

Filed on behalf of Cortex MCP, Inc.
By: Michelle E. Armond
Douglas R. Wilson
Yue Han
ARMOND WILSON LLP
4685 MacArthur Court, Suite 390
Newport Beach, CA 92660
Telephone: (949) 932-0778
Email: ipr@armondwilson.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

VISA INC.,
Petitioner,

v.

CORTEX MCP, INC.,
Patent Owner.

Case No. IPR2024-00486
U.S. Patent No. 9,251,531

PATENT OWNER'S NOTICE OF APPEAL

Pursuant to 35 U.S.C. §§ 141(c), 142, and 319 and 37 C.F.R. § 90.2(a), Patent Owner Cortex MCP, Inc. hereby provides notice of appeal to the United States Court of Appeals for the Federal Circuit from the Final Written Decision of the Patent Trial and Appeal Board entered on July 21, 2025 (Paper 31) (“Final Written Decision”), the Delegated Director Review Decision entered on November 7, 2025 (Paper 36) (“Director Review Decision”), and from all underlying orders, decisions, rulings, and opinions relating to the *inter partes* review of U.S. Patent No. 9,251,531 (“’531 Patent”) in Case No. IPR2024-00486. This Notice is timely under 37 C.F.R. § 90.3(a)(1), having been filed no later than sixty-three (63) days after issuance of the Director Review Decision. Copies of the Final Written Decision and the Director Review Decision are attached hereto as Exhibits 1 and 2.

In accordance with 37 C.F.R. § 90.2(a)(3)(ii), Patent Owner states that the issues on appeal include, but are not limited to:

- The determination that Claims 1, 3-6, 8-18, and 21-33 of the ’531 Patent have been shown to be unpatentable under 35 U.S.C. § 103, and any finding or determination supporting or related to those issues;
- Whether the Board improperly relied on a theory of unpatentability not presented by Petitioner Visa Inc. in its Petition or advanced by either party in the *inter partes* review proceeding in violation of the Administrative Procedure Act, including 5 U.S.C. § 554, the America

Invents Act, including 35 U.S.C. § 312(a)(3), and the Board’s own rules, including 37 C.F.R. § 42.104(b)(4); and

- All other issues decided adversely to Patent Owner in any orders, decisions, rulings, and opinions.

Pursuant to 35 U.S.C. § 142 and 37 C.F.R. § 90.2(a)(1), this Notice is being filed with the Director of the United States Patent and Trademark Office, and a copy of this Notice is being filed concurrently with the Board. In addition, a copy of this Notice and the required docketing fees are being filed with the Clerk’s Office for the United States Court of Appeals for the Federal Circuit via CM/ECF in accordance with 37 C.F.R. § 90.2(a)(2), Federal Rule of Appellate Procedure 15, and Federal Circuit Rule 15.

ARMOND WILSON LLP

Dated: December 12, 2025

By: /Michelle E. Armond/
Michelle E. Armond (Reg. No. 53,954)
Douglas R. Wilson (Reg. No. 54,542)
Yue Han (Reg. No. 80,950)
Attorneys for Cortex MCP, Inc.

CERTIFICATE OF SERVICE

I hereby certify that on December 12, 2025, in addition to being filed and served electronically through the Patent Trial and Appeal Board's P-TACTS System, the foregoing **PATENT OWNER'S NOTICE OF APPEAL** was filed with and served on the Director of the United States Patent and Trademark Office via e-mail at the following:

Office of the General Counsel
U.S. Patent and Trademark Office
efileSO@uspto.gov

I also hereby certify that on December 12, 2025, the foregoing **PATENT OWNER'S NOTICE OF APPEAL** and the requisite docketing fees were filed with the Clerk's Office of the United States Court of Appeals for the Federal Circuit via CM/ECF.

I further hereby certify that on December 12, 2025, the foregoing **PATENT OWNER'S NOTICE OF APPEAL** was served by electronic mail on the following counsel for Petitioner:

Matthew A. Argenti
margenti@wsgr.com

Michael T. Rosato
mrosato@wsgr.com

Patrick M. Medley
pmedley@wsgr.com

Visa v. Cortex MCP
Patent No. 9,251,531 – IPR2024-00486

Joseph M. Baillargeon
jbaillargeon@wsgr.com

Wesley E. Derryberry
wderryberry@wsgr.com

ARMOND WILSON LLP

Dated: December 12, 2025

By: /Michelle E. Armond/
Michelle E. Armond (Reg. No. 53,954)
Douglas R. Wilson (Reg. No. 54,542)
Yue Han (Reg. No. 80,950)
Attorneys for Cortex MCP, Inc.

EXHIBIT 1

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

VISA, INC.,
Petitioner,

v.

CORTEX MCP, INC.,
Patent Owner.

IPR2024-00486¹
Patent 9,251,531 B2

Before SHEILA F. McSHANE, KARA L. SZPONDOWSKI, and
RUSSELL E. CASS, *Administrative Patent Judges*.

McSHANE, *Administrative Patent Judge*.

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

¹ IPR2024-00487 has been consolidated with IPR2024-00486.

I. INTRODUCTION

A. Background

Visa, Inc. (“Petitioner”) filed a Petition (Paper 2, “Pet.”) in IPR2024-00486 (“IPR486”) requesting *inter partes* review of claims 1–20 (the “challenged claims”) of U.S. Patent No. 9,251,531 B2 (Ex. 1001, “the ’531 patent”), as well as a Declaration of Michael I. Shamos, Ph.D. (Ex. 1005). Petitioner also filed a Petition in IPR2024-00487 (“IPR487”) which challenges claims 21–33 of the ’531 patent, as well as a Declaration of Michael I. Shamos, Ph.D. *See* IPR487, Paper 2 (“IPR487, Pet.”), Ex. 1005. Cortex MCP, Inc. (“Patent Owner”) filed a Preliminary Response (Paper 7) in this case, as well as in IPR487 (IPR487, Paper 7).

On August 2, 2024, the Board instituted an *inter partes* review of all the challenged claims in IPR486 and IPR487 pursuant to 35 U.S.C. § 314. Paper 8 (“Dec.”); IPR487, Paper 8. The Board consolidated IPR487 with IPR486, administratively terminated IPR487, and ordered that all future papers and exhibits addressing the claims at issue in both cases were to be filed in IPR486. IPR487, Paper 10, 2; IPR486, Paper 10.

Patent Owner filed a Patent Owner Response (Paper 14, “PO Resp.”), along with a Declaration of Sam Malek, Ph.D. (Ex. 2009). Petitioner filed a Reply (Paper 18, “Pet. Reply”), along with the Reply Declaration of Dr. Shamos (Ex. 1048). Patent Owner filed a Sur-reply (Paper 26, “PO Sur-reply”). The parties presented oral arguments at a May 6, 2025 hearing, and a hearing transcript has been entered into the record (Paper 30, “Tr.”).

For the reasons set forth in this Final Written Decision pursuant to 35 U.S.C. § 318(a), we determine that Petitioner has demonstrated, by a preponderance of the evidence, that claims 1, 3–6, 8–18, and 21–33 of the ’531 patent are unpatentable, and has not demonstrated, by a preponderance of the evidence, that claims 2, 7, 19, and 20 of the ’531 patent are unpatentable.

B. Real Party in Interest

Visa Inc. identifies itself as the real party in interest for Petitioner. Pet. 83. Cortex MCP, Inc. identifies itself as the real party in interest for Patent Owner. Paper 5, 1 (Patent Owner Mandatory Notice); *see also* Papers 20, 27.

C. Related Matters

The parties identify *Cortex MCP, Inc. v. Visa, Inc.*, No. 5:23-cv-05720 (N.D. Cal.) as a related matter. Pet. 83; Paper 5, 1.

D. The ’531 Patent

The ’531 patent is titled “File Format and Platform for Storage and Verification of Credentials” and issued on February 2, 2016 from an application filed on March 12, 2013. Ex. 1001, codes (54), (45), (22). The ’531 patent identifies Provisional Application No. 61/740,731, filed on December 21, 2012, as a related application. *Id.* at code (60).

The ’531 patent is directed to “a computer-implemented method for generating and verifying officially verifiable electronic representations [OVER files]” of user credentials. Ex. 1001, code (57). The method comprises a credential database receiving a request for credential action, where “[t]he credential database may be configured to store one or more

credentials comprising a status indicator.” *Id.* The credential database may then determine “a response to the credential action based on the . . . user credentials stored in the credential database” and transmit “the response to a client device.” *Id.* Figure 1, reproduced below, illustrates the embodiment of invention identified as the OVER file management platform. *Id.* at 3:53–54.

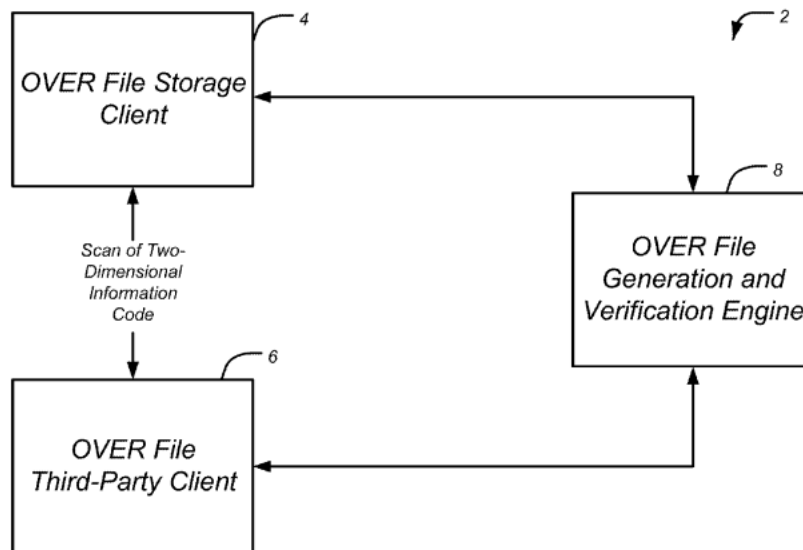


Fig. 1

Figure 1, above, depicts the components of the OVER file management platform. Ex. 1001, 3:53–54. The OVER file management platform has three main components: OVER file storage client 4; OVER file third party client 6; and OVER file generation and authorization engine 8. *Id.* at 3:50–57.

C. Illustrative Claim

Claims 1–33 of the '531 patent are challenged in this consolidated proceeding. Claims 1, 15, and 21 are independent. Claim 1 is representative and is reproduced below, with bracketed designations used by Petitioner added for reference purposes.

1. [Preamble] A computer-implemented method comprising:
 - [1.1] storing, in a memory of an officially verifiable electronic representation (OVER) generation and verification engine, information associated with a credential of a user for proving the user's identity or qualifications;
 - [1.2] receiving, from an OVER file storage client device of the user, an OVER file generation request to provide authentication of the user based on the information associated with the credential;
 - [1.3] generating, by a processor of the OVER engine, an OVER file comprising a virtual representation of the credential that has been verified by an issuing agency to be an official representation of the credential, based on the information associated with the credential of the user;
 - [1.4] transmitting, to the OVER file storage client device of the user, the OVER file in response to the OVER file generation request;
 - [1.5] receiving, from an OVER file third-party client verifying device, a verifying request to verify that the OVER file transmitted to the user authenticates the user based on a scan associated with the OVER file on the OVER file store client device of the user;
 - [1.6] verifying that the scan associated with the OVER file corresponds with the information associated with the credential of the user that is stored in the OVER engine, in response to the verifying request; and
 - [1.7] transmitting, to the OVER file third-party client verifying device, an authentication message comprising an indication of whether the scan associated with the OVER file on the device of the

user corresponds to the information associated with the credential of the user that is stored in the OVER engine.

Ex. 1001, 21:15–46.

D. Asserted Grounds of Unpatentability

Petitioner challenges the patentability of claims 1–33 of the ’531 patent on the following grounds:

Claim(s) Challenged	35 U.S.C. §²	Reference(s)
1, 2, 4–14, 21, 27	103(a)	Oborne ³
3, 22–26, 28–33	103(a)	Oborne, Purves ⁴
1, 2, 4–18, 20, 21, 27	103(a)	Oborne, Neafsey ⁵
3, 19, 22–26, 28–33	103(a)	Oborne, Neafsey, Purves
1, 3–5, 7–16, 18–26, 28–33	103(a)	Stafford, ⁶ Purves
2, 6, 17, 27	103(a)	Stafford, Purves, Neafsey

Pet. 9–11; IPR487, Pet. 9–10.

II. ANALYSIS

A. Level of Ordinary Skill in the Art

Petitioner contends that a person of ordinary skill in the art at the time of the alleged invention “would typically have a bachelor’s degree in

² The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284, 287–88 (2011), amended 35 U.S.C. § 103, effective March 16, 2013. Because the application and provisional application for the ’531 patent were filed before this date, the pre-AIA version of § 103 applies. *See* Ex. 1001, codes (22), (60).

³ US 2012/0316992 A1, published December 13, 2012 (Ex. 1011).

⁴ US 2013/0054454 A1, published February 28, 2013 (Ex. 1013).

⁵ US 2013/0212248 A1, published August 15, 2013 (Ex. 1015).

⁶ US 2009/0271321 A1, published October 29, 2009 (Ex. 1012).

computer science, computer engineering, or a related field, with at least two years of work involving electronic payment systems, network authentication systems, or related areas.” Pet. 9 (citing Ex. 1005 ¶¶ 89–94). Petitioner further states that a person of ordinary skill “could have less education but significant professional experience in one or more of these fields.” *Id.* We adopted this proposed level of skill for the Institution Decision. *See* Dec. 6–7. Patent Owner agrees with this definition of the level of ordinary skill in the art. PO Resp. 8 (citing Ex. 2009 ¶¶ 37–41).

For the purposes of this Decision, we adopt the assessment offered by Petitioner as it is consistent with the ’531 patent and the prior art before us. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001).

B. Claim Construction

A claim “shall be construed using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. § 282(b).” 37 C.F.R. § 42.100(b) (2020). Petitioner identifies three claim terms: “officially verifiable electronic representation (OVER) file,” “scan,” and “verified by an issuing agency.” Pet. 11–14. The term “scan” is not in dispute because the parties have both applied the same interpretation of this term. *See id.* at 14; PO Resp. 9. These remaining two terms will be discussed below.

1. “Officially Verifiable Electronic Representation (OVER) File”

Petitioner argues that “[e]ach independent claim recites an ‘officially verifiable electronic representation (OVER)’ file,” and that the ’531 patent Specification “uses the term ‘OVER’ to refer to an ‘Officially Verifiable

Electronic Representation.” Pet. 12 (citing Ex. 1001, 2:28–30). Petitioner asserts that “[t]he specification describes that an OVER file may contain ‘credential information’” and “may also contain or act as a credential, which may in turn be representative of another credential, such as a driver’s license.” *Id.* (citing Ex. 1001, 6:20–22, 6:54–56, 12:3–6). Additionally, according to Petitioner, “[t]his ‘OVER file credential’ may include an image from an issuing agency, such as a logo or a card image” or a “scannable code, like a QR code.” *Id.* (citing Ex. 1001, 9:11–15, 13:61–14:4, Fig. 11; Ex. 1005 ¶¶ 98–100).

Petitioner asserts that “[t]he ’531 patent does not describe that tokens may be either an OVER file or a part of one (such as a representation of a credential),” but “Patent Owner’s complaint expressly identifies tokens as OVER files.” Pet. 12–13 (citing Ex. 1018, 4, 9, 16–17). Thus, Petitioner states, “[f]or purposes of this petition, [Petitioner] applies a construction that [is] based on Patent Owner’s interpretation of this term.” *Id.* at 13. “Accordingly,” Petitioner states, it is applying “an interpretation of ‘OVER file’ as encompassing a file comprising an image of (or associated with) the credential (as described in the specification and addressed in grounds 5–6), but also encompassing a file comprising a token (as asserted in Patent Owner’s infringement complaint and addressed in grounds 1–4).” *Id.* at 13 (citing Ex. 1005 ¶¶ 98–103).

In our Institution Decision, we preliminarily determined that the term “OVER file” encompasses a virtual representation of one or more credentials, to be used for verification of those credentials. Dec. 9. We also explained that we did not need to determine whether the term “OVER file”

necessarily includes “tokens” as a general matter, or further elaborate on what additional characteristics might be required to qualify as an “OVER file” for purposes of institution. *Id.* We also determined that Petitioner had made a sufficient showing for purposes of institution that Osborne’s tokens qualify as “OVER files.” *Id.* at 10, 23–27. In its Response, Patent Owner states that no construction of “OVER file” is required and that “the claims may be confirmed under the Board’s construction.” PO Resp. 9 (citing Ex. 2009 ¶¶ 43, 46–48).

In its Reply, Petitioner argues that Patent Owner is treating the Institution Decision’s construction “as requiring that the virtual representation itself (not merely the OVER file) be used for verification of the credential,” even though “the claims impose no such requirement on the virtual representation.” Pet. Reply 1–2 (citing PO Resp. 54). “For example,” Petitioner asserts, “verification in subsequent claim elements involves a scan associated with the OVER file, and while the OVER file ‘compris[es]’ the virtual representation, it may encompass other things.” *Id.* at 2 (citing Ex. 1047, 30:16–31:24; Ex. 1048 ¶ 27). We will consider this issue further below when construing the term “verified by an issuing agency.”

Based on the full trial record, we maintain our determination in the Institution Decision that the term “OVER file” encompasses a virtual representation of one or more credentials, to be used for verification of those credentials. *See* Dec. 9.

2. “*verified by an issuing agency*”

Petitioner states that claims 1 and 15⁷ “recite an OVER file comprising ‘a virtual representation of the credential that has been verified by an issuing agency to be an official representation of the credential.’” Pet. 14. Petitioner asserts that, “[d]uring prosecution, Applicant argued that this phrase requires that the issuing agency verify that the *virtual representation* is an official representation of the credential.” *Id.* (citing Ex. 1007, 40, 44–45). “Accordingly,” Petitioner contends, “this petition construes this phrase to require that an issuing agency have verified a *virtual representation* in an OVER file as being an official representation of a credential.” *Id.* (citing Ex. 1005 ¶¶ 112–115).

