Trials@uspto.gov
571-272-7822

Paper 31
Date: July 29, 2025

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

VISA INC.,
Petitioner,

v.

CORTEX MCP, INC.,
Patent Owner.

IPR2024-00490
Patent 11,329,973 B2

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

CASS, *Administrative Patent Judge*.

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

I. INTRODUCTION

A. Background

In this *inter partes* review, Visa, Inc. ("Petitioner") challenges the patentability of claims 1–17 of U.S. Patent No. 11,329,973 B2 (Ex. 1004, "the '973 patent"), which is assigned to Cortex MCP, Inc. ("Patent Owner").

We have jurisdiction under 35 U.S.C. § 6. This Final Written Decision, issued pursuant to 35 U.S.C. § 318(a), addresses issues and arguments raised during the trial in this *inter partes* review. For the reasons discussed below, Petitioner has proven by a preponderance of the evidence that claims 1, 3–8, 10–16 are unpatentable. Petitioner has not proven by a preponderance of the evidence that any of claims 2, 9, and 17 are unpatentable.

B. Procedural History

In the Petition, Petitioner challenged claims 1–17 of the '859 patent. Paper 2 ("Pet.") 9–10. Following the Petition, Patent Owner filed a Preliminary Response. Paper 6 ("Prelim Resp."). We instituted trial on all challenged claims. Paper 7 ("Inst. Dec.") 51. Following institution, Patent Owner filed a Response (Paper 12, "PO Resp."), Petitioner filed a Reply (Paper 17, "Pet. Reply"), and Patent Owner filed a Sur-reply (Paper 25, "PO Sur-reply").

Petitioner submitted a Declaration of Michael Ian Shamos, Ph.D., with its Petition (Ex. 1005, "Shamos Decl.") and another Declaration from Dr. Shamos in opposition to the Patent Owner Response (Ex. 1048, "Reply Shamos Decl."). Patent Owner submitted a Declaration of Sam Malek (Ex. 2009, "Malek Decl.") with its Patent Owner Response. An oral hearing was held on May 6, 2025, a transcript of which appears in the record. Paper

30, "Tr."

C. Applied References

In this proceeding, Petitioner relies on the references listed below.

> Oborne, US 2012/0316992 A1, published Dec. 13, 2012 (Ex. 1011, "Oborne");
>
> Stafford, US 2009/0271321 A1, published Oct. 29, 2009 (Ex. 1012, "Stafford");
>
> Purves et al., US 2013/0054454 A1, published Feb. 28, 2013 (Ex. 1013, "Purves");
>
> Neafsey et al., US 2013/0212248 A1, published Aug. 15, 2013 (Ex. 1015, "Neafsey").

Pet. 10.

D. Asserted Grounds

Petitioner asserts that the challenged claims of the '973 patent are unpatentable based on the following grounds summarized in the table below:

Claims Challenged	35 U.S.C. §	Reference(s)/Basis
1, 2, 4–7, 16, 17	103(a)[1]	Oborne
3, 8–15	103(a)	Oborne, Purves
1, 3, 5–8, 10, 12–15	103(a)	Stafford, Purves
2, 4, 9, 11, 16, 17	103(a)	Stafford, Purves, Neafsey

Pet. 10.

[1] The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) ("AIA"), included revisions to 35 U.S.C. § 103 that became effective after the filing of an application to which the '973 patent claims priority. Therefore, we apply the pre-AIA version of 35 U.S.C. § 103.

E. Real Parties in Interest

Petitioner states that Visa Inc. is the real party in interest in this proceeding. Pet. 83. Patent Owner states that Cortex MCP, Inc. is the patent owner and real party in interest. Paper 4, 1.

F. Related Proceedings

The parties identify the following district court case involving the '859 patent: *Cortex MCP, Inc. v. Visa, Inc.*, No. 5:23-cv-05720 (N.D. Cal.). Pet. 83; Paper 4, 1. Petitioner further states that it has concurrently filed petitions against three related patents: U.S. Patent No. 9,251,531 (IPR2024-00486 and IPR2024-00487); U.S. Patent No. 9,954,854 (IPR2024-00488); and U.S. Patent No. 10,749,859 (IPR2024-00489). Pet. 83.

