasive and entitled to little weight. Upon consideration of all the evidence, we conclude that Petitioner has proved by a preponderance of the evidence that claims 1–4, 12, 14–16, 18, and 19 would have been obvious over Sunada and OASIS, but has not proved, by a preponderance of the evidence, that claims 5–9, 11, 17, and 20 would have been obvious over Sunada and OASIS.

E. Obviousness Over Sunada, OASIS, and Dutcher

Dutcher relates to "authenticating a user of a client machine running a native operating system against a user account held at a non-native server domain." Ex. 1007, 1:13–15.

Petitioner contends that claims 10 and 13 would have been obvious over Sunada, OASIS, and Dutcher. Pet. 65–73.

Claim 10 depends from claim 5, which Petitioner has not shown to be obvious over Sunada and OASIS for the reasons given above. Petitioner does not allege that Dutcher remedies the deficiencies noted above in its allegations for claim 5. Pet. 69–71. Accordingly, Petitioner has not proved, by a preponderance of the evidence, that claim 10 would have been obvious over Sunada, OASIS, and Dutcher.

Claim 13 depends from claim 12 and adds "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."

Petitioner cites Dutcher as providing "implementation details" for "asking the user which domains/enterprises they would like to authenticate using a SSO." Pet. 65–66. In particular, Petitioner argues that "Dutcher

discloses that 'the user is presented with the names and locations of the Server domains available for authentication, or the user may initiate his or her own 'discovery' of such information (if that capability is enabled).'" *Id.* at 68 (quoting Ex. 1007, 6:11–14). Petitioner argues that "OASIS discloses that SAML assertions, which are generated after triggering the single-sign-on operation, include elements that identify the user to be authenticated." *Id.* at 72 (citing Ex. 1013, 17–18). Petitioner further argues that

> Dutcher discloses that the user may "[s]elect a particular location against which he or she desires to be authenticated," that "[f]ollowing selection of a domain, the user is then authenticated at step 38," and that "[w]hen the 'Discover' button on the Logon panel is clicked, the browser Service" is "queried for an updated list of available authentication locations."

Id. at 72–73 (quoting Ex. 1007, 5:46–6:23, 19:2–13) (alterations by Petitioner). According to Petitioner, this shows that a skilled artisan "would have understood that this constitutes prompting the user to select an identity provider prior to the user determining the domain at which it should be authenticated." *Id.* at 73 (citing Ex. 1011 ¶¶ 270–271).

Petitioner argues that "prompting the user to select from a number of available authentication domains would allow the user to have separate accounts for different SSO services," and gives the example that "a banking SSO may require a different login than non-financial SSOs, e.g., for security purposes." *Id.* at 68–69 (citing Ex. 1007, 7:19–28, 7:46–50; Ex. 1011 ¶¶ 256–257). Petitioner contends that a skilled artisan would have had a reasonable expectation of success because implementing Dutcher's

teachings with Sunada and OASIS would have required no more than conventional programming. *Id.* at 69 (citing Ex. 1011 ¶ 258).

We credit Dr. Crovella's uncontroverted testimony (Ex. 1011 ¶¶ 256–258, 264, 269–271) and find that Dutcher teaches "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," as recited in claim 13, and that a skilled artisan would have reasons, with rational underpinning, to combine the teachings of Dutcher with those of Sunada and OASIS, with a reasonable expectation of success. Patent Owner does not argue claim 13 separately.

In sum, Petitioner's proposed combination of Sunada, OASIS, and Dutcher teaches each limitation of claim 13, but not claim 10. A skilled artisan would have had reasons, with rational underpinning, to combine the teachings of Sunada, OASIS, and Dutcher. Patent Owner's objective indicia of nonobviousness are unpersuasive and entitled to little weight. Upon consideration of all the evidence, we conclude that Petitioner has proved by a preponderance of the evidence that claim 13 would have been obvious over Sunada, OASIS, and Dutcher, but has not proved, by a preponderance of the evidence, that claim 10 would have been obvious over Sunada, OASIS, and Dutcher.

IV. CONCLUSION[16]

Petitioner has proved by a preponderance of the evidence that claims 1–4, 12–16, 18, and 19 would have been obvious, but has not proved by a preponderance of the evidence that claims 5–11, 17, and 20 would have been obvious. The outcome for the challenged claims of this Final Written Decision follows. In summary:[17]

Claim(s)	35 U.S.C. §	Reference(s) /Basis	Claims Shown Unpatentable	Claims Not shown Unpatentable
1, 3, 12, 14, 15, 18	102(a)	Sunada		1, 3, 12, 14, 15, 18
1, 3, 12, 14, 15, 18	103(a)	Sunada		
1, 3, 12, 14, 15, 18	103(a)	Sunada, AAPA	1, 3, 12, 14, 15, 18	
1–9, 11, 12, 14–20	103(a)	Sunada, OASIS	1–4, 12, 14–16, 18, 19	5–9, 11, 17, 20
10, 13	103(a)	Sunada, OASIS, Dutcher	13	10

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

[17] For the reasons given above, we do not reach whether claims 1, 3, 12, 14, 15, and 18 would have been obvious over Sunada alone.

Claim(s)	35 U.S.C. §	Reference(s) /Basis	Claims Shown Unpatentable	Claims Not shown Unpatentable
Overall Outcome			1–4, 12–16, 18, 19	5–11, 17, 20

As to confidential information, this Final Written Decision is being filed Board and Parties Only. The parties are authorized to file, within five business days of this Decision, a motion to seal this Decision and other papers filed Board and Parties Only not already addressed in Patent Owner's Motion to Seal (Paper 34), including Papers 45, 52, and 55. A party filing a motion to seal one of these papers must also file a proposed redacted version. A public version of this Final Written Decision will be issued after consideration of a motion to seal or expiration of the time period to file a motion to seal.

V. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that claims 1–4, 12–16, 18, and 19 of the '346 patent are unpatentable;

FURTHER ORDERED that claims 5–11, 17, and 20 of the '346 patent are not unpatentable;

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;

FURTHER ORDERED that this Final Written Decision is being filed as Board and Parties Only;

FURTHER ORDERED that the parties are authorized to file, within five business days of this Decision, a motion to seal this Final Written Decision and any other papers filed as Board and Parties Only not already address in a motion to seal; and

FURTHER ORDERED that a public version of this Decision will be issued in due course.

IPR2022-00646
Patent 7,631,346 B2

FOR PETITIONER:

Heath J. Briggs
Joshua Raskin
Vimal M. Kapadia
Leif Olson
GREENBERG TRAURIG, LLP
briggsh@gtlaw.com
raskinj@gtlaw.com
kapadiav@gtlaw.com
olsonl@gtlaw.com

FOR PETITIONER SIDE – IPR2023-00259 (JOINED)

Shawn Blackburn
SUSMAN GODFREY LLP
sblackburn@susmangodfrey.com

FOR PATENT OWNER:

Taeg Sang Cho
Yung-Hoon Ha
DESMARAIS LLP
tcho@desmaraisllp.com
yha@desmaraisllp.com