In our Institution Decision, we preliminary agreed with Petitioner’s construction “to require that an issuing agency ha[s] verified a virtual representation in an OVER file as being an official representation of the credential.” Dec. 13 (emphasis omitted).

In its Response, Patent Owner states that it “agrees in substance with the Board’s construction” of this term, and clarifies its understanding of that construction as requiring that “the issuing agency has verified the ‘virtual representation’ (and not the ‘credential’) to be ‘an official representation of the credential.’” PO Resp. 10 (citing Ex. 2013, 10–11; Ex. 2009 ¶ 45).

In its Reply, Petitioner points to Patent Owner’s reliance on an example in the ’531 patent Specification involving the checking of a driver’s license identification number against a DMV database to show verification

⁷ We note that claim 21 of the ’531 patent, which is at issue in IPR487 and which has been consolidated with IPR486, also contains the same phrase.

of information in an OVER File generation request. Pet. Reply 2 (citing PO Resp. 12–13; Ex. 1001, 6:22–27, 6:47–54). Based on this portion of the Patent Owner Response, as well as portions of Dr. Malek’s deposition, Petitioner argues that Patent Owner “admits that a virtual representation of a credential may be ‘verified by an issuing agency’ by checking credential data against an issuing agency database. *Id.* (citing Ex. 1047, 37:24–41:1, 41:2–22). In its Sur-reply, Patent Owner argues that Petitioner misinterprets its discussion of the DMV example, and contends that what Patent Owner was actually arguing based on that example is that the “credential” (the “OVER file”) is verified, not that “credential data” is verified. PO Sur-reply 1–2.

After considering the full trial record, we adhere to the construction in our Institution Decision interpreting the claim language at issue “to require that an issuing agency ha[s] verified a virtual representation in an OVER file as being an official representation of the credential.” Dec. 13 (emphasis omitted). In light of Patent Owner’s statements in its Sur-reply, we further clarify that this construction encompasses (1) considering the OVER file as the credential and verifying the OVER file, or (2) verifying a virtual representation of the credential contained within the OVER file.

3. Other Terms

The parties do not propose or dispute constructions for any other claim terms, and we determine that it is not necessary to provide an express interpretation of any other claim terms at this stage of the proceeding. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013,

1017 (Fed. Cir. 2017); *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)..

C. Obviousness of Claims 1, 2, 4–14, 21, and 27 Over Osborne

Petitioner contends that claims 1, 2, 4–14, 21, and 27 would have been obvious over Osborne. Pet. 15–41; IPR487, Pet. 14–34. To support its contentions, Petitioner provides explanations as to how the combination of the prior art teaches each claim limitation and provides rationale to combine the references. *Id.* Petitioner also relies upon the Shamos Declaration (Ex. 1005) and the Shamos Reply Declaration (Ex. 1048) to support its positions. Patent Owner contends that Osborne fails to teach certain limitations of the claims. PO Resp. 10–29, 34–48; PO Sur-reply 3–8, 10–16. Patent Owner also relies upon the Malek Declaration (Ex. 2009) to support its positions.

We begin our discussion with a brief summary of Osborne and then address the evidence and arguments presented.

1. Osborne (Ex. 1011)

Osborne is directed to a payment privacy tokenization (PPT) system that transforms payment token-based purchase orders into multi-issuer purchase payment funds transfers. Ex. 1011, code (57), ¶ 22. Figure 1A, reproduced below, depicts diagrams illustrating aspects of the payment tokenization in some embodiments of the invention. *Id.* ¶ 7.

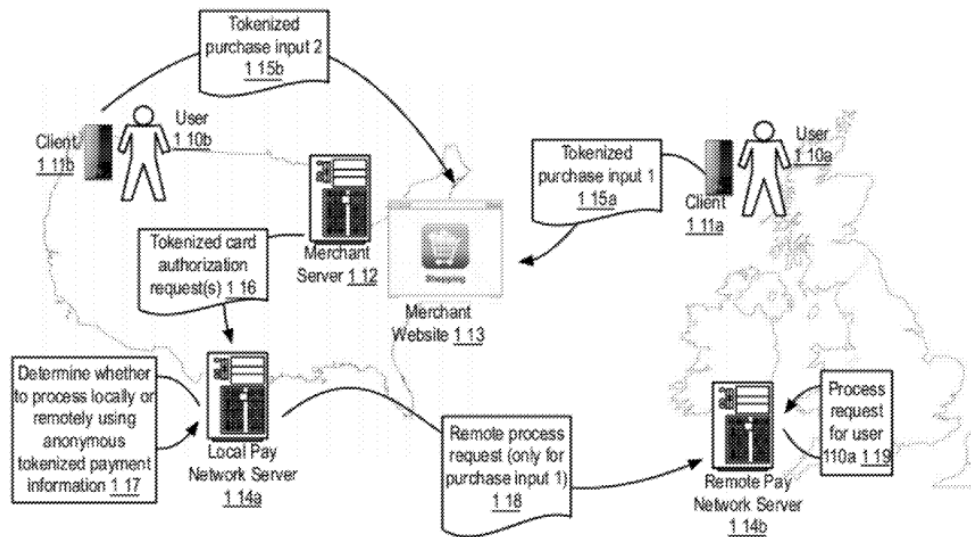


FIGURE 1A

Example: Payment Tokenization

Figure 1A, above, depicts some implementations of the payment tokenization system where “a payment network system, comprised of payment network servers located in distant geographical regions . . . may be required to determine where to process a purchase transaction.” Ex. 1011 ¶ 23. The system of Figure 1A includes local pay network server 114a, remote pay network server 114b), user 110a, and merchant 112 with website 113. *Id.*

In some implementations of Osborne, a user may wish to purchase a product, service, offering, etc. from a merchant. Ex. 1011 ¶ 35. The user may provide user input for the purchase, and the token server may generate a tokenization invitation and an application form for the user to complete to sign up for tokenization services. *Id.* ¶¶ 36, 39. The user may provide token creation input to complete an application form. *Id.* ¶ 40. “The token server

may obtain the application form, and parse the form to extract data fields and values from the form to generate a token data record.” *Id.* ¶ 41. The token server may store the data extracted from the application form to a token database. *Id.* ¶ 44. Figure 4, reproduced below, depicts this process, that is, “a data flow diagram illustrating an example procedure to enroll in a token-based purchase payment program in some embodiments of the PPT.” *Id.* ¶ 9.

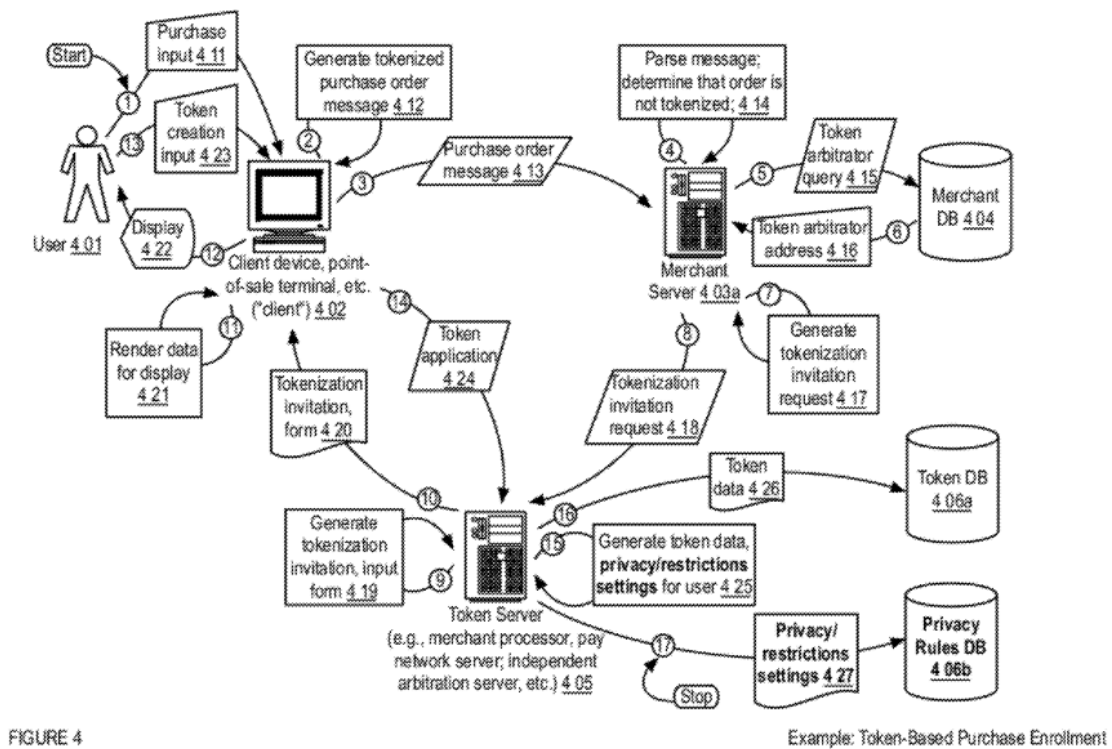


Figure 4, above, illustrates an example procedure to enroll in a token-based purchase payment program. Ex. 1011 ¶ 35. Figure 4 illustrates the interactions between user 401, client device 402, merchant server 403a, and a token server 405. *Id.* ¶¶ 35–44.

2. Analysis of Claim 1

a. 1. [preamble]: “[a] computer-implemented method comprising:”

Petitioner argues that “Oborne teaches a computer-implemented method.” Pet. 16 (citing Ex. 1011 ¶¶ 114–122; Ex. 1005 ¶ 231). Patent Owner does not present arguments specific to the preamble. *See generally* PO Resp.

We have reviewed Petitioner’s arguments and evidence on the teaching of the preamble. Osborne describes the use of computer-based processing to perform steps of a method for tokenization. *See* Ex. 1011 ¶¶ 144–122, code (57). On this complete record, we agree with Petitioner that Osborne teaches the preamble of claim 1.⁸

b. [1.1]: “storing, in a memory of an officially verifiable electronic representation (OVER) generation and verification engine, information associated with a credential of a user for proving the user’s identity or qualifications;”

Petitioner argues that Osborne teaches an “OVER generation and verification engine (OVER engine)” in the form of a “payment privacy tokenization apparatus” or “PPT” apparatus to “transform payment token-based purchase orders, via PPT components, into multi-issuer purchase payment funds transfers.” Pet. 16 (citing Ex. 1011 ¶¶ 22, 166). Petitioner asserts that “[t]his system includes a ‘token server,’ also referred to as a

⁸ Because we are persuaded that Petitioner has shown that Osborne teaches the subject matter recited in the preamble, we need not decide whether the preamble is limiting for purposes of this Decision.

‘token arbitrator,’ that may be any entity involved in the PPT, such as ‘a pay network server.’” *Id.* at 16–17 (citing Ex. 1011 ¶ 53). According to Petitioner, “Oborne also notes that ‘the source of the token’ may be the ‘issuer’ (e.g., a funding source for the user’s account).” *Id.* at 17 (citing Ex. 1011 ¶¶ 29, 47, 48). Petitioner further contends that Oborne’s Figure 4 “depicts the general arrangement of customers, parties, and the pay network server (which can include the PPT apparatus).” *Id.* (citing Ex. 1011, Fig. 4). Referencing its discussion for limitations [1.3] and [1.6], Petitioner contends that “this apparatus generates and verifies OVER files,” and thus Oborne “discloses the recited OVER engine.” *Id.* at 18 (citing Ex. 1005 ¶¶ 232–233).

Petitioner also argues that “Oborne’s PPT apparatus stores information associated with a credential of a user for proving the user’s identity or qualifications” using “a storage device storing account information in a database,” as shown in Oborne’s Figure 15. Pet. 18–19 (citing Ex. 1011, Fig. 15, ¶¶ 114, 146–151). Petitioner asserts that this database’s “Accounts table 1519d” includes “fields with *information associated with a credential useful for proving the user’s identity or qualifications.*” *Id.* at 19 (citing Ex. 1011 ¶ 147). Petitioner further contends that “Oborne teaches that a user ‘desir[ing] to utilize a card’ may use ‘tokens in lieu of payment information’ (thus, *proving the user’s identity or qualifications.*)” *Id.* (citing Ex. 1011 ¶ 25; Ex. 1005 ¶ 234).

We have reviewed Petitioner’s arguments and evidence on the teaching of limitation [1.1]. On this complete record, we agree with Petitioner that Oborne teaches limitation [1.1].

Patent Owner contends that Petitioner never meets its burden to demonstrate obviousness because Petitioner fails to identify specific components of Osborne's PPT that perform the functions of the OVER engine. PO Resp. 30–34 (citing, *inter alia*, Pet. 16–18). Patent Owner argues that Petitioner vaguely identifies Osborne's PPT apparatus as the claimed OVER engine but Osborne describes the entire invention as the “Payment Privacy Tokenization Apparatuses, Methods, and Systems (hereinafter ‘PPT’).” *Id.* at 30–31 (citing Ex. 1011 ¶ 22, code (57)). Patent Owner also asserts that Petitioner improperly points to different components of Osborne's PPT system to teach different claim limitations. *Id.* at 31–33. For instance, Patent Owner points to the Petition's Osborne's “identification merchant server” to satisfy the “OVER file third-party client verifying device” (limitation 1.5), whereas Petitioner relies on Osborne's “first OVER file client device.” *Id.* at 31–33. Patent Owner also contends that Dr. Shamos fails to identify the OVER engine in Osborne. *Id.* at 31 (citing Ex. 2016, 66:20–76:9, 73:20–74:3).

In Reply, Petitioner asserts that the PPT's token server satisfies all the requirements of the OVER engine, and refers to the statement relating to the details addressed for elements 1.3 and 1.6. Pet. Reply 7 (citing Pet. 18). Patent Owner responds that this argument fails because the Petition relies upon the token database 406a for the teaching of some of the limitations and not the token server. PO Sur-reply 8–10 (citing, *inter alia*, Pet. 27–29).

We have reviewed the full trial record, and find that Petitioner has sufficiently proven that Osborne teaches limitation [1.1]. We also find that Petitioner has sufficiently identified Osborne's PPT token server and token

database as the OVER engine. The Petition refers to Osborne's PPT apparatus, shown in Figure 4, as the claimed "OVER generation and verification engine (OVER engine)." Pet. 16–18. The Petition also refers to the PPT apparatus's token server, which is a part of the PPT apparatus, in the discussion of limitation [1.1], but also refers to additional detail provided in "elements 1.3 and 1.6," where the "token server" of the PPT apparatus is relied upon for the teaching of those limitations. *See id.* at 16, 18, 21, 27. The Petition makes clear that Petitioner is relying on the token server to carry out the functions of the OVER engine. *Id.* at 21 (asserting that Osborne's "token server . . . generate[s] a date record and data structure for a token (OVER file)"), 27 ("referring to "the OVER engine (token server)"), *id.* (explaining that Osborne's token server processes the token arbitration request triggered by the scan). As for Patent Owner's argument that Petitioner also pointed to the token database in its Reply, Osborne discloses that the token server and token database, as well as other components of the PPT, can be combined and integrated together. Ex. 1011 ¶ 152, Fig. 15; *see* Tr. 24:5–10. Thus, we find that Petitioner has sufficiently identified Osborne's token server (including a token database that can be integrated with the token server) as the OVER engine.

On this complete record, we agree with Petitioner that Osborne teaches limitation [1.1].

c. [1.2]: “receiving, from an OVER file storage client device of the user, an OVER file generation request to provide authentication of the user based on the information associated with the credential;”

Petitioner argues that, “[t]o generate token information, the user in Osborne communicates ‘via a client such as, but not limited to: a personal computer, mobile device, television, point-of-sale terminal, kiosk, ATM, and/or the like,’ providing input ‘indicating the user’s desire to purchase the product.’” Pet. 19 (citing Ex. 1011 ¶ 35). According to Petitioner, “[i]f the user desires to use tokenization, the client ‘may generate a completed application form, and provide, e.g., 424, the token application to the token server (either directly or via the merchant server).’” *Id.* (citing Ex. 1011 ¶ 40).

Petitioner also argues that Osborne provides an example encoding of a tokenization application form in paragraph 40, which includes “*information associated with the credential*, such as account number, type, billing address, etc., which are stored by Osborne’s PPT apparatus.” Pet. 20–21 (citing Ex. 1011 ¶ 40). The token server, according to Petitioner, “uses values extracted from the form when generating a token record.” *Id.* at 21 (citing Ex. 1011 ¶ 41). Therefore, Petitioner contends, the request is “based on the information associated with the credential,” as limitation [1.2] requires. *Id.* (citing Ex. 1005 ¶¶ 236–237).

Patent Owner does not present arguments specific to this limitation. *See generally* PO Resp.