G. The '973 Patent (Ex. 1004)

The '973 patent is titled "File Format and Platform for Storage and Verification of Credentials" and issued on May 10, 2022, from an application filed on June 4, 2020. Ex. 1004, codes (54), (45), (22).

The '973 patent is directed to "a computer-implemented method for generating and verifying officially variable electronic representations [OVER files]" of user credentials. Ex. 1004, code (57). The method comprises

> storing information associated with a credential of a user for proving the user's identity or qualifications; receiving a file generation request to provide authentication of the user based on the information associated with the credential; generating a file comprising a virtual representation of the credential that has been verified by an issuing agency to be an official representation of the credential; transmitting the file; receiving a verifying request whether the file transmitted to the user authenticates the user; verifying that a NFC or Bluetooth protocol-based communication associated with the file corresponds with the credential of the user, in response to the

> verifying request; and transmitting an authentication message indicating whether the NFC or Bluetooth protocol-based communication corresponds to the information associated with the credential of the user.

Id.

The ’973 patent Specification explains that an OVER File “may provide a secure file format and platform for the storage and verification of key user or consumer credentials.” Ex. 1004, 4:4–6. The OVER File credentials “may comprise any officially verifiable electronic credential, such as, for example, a government issued identification, such as a driver’s license, non-driver’s identification card, or professional license,” as well as “privately issued credentials, such as, for example, employee identification cards, merchant loyalty cards, access cards, insurance credentials, transportation credentials, or any other credential that may be electronically verified by an issuing agency.” *Id.* at 4:18–27.

Figure 1, reproduced below, illustrates one embodiment of a virtual credential management platform in accordance with the invention. *Id.* at 2:44–46.

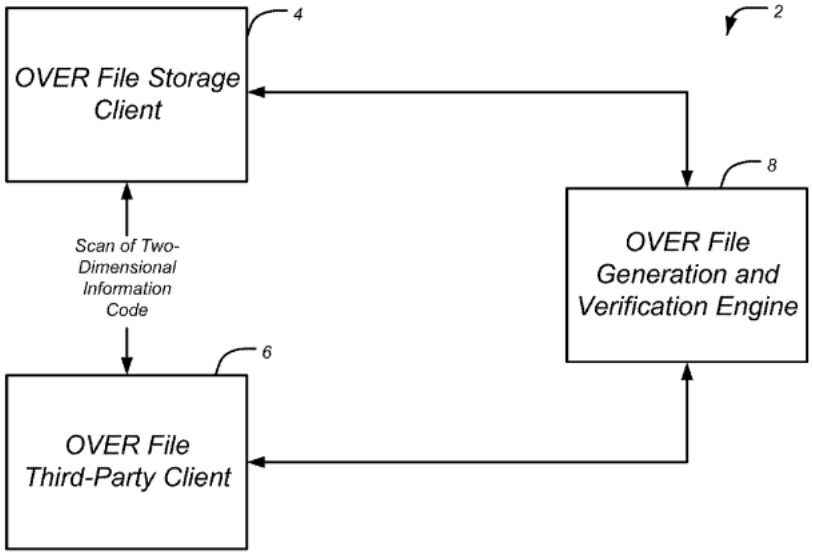

Fig. 1

As shown in Figure 1, OVER File management platform 2 has three main components: OVER File Storage Client 4; OVER File Third-Party Client 6; and OVER File Generation and Verification Engine 8. *Id.* at 4:6–4:10. OVER File Storage Client 4 "may be executed by a user device to store generated OVER Files representative of the user's credentials," and "may initiate generation of new OVER Files and comprise a display function for displaying stored user credentials for third-party verification." *Id.* at 4:11–18. OVER File Third-Party Client 6 "may be executed by a third party device to verify the existence and validity of OVER File credentials presented by a user," for example by "allow[ing] a third party to scan or otherwise interact with OVER File credentials displayed on a user device" and "contact[ing] a remote server, such as the OVER File generation and verification engine 8, for verification of the displayed user credential." *Id.* at 4:29–36. OVER File Generation and Verification Engine 8 "may generate OVER File credentials in response to requests from an OVER File storage

client 4 or an OVER File third party client 6" from "data provided by a user, a third party, or an issuing agency or authority," and may also "provide authorization of OVER File credentials requested by third parties." *Id.* at 4:47–54.

H. Illustrative Claims

Of the challenged claims, claims 1, 8, and 16 are independent. Claim 1 is illustrative and is reproduced below.