We have reviewed Petitioner’s arguments and evidence on the teaching of limitation [1.2]. On this complete record, we agree with Petitioner that Osborne teaches limitation [1.2].

d. [1.3]: “generating, by a processor of the OVER engine, an OVER file comprising a virtual representation of the credential that has been verified by an issuing agency to be an official representation of the credential, based on the information associated with the credential of the user;”

Petitioner argues that “Osborne teaches that the token server ‘parse[s] the form to extract data fields and values from the form’ to generate a data record and data structure for a token (*OVER file*), as well as a ‘token identifier’ representing the token, which is provided to the user.” Pet. 21 (citing Ex. 1011 ¶¶ 47–48, Fig. 5; Ex. 1005 ¶ 238). Petitioner argues that “the token is a virtual representation of a credential, such as a credit card,” as shown in Figure 1B of Osborne, reproduced below. *Id.*

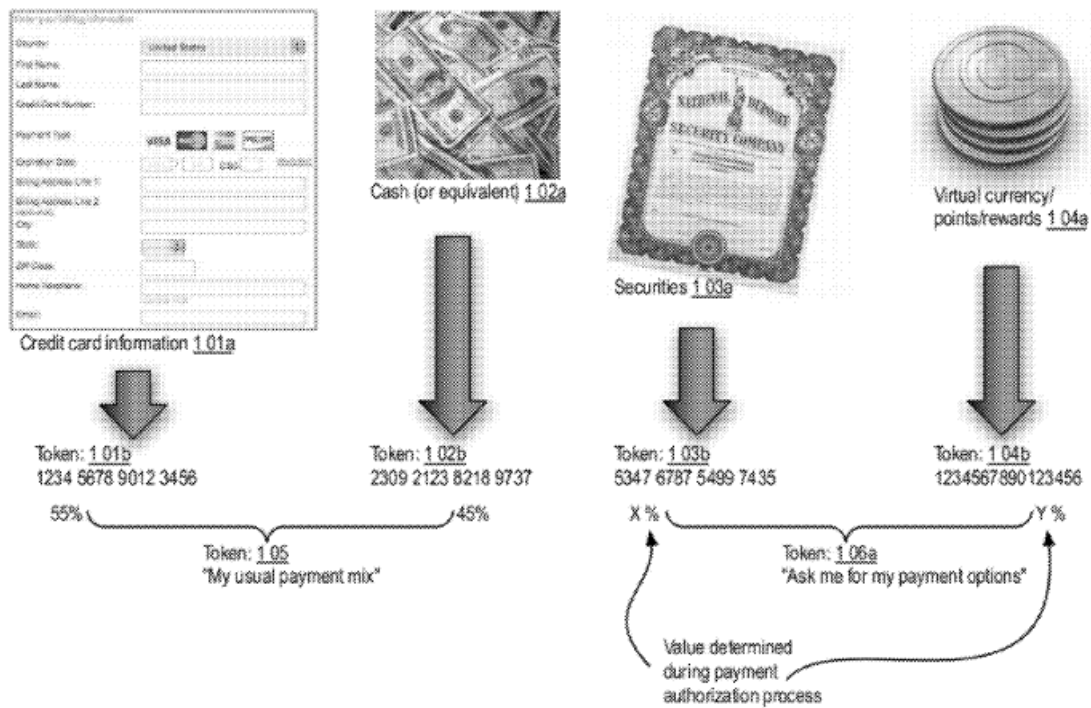


FIGURE 1B

Example: Payment Tokenization

Oborne’s Figure 1B, above, is a block diagram illustrating aspects of payment tokenization in some embodiments of the PPT. Pet. 21–22; Ex. 1011, ¶ 6, Fig. 1B.

Petitioner also points to Oborne’s disclosure that the token is “linked to credit card information” and used “in lieu of . . . card information.” Pet. 22 (citing Ex. 1011 ¶ 25). Thus, Petitioner contends, the token is a “virtual representation of the credential generated based on the information associated with the credential.” *Id.* (citing Ex. 1005 ¶ 239) (emphasis omitted).

Petitioner also argues that “Oborne teaches or at least suggests that the token would be verified by the issuing agency as an official representation.” Pet. 22. Referencing its argument for limitation [1.1],

Petitioner asserts that “Oborne teaches that any entity can operate as the token server, and it specifically identifies that the token may be provided by the credential’s ‘funding source’—that is, by the agency that issued the credential.” *Id.* (citing Ex. 1011 ¶¶ 29, 47–48, 53, 58). “By generating the token and providing it to the user to represent the credential it has issued,” Petitioner contends, “the issuer would be verifying it to be an official representation of the credential.” *Id.* at 23 (citing Ex. 1005 ¶¶ 240–242). Additionally, according to Petitioner, one of ordinary skill “would have found it obvious for an issuer, upon generating the token, to verify that it was an official representation of the credential, using stored . . . credential information identified by the token application form when generating the token,” because “verifying the token would be a routine step based on the credential data received and doing so would increase confidence that the token legitimately represented the credential.” *Id.*

Patent Owner responds by arguing that Osborne does not teach or make obvious issuing agency verification of an OVER file. PO Resp. 10–30; PO Sur-reply 3–8. First, Patent Owner argues that Petitioner “does not point to a disclosure of any such verification by an issuing agency in Osborne.” PO Resp. 13. In this regard, Patent Owner argues that Osborne’s Figure 5, cited by Petitioner, “does not include any verification of a token, much less the claimed ‘issuing agency verification’ and “moves directly from a user sending a token input form (514) to creating a token (515) without any verification step.” *Id.* at 13–14 (citing Ex. 2009 ¶¶ 50–59; Ex. 1011 ¶ 47, Fig. 5). Patent Owner further asserts that Petitioner’s reliance on Osborne’s embodiment, in which the issuer of the credential can operate

as the token server, is not persuasive because Petitioner “does not demonstrate that this alleged issuer-token server embodiment would operate any differently than Osborne’s standard Figure 5 process, which shows no verification step whatsoever.” *Id.* at 14 (citing Pet. 21–22; Ex. 2009 ¶¶ 60–62; Ex. 1011 ¶¶ 29, 47, 48, 53, 58). Thus, according to Patent Owner, Petitioner improperly “removes the verification step from the claim and ignores that Osborne’s token server (no matter who operates it) generates a token without any verification step.” *Id.* at 15 (emphasis omitted). Finally, Patent Owner argues that Petitioner failed to prove that issuing agency verification would have been obvious over Osborne. *Id.* at 16–30.

In its Reply, Petitioner argues that Osborne teaches checking credential data for the tokens. Pet. Reply 3–4. More specifically, Petitioner contends that Osborne’s paragraph 47 teaches tokens that are “‘pre-authorized’ by ‘obtaining ‘assurance’ of sufficient funds from the issuer for pre-funded tokens.’” *Id.* at 4 (citing Ex. 1011 ¶ 47). “Confirming funds in an account,” Petitioner argues, “would of course involve checking account information (e.g., an account number).” *Id.*

In its Sur-reply, Patent Owner argues that Petitioner’s Reply argument invokes an “improper new construction that verification simply requires checking ‘credential data’” rather than verifying “the ‘virtual representation,’” as the claim requires. PO Sur-reply 4 (citing Pet. Reply 3–4; Pet. 14). Patent Owner also argues that this “new theory should not be considered.” *Id.*

After considering the full trial record, we determine that Petitioner has sufficiently shown that Osborne discloses this limitation. First, we find that

Oborne's tokens qualify as "OVER files" because they include a virtual representation of one or more credentials, to be used for verification of those credentials, as we have construed the term "OVER file." *See supra* § II.B.1. For example, Oborne teaches that its token may include a virtual representation of a credential in the form of a credit card, debit card, prepaid card, or other account information used to specify a funding source. Ex. 1011, Fig. 1B, ¶ 25 (referencing the use of "a card (e.g., debit, credit, prepaid, etc.)" and confirming that the token is "linked to credit card information" and used "in lieu of . . . card information"). Oborne also discloses that the token can be implemented as an "XML-encoded data structure" including bank checking account information for a funding source in XML format, which is a "virtual representation" of the bank account credential, as shown below.

```
<?XML version = "1.0" encoding = "UTF-8"?>
<token>
. . . .
  <accounts>
    <1>
      < issuer_name>BankA</issuer_name>
      <account_num>123456789012345</account_num>
      <account_type>checking</account_type>
      <cibfurn_type>email</confirm_type>
      <!--fields below optional in some embodiments-->
      <account_name>John Q. Public</account_name>
      <billing_address>123 Green Street Apt
        1</billing_address>
      <phone>909-333-2345</phone>
      <sign>/jqp</sign>
      <contact_info>jqp@gmail.com</contact_info>
      <default_cost_share>65%</default_cost_share>
    </1>
```

Ex. 1011 ¶ 47.

We also find that Osborne discloses use of an OVER file “comprising a virtual representation of the credential that has been verified by an issuing agency to be an official representation of the credential, based on the information associated with the credential of the user.” As discussed above, we have construed this phrase “to require that an issuing agency ha[s] verified a virtual representation in an OVER file as being an official representation of a credential.” *See supra* § II.B.2. Osborne discloses that a token may be issued by, or in conjunction with, an issuing agency, such as a bank. *See* Ex. 1011 ¶¶ 47 (explaining that the “token requesting channel” may include an “issuer” and that “the source of the token” may be an “issuer”, 53 (explaining that the token server may operate “in conjunction with” the “issuer”), 58 (explaining that “the user’s payment token may be linked to one or more issuer financial institutions (‘issuers’), such as banking institutions, which issued the account(s) for the user linked to the payment token”); Ex. 1005 ¶ 240.

We also find that Osborne discloses that the issuing agency verifies the token (which includes the XML virtual representation of the bank checking account credential) by “pre-authorizing” the token for a predefined amount. Specifically, Osborne discloses that:

In some implementations, each token may be pre-funded. For example, *the source of the token* (e.g., issuer, acquirer, independent token arbitrator) *may first obtain assurance that the funds have been uniquely and exclusively allocated for the token from source to which the token points*. Thus, in some implementations, *the token may be pre-funded and pre-authorized for up to (or in in the alternative, for exactly) a predefined amount* of a purchase transaction.

Ex. 1011 ¶ 47 (emphasis added); *see id.* ¶ 29 (describing “pre-funding, and/or “p[re] authorization” of a token). We agree with Petitioner that pre-authorizing the token and confirming that there are sufficient funds in the bank account to which the token points would involve checking, based on the token information, to confirm that the bank account is a valid account; otherwise no check could be made to see whether funds are allocated or pre-authorized. *See* Pet. Reply 4; Ex. 1011 ¶ 47. During the hearing, Patent Owner agreed that Osborne’s paragraph 47 discloses that, “before the token actually gets issued,” the issuer would “go back and actually verify that the account number was correctly entered in the file” and was “actually correct by verifying it against some official record of it.” Tr. 54:23–55:4. Patent Owner further acknowledged that if “I want a token to represent this bank account, Osborne will go and verify that there is actually a bank account there, maybe even that there are funds in it, to verify that what you’re reference is actually a real credential and there is actually a real credential here before it generates a token.” *Id.* at 55:4–9.

We find that this checking of the XML bank account information in the token against the account information at the bank would be a verification that the token including the XML bank account information (the virtual representation of the bank account credential) is an official representation of the credential (the bank account), as our construction of this limitation requires.

Patent Owner does not directly address the disclosures of Osborne’s paragraph 47 quoted above in either its Patent Owner Response or Sur-reply. *See* PO Resp. 12–16; PO Sur-reply 3–4. During the oral hearing,

Patent Owner argued that the disclosure in paragraph 47 was only “verifying the underlying credential” rather than “verification that a token, for example, is an official representation of the underlying credential.” Tr. 45:23–46:7. Similarly, Patent Owner argued that “Dr. Shamos plainly stated that verifying credential data alone is insufficient to meet the [P]etition’s construction of” this claim limitation when he agreed that ““verifying that the credential data supplied by the user’ . . . does not “meet your construction of ‘verified by an issuing agency’ supplied in your opening declaration.” Tr. 45:14–22; Ex. 2027, 27:18–28:2.

We disagree with these assertions. As we explain above, Osborne discloses more than simply verifying in the abstract that credential data supplied by the user is correct. Osborne discloses that the issuer may first generate a token by parsing a form submitted by the client “to extract data fields and values from the form to generate a token data record,” such as the XML data structure in Osborne’s paragraph 47. Ex. 1011 ¶ 47. Then, the “*token* may be pre-funded” by “obtain[ing] assurance that the funds have been uniquely and exclusively allocated for the token from the source *to which the token points.*” *Id.* (emphasis added). Thus, Osborne discloses verifying that the *token* including the XML bank account information in its data structure (the virtual representation of the bank account information) is valid, not merely that bank account information, standing alone, is valid.

Finally, we do not agree with Patent Owner that Petitioner has improperly raised a new argument on reply. The Petition specifically cited to paragraph 47 of Osborne to meet the “verified by an issuing agency” language in limitation 1.3. Pet. 21–23. Petitioner’s Reply permissibly

fleshed out that argument in response to Patent Owner's Response by further explaining how the "pre-authorization" and "pre-funding" portions of paragraph 47 supported Petitioner's position. Pet. Reply 4. Patent Owner had the opportunity to respond to this argument in its Sur-reply, but failed to do so with any specificity.

Accordingly, we find that Petitioner has sufficiently shown that Osborne teaches limitation 1.3.

e. [1.4]: "transmitting, to the OVER file storage client device of the user, the OVER file in response to the OVER file generation request;"

Petitioner argues that "Osborne teaches that a 'token may be provided as a data structure via HTTP(S) POST, as a file, as an attachment (e.g. via email), and/or provided to the client device for later use.'" Pet. 24 (citing Ex. 1011 ¶ 48). According to Petitioner, "[t]his transmission to the client device is performed after receiving the token application as shown in Fig. 5, with step 517 occurring as a step after receiving a token generation request from the user (shown in steps 508 and 515). *Id.* (citing Ex. 1011 ¶¶ 40–41, 46–47), Fig. 5. Thus, Petitioner contends, Osborne "sends a token (*OVER file*) to the user's device (*OVER file storage client device of the user*) in response to the *OVER file generation request*." *Id.* (citing Ex. 1005 ¶ 243).

Patent Owner does not present arguments specific to this limitation. *See generally* PO Resp.

We have reviewed Petitioner's arguments and evidence on the teaching of limitation [1.4]. On this complete record, we agree with Petitioner that Osborne teaches limitation [1.4].

f. [1.5]: “receiving, from an OVER file third-party client verifying device, a verifying request to verify that the OVER file transmitted to the user authenticates the user, based on scan associated with the OVER file on the OVER file storage client device of the user;”

Petitioner argues that “Oborne teaches this element as part of a merchant’s token arbitration request (*verifying request*) triggered by a purchase order request from a user (*based on a scan*).” Pet. 25. “Beginning with the scan aspect,” Petitioner asserts, “a user communicates with a merchant server via a client (e.g., ‘mobile device’ or ‘point-of-sale terminal’) by ‘activating a RFID/NFC enabled hardware device.’” *Id.* (citing Ex. 1011 ¶ 49). According to Petitioner, “[t]his triggers a tokenized purchase with the merchant, *via a third-party client verifying device* (the merchant server, alone or in conjunction with the merchant’s point-of-sale device interacting with the user’s device via NFC).” *Id.* (citing Ex. 1011 ¶ 50). Petitioner contends, that because Patent Owner has asserted that transmitting NFC-based payment requests constitutes a scan, applying this to Oborne, “Oborne’s RFID/NFC activation triggers the purchase to be performed with the token, the RFID/NFC activation would be a *scan associated with the OVER file on the OVER file storage client device of the user*.” *Id.* (citing Ex. 1005 ¶ 244).

Petitioner also argues that, “[t]o process the purchase order request, the merchant server sends a ‘token arbitration request . . . to a token server,’” which reads on the “verifying request” of limitation [1.5]. Pet. 25–26 (citing Ex. 1011 ¶¶ 51–52). According to Petitioner, an example of the encoding of such a request is included in the code listing in Oborne, which references a

token_id field representing a token. *Id.* at 25–26 (citing Ex. 1005 ¶ 245). Referencing its argument for claim limitation [1.6], Petitioner further argues that “Oborne teaches that the ‘token server may parse the token arbitration request message’ and ‘determine whether the user token is authenticated.’” *Id.* at 26 (citing Ex. 1011 ¶¶ 25, 53–55). Thus, Petitioner contends, applying Patent Owner’s interpretation of “scan,” Oborne “teaches that the *OVER engine* (token server) receives the recited verifying request from a third-party device based on the recited scan.” *Id.* at 26–27 (citing Ex. 1005 ¶ 245).

Patent Owner does not present arguments specific to this limitation. *See generally* PO Resp.

We have reviewed Petitioner’s arguments and evidence on the teaching of limitation [1.5]. On this complete record, we agree with Petitioner that Oborne teaches limitation [1.5].

g. [1.6]: “verifying that the scan associated with the OVER file corresponds with the information associated with the credential of the user that is stored in the OVER engine, in response to the verifying request; and”

Petitioner argues that “Oborne teaches that the token server processes the token arbitration request triggered by the scan (discussed above for element [1.5]) by looking up the account number in a token database” and then “‘extract[s] the payment token from the message’” and “‘issues a query to a database ‘using the payment token as a search term.’” Pet. 27 (citing Ex. 1011 ¶ 53). According to Petitioner, “the database provides ‘instructions for the token server on how to proceed with payment processing’” including

“credential information such as user account numbers,” as shown in the code listing in paragraph 53 of Osborne. *Id.* at 27–28 (citing Ex. 1011 ¶ 53).

Additionally, Petitioner asserts, the “token server may determine whether the user token is authenticated.” *Id.* at 28 (citing Ex. 1011 ¶¶ 54, 69). “In other words,” according to Petitioner, “the query determines whether the *scan* (RFID/NFC interaction) *associated with the OVER file* (token) *corresponds with the information associated with the credential of the user stored in the OVER engine* (whether the database query for the token returns the user’s account details or not), thereby performing the recited step of verifying.” *Id.* at 28–29 (citing Ex. 1005 ¶ 246).

Additionally, Petitioner argues, Osborne teaches that further verification may optionally be performed, such as verification using biometric information, a user name and password, or an authentication chip communicating in proximity with the user’s card via RFID or similar technology. Pet. 29 (citing Ex. 1011 ¶¶ 26, 54). “Thus,” Petitioner contends, “Osborne teaches that a scan’s correspondence with the user’s credential information may be verified using various complementary techniques.” *Id.* (citing Ex. 1005 ¶ 247).

Patent Owner does not present arguments specific to this limitation. *See generally* PO Resp.

We have reviewed Petitioner’s arguments and evidence on the teaching of limitation [1.6]. On this complete record, we agree with Petitioner that Osborne teaches limitation [1.6].

h. [1.7]: “transmitting, to the OVER file third-party client verifying device, an authentication message comprising an indication of whether

the scan associated with the OVER file on the OVER file storage client device of the user corresponds to information associated with the credential of the user that is stored in the OVER engine.”

Petitioner argues that Osborne “teaches sending *an authenticating message comprising an indicator*” of whether the user token has been authenticated. Pet. 30. “For example,” Petitioner asserts, Osborne teaches that if “the token server determines that the user is not authenticated, e.g., 711, option ‘No,’ the token server may generate an ‘authentication fail message,’” which is sent to the merchant server (mapped to the “third-party client verifying device”), as shown in steps 712a–b of Figure 7A. *Id.* (citing Ex. 1011 ¶ 69, Fig. 7A). According to Petitioner, “[t]his is an indication that the scan is not associated with the stored user data.” *Id.* (citing Ex. 1005 ¶ 249). “On the other hand,” Petitioner contends, “[i]f the user token is authenticated, then the ‘token server may continue processing,’” and “[t]he stored user account information is . . . used to procure payment authorization, and a message is sent to the merchant server indicating the result.” *Id.* at 31 (citing Ex. 1011 ¶¶ 61, 53, 70, Figs. 7B–7C). “Any of these messages,” according to Petitioner, “is an indicator that the token was authenticated, and thus that the scan corresponded to the stored user credential information.” *Id.* (citing Ex. 1005 ¶¶ 250–251).

Patent Owner does not present arguments specific to this limitation. *See generally* PO Resp.

We have reviewed Petitioner’s arguments and evidence on the teaching of limitation [1.7]. On this complete record, we agree with Petitioner that Osborne teaches limitation [1.7].

i. Summary for Claim 1

Weighing the record as a whole in view of the findings and analysis above, we conclude that Petitioner has met its burden to show, by a preponderance of the evidence, that claim 1 would have been obvious over Osborne.

3. Dependent Claim 2

Petitioner asserts that

Claim 2 then recites three elements identical to elements 1.2–1.4, except that (1) the word ‘second’ is applied instead of the word ‘first’; (2) the generation copied from element 1.3 need not be ‘based on the information associated with the credential of the user’; and (3) the second OVER file is ‘is invalid for use in the first OVER file storage client device for authenticating the user.’

Pet. 31.

Petitioner contends that “the first two aspects of claim 2 [the use of the word “second” instead of “first” and that generation need not be based on information associated with the credential] are satisfied by a user having two devices and receiving respective OVER files on each device.” Pet. 32. According to Petitioner, a person of ordinary skill in the art “would have expected users to use multiple devices,” and “Osborne teaches that the token server may keep a device table with various identifiers for a user’s devices.” *Id.* (citing Ex. 1011 ¶ 148; Ex. 1005 ¶¶ 252–253).

Petitioner argues that it would have been obvious to a person of ordinary skill in the art in light of Osborne’s disclosure that the second OVER file be a new, device-specific credential that is invalid on the first OVER file client device. Pet. 32. Petitioner relies on Osborne’s teaching of using device fingerprinting to provide additional security of Osborne’s tokens, as

well as Osborne's example token data structure that includes a "client_fingerprint." *Id.* (citing Ex. 1011 ¶¶ 26, 47). According to Petitioner, a person of ordinary skill in the art "would have been motivated to employ Osborne's device fingerprinting to tie a given token to a given device, such that the token for a second device would be a new credential, different from the first token (with both being different credentials from the original credential), with the second device's token being invalid in the first device (since the first device's fingerprint would not match)." *Id.* (citing Ex. 1005 ¶¶ 254–255).

Patent Owner argues that Osborne does not teach or suggest a "second OVER file" as claimed. PO Resp. 35–38. According to Patent Owner, "Claim 2 requires a user with two devices ('first'/'second' device), each receiving a different OVER file comprising a different virtual representation ('first'/'second' OVER file comprising a 'first'/'second' virtual representation) of the same credential." *Id.* at 35 (citing Ex. 1001, 21:47–50; Ex. 2009 ¶¶ 100–102). Specifically, Patent Owner argues that Petitioner has not shown that it would have been obvious for Osborne to (1) generate a "second OVER file comprising a second virtual representation" of the same "credential" for the user's "second" device; and (2) have a "second OVER file" that is "invalid for use in the first OVER file client device." *Id.*

Claim 2 requires Petitioner to show that Osborne teaches the generation of a second OVER file which comprises a second virtual representation of the original credential that has been verified by the issuing agency to be a second official representation of the original credential that is

invalid for use in the first OVER file client device for authenticating the user.

We agree with Patent Owner that Petitioner has not met its burden to establish that Osborne teaches or suggests all of the limitations of claim 2. First, we consider whether Petitioner has shown that Osborne teaches or suggests generating “a second OVER file comprising a *second virtual representation of the original credential* that has been verified by the issuing agency to be a second official representation of the original credential.” Patent Owner contends that the “Petition does not explain why one of skill would have been motivated to adapt Osborne’s system to allow a user to receive tokens on multiple devices.” PO Resp. 36. Patent Owner argues that Petitioner “does not show that a user receiving an OVER file on two devices meets the claimed ‘*second* OVER file comprising a *second* virtual representation’ of the same credential for the user’s second device.” *Id.* at 37 (citing Ex. 2009 ¶¶ 106–109). According to Patent Owner, the “logical” and “conventional” option would be to use the first OVER file comprising the first virtual representation of the original credential that had already been created and stored. *Id.* at 37–38 (citing Ex. 1001, 21:47–62; Ex. 2009 ¶¶ 108–109).

We agree with Patent Owner. The basis of Petitioner’s contentions for the teaching of the limitation is that the user has two devices and receives respective OVER files (i.e., tokens) to be used on each device. *See* Pet. 32. But it is not enough that there is a second token used for a second device, or a “device-specific token.” *See* Pet. Reply 9–10. Petitioner fails to explain how Osborne teaches that the second OVER file (i.e., second token) is “a

second virtual representation of the original credential that has been verified by the issuing agency to be a second official representation of the original credential.” Rather, Petitioner refers to its contentions, which do not address, for example, how the second token is a *second virtual representation of the original credential*. *Id.*; see PO Sur-reply 10–11 (arguing that “Oborne does not teach two devices with distinct OVER files representing the same credential”); see PO Resp. 36–38. We find persuasive Dr. Malek’s testimony that Petitioner has not shown why a person of ordinary skill in the art would choose to generate a new token that is a virtual representation of the original credential when a user requested a token on a second device, rather than simply re-using the original token that is a virtual representation of the same credential. See Ex. 2009 ¶ 108; see PO Resp. 36–38.

Petitioner has also failed to sufficiently explain how Oborne teaches or suggests that “the second OVER file . . . is invalid for use in the first OVER file client device for authenticating the user.” Petitioner relies on Oborne’s disclosure of device fingerprinting, which is cursory and states as follows:

In some implementations, additional security may be layered by using authentication methods. . . . As another example, ***device fingerprinting*** may be utilized. For example, a client device of a user may be a device that is used exclusively by the user, such as a smartphone, tablet computer, laptop computer, and/or the like.

Ex. 1011 ¶ 26 (emphasis added).

Based on this disclosure, Petitioner argues that:

To obtain the additional security taught by Osborne, a [person of ordinary skill in the art] would have been motivated to employ Osborne's device fingerprinting to tie a given token to a given device, such that the token for a second device would be invalid in a first device (since the device's fingerprint would not match).

Pet. 32 (citing Ex. 1005 ¶ 254–255). Petitioner also relies on testimony from Dr. Shamos to support its position that the purpose of the device fingerprinting is to tie a token to a device. *Id.* Dr. Shamos testifies that “[t]here would be no purpose to device fingerprinting if a token could be used on any device.” Ex. 1005 ¶ 254. Dr. Shamos refers to Osborne's disclosures on “digital fingerprinting” and a client's MAC address in the token data structure. *Id.* (citing Ex. 1011 ¶¶ 26, 47).

We have considered Petitioner's arguments in light of Osborne's disclosure, but find Dr. Malek's responsive testimony to be more persuasive. We agree with Dr. Malek that, in Osborne, “device fingerprinting simply refers to identifying a device and the user associated with that device.” Ex. 2009 ¶ 111. Specifically, paragraph 26 of Osborne (quoted above) discloses authentication of a user, where “device fingerprinting” is utilized to verify a user's identity where a user *exclusively* uses a client device such as a smartphone or laptop computer. Ex. 1011 ¶ 26 (emphasis added). The use of the device fingerprinting for determining the device identity in order to authenticate a user is corroborated by the disclosures in paragraph 47 of Osborne which refer, in part, to the “<client_details” which can include a “<client_type>smartphone” and “client_fingerprint>font list, MAC address, memory size, memory.” *Id.* ¶ 47 (emphasis added). So, contrary to Petitioner's arguments, we do not discern any disclosure in Osborne that “device fingerprinting” ties a *token* to a particular device. *See*, Ex. 1011

¶¶ 26, 47. Rather, Osborne’s disclosures support Dr. Malek’s testimony that, contrary to Petitioner’s position, “device fingerprinting could be used to limit a token to a *set* of fingerprinted devices, such as each device belonging to the user.” Ex. 2009 ¶ 113.

Accordingly, for the reasons described above, we find that Petitioner’s contentions and evidence are lacking for claim 2, and we, therefore, determine that Petitioner has not demonstrated by a preponderance of the evidence that claim 2 is unpatentable over Osborne.

4. Dependent Claim 7

Dependent claim 7 recites “wherein the status indicator [recited in claim 4] indicates an invalid credential and the credential information indicates a reason for the invalid credential.” Ex. 1001, 22:19–22.

Petitioner asserts that in Osborne, the “issuer response can indicate lack of funds, or indicate that a ‘number of failed authorization attempts exceeds a threshold’ by sending a ‘transaction terminated’ message.” Pet. 36 (citing Ex. 1011 ¶ 72). Petitioner also contends that it would be obvious for the credential information to indicate a reason for the invalidity, with Dr. Shamos testifying that “it would be routine” and “[t]o do otherwise would leave a customer confused about why the transaction did not go through.” Ex. 1005 ¶ 264.

Patent Owner argues that “neither Osborne’s ‘authorization fails message 644’ or Osborne’s ‘transaction terminated’ message . . . ‘indicates a reason for the invalid credential,’” as the claim requires. PO Resp. 43–44 (citing Ex. 1011 ¶¶ 61, 72; Ex. 2009 ¶¶ 121–122). Patent Owner also contends that Dr. Shamos’ testimony on obviousness is conclusory and

unsupported, such as not providing a reason about why a lack of a reason would leave a customer confused. *Id.* at 43 (citing Ex. 1005 ¶ 264). Patent Owner also asserts that this testimony does not consider the fact that a user may not want the reason for an invalid credential to be sent to the merchant, such as the card being over its limit, which would cause embarrassment. *Id.* (citing Ex. 2009 ¶¶ 119–120). Patent Owner also argues that Petitioner’s assertion that providing a reason would be routine employs common sense and does not provide a reasoned analysis and evidentiary support, as well as impermissibly attempting to fill in a limitation missing from the prior art. *Id.* at 42 (citing Ex. 2009 ¶ 119; *DSS Tech. Mgmt., Inc. v. Apple Inc.*, 885 F.3d 1367, 1374 (Fed. Cir. 2018); *Arendi S.A.R.L. v. Apple Inc.*, 832 F.3d 1355, 1361–62 (Fed. Cir. 2016)).

We agree with Patent Owner. Osborne’s discloses messages for authorization requests (“No”) or “transaction terminated” if there too many re-attempts for authorization, but these messages do not indicate a *reason* for the denials. *See* Ex. 1011 ¶ 72. Petitioner argues that the “claims do not require that the credential information indicate the reason in a particular way,” but, nonetheless, the messages have to include a reason. *See* Pet. Reply 11. Petitioner’s reliance on the assertion that including a reason was routine, commonplace, and a “conventional approach” (see Pet. 36; Pet. Reply 12; Ex. 1005 ¶ 264) amounts to reliance on common sense and that is insufficient. This is because the testimony regarding common sense attempts to supply a limitation missing from the prior art, which cannot be used as a substitute for reasoned analysis and evidentiary support, which has not been provided by Petitioner. *See DSS Tech.*, 885 F.3d at 1374

(“common sense and common knowledge have their proper place in the obviousness inquiry . . . ‘if explained with sufficient reasoning.’”). Here, Dr. Shamos’s rationale is that a customer would be confused (Ex. 1005 ¶ 264), but this assertion is not supported by evidence. Dr. Shamos refers to examples of references which disclose that reasons are provided with responses to authentication requests (*id.* ¶¶ 219–227), and while these references do show that reasons could be sent, transactions are routinely denied without any indication of why denial occurred, as Dr. Malek testifies (Ex. 2009 ¶ 119); in particular, that is the case with Osborne which does not provide a reason, as discussed above. Here, short of opining that Osborne’s disclosures expressly disclose that a reason is sent in messages (Ex. 1005 ¶ 264), which we disagree with, Dr. Shamos’s testimony only addresses the alleged “routine” nature of providing a reason with a message (*id.*). Accordingly, Petitioner has not carried its burden to demonstrate that Osborne teaches the claim limitation in the view of one of ordinary skill in the art nor has provided sufficient support and evidence for supplying the missing limitation by reliance on the common sense rationale that including a message would be routine.

Thus, for the reasons described above, we find that Petitioner’s contentions are lacking for the teaching of the limitations of claim 7, and we, therefore, determine that Petitioner has not demonstrated by a preponderance of the evidence that claim 7 is unpatentable over Osborne.

5. Dependent Claim 8

Claim 8 recites “further comprising generating, by the OVER engine, a reference to a remotely stored credential, wherein the information

associated with the credential of the user comprises the reference to the remotely stored credential.” Ex. 1001, 22:23–27.

Petitioner asserts that Osborne teaches storing information associated with a credential in a database. Pet. 37 (citing Ex. 1011 ¶¶ 47, 148 (listing fields such as “account_number,” “routing_number.”)). Dr. Shamos testifies that Osborne teaches that its systems may store data objects locally or in “remote storage facilities through a communications network.” Ex. 1005 ¶ 267 (citing Ex. 1011 ¶ 133). In Reply, Petitioner notes Osborne’s discussion of distributed databases. Pet. Reply 13 (citing Ex. 1011 ¶¶ 147–150, Fig. 15).

We have reviewed Petitioner’s arguments and evidence and we agree with Petitioner that Osborne teaches the limitations of claim 8.

Patent Owner asserts that Osborne discloses that “program components” “may also be” stored in “remote storage facilities,” and not that “data objects” may be stored in “remote storage facilities,” as Petitioner asserts. PO Resp. 44 (citing Pet. 37; Ex. 1011 ¶ 133). Patent Owner contends that “Osborne distinguishes between ‘program and/or database components and/or data,’ indicating that Osborne was not teaching that ‘data objects’ could be stored remotely, as the Petitions assert.” *Id.* at 44–45 (emphasis omitted).

We find that Petitioner has provided sufficient evidence that Osborne teaches the limitations of claim 8. Osborne discloses that the memory may contain a “collection of programs and/or database components and/or data” “such as” “a component collection.” Ex. 1011 ¶ 133. Osborne further discloses that “non-conventional program components such as those in the

component collection” “may be loaded and/or stored” “in remote storage facilities.” *Id.* As an initial matter, the use of “and/or” does not distinguish between the “collection of programs and/or database components and/or data” and although Osborne uses the phrase “non-conventional program components” when referring to remote storage, it is immediately followed by “such as those in the component collection.” *Id.* Further, in Reply, Petitioner refers to Osborne’s disclosure concerning distributed databases, which states that databases may be distributed “over several computer systemizations and/or storage devices,” which supports that Osborne teaches that data, such as credentials, may be stored remotely. Pet. Reply 13; Ex. 1011 ¶ 150. Although Patent Owner argues that Petitioner’s reference to paragraph 150 of Osborne in Reply is a new theory (PO Sur-reply 13), we do not agree. Petitioner’s response is properly presented in response to arguments presented in Patent Owner’s Response in that paragraph 150 of Osborne refers to “databases” and provides more specificity on an embodiment with “database components,” that are more generally discussed in the “Component Collection” disclosure in paragraph 133 that was discussed in the Petition. 37 C.F.R. § 42.23(b). Additionally, we are not persuaded by Patent Owner’s argument also that “storing data over ‘several computer systemizations and/or storage devices,’ . . . does not describe where they are located or that any are ‘remote.’” PO Sur-reply 13. Patent Owner asks too much; Osborne’s disclosure indicates that its databases may be distributed, that is, separate from each other, which is sufficient.

Accordingly, on the full record, we conclude that Petitioner has met its burden to show, by a preponderance of the evidence, that claim 8 would have been obvious over Osborne.

6. Dependent Claims 12 and 13

Claim 12 recites “verifying that the scan of the OVER file corresponds with the credential of the user comprises comparing the credential identifier with one or more stored credentials,” and claim 13 recites “wherein the authentication message comprises the status indicator of the stored credential when the credential identifier matches a stored credential.” Ex. 1001, 22:42–49.

For claim 12, Petitioner asserts that when a token arbitration request is processed, there is a query to retrieve token data that includes stored credential information like account numbers. Pet. 39 (citing Ex. 1011 ¶¶ 67, 47, 147). Petitioner contends that by using the token identifier to query a database and retrieve the stored credential, Osborne is comparing the credential identifier with the stored credential. *Id.* (citing Ex. 1005 ¶¶ 275–276). For claim 13, Petitioner relies on the disclosure in Osborne of an authentication message that is sent when the credential identifier (token ID) is used to retrieve the stored account information. *Id.* at 40 (citing Ex. 1011 ¶¶ 61–63, 69).

We have reviewed Petitioner’s arguments and evidence on the teaching of claims 12 and 13 by Osborne. On this complete record, we agree that Osborne teaches the limitations of claims 12 and 13.

Patent Owner refers to Petitioner’s assertions for claim 11 and argues that Petitioner relies on different “credential identifiers” for claim 11 and for

claims 12 and 13. PO Resp. 46. Patent Owner asserts that “claim 11’s ‘OVER file generation request compris[ing] a credential identifier’ is met by Osborne’s ‘token application’ including an account number,” and for claims 12 and 13, Petitioner “switches its mapping to argue that ‘credential identifier’ corresponds to Osborne’s ‘token identifier.’” *Id.* at 46–47 (citing Pet. 38–40).