> 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 an 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 Near Field Communication (NFC) protocol-based communication associated with the OVER file on the OVER file storage client device of the user;
>
> [1.6] verifying that the NFC protocol-based communication 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;

[1.7] transmitting, to the OVER file third-party client verifying device, an authentication message comprising an indication of whether the NFC protocol-based communication associated with the OVER file on the OVER file storage client device of the user corresponds to the information associated with the credential of the user that is stored in the OVER engine;

[1.8] requesting, by the processor of the OVER engine to the issuing agency, an agency authentication to validate the credential, wherein the issuing agency issued the credential of the user; and

[1.9] receiving, by the OVER engine, a status indicator and credential information associated with the credential; and

[1.10] storing, by the OVER engine, the status indicator.

Ex. 1004, 21:59–22:34 (bracketed paragraph identifiers added).

II. DISCUSSION

A. Level of Ordinary Skill in the Art

Relying on Dr. Shamos, 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 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 ¶¶ 74–79). Petitioner further states that a person of ordinary skill "could have less education but significant professional experience in one or more of those fields." *Id.* In our Institution Decision, we adopted Petitioner's assessment of the level of ordinary skill in the art. Inst. Dec. 15. Patent Owner states that it agrees with the level of ordinary skill set forth in our Institution Decision. PO Resp. 9.

Based on the full trial record, we continue to adopt Petitioner's assessment of the level of skill in the art, which is consistent with the '973 patent and the asserted prior art of record.

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 two claim terms for construction: "officially verifiable electronic representation (OVER) file" and "verified by an issuing agency." Pet. 12–13. These 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 '973 patent Specification "uses the term 'OVER' to refer to an 'Officially Verifiable Electronic Representation.'" Pet. 12 (citing Ex. 1004, 2:46–48). 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. 1004, 6:46–48, 7:13–16, 12:36–39). 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." *Id.* (citing Ex. 1004, 9:39–43, 14:31–39; Ex. 1005 ¶¶ 83–88). "In some embodiments," Petitioner contends, "an OVER File storage client (e.g., a client device) generates an information code in the form of a networked or radio transmission such as an NFC or Bluetooth communication to verify the

user's credential by a third party." *Id.* (citing Ex. 1004, code (57), 12:39–48; Ex. 1005 ¶¶ 155, 163, 177–184).

Petitioner asserts that "[t]he '973 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 the purposes of this petition, [Petitioner] applies a construction that includes 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 3–4), but also encompassing a file comprising a token (as asserted in Patent Owner's infringement complaint and addressed in grounds 1–2)." *Id.* (citing Ex. 1005 ¶¶ 86–88).

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. Inst. Dec. 11. We also explained that we did not need to determine for purposes of institution 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." *Id.* We also determined that Petitioner had made a sufficient showing for purposes of institution that Oborne's tokens qualify as "OVER files." *Id.* at 11, 24.

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. 10 (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. 53–54). "For example," Petitioner asserts, "verification in subsequent claim elements involves the OVER file, and while the OVER file 'compris[es]' the virtual representation, it may encompass other things, as PO's expert admits." *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* Inst. Dec. 11.

2. "verified by an issuing agency"

Petitioner states that "[c]laims 1, 2, 8, 9, 16, and 17 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. 13. Petitioner argues that "[d]uring prosecution of the parent application, 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 ¶¶ 89–92).

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." Inst. Dec. 13.

In its Response, Patent Owner stated that it "agrees in substance with the Board's construction" of this term, and clarified 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. 10–11.

In its Reply, Petitioner points to Patent Owner's reliance on an example in the '973 patent Specification involving the checking of a driver's license identification number against a DMV database to show verification of information in an OVER File generation request. Pet. Reply 2 (citing PO Resp. 12–14; Ex. 1004, 6:48–7:6). 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 2–3.

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." Inst. Dec. 13. 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 constructions for any other claim terms, and we determine that it is not necessary to provide an express interpretation of any other claim terms. *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. Principles of Law

A claim is unpatentable under 35 U.S.C. § 103 if "the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) where in evidence, objective evidence of non-obviousness.[2] *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). When evaluating a combination of teachings, we must also "determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue." *KSR*, 550 U.S. at 418 (citing *In re*

[2] Patent Owner has not presented objective evidence of non-obviousness.