We are not persuaded by Patent Owner’s arguments. The issue is not, as Patent Owner argues, whether the token identifier and credential identifier are *per se* the same thing, but rather that they may be the same thing, such as the account number, for instance, as Petitioner asserts. *See* Pet. 38–40; Pet. Reply 13–14. That is, for example, the account number can be both a token identifier and a credential identifier. *See* Pet. Reply 13–14. For claim 11, Petitioner relies upon Osborne’s disclosure “that the token application identifies a user credential by a credential identifier (*account_num field*), which is stored when creating a token, with the token data structure indicating which account number(s) correspond to a given token” for the teaching of a “credential identifier,” wherein a “token may indicate [a] mix of one or more credentials via token indicators.” Pet. 38–39 (citing Ex. 1011 ¶¶ 25, 40, 47) (emphasis added); Ex. 1005 ¶¶ 208–212, 271–274). As Petitioner asserts (*see* Pet. 38; Ex. 1005 ¶ 209), the credential identifier may be the same as the token identifier. *See* Ex. 1011, Fig. 1B (identifying the credential with the same identifier as the token identifier). For claim 12, Petitioner asserts that “by using the token identifier to query a database and retrieve the stored credential (e.g. cards’ *account number*), Osborne is comparing the credential identifier with the stored credential.” *Id.* at 39

(emphasis added). Because the token identifier may be the same as the credential identifier, we find that Petitioner has sufficiently demonstrated that Osborne teaches the limitations of claims 12 and 13.

We are not persuaded by Patent Owner’s additional argument in sur-reply, that there is nothing in Osborne showing that prefunded token <2> that teaches a token with an “account_num” field. PO Sur-reply 14–15 (citing Ex. 1011 ¶ 47). This may be so, but the token data structure shown in paragraph 47 is exemplary, and other funding sources within the token data structure do include an “account_num” field, as highlighted by Patent Owner, so we are not persuaded that Osborne precludes a prefunded token with an “account_num” field.

Accordingly, on the full record, we conclude that Petitioner has met its burden to show, by a preponderance of the evidence, that claims 12 and 13 would have been obvious over Osborne.

7. Dependent Claims 4–6, 9–11, 14, 21, and 27

Petitioner asserts that Osborne teaches the limitations of claims 4–6, 9–11, 14, 21, and 27. Pet. 33–39, 40–41; IPR487, Pet. 15–34. We have reviewed the argument and evidence presented and find that it is sufficient to demonstrate that Osborne teaches all the limitations of these claims.

Patent Owner does not present any arguments specifically related to these claims. *See generally* PO Resp.

We have reviewed the argument and evidence provided and conclude that Petitioner has met its burden to show, by a preponderance of the evidence, that claims 4–6, 9–11, 14, 21, and 27 would have been obvious over Osborne.

D. Obviousness of Claims 3, 22–26, and 28–33 over Osborne and Purves

Petitioner asserts that claims 3, 22–26, and 28–33 would have been obvious over the combination of Osborne and Purves. Pet. 42–43; IPR487, Pet. 34–45. Patent Owner argues that Petitioner has not carried its burden to provide a reason to combine Purves’ payment account retrieval with Osborne in its assertions for claims 23–26 and 28–33. PO Resp. 48–49.

We begin with a brief summary of Purves and then address the argument and evidence presented.

1. Purves (Ex. 1013)

Purves is directed to a wallet service enrollment platform (“WSEP”). Ex. 1013, code (57). Purves uses a platform that “facilitates the enrollment of payment accounts in a consumer’s virtual wallet.” *Id.* In Purves, a “consumer may be logged into their payment account issuer’s web site” and designate “payment accounts for enrollment in a virtual wallet.” *Id.* The issuer can then share relevant information with the virtual wallet provider to facilitate the enrollment of the accounts into the virtual wallet. *Id.* In Purves “[t]he WSEP may also be configured to facilitate the creation and funding of pre-paid accounts in a consumer’s virtual wallet.” *Id.* A Quick Response (QR) code scan may be used to trigger a wallet account connection or login during a point-of-sale interaction. *Id.* ¶ 64.

2. Analysis

Claim 23 recites:

23. The apparatus of claim 21, wherein the instructions are further configured to program the processor to:

request the credential from the issuing agency, wherein the issuing agency stores credentials issued by the issuing agency; receive the status indicator and credential information associated with the credential transmitted by the issuing agency; and store the credential and the status indicator.

Ex. 1001, 24:9–18.

Petitioner asserts that Purves teaches the generation of new credentials like a gift card or prepaid card. IPR487, Pet. 37 (citing Ex. 1013 ¶ 83). Petitioner contends that Purves also teaches that its system may retrieve the user’s “payment account information from the payment account issuer,” with the issuer responding by providing the user’s account information, such as “data for use in establishing a virtual wallet account,” so “Purves teaches requesting the credential from the issuing agency and receiving the credential information transmitted by the issuing agency.” *Id.* (citing Ex. 1013 ¶¶ 83, 108; Ex. 1005 ¶ 301). Petitioner argues that Osborne teaches receiving status indication from the issuer, where, for example, “in response to a request for authorization, an issuer queries a database to determine whether the account number sent for the token matches an account of the issuer with available funds for the transaction,” and the issuer then sends a message indicating authorization success or failure. *Id.* (citing Ex. 1011 ¶¶ 60–63; Ex. 1005 ¶¶ 246, 249–250).

Petitioner asserts that a person of ordinary skill in the art “would have been motivated to combine Osborne and Purves . . . because both references are directed to similar applications, including the use of virtual wallets and credentials, and because the teachings of Purves would be recognized as

useful to add new credentials to the digital wallet of Osborne’s PPT apparatus (for example, where a user had not yet added any credentials, or where adding further credentials were desired).” IPR487, Pet. 35 (citing Ex. 1005 ¶ 295).

Patent Owner argues that “Claims 23–26 and 28–33 require, either directly or through dependency, the ‘processor’ of Claim 21 to further ‘request the credential from the issuing agency.’” PO Resp. 48 (citing Ex. 1001, 24:9–27, 24:33–52; IPR487, Pet. 34). Patent Owner contends that Petitioner fails to teach a rationale to combine Purves’ payment account retrieval with Osborne, in view of the reliance on Purves’ teaching of the claimed “request” by “retriev[ing] the user’s ‘payment account information from the payment account issuer.’” *Id.* at 48–49 (citing IPR487, Pet. at 37, 47–48). Patent Owner asserts that Petitioner argues that it would have been obvious to combine the references because both references are directed to similar applications, but that is not enough to demonstrate a motivation to combine. *Id.* at 49 (citing IPR487, Pet. 35; *Securus Techs. Inc. v. Glob. Tel*Link Corp.*, 701 F. App’x 971, 977 (Fed. Cir. 2017)). Patent Owner also asserts that Petitioner generically argues that “the teachings of Purves would be recognized as useful to add new credentials to the digital wallet of Osborne’s PPT apparatus,” but that does not explain why the specific addition of Purves alleged “request [for] the credential from the issuing agency” would be useful to the specific embodiment in Osborne that Petitioner relies on for this claim. *Id.* at 49–50 (citing *Sisvel Int’l S.A. v. Sierra Wireless, Inc.*, 82 F.4th 1355, 1364 (Fed. Cir. 2023)). Patent Owner

further argues that Dr. Shamos’ testimony does not provide any evidentiary support. *Id.* at 50 (citing IPR487, Pet. 35; Ex. 1005 ¶ 295).⁹

Petitioner has provided sufficient articulated reasoning to support the rationale for the combination of Osborne and Purves for the teaching of the limitation “requesting the credential.” As Petitioner points out (Pet. Reply 15), in the discussion of claim 23, the Petition refers to claim 22, which requires “generat[ion] of the credential.” IPR487, Pet. 37; *see also* Ex. 1005 ¶ 301. That discussion explains that a person of ordinary skill in the art would be motivated to combine Osborne and Purves because “the teachings of Purves would be recognized as useful to add new credentials to the digital wallet of Osborne’s PPT apparatus (for example, where a user had not yet added any credentials, or where adding further credentials were desired).” IPR487, Pet. 35 (citing Ex. 1005 ¶ 295). Dr. Shamos testifies that the credential that Purves teaches is a new gift card or reloadable prepaid card. Ex. 1005 ¶ 294 (citing Ex. 1013 ¶ 83). The Petition explains that a person of skill “would generate the new credential,” as Purves teaches that a customer may obtain a new gift card or prepaid card. IPR487, Pet. 37 (citing Ex. 1013 ¶ 83). Dr. Shamos testifies that “when the processor determines that no matching credential is stored” “a new credential would be generated because “the purpose of Osborne’s tokens is to represent a credential” and “by generating the new credential, the user becomes able to benefit from

⁹ We note that Patent Owner does not assert that there would be any security concerns with the combination of Osborne and Purves under this ground, which is based on the Purves’ embodiment concerning requests for a gift card or prepaid card credential. *See* PO Resp. 48–50.

Oborne's tokenization system, and if the credential was already stored, there would be no reason to generate it, since it would already exist." Ex. 1005 ¶ 298. For claim 23, which "requests the credential from the issuing agency," Dr. Shamos further testifies that "when new credentials were generated upon user request, such as the gift and prepaid cards taught by Purves. . . , it would be natural for the issuer to store such new credentials, at least until they were sent to the recipient, and more practically for as long as they remained valid, so that the issuer's system would confirm their existence and validity." *Id.* ¶ 304.

Patent Owner does not present any arguments challenging the sufficiency of Petitioner's showing as to claim 22. As explained for claim 22, Petitioner relies upon Purves to teach the generation of a credential like a gift card or reloadable prepaid card, which would be useful to have as a credential in Osborne, and Patent Owner does not dispute this rationale. IPR487, Pet. 35; *see generally* PO Resp. As Petitioner also explains, a user would want to store credentials like a gift card or reloadable prepaid card in Osborne's PPT, at least until they were sent to the recipient, "and more practically for as long as they remained valid, so that the issuer's systems could confirm their existence." IPR487, Pet. 38. As Dr. Shamos testifies, this is taught by Purves' disclosure of retrieving the user's "payment account information from the payment account issuer," with user's consent, and the issuer responding with information for data for establishing a virtual wallet including a "payment account in a virtual wallet." *See* Ex. 1005 ¶ 301 (citing Ex. 1013 ¶¶ 83, 107–108 ("The user may then indicate that they desire to add a new payment account to their virtual wallet")). Accordingly,

Petitioner provides sufficient motivation for the combination of Osborne and Purves for requesting the credential in order to have the desired storage of a credential. Thus, we find that based on the evidence and analysis above, Petitioner has demonstrated that the combination of Osborne and Purves teach the limitations of claim 23 with articulated reasoning to support the rationale for the combination.

Patent Owner does not present any arguments specifically related to claims 3, 22, 24–26, and 28–33. *See generally* PO Resp.

We have reviewed the argument and evidence provided and conclude that Petitioner has met its burden to show, by a preponderance of the evidence, that claims 3, 22–26, and 28–33 would have been obvious over Osborne and Purves.

E. Obviousness of Claims 1, 2, 4–18, 20, 21, and 27 over Osborne and Neafsey

Petitioner asserts that claims 1, 2, 4–18, 20, 21, and 27 would have been obvious over the combination of Osborne and Neafsey. Pet. 43–52; IPR487, Pet. 45–47. Patent Owner asserts that Petitioner fails to demonstrate that the combination of Osborne and Neafsey teaches the limitations of claims 1, 2, 7, 8, 12, 13, and 20. *See* PO Resp. 34–47.

Neafsey discloses the use of different forms of representations of virtual credentials in transactions. Ex. 1015 ¶ 61. The forms include optically-scannable codes, such as QR codes and bar codes. *Id.* Petitioner asserts that one of ordinary skill in the art would have been motivated “to incorporate an [Neafsey’s] optically-scannable code into an OVER file to be used to trigger the use of tokens to purchase goods, in a manner similar to

Oborne’s disclosure of using NFC or mag stripe interactions” because the scannable codes serve similar roles and would have been the simple substitution of known elements. Pet. 44 (citing Ex. 1005 ¶¶ 317–318).

As discussed above, we have determined that Osborne alone teaches the limitations of claims 1, 4–6, 8–14, 21, and 27, and Petitioner similarly relies upon Osborne’s teachings with the use of Neafsey’s scannable codes (Pet. 44–52), which we find sufficiently teaches the limitations of the claims with sufficient reasoning provided for a combination of the references.

We have also reviewed the Petition’s argument and evidence provided for the obviousness of claims 15–18, 21, and 27. Claim 15, similar to claim 1, recites that the OVER file that comprises a virtual representation “has been verified by an issuing agency to be an official representation of the credential.” As discussed above, Patent Owner disputes that Osborne teaches this claim limitation, but for the reasons discussed, *supra* Section II.C.2.d, we find that Petitioner has provided sufficient supporting evidence for the teaching of this limitation. Petitioner relies upon Neafsey combined with Osborne for the teaching of the limitation “displaying a portion of the OVER file” in claim 15, wherein Neafsey’s scannable code would involve display of a portion of the OVER file for verification, which Patent Owner does not dispute. *See* Pet. 47; *see generally* PO Resp. Patent Owner also does not present any arguments specifically related to claims 16–18, 21, and 27 (*see generally* PO Resp.). We find that Petitioner sufficiently demonstrates that the combination of Osborne and Neafsey renders these claims obvious.

For claim 2, Petitioner only relies upon Neafsey for the teaching of optically-scannable QR code in place of Osborne’s teaching of an NFC.

Pet. 44–45. As discussed above, we find that Osborne’s teaching are insufficient to teach the limitations of claim 2 and Neafsey fails to cure that deficiency. For claim 7, Petitioner similarly relies on Neafsey only for the teaching of QR code (*id.*), and, again, Neafsey fails to cure the deficiencies of Osborne’s teachings. Claim 20 recites a similar limitation to claim 7, and for the reasons discussed above for claim 7, we find that Petitioner has not sufficiently demonstrated that claim 20 is obvious.

Weighing the record as a whole in view of the findings and analysis above, we conclude that Petitioner has met its burden to show, by a preponderance of the evidence, that claims 1, 4–6, 8–18, 21, and 27 would have been obvious over the combination of Osborne and Neafsey, and has not met its burden to show that claims 2, 7, and 20 would have been obvious over this combination.

F. Obviousness of Claims 1, 3–5, 7–16, 18–26, and 28–33 over Stafford and Purves; Obviousness of Claims 2, 6, 17, and 27 over Stafford, Purves, and Neafsey

Petitioner contends that claims 1, 3–5, 7–16, 18–26, and 28–33 would have been obvious over the combination of Stafford and Purves and claims 2, 6, 17, and 27 would have been obvious over the combination of Stafford, Purves, and Neafsey. Pet. 54–81; IPR487, Pet. 48–75. To support its contentions, Petitioner provides explanations as to how the combination of the prior art teaches each claim limitation and provides rationale to combine the references. *Id.* Patent Owner asserts that the claims are not obvious under this ground. PO Resp. 51–67. Patent Owner alleges that the

combination of Stafford and Purves fails to teach certain limitations and Petitioner fails to establish a rationale to combine the references. *Id.*

We begin our discussion with a brief summary of Stafford and then address the arguments and evidence.

1. Stafford (Ex. 1012)

Stafford is directed to “a system . . . for storing, validating, and disseminating credential information about an entity.” Ex. 1012, code (57). Stafford’s system “generates data representing at least part of the credential information and a data representation of at least part of a document supporting that information and stores the credential information and data representation in a database . . . in an encrypted form.” *Id.* Figure 2, reproduced below, depicts “a flow chart illustrating a process for preparing information for release to a third party in an embodiment of the present invention.” *Id.* ¶ 31.

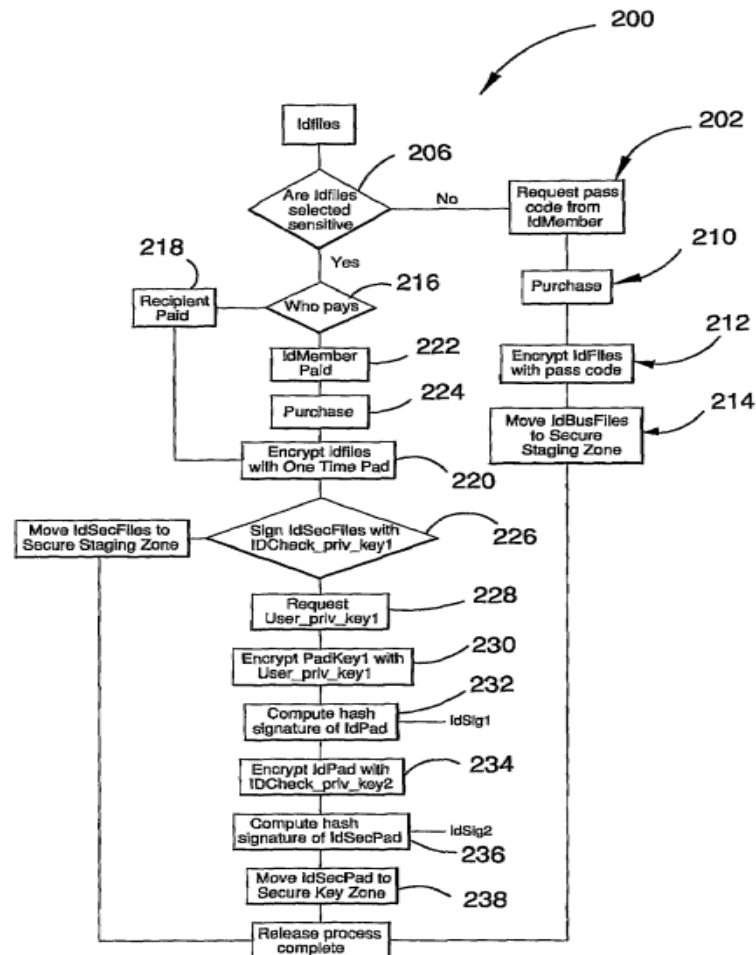


FIGURE 2

Figure 2, above, “shows a flowchart of a method of releasing credential information stored in the Secure [Z]one (120) to a party (called the recipient).” Ex. 1012 ¶ 73. Specifically, Figure 2 details the steps of process 200 for releasing securely stored credential information from the Secure Zone to a Secure Staging Zone where the credential can be released to the entity that owns the credential information or another recipient. *Id.* ¶¶ 40, 84, 85, 103–106. The process starts by digitally signing original files,

and additional steps are used to secure information that contains sensitive information. *Id.* ¶¶ 86–88, 93–105. For sensitive information, “a highly secure symmetric or similar encryption process” is used that employs one-time pads and hash values. *Id.* ¶¶ 88, 102–106.

Figure 3, reproduced below, depicts a method of transmitting released data to a third party in an embodiment of the invention. Ex. 1012 ¶ 32.

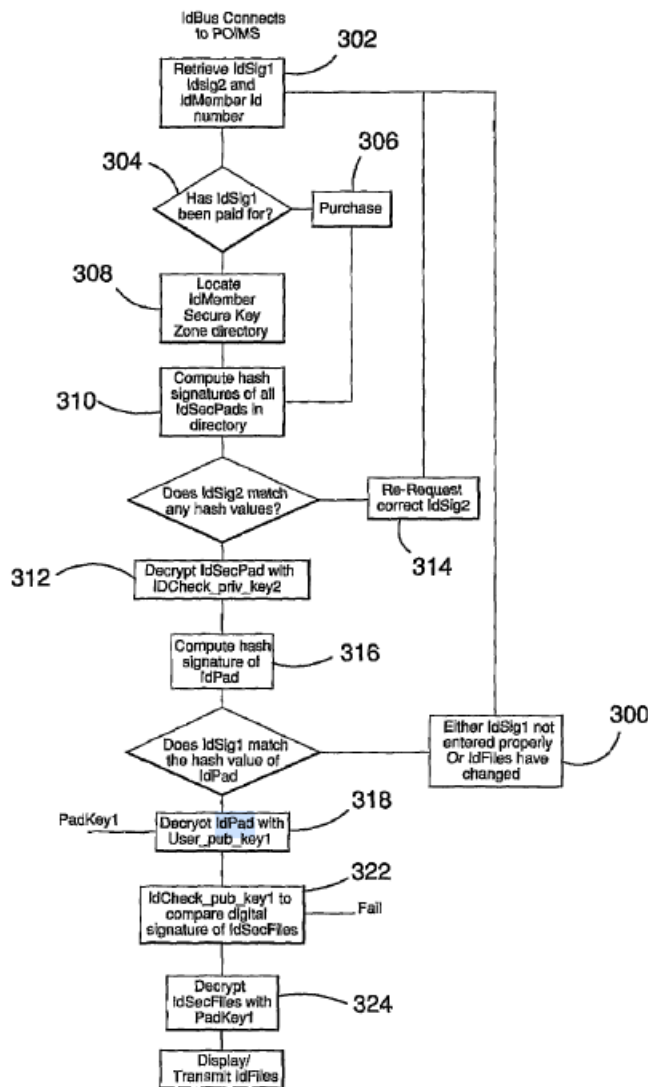


FIGURE 3

Figure 3, above, shows the steps for allowing a third party to obtain secured credentials. Ex. 1012 ¶¶ 107–125.

1. Analysis

a. Petitioner's Contentions

Petitioner asserts that limitation [1.3] is taught by Stafford, in combination with Purves, because it teaches an OVER engine that generates an OVER file comprising a virtual representation of the credential that the has been verified by an issuing agency, where Stafford's hash value "acts as a virtual credential representation of the stored credential, derived based on the information associated with the credential." Pet. 61 (citing Ex. 1005 ¶ 364). Petitioner argues that "[t]he key signatures Stafford's system generates to release sensitive files can comprise hash values (IdSig1 and IdSig2) provided to the user." *Id.* (citing Ex. 1012 ¶¶ 97–99). Petitioner contends that:

The release of the credential is authorized by comparing the hash values to the IdSecPad and IdPad corresponding to the credential to determine if they match. [Ex. 1012 ¶¶ 166–122]. *A hash value thus acts as a virtual credential representation of the stored credential, derived based on the information associated with the credential, so generating the hash values or similar key signature corresponds to the step of generating the OVER file.* Ex. 1005 ¶ 364.

Pet. 61 (emphasis added).

Petitioner argues that "Stafford teaches that its encrypted credentials may be verified by the issuer and may include storing an image of the credential (e.g., a scanned copy)." Pet. 61 (citing Ex. 1012 ¶¶ 62, 65, 67). Petitioner asserts, however, that to the extent that Stafford does not expressly teach that the key signature files include a virtual representation verified by

the issuing agency, Purves would teach the verification. *Id.* at 61–62 (citing Ex. 1005 ¶ 365).

Petitioner contends that Purves teaches that a user device “may be sent an image of a credential such as a credit card, to conveniently represent a real credential,” where confidential information may be obscured. Pet. 62 (citing Ex. 1013 ¶¶ 102, 108–109, 122). Petitioner asserts that this card image is from an issuer. *Id.* (citing Ex. 1013 ¶ 85). Petitioner argues that the “representative image provided ‘from an issuer’ would be *verified by the issuing agency to be an official representation*, as would an image produced from an actual credential, since an actual credential naturally represents itself.” *Id.* (citing Ex. 1005 ¶ 366).

Petitioner asserts that, in view of Purves’s teaching to provide user devices with images representing a credential, “it would have been obvious to use similar images in the context of Stafford.” Pet. 62. Petitioner argues that providing “an image of the user’s credential (e.g., a generally-representative, issuer-provided image or a real image of the credential with optionally-obscured confidential information) along with the encoded key signature” would “remind users which credential the key signature represents and enable quick selection from among a plurality of options available on the user’s device.” *Id.* (citing Ex. 1013 ¶¶ 85, 122). Petitioner contends that this image would be “a virtual representation verified by the issuer as being an official representation of the credential.” *Id.* at 62–63 (citing Ex. 1005 ¶ 367).

According to Petitioner, a person of ordinary skill in the art “would have recognized various benefits from incorporating Purves’s credential

images into Stafford’s system,” such as “the images would improve ease-of-use and reduce user error by providing users images matching the credentials the user seeks to provide to third parties.” Pet. 56 (citing Ex. 1005 ¶ 355).

Petitioner additionally argues that it would have been obvious to a person of ordinary skill in the art to generate a QR code to convey the key signature. Pet. 63. Petitioner contends that Purves teaches that a QR code may be used to trigger a wallet connection or login, and a QR code scan could be used in place of a physical credential swipe or interaction. *Id.* (citing Ex. 1015 ¶ 61; Ex. 1016, 12; Ex. 1005 ¶ 369). Petitioner asserts that “it was known that QR codes could be used as a virtual stand-in for a credential.” *Id.* Petitioner argues that it would have been obvious to use a QR code, as Purves teaches, “to encode Stafford’s key signature, as doing so would allow the user to more easily transmit the key signature to a third party using a QR code scan.” *Id.* (citing Ex. 1005 ¶ 369). Petitioner asserts that a person of ordinary skill in the art “would have viewed Purves’s QR codes as a convenient way to convey key signatures to third parties in a more efficient and reliable manner than reading or typing a code manually, both of which are slow and error-prone.” *Id.* at 56.

b. Analysis

Limitation [1.3] requires the generation of an “OVER file comprising a virtual representation of an original credential of a user that has been verified by an issuing agency to be an official representation of the credential, based on the information associated with the original credential.” Ex. 1001, 21:24–28.

Petitioner relies on Stafford to teach the “OVER engine” which uses its system to generate a “virtual representation of the original credential.” Pet. 61–63. In Stafford’s system, when IdMember selects information for release to a third-party recipient, and that information is prepared for release, IdMember receives two key signatures, IdSig1 and IdSig2. Ex. 1012 ¶¶ 84–105. IdMember can either copy IdSig1 and IdSig2 from the display, or IdSig1 and IdSig2 can be sent in an email. *Id.* ¶¶ 97, 99; *see* Pet. 60. Then, when the third-party recipient makes a request for the information, IdMember provides IdSig1 and IdSig2 to the third-party recipient, to be used for the request. Ex. 1012 ¶¶ 106, 107, 113, 115. Petitioner asserts that Stafford’s hash value “acts as a virtual credential representation of the stored credential” and is “derived based on the information associated with the credential, so generating the hash values or similar key signature corresponds to the step of generating the OVER file.” Pet. 61 (citing Ex. 1005 ¶ 364).

As an initial matter, we do not find that Stafford teaches that its OVER engine generates a “virtual representation of the original credential.” As discussed in the Institution Decision (Dec. 37–39), we preliminarily found that Stafford discloses that the hash values IdSig1 and IdSig2, which are components of the key signature, and which are asserted to be the claimed “virtual representation” by Petitioner, are not based on information associated with the credential. On the complete record, as Patent Owner argues and we agree, Stafford teaches that both IdSig1 and IdSig2 are hashes derived from a One Time Pad and are not based on information associated

with a credential. PO Resp. 52–54 (citing Ex. 1012 ¶¶ 47–48, 94–103, Fig. 2; Ex. 2009 ¶¶ 139–148); PO Sur-reply 16–19.

In Reply, Petitioner asserts that the claims “do not impose content or formatting requirements on the virtual representation” and that Patent Owner’s witness, Dr. Malek, admitted that a “virtual representation” need not depict the credential or have a particular format. Pet. Reply 17 (citing Ex. 1047, 31:25–34:5). Petitioner also asserts that a “representation” does not have to look like or include the content of the thing it represents, and, for instance, “a coat-check ticket ‘represents’ the coat even though it does not look like or describe the coat.” *Id.* (citing Ex. 1048 ¶¶ 9–10). Petitioner further asserts that Stafford’s key signatures are generated based on information associated with the original credential because “[t]hey are derived as a result of a request to release the credential information” and are “tied to the credential information and facilitate its release.” *Id.* at 18. Petitioner argues that “OTP [One Time Pad], IdPad, IdSecPad, and the private key are all information ‘associated’ with the credential due to their association with the credential in the release process and in the system’s datastores.” *Id.* at 18–19.

Although we agree with Petitioner that “the virtual representation of the credential” does not have to have certain formatting or be a visual representation of the credential itself, the virtual representation nevertheless has to be based on information associated with the original credential, that is, as the claim recites, it must be a “virtual representation of an original credential.” *See* Ex. 1001, 21:24–28. We do not agree with Petitioner’s arguments that Stafford’s key signatures “represent” a credential like a coat

check ticket “represents” a coat or, alternatively, that key signatures are representative of the original credential by virtue of being derived as a result of a request. As discussed above, a key signature is developed independently from the credential (i.e., is a hash value of a One Time Pad), and although it allows a user to release a stored credential, like a coat check ticket allows a user to retrieve a coat, there is nothing in the key signatures in Stafford that is based on information associated with the original credential. We find more persuasive Patent Owner’s comparison of the key signatures to a stamp on an envelope, where the stamp is not based on anything inside the envelope. *See* PO Sur-reply 18. Further, as pointed out by Patent Owner, Stafford discloses that the private keys, which the key signatures are based upon, are not associated with any credential, but rather a user can access any of multiple credentials. *Id.* at 18–19; Ex. 1012 ¶¶ 68–69, 94. Dr. Shamos agrees with this. *See* Ex. 2027, 9:12–22, 18:4–7; 33:22–33:9. Accordingly, Petitioner has not carried its burden to demonstrate that Stafford teaches an OVER engine that generates a “virtual representation of an original credential . . . based on information associated with the original credential of the user.”¹⁰

¹⁰ In Reply, Petitioner argues that Purves “credential image” should be considered to teach the “virtual representation” that is “based on information associated with the original credential of the user.” Pet. Reply 18. We agree with Patent Owner that the Petition relies on Stafford to teach a “virtual representation” that is “based on information associated with the original credential of the user” and on Purves to teach a “virtual representation” that has been “verified by an issuing agency.” PO Sur-reply 16; Pet. 61–62. However, even assuming Petitioner relies on the

Petitioner has also not shown that Stafford teaches “a virtual representation of an original credential that has been verified by an issuing agency.” As discussed above in Section II.C.2, the claim language requires that the issuing agency has verified the OVER file comprising a virtual representation of the original credential. Petitioner asserts that Stafford’s “request [third-party OVER file verifying device request for the release of information] includes the key signatures that are used to verify that an *OVER file* (encoding the signatures) authenticates the user, as only if the key signatures match the hash values of the encrypted credential file are the credential files transmitted.” Pet. 64–65 (citing Ex. 1012 ¶¶ 119–122; Ex. 1005 ¶ 372) (emphasis omitted). Petitioner argues that “Stafford teaches that its encrypted credentials may be verified by the issuer and may include storing an image of the credential (e.g., a scanned copy).” *Id.* at 61 (citing Ex. 1012 ¶¶ 62, 65, 67).

Petitioner’s argument that Stafford’s encrypted credentials may be verified only addresses that the encrypted credential may be verified by the issuing agency, not that the key signatures, which are the alleged virtual representation, have been verified by the issuing agency. Pet. 61–62. Petitioner does not provide further argument or explanation as to whether or how Stafford’s key signatures are verified by an issuing agency. *See id.* Apparently recognizing this deficiency, Petitioner relies on the combination

combination of Stafford and Purves, as discussed below, Petitioner’s explanation of the combination of Stafford and Purves is unclear, and we further find that Petitioner has not established a motivation to combine Stafford and Purves.

with Purves. *See id.* (arguing that “to the extent that Stafford does not expressly teach that the key signature files sent to the user include a virtual representation *verified by the issuing agency*, this aspect of the claim is met by Purves”).

We agree with Patent Owner that Petitioner has not sufficiently established that a person of ordinary skill in the art would have been motivated to combine Stafford and Purves. *See* PO Resp. 60–67; PO Sur-reply 23–28. Specifically, Petitioner does not articulate sufficiently how the teachings of Stafford and Purves would have been combined, or why such a combination would have been desirable to one of ordinary skill in the art at the time of the invention.

Petitioner’s explanation of the combination of Stafford and Purves lacks clarity, as will be further discussed below. *See Sisvel*, 82 F.4th at 1364 (stating “we cannot fault the Board for being at a loss in trying to decipher Cross-Appellants kitchen-sink of unclear and confusing motivation-to-combine arguments”); Pet. 48–50, 59–60. “Ultimately, it is the petitioner’s burden to present a clear argument.” *See Netflix Inc. v. DivX, LLC*, 84 F.4th, 1371, 1377 (Fed. Cir. 2023); *see also Intelligent Bio-Sys. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1369 (Fed. Cir. 2016). Nonetheless, we will set forth our understanding of Petitioner’s proposed combination.

Petitioner takes Stafford’s teaching of key signatures (which includes hash values), and asserts that it would have been obvious to further provide an image of the user’s credential along with the encoded key signatures, based upon Purves’s teachings. Pet. 62–63. Petitioner argues that “the [combined] system would provide an image of the user’s credential . . .

along with the encoded key signature to remind users which credential the key signature represents and enable quick selection from among a plurality of options available on the user's device." Pet. 62 (citing Ex. 1013 ¶¶ 85, 122; Ex. 1005 ¶ 367); *see also* Pet. 56 (citing Ex. 1005 ¶ 355) (arguing that "the images would improve ease-of-use and reduce error by providing users images matching the credentials the user seeks to provide to third parties"). Additionally, Petitioner also modifies Stafford's system to use scannable code formats such as QR, as taught in Purves, in place of a physical swipe or interaction, and to "allow the user to more easily transmit the key signature to a third party using a QR code scan." *Id.* at 63 (citing Ex. 1005 ¶ 369).

Therefore, Petitioner proposes providing the user with Stafford's key signatures in a scannable format, such as a QR code, and also providing the user with an image of the credential associated with the key signatures. In other words, under Petitioner's apparent theory, the user would be provided with two virtual representations of the credential, i.e., key signatures in a scannable code format and an image of the credential. *See* Pet. 61 ("[a] hash value acts as a virtual representation of the stored credential"), 55 (stating that "Purves teaches providing issuer-verified representations of credentials"), 62 (stating that "Purves's teaching . . . provide[s] user devices with images representing a credential"). Further, under Petitioner's theory, the scannable key signatures would be transferred from the user to the recipient so that the information can be released. The user (IdMember) would presumably use the image of the credential to select the appropriate scannable key signature.

We recognize the application of “an expansive and flexible approach” to the question of obviousness. *KSR Int’l Co. v. Teleflex, Inc.*, 550 U.S. 398, 415 (2007). However, we “must still be careful not to allow hindsight reconstruction of references . . . without any explanation as to *how* or *why* the references would be combined to produce the claimed invention.” *Kinetic Concepts, Inc. v. Smith & Nephew, Inc.*, 688 F.3d 1342, 1368 (Fed. Cir. 2012) (emphases added). Although Stafford discloses that the key signatures may be copied from the display or delivered to the user via email, Petitioner does not expand upon whether the user would also copy the image from the display, whether the image would be provided via email as well, or provide any other explanation other than that the image credential would be provided with the scannable key signatures. Ex. 1012 ¶¶ 97, 99; Pet. 62–63. Nor does Petitioner address whether the QR code would be provided to the user in a similar manner. *See* PO Resp. 60–61. Although a credential image would presumably need to be retrieved or generated in some manner, and associated with the key signatures in some manner, Petitioner also does not sufficiently explain how this would work in the proposed combination, or how the user would transmit the scannable key signature to the recipient.¹¹ Although proof of physical or bodily

¹¹ Dr. Shamos’ testimony that “[t]he user then presents the QR code image to the third-party recipient for scanning . . . according to well-known QR-code-scanning techniques” appears inconsistent with the ecommerce example relied upon in Stafford. Ex. 1048 ¶ 43; *see* Ex. 1012 ¶ 74 (“In the exemplary embodiment, the system 100 has a web interface through which entities and recipients of data may interact with the system to store, administer, release and obtain verified credential data”), ¶ 106 (“ecommerce

incorporation is not required, a satisfactory explanation of “*how* the combination of the . . . references [is] supposed to work” is necessary to support “a conclusion that a relevant skilled artisan would have been motivated to make the combination and reasonably expect success in doing so.” *Personal Web Techs., LLC v. Apple, Inc.*, 848 F.3d 987, 994 (Fed. Cir. 2017); *see also TriVascular, Inc. v. Samuels*, 812 F.3d 1056, 1066 (Fed. Cir. 2016) (finding no error where the Board required petitioner to explain how a person of ordinary skill in the art would have implemented petitioner’s proposed substitution). Petitioner fails to provide “a clear, evidence-supported account of the contemplated workings” of the proposed combination of Stafford and Purves. *See Personal Web*, 848 F.3d at 994.