Kahn, 441 F.3d 977, 988 (Fed. Cir. 2006)). Whether a combination of prior art elements would have produced a predictable result weighs in the ultimate determination of obviousness. *Id.* at 416–417.

In an *inter partes* review, the petitioner must show with particularity why each challenged claim is unpatentable. *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016); 37 C.F.R. § 42.104(b) (2020). The burden of persuasion never shifts to Patent Owner. *Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015).

We analyze the challenges presented in the Petition in accordance with the above-stated principles.

D. Ground 1: Obviousness of Claims 1, 2, 4–7, 16, and 17 over Oborne

Petitioner contends that claims 1, 2, 4–7, 16, and 17 would have been obvious over Oborne. Pet. 10, 14–39. To support its contentions, Petitioner provides explanations as to how the prior art teaches each claim limitation and provides rationales to support its obviousness contentions. *Id.* Petitioner also relies upon the Shamos Declaration (Ex. 1005) to support its positions. Patent Owner asserts that the claims are not obvious over Oborne. PO Resp. 11–46. In particular, Patent Owner alleges that Oborne fails to teach limitations [1.1] and [1.3]. *Id.*

1. Overview of Oborne (Ex. 1011)

Oborne 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.

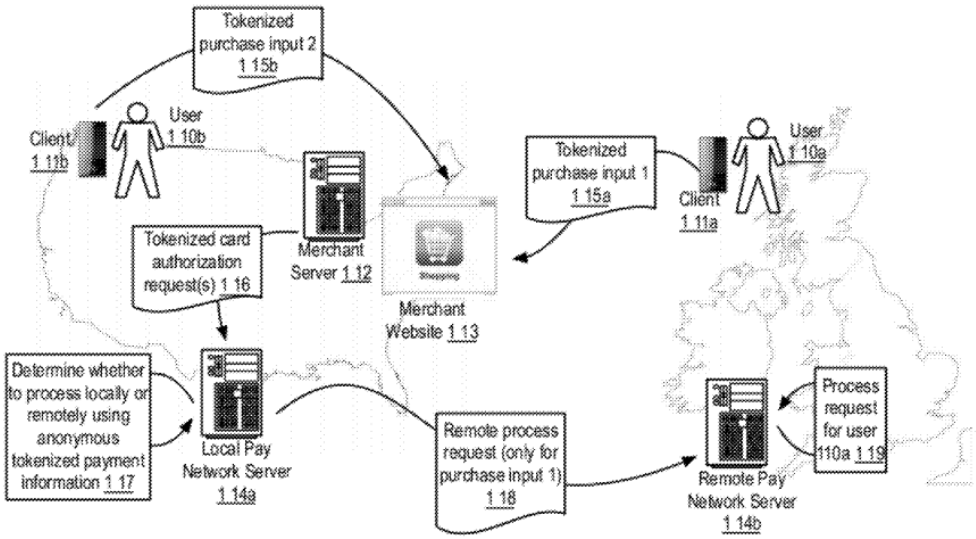

FIGURE 1A Example: Payment Tokenization

Figure 1A, above, depicts a 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.*

Figure 4, reproduced below, is "a data flow diagram illustrating an example procedure to enroll in a token-based purchase payment program in some embodiments of the PPT." Ex. 1011 ¶ 9.