Petitioner argues that Stafford suggests that other information may also be included with its key signatures, but relies on portions of Stafford relating to the recipient making a request for information, not on the portions of Stafford relating to the release process. *See, e.g.*, Pet. 55 (citing Ex. 1012 ¶¶ 106–113; 1005 ¶ 353); Pet. Reply 21 (citing Pet. 55–56, 63; Ex. 1005 ¶¶ 353–354; Ex. 1012 ¶¶ 106–113). Although we agree with Petitioner that Stafford teaches the user (i.e., IdMember) providing to the recipient (i.e., IdBus1) other information along with its key signatures, such as required information for a loan application, Petitioner does not sufficiently explain how this disclosure has any bearing on the combination with Purves, and providing the user (i.e., IdMember) with an image of the credential along

related activities”), ¶ 107 (stating that the example in Figure 3 “is applicable to situations such as when an IdMember (the entity) is using an online application form, such as an on-line loan application”).

with the optically-scannable coded key signatures during the release process. Dr. Shamos’s cited testimony also does not provide any further insight, and instead generally repeats the arguments in the Petition. *See* Ex. 1005 ¶¶ 353–354.

Petitioner argues that the combination provides images of the credentials and allows “quick selection” of the credential. Pet. 62 (citing Ex. 1005 ¶ 367). However, as Patent Owner points out, Stafford’s key signatures are created after the files (credentials) have been selected for release, so it is not clear how Purves’s credential images would assist in selecting credentials. PO Resp. 61; PO Sur-reply 23; *see* Ex. 1012 ¶¶ 84–105. Dr. Shamos provides testimony that, in Stafford, a user may “hold multiple sets of key signatures . . . [and] [u]sing images (rather than abstruse key signature character strings) *to identify/select particular items that were previously set up for release thus makes perfect sense.*” Ex. 1048 ¶ 33 (emphasis added); Pet. Reply 22–23. We agree with Dr. Shamos that Stafford discloses that a user may have multiple items set up for release, and therefore may have key signatures for each item that has been set up for release.¹² *See* Ex. 1048 ¶ 33; Ex. 1012 ¶¶ 74, 118. However, as discussed above, and further discussed herein, we find Petitioner lacks sufficient explanation as to the proposed combination, e.g., a user selecting or providing key signatures through the use of a credential image.

Petitioner does little more than identify Purves’s teaching of an image representing a credential and a QR code, and add these teachings to Stafford,

¹² It is undisputed that Stafford’s key signatures are used only one time. Pet. 59, 61; PO Resp. 52; PO Sur-reply 17; Ex. 2027, 14:9–13.

supplying a generic reason for the combination. *See In re Kahn*, 441 F.3d 977, 986 (Fed. Cir. 2006) (stating that “mere identification in the prior art of each element is insufficient to defeat the patentability of the combined subject matter as a whole”); *In re Kotzab*, 217 F.3d 1365, 1371, (Fed. Cir. 2000) (“[A] rejection cannot be predicated on the mere identification . . . of individual components of claimed limitations. Rather, particular findings must be made as to the reason the skilled artisan, with no knowledge of the claimed invention, would have selected these components for combination in the manner claimed.”). To that end, Petitioner’s proposed combination seems influenced by impermissible hindsight. *See Metalcraft of Mayville, Inc. v. The Toro Co.*, 848 F.3d 1358, 1367 (Fed. Cir. 2017) (“[W]e cannot allow hindsight bias to be the thread that stitches together prior art patches into something that is the claimed invention.”); *InTouch Techs., Inc. v. VGO Commc’ns, Inc.*, 751 F.3d 1327, 1351 (Fed. Cir. 2014) (criticizing use of the challenged patent as a “roadmap” for putting what the expert referred to as “pieces of a ‘jigsaw puzzle’” together).

Petitioner’s proffered reasons for the combination, i.e., to “improve ease-of-use and reduce error” by providing the credential images; and providing the key signatures as a scannable code to enable transfer in a “simple, reliable manner,” are not persuasive. We find these reasons to be generic and to lack the specificity that our precedent requires of a motivation to combine. *See, e.g., In re NuVasive*, 842 F.3d 1376, 1381–82 (Fed. Cir. 2016) (“[T]he factual inquiry whether to combine references must be thorough and searching, and the need for specificity pervades” (quotations omitted)); *In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364,

1380 (Fed. Cir. 2016) (“To satisfy its burden of proving obviousness, a petitioner cannot employ mere conclusory statements” and “must instead articulate specific reasoning, based on evidence of record . . .”).

Petitioner’s reasoning at best shows a generic benefit of providing a credential image or using a scannable code. *See* Pet. Reply 21 (stating that a person of ordinary skill in the art “would have been motivated to obtain known benefits from using credential images (e.g., convenience and error-reduction) and QR codes (e.g., convenience, efficiency, and reliability)”). However, we are not persuaded that these generic benefits would have motivated a person of ordinary skill in the art to make these modifications to Stafford. *See Belden Inc. v. Berk-Tek LLC*, 805 F.3d 1064, 1073 (Fed. Cir. 2015) (“[O]bviousness concerns whether a skilled artisan not only *could have made* but *would have been motivated to make* the combinations or modifications of prior art to arrive at the claimed invention.”) (emphasis added). As Patent Owner points out, Stafford proposes a number of safety measures as part of the key signature release process to protect sensitive information. PO Resp. 62–63 (citing Ex. 1012 ¶¶ 81, 93–106). For example, Stafford explains that “[a]dvantageously, embodiments of a key signature purchase process involves multiple controls to ensure that the release of sensitive information is intentional, secure and ensures data is delivered to the intended recipient.” Ex. 1012 ¶ 81.

The parties dispute whether the modifications to Stafford in view of Purves would compromise Stafford’s security. *See* PO Resp. 63–67; Pet. Reply 23–27; PO Sur-reply 25–28. Patent Owner generally argues that sending cards and QR codes “would open vulnerabilities in Stafford’s

system . . . defeating the purpose of using Stafford’s key signatures in the first place.” PO Resp. 62 (citing Ex. 2009 ¶¶ 165–170). According to Patent Owner, sending a real image of the credential “would allow attackers to easily intercept and steal valuable cardholder information.” *Id.* at 63 (citing Ex. 1005 ¶ 367; Ex. 2009 ¶ 166). Patent Owner further argues that even if the image obscured confidential information, it would still “create an undesirable and unnecessary risk.” *Id.* at 64–65 (citing Ex. 2009 ¶¶ 167–170). Additionally, Patent Owner argues that neither of Stafford’s delivery mechanisms for IdSig1 and IdSig2 (i.e., email or copying from the display) “would work with a QR code.” *Id.* at 66 (citing, e.g., Ex. 2009 ¶¶ 173–174, 176).

Petitioner, on the other hand, generally argues that using representative images “was conventional and viewed as sufficiently secure,” that Purves “teaches using an obscured image for sensitive credentials like credit cards,” and that “virtual wallets routinely displayed partially obscured account information and that irrecoverable image-obscuring was commonplace and readily achieved.” Pet. Reply 23–25 (citing, e.g., Ex. 1048 ¶¶ 34–36, Ex. 1013 ¶ 122). Petitioner further argues that “storing QR-encoded key signatures is just as secure as storing non-QR-encoded key signatures.” *See id.* at 25–26 (citing e.g., Ex. 1048 ¶¶ 40, 50–51). In addition, Petitioner argues that QR-code-mediated transfer of key signatures is more secure than manual entry of the key-signature characters, and that “Purves itself demonstrates the sufficient security of QR codes since it teaches using them for payment transactions.” *Id.* at 26 (citing e.g., Ex. 1048 ¶¶ 41, 52, 53; Ex. 1013 ¶ 64).

On balance, Petitioner’s generic benefits do not outweigh Patent Owner’s concerns as to the introduction of security vulnerabilities to Stafford’s system. PO Resp. 62–67; *see Winner Int’l Royalty Corp. v. Wang*, 202 F.3d 1340 (Fed. Cir. 2000) (stating that motivation to combine requires weighing the trade-offs of desirability: “the benefits, both lost and gained, should be weighed against one another”). In *Winner*, the court analyzed a district court’s reversal of the Board’s finding in an interference trial that there was sufficient motivation to combine four references at issue. *Winner*, 202 F.3d at 1349. The *Winner* court affirmed the district court, reasoning, in part, as follows:

First, although there was conflicting evidence before the district court on whether one would see the trade-off between using a dead-bolt and using a ratcheting mechanism and conclude that the more secure dead-bolt should be replaced with the more convenient ratcheting mechanism, *the district court did not clearly err in finding that one of ordinary skill in the art would not have reasonably elected trading the benefit of security for that of convenience*. Trade-offs often concern what is feasible, not what is, on balance, desirable. Motivation to combine requires the latter.

Winner, 202 F.3d at 1349 (emphasis added). Here, analogous to the situation in *Winner*, “one of ordinary skill in the art would not have reasonably elected trading the benefit of security for that of convenience.” Accordingly, we are not persuaded by Petitioner’s arguments that “significant benefits easily outweigh any corresponding security risk.” Pet. Reply 28 (citing Ex. 1048 ¶¶ 55–60).

We also find Dr. Malek’s testimony on this point more persuasive than Dr. Shamos’s testimony. *See* Ex. 2009 ¶¶ 165–170; Ex. 1048 ¶¶ 35–39;

Pet. Reply 27–28 (citing Ex. 1048 ¶¶ 55–60). For example, Dr. Shamos testifies that the combination’s use of obscured credential images would not “have risked exposure of the key signatures themselves since the image does not depict or otherwise convey the key signatures.” Ex. 1048 ¶ 37.

However, although Petitioner fails to sufficiently explain the proposed combination, as discussed above, presumably there is some relationship between the credential image and the key signatures, since the proposed combination purportedly allows for the user to identify items that were previously selected for release, in order to provide the relevant key signatures to the recipient. Pet. 62–63; Ex. 1005 ¶ 367; Ex. 1048 ¶ 33. In contrast, Dr. Malek testifies, and we agree, that providing an unencrypted image of a credit card, for example, would inform potential attackers of the payload of the credential that is being attempted to be securely transmitted which is a security vulnerability. Ex. 2009 ¶ 169. Although Dr. Shamos testifies that Purves teaches associating wallet items with obscured or representative images and that such representative images were routinely used in virtual wallets, Ex. 1048 ¶¶ 35, 38 (citing Ex. 1013 ¶ 85), we do not find this persuasive in the context of the proposed combination with Stafford’s system for securely storing, transmitting, and authenticating credential information relating to an entity, with use of key signatures. Ex. 2009 ¶ 160; Ex. 1012 ¶ 2.

Accordingly, Petitioner’s generic reasons for the proposed combination, coupled with Petitioner’s lack of specificity as to the proposed combination, leads us to determine that Petitioner’s reasons explaining why a person of ordinary skill in the art would have combined Stafford and

Purves are not persuasive in light of the teachings of those references and the testimonial evidence provided by Dr. Shamos, as discussed above. Further, as also discussed, the prior art fails to teach an “OVER engine” as claimed. Therefore, Petitioner has not established by a preponderance of the evidence that the claims 1, 15, and 21 are unpatentable over Stafford and Purves. We determine that Petitioner has not demonstrated by a preponderance of the evidence that claims 3–5, 7–14, 16, 18–20, 22–26, and 28–33, which depend from claims 1, 15, and 21, are unpatentable over Stafford and Purves. Further, we have reviewed Petitioner’s showing for the obviousness of claims 2, 6, 17, and 27 over Stafford, Purves, and Neafsey (Pet. 79–81), and the argument and evidence presented fail to remedy the deficiencies of the associated independent claims. Accordingly, we determine that Petitioner has not demonstrated by a preponderance of the evidence that claims 2, 6, 17, and 27, are unpatentable over Stafford, Purves, and Neafsey.

G. Obviousness of Claims 3, 19, 22–26 and 28–33 over Osborne, Purves, and Neafsey

Petitioner asserts that claims 3, 19, 22–26 and 28–33 would have been obvious over the combination of Osborne, Purves, and Neafsey. Pet. 52–54; IPR487, Pet. 47–48. Patent Owner argues that Petitioner fails to show that it would have been obvious to include an image in Osborne’s token under the assertions for claim 19. PO Resp. 47–48.

We have addressed the obviousness of claims 3, 22–26 and 28–33 over Osborne and Purves, *supra* Section II.D, and held these claims unpatentable. We need not further address these claims under this ground.

Claim 19 depends from claim 15, and further recites “wherein when the OVER file comprises a credential image.” Ex. 1001, 23:21–22. The Petition relies upon Purves, and its image of a credit card, for the teaching of a “credential image.” Pet. 53 (citing Ex. 1013 ¶¶ 39, 85). Petitioner asserts that “the credential image may be a card image including account information (or a virtual simulation of such an image), optionally with sensitive information obscured.” *Id.* (citing Ex. 1013 ¶¶ 81, 112; Ex. 1005 ¶¶ 73–74, 342–344). Petitioner argues that Osborne, Purves, and Neafsey each provide complementary teachings on virtual credentials and a person of ordinary skill in the art “would have been motivated to combine Purves’s disclosure regarding providing credential images with Osborne and Neafsey’s virtual credentials to include a credential image as part of an OVER file also including a token as taught by Osborne and a scannable code as taught by Neafsey to provide an improved interface for users with a simple visual indication of the credentials to be invoked in a tokenized transaction.” *Id.* at 53–54 (citing Ex. 1005 ¶¶ 345–346).

Patent Owner contends that, as with the Stafford-Purves ground, Petitioner does not address security concerns in providing a credential image to a user’s device, so the combination of Osborne, Purves, and Neafsey combination for this claim fails for the same reasons as the Stafford-Purves combination. PO Resp. 48 (citing Pet. 53–54; Ex. 2016, 109:11–12). Petitioner replies that “as explained [] for the Stafford grounds, sending credential images does not create security problems.” Pet. Reply 14.

Here, Petitioner makes similar assertions to those discussed for the Stafford-Purves combination discussed *supra* Section II.F, but using

Oborne's token, that is: providing Purves' credential images with Osborne and Neafsey's virtual credentials to include a credential image as part of an OVER file also including a token as taught by Osborne and a scannable code as taught by Neafsey. This proposed combination suffers from the same deficiencies in Petitioner's reasoning provided to explain why a person of ordinary skill would have made this combination, as discussed for the Stafford-Purves ground, *supra* Section II.F. We therefore determine that Petitioner has not demonstrated by a preponderance of the evidence that claim 19 is unpatentable over Osborne, Neafsey, and Purves.

III. CONCLUSION¹³

The outcome for the challenged claims of this Final Written Decision follows. In summary:

¹³ 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).

Claim(s)	35 U.S.C. §	Reference(s) /Basis	Claim(s) Shown Unpatentable	Claim(s) Not Shown Unpatentable
1, 2, 4–14, 21, 27	103(a)	Oborne	1, 4–6, 8–14, 21, 27	2, 7
3, 22–26, 28–33	103(a)	Oborne, Purves	3, 22–26, 28– 33	
1, 2, 4–18, 20, 21, 27	103(a)	Oborne, Neafsey	1, 4–6, 8–18, 21, 27	2, 7, 20
3, 19, 22– 26, 28– 33 ¹⁴	103(a)	Oborne, Neafsey, Purves		19
1, 3–5, 7– 16, 18–26, 28–33	103(a)	Stafford, Purves		1, 3–5, 7–16, 18–26, 28–33
2, 6, 17, 27	103(a)	Stafford, Purves, Neafsey		2, 6, 17, 27
Overall Outcome			1, 3–6, 8–18, 21–33	2, 7, 19, 20

IV. ORDER

Accordingly, it is:

ORDERED that claims 1, 3–6, 8–18, and 21–33 of the '531 patent have been shown to be unpatentable and claims 2, 7, 19, and 20 of the '531 patent have not been shown to be unpatentable; and

FURTHER ORDERED that, because this is a Final Written Decision, the 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.

¹⁴ We have determined that claims 3, 22–26, and 28–33 are unpatentable under the Osborne-Purves ground, so these claims are not addressed in this ground.

IPR2024-00486
Patent 9,251,531 B2

PETITIONER:

Matthew Argenti
Michael Rosato
Patrick Medley
Joseph Baillargeon
WILSON SONSINI GOODRICH & ROSATI
margenti@wsgr.com
mrosato@wsgr.com
pmedley@wsgr.com
jbaillargeon@wsgr.com

PATENT OWNER:

Michelle Armond
Douglas Wilson
Patrick Maloney
Yue Han
ARMOND WILSON LLP
michelle.armond@armondwilson.com
doug.wilson@armondwilson.com
patrick.maloney@armondwilson.com
amy.han@armondwilson.com

EXHIBIT 2

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

VISA, INC.,
Petitioners,

v.

CORTEX MCP, INC.,
Patent Owner.

IPR2024-00486 (Patent 9,251,531 B2)¹
IPR2024-00489 (Patent 10,749,859 B2)
IPR2024-00490 (Patent 11,329,973 B2)

Before KALYAN K. DESHPANDE, *Acting Chief Administrative Patent Judge*, MICHAEL W. KIM, *Vice Chief Administrative Patent Judge*, and JEFFREY W. ABRAHAM, *Acting Vice Chief Administrative Patent Judge*.

DESHPANDE, *Acting Chief Administrative Patent Judge*.

DECISION

Delegated Director Review of
Final Written Decision Determining All Challenged Claims Unpatentable
37 C.F.R. § 42.75

¹ IPR2024-00487 has been consolidated with IPR2024-00486. This Decision applies to each of the above-listed proceedings.

IPR2024-00486 (Patent 9,251,531 B2)
IPR2024-00489 (Patent 10,749,859 B2)
IPR2024-00490 (Patent 11,329,973 B2)

A. INTRODUCTION

Visa, Inc. (“Petitioner”) filed a Petition requesting *inter partes* review of claims 1–20 (“the challenged claims”) of U.S. Patent No. 9,251,531 B2 (Ex. 1001, “the ’531 patent”). Paper 2 (“Pet.”).² On August 2, 2024, the Board instituted *inter partes* review as to all challenged claims and all asserted grounds of unpatentability. Paper 8. Following institution, Cortex MCP, Inc. (“Patent Owner”) filed a Response (Paper 14, “PO Resp.”), Petitioner filed a Reply (Paper 18, “Pet. Reply”), and Patent Owner filed a Sur-reply (Paper 26, “PO Sur-reply”). At the conclusion of trial, the Board issued a Final Written Decision determining that (a) Petitioner had met its burden of showing, by a preponderance of the evidence, claims 1, 3–6, 8–18, and 21–33 unpatentable, and (b) Petitioner failed to meet its burden in showing claims 2, 7, 19, and 20 unpatentable.³ Paper 31 (“Dec.”).

Patent Owner filed a Request for Director Review seeking to reverse the Board’s Final Written Decision with respect to claims 1, 3–6, 8–18, and 21–33 (Paper 32 “Req.”), and Petitioner filed a Response to the Request for Director Review (Paper 33). The Director delegated review to a Delegated Rehearing Panel to determine whether the Board panel misapprehended or overlooked any issue⁴, including (1) whether the Board failed to meaningfully evaluate the parties’ claim construction positions as to the

² Citations are to the record in IPR2024-00486. The parties filed similar papers in IPR2024-00489 and IPR2024-00490 presenting similar issues.

³ The Final Written Decision addressed claims 1–20 challenged in IPR2024-00486 and claims 20–33 challenged in IPR2024-00487.

⁴ We reviewed whether the Board panel misapprehended or overlooked any issue as instructed in the Director’s Order. DRP Order 3.

IPR2024-00486 (Patent 9,251,531 B2)
IPR2024-00489 (Patent 10,749,859 B2)
IPR2024-00490 (Patent 11,329,973 B2)

disputed limitation; (2) whether the Board advanced its own theory of unpatentability as to Osborne; and (3) whether Petitioner established that Osborne discloses or teaches the disputed limitation based on the arguments and evidence the parties presented during trial. Paper 34 (“DRP Order”). Having reviewed the entire record, we conclude that the Board panel did not misapprehend or overlook any issue that was previously addressed in papers filed with the Board, in determining that the challenged claims were unpatentable. We therefore deny Patent Owner’s request.

B. BOARD ANALYSIS

1. Whether the Board panel failed to meaningfully evaluate the parties’ claim construction positions

We are unpersuaded that the Board panel failed to meaningfully evaluate the parties’ claim construction positions as to the disputed limitation.

In the Petition, Petitioner proposed a construction for “a virtual representation of the credential that has been verified by an issuing agency to be an official representation of the credential” to “require that an issuing agency have verified a *virtual representation* in an OVER⁵ file as being an official representation of a credential.” Pet. 14 (citing Ex. 1005 ¶¶ 112–15) (emphasis in original). Patent Owner did not offer a construction, stating that “the Board does not need to construe any terms.” Prelim. Resp. 20–21.

⁵ “OVER” refers to an “Official Verifiable Electronic Representation.” Ex. 1001, 3:50–51.

IPR2024-00486 (Patent 9,251,531 B2)
IPR2024-00489 (Patent 10,749,859 B2)
IPR2024-00490 (Patent 11,329,973 B2)

In the Decision Granting Institution, the Board panel construed the disputed term as proposed by Petitioner. Paper 8, 13.

After institution, Patent Owner reiterated that “no construction is necessary to confirm the claims,” stated that it agreed in substance with the Board’s construction, and clarified that the limitation requires “the issuing agency has verified the ‘virtual representation’ (and not the ‘credential’) to be ‘an official representation of the credential.’” PO Resp. 10 (citing Ex. 2013, 10–11; Ex. 2009 ¶ 45). When arguing that Osborne does not teach the claimed verification, Patent Owner identified an embodiment of the ’531 patent describing the claimed verification as

[t]he OVER File database 128 may contact the issuing agency database 130, such as a state DMV database, and provide the driver’s license identification number to the issuing agency database 130. The issuing agency database may respond by indicating the validity of the requested credential containing the driver’s license identification number and may provide the legal name, address, and birth date of the person associated with the driver’s license identification number.

Id. at 12 (citing Ex. 1001, 6:44–52; Ex. 2009 ¶ 49).

In its Reply, Petitioner referenced Patent Owner’s cited example when arguing that “[Patent Owner] thus admits that a virtual representation of the credential may be ‘verified by an issuing agency’ by checking credential data against an issuing-agency database.” Pet. Reply 2 (citing Ex. 1001, 6:22–54; Ex. 1047, 37:24–41, 41:2–22). In its Sur-Reply, Patent Owner again states that no construction is needed and further argued that Petitioner misinterpreted the Response’s example of verifying a driver’s license identification number. PO Sur-reply 1–2. Specifically, Patent Owner argued that “[r]ather than ‘checking credential data’ in a database, the cited

IPR2024-00486 (Patent 9,251,531 B2)
IPR2024-00489 (Patent 10,749,859 B2)
IPR2024-00490 (Patent 11,329,973 B2)

example explains that the credential is verified.” *Id.* at 2 (citing Ex. 1001, 6:18–20 (“The application gateway may request 126 generation of an OVER File and ***verification of the generated OVER File credential.***”) (emphasis in original), 6:12–61; Tr. 39:3–20).

We have considered the claim constructions positions set forth by both parties and determine that the Board panel addressed meaningfully both Petitioner and Patent Owner’s positions. *See* Dec. 10–11. In its Final Written Decisions, the Board panel maintained its construction from the Institution Decision requiring “that an issuing agency have verified a virtual representation in an OVER file as being an official representation of a credential.” *Id.* at 11. This construction was proposed by Petitioner, and Patent Owner agreed in substance. PO Resp. 10. In addition, in response to Patent Owner’s arguments, the Board panel clarified its construction as “encompass[ing] (1) considering the OVER file as the credential and verifying the OVER file, or (2) verifying a virtual representation of the credential contained within the OVER file.” Dec. 11. This clarification was responsive to Patent Owner’s argument. For these reasons, we determine the Board panel fully and meaningfully considered the parties’ claim construction positions.

2. Whether the Board advanced its own theory of unpatentability as to Osborne

In the Final Written Decision, the Board panel found that Osborne discloses the disputed limitation by teaching that “the issuing agency verifies the token (which includes the XML virtual representation of the bank checking account credential) by ‘pre-authorizing’ the token for a predefined

IPR2024-00486 (Patent 9,251,531 B2)
IPR2024-00489 (Patent 10,749,859 B2)
IPR2024-00490 (Patent 11,329,973 B2)

amount.” Dec. 25. In addressing Patent Owner’s argument that verifying credential data alone is insufficient to meet the claimed verifying limitation, the Board panel stated:

Osborne discloses more than simply verifying in the abstract that credential data supplied by the user is correct. Osborne discloses that the issuer may first generate a token by parsing a form submitted by the client “to extract data fields and values from the form to generate a token data record,” such as the XML data structure in Osborne’s paragraph 47. Ex. 1011 ¶ 47. Then, the “**token** may be pre-funded” by “obtain[ing] assurance that the funds have been uniquely and exclusively allocated for the token from the source **to which the token points.**” *Id.* (emphasis added). Thus, Osborne discloses verifying that the **token** including the XML bank account information in its data structure (the virtual representation of the bank account information) is valid, not merely that bank account information, standing alone, is valid.

Dec. 27.

In its Request for Director Review, Patent Owner characterizes the Board’s reliance on Osborne’s “two-step process for pre-funded tokens” as a new theory that was never presented in the Petition or during trial. Req. 4 (citing Dec. 25–27). In particular, Patent Owner argues that “the Petitions offered only a single sentence vaguely asserting that Osborne disclosed this limitation when an issuer operated the token server.” Req. 8 (citing Pet. 23). According to Patent Owner, Petitioner did not assert that Osborne taught a first step of generating a token and a second step of credential checking. *Id.* at 6–8 (citing Dec. 27). Patent Owner acknowledges that Petitioner’s Reply discussed Osborne’s discussion of pre-funding tokens, but contends that “[u]nlike the Board’s unpatentability finding, [Petitioner] never argued that Osborne’s pre-funded tokens are checked **after** the token is generated.” *Id.* at

IPR2024-00486 (Patent 9,251,531 B2)
IPR2024-00489 (Patent 10,749,859 B2)
IPR2024-00490 (Patent 11,329,973 B2)

7 (citing Pet. Reply 3–4). Instead, Patent Owner argues that the Reply “referred to checking credential data before generating the token.” *Id.* Consequently, Patent Owner argues that the Board panel violated the Administrative Procedure Act by depriving Patent Owner of notice of this alleged new theory of unpatentability. *Id.* at 9–11.

We are not persuaded that the Board advanced its own new theory of unpatentability. To the contrary, as discussed in more detail below, the Final Written Decision properly relied upon evidence and arguments presented in the Petition and permissibly clarified in the Reply by Petitioner in response to arguments raised by Patent Owner.

Patent Owner’s assertion that “[t]he Final Written Decision canceled the claims because a two-step process for Osborne’s pre-funded tokens allegedly disclosed the [disputed] limitation” is inapposite. Req. 4. The Final Written Decision cited paragraph 47—a paragraph first cited in the Petition, and relied on throughout the trial. Dec. 27; Pet. 21–23; Reply 3–4. The Final Written Decision need not be a verbatim recounting of the Petition; rather the Board may articulate the same reasoning in the Petition in its own words. *See Sirona Dental Sys. GmbH v. Institut Straumann AG*, 892 F.3d 1349, 1356 (Fed. Cir. 2018) (concluding that “the Board did not deviate from the grounds in the petition” by relying upon different terms than those used in the petition and citing for support the same portions of the prior art that the petition cited.)

Second, the Final Written Decision provided this reasoning in response to Patent Owner’s argument that Osborne discloses only “verifying the underlying credential” rather than verifying “that a token . . . is an

IPR2024-00486 (Patent 9,251,531 B2)
IPR2024-00489 (Patent 10,749,859 B2)
IPR2024-00490 (Patent 11,329,973 B2)

official representation of the underlying credential.” Dec. 26–27. That is, the Board provided further clarification to the same theory advanced by the Petitioner and disputed by Patent Owner throughout the trial. *Id.* at 27. Patent Owner acknowledges that Petitioner addressed this issue in its Reply. Req. 6 (citing Reply 4). Petitioner’s Reply, which Patent Owner cites, itself includes a citation to paragraph 47 of Osborne, further demonstrating that this is not a new theory. Reply 4 (citing Ex. 1011 ¶ 47). *See Sirona*, 982 F.3d at 1356 (“Because the petition provided [Patent Owner] notice and opportunity to address the portions of [the prior art] relied on by the Board, the Board’s reliance on these portions of [the prior art] did not violate the APA and is not inconsistent with *SAS*”).

We note that paragraph 47 of Osborne appears to disclose multiple embodiments, some of which may include a two-step process. But there is sufficient evidence demonstrating that Petitioner relied on Osborne’s disclosure of a pre-funded token throughout the trial, which further undermines Patent Owner’s assertion that the Board panel presented and relied upon a new theory in the Final Written Decision. Patent Owner appears to acknowledge this in its Request. Req. 7 (“[T]he only reasonable interpretation of Visa’s Reply is that it referred to checking credential data *before* generating the token.”). Additionally, prior to the Request, Patent Owner never argued that the disputed claim limitation required any particular ordering of events. Thus, to the extent the Board’s final determination did depend on a particular order of events in Osborne, there is no evidence in the record that indicates it would have had any impact on the outcome.

IPR2024-00486 (Patent 9,251,531 B2)
IPR2024-00489 (Patent 10,749,859 B2)
IPR2024-00490 (Patent 11,329,973 B2)

For these reasons, we determine the Board panel did not advance its own theory of unpatentability as to Osborne.

3. Whether Petitioner established that Osborne discloses or teaches the disputed limitation based on the arguments and evidence the parties presented during trial

We determine that Petitioner established that Osborne discloses the disputed limitation based on the arguments and evidence the parties presented during trial.

As discussed above, Petitioner asserted that Osborne discloses the disputed limitation because Osborne discloses “any entity can operate as the token server, and it specifically identifies that the token may be provided by the credential’s ‘funding source’—that is, by the agency that issued the credential.” Pet. 22–23 (citing Ex. 1011 ¶¶ 29, 47–48, 53, 58). Petitioner further contended, relying on its expert Dr. Shamos, that “[b]y generating the token and providing it to the user to represent the credential it has issued, the issuer would be verifying it to be an official representation of the credential.” Ex. 1005 ¶¶ 240–42. In the Reply, Petitioner further contends that Osborne discloses verification by “obtaining ‘assurance’ of sufficient funds from the issuer for pre-funded tokens.” Pet. Reply 4 (citing Ex. 1011 ¶ 47). We agree with the Board panel that Petitioner’s evidence demonstrates that Osborne discloses the disputed limitation.

Specifically, the Board panel found that Osborne teaches the disputed limitation because “Osborne discloses that the issuing agency verifies the token (which includes the XML virtual representation of the bank checking account credential) by ‘pre-authorizing’ the token for a predefined amount” through the following disclosure of Osborne:

IPR2024-00486 (Patent 9,251,531 B2)
IPR2024-00489 (Patent 10,749,859 B2)
IPR2024-00490 (Patent 11,329,973 B2)

In some implementations, each token may be pre-funded. For example, *the source of the token* (e.g., issuer, acquirer, independent token arbitrator) *may first obtain assurance that the funds have been uniquely and exclusively allocated for the token from source to which the token points*. Thus, in some implementations, *the token may be pre-funded and preauthorized for up to (or in in the alternative, for exactly) a predefined amount* of a purchase transaction.

Dec. 25 (citing Ex. 1011 ¶ 47). We agree with the Board panel that Osborne’s disclosure of pre-funding and pre-authorizing a bank issued token and providing that token to a user demonstrates that the token is verified. *Id.* at 25–27 (citing Ex. 1011 ¶ 47).

In the Request for Director Review, Patent Owner characterizes the Board panel’s finding as Osborne teaching *post*-funding tokens because “[t]he Final Written Decision found that Osborne’s ¶ 47 disclosed first creating a token in the form of the XML data structure shown in that paragraph and then verifying the information contained in the token with the database of the issuing agency.” Req. 11–12 (citing Dec. 27). Based on this characterization, Patent Owner argues that “[t]he Board clearly abused its discretion by finding that Osborne disclosed issuing agency verification by purportedly *post*-funding tokens, when in fact Osborne’s ¶ 47 exclusively taught *pre*-funding tokens.” *Id.* at 11 (citing Dec. 26–27; Ex. 1011 ¶ 47).

We are not persuaded by Patent Owner’s argument. First, the Board panel did not find that Osborne discloses post-funding tokens. Instead, as explained above, the Board panel found that Osborne discloses pre-funding or pre-authorizing a token. Dec. 25–27 (citing Ex. 1011 ¶ 47). Second, Patent Owner argues that Osborne’s pre-funding and pre-authorization “refer to *before* generating the token data structure in Osborne’s ¶ 47” (Req. 12), but

IPR2024-00486 (Patent 9,251,531 B2)
IPR2024-00489 (Patent 10,749,859 B2)
IPR2024-00490 (Patent 11,329,973 B2)

Patent Owner does not provide any evidence to support this assertion.

Rather than referring to a time before generating the token data structure, Osborne’s describes the pre-funding and pre-authorization in reference to a purchase transaction. Ex. 1011 ¶ 47 (“Some implementations, the token may be pre-funded and pre-authorized for up to (or in the alternative, for exactly) a predefined amount *of a purchase transaction.*”).

Finally, Patent Owner does not persuasively show that this argument is material to the Board panel’s finding that Osborne teaches the disputed limitation. The disputed limitation does not include a temporal requirement, instead only reciting “an OVER file comprising a virtual representation of the credential that has been verified by an issuing agency to be an official representation of the credential.” Ex. 1001, 21:24–27. Petitioner’s assertion that Osborne discloses verification, by “obtaining ‘assurance’ of sufficient funds from the issuer for pre-funded tokens” (Pet. Reply 4), teaches verification of the recited virtual representation of the credential, whether pre-funding or pre-authorization occur before or after the token is generated.

C. CONCLUSION

We conclude that the panel did not err in its unpatentability determinations for the challenged claims.

D. ORDER

Accordingly, it is

ORDERED that Patent Owner’s Request for Director Review is denied.

IPR2024-00486 (Patent 9,251,531 B2)
IPR2024-00489 (Patent 10,749,859 B2)
IPR2024-00490 (Patent 11,329,973 B2)

FOR PETITIONER:

Matthew Argenti
Michael Rosato
Patrick Medley
Joseph Baillargeon
WILSON SONSINI GOODRICH & ROSATI
margenti@wsgr.com
mrosato@wsgr.com
pmedley@wsgr.com
jbaillargeon@wsgr.com

FOR PATENT OWNER:

Douglas Wilson
Michelle Armond
Yue Han
Patrick Maloney
ARMOND WILSON LLP
michelle.armond@armondwilson.com
doug.wilson@armondwilson.com
amy.han@armondwilson.com
patrick.maloney@armondwilson.com