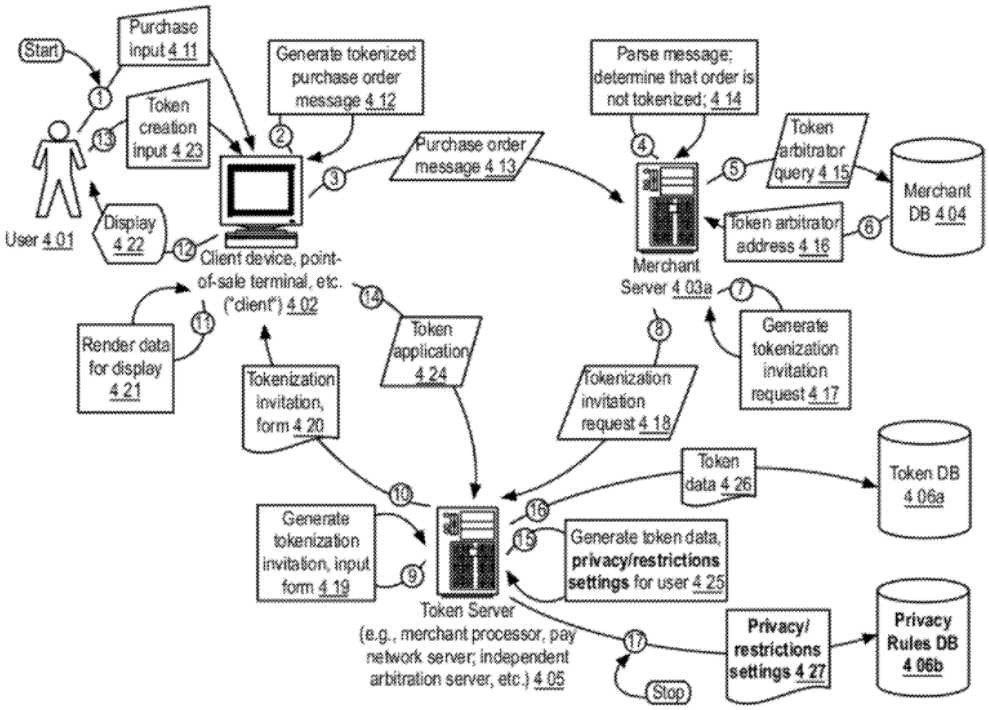

FIGURE 4 Example: Token-Based Purchase Enrollment

Figure 4, above, illustrates an example procedure to enroll in a token-based purchase payment program, and shows the interactions between user 401, client device 402, merchant server 403a, and token server 405. *Id.* ¶¶ 35–44. As shown in Figure 4, user 401 may wish to purchase a product, service, or offering from a merchant, and provide purchase input 411 to merchant server 403a via client device 402. *Id.* ¶ 35. For example, the client 402 may generate a purchase order message and provide it to merchant server 403a (412, 413). *Id.* ¶ 36. If merchant server 403a determines that the purchase order message 413 is not tokenized, the merchant server can send a tokenization invitation on behalf of the user and send it to token server 405 (417, 418). *Id.* ¶¶ 37, 38. Token server 405 may generate a tokenization invitation and application form and provide it to the client (419, 420).

If the user wishes to enroll in payment tokenization services, it "may provide token creation input to complete the application form." Ex. 1011

¶ 40. The client "may generate a completed application form," and provide "the token application to the token server (either directly or via the merchant server)." *Id.* "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.

2. Analysis of Independent Claim 1

a) 1. [preamble]: "[a] computer-implemented method comprising:"

Petitioner argues that "Oborne teaches a computer-implemented method." Pet. 15 (citing Ex. 1011 Figs. 1A, 4, 6A–6E, ¶¶ 114–122; Ex. 1005 ¶ 202). Patent Owner does not present arguments regarding the preamble. *See generally* PO Resp. We determine that, on the record before us, Petitioner's cited evidence sufficiently supports its contentions regarding the preamble.[3]

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 Oborne 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-issue purchase payment funds transfers." Pet. 15 (citing Ex. 1011 ¶¶ 22, 166). Petitioner asserts that "[t]his system includes a 'token server,' also referred to as a

[3] Because we are persuaded that Petitioner has shown that Oborne 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 an entity involved in the PPT, such as 'a pay network server.'" *Id.* at 15–16 (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 16 (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 elements [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 17 (citing Ex. 1005 ¶¶ 203, 204).

Petitioner also argues that "Oborne's PPT apparatus stores information associated with a credential of a user for providing the user's identity or qualifications" using "a storage device storing account information in a database," as shown in Oborne's Figure 15. Pet. 17–18 (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* (e.g., information about the user's credit cards) useful *for proving the identity or qualifications of a user*, such as 'account_number,' 'issuer_name,' 'account address,' 'routing number, etc.'" *Id.* at 17 (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' using the token to prove identity to a merchant as a stand-in for credit card or account information (thus, *for proving the user's identity or qualifications*)." *Id.* at 18 (citing Ex. 1011 ¶ 25; Ex. 1005 ¶ 205).

Patent Owner contends that Petitioner never meets its burden to demonstrate obviousness because Petitioner fails to identify specific components of Oborne's PPT that perform the functions of the OVER engine. PO Resp. 30–34. Patent Owner argues that Petitioner vaguely identifies Oborne's PPT apparatus as the claimed OVER engine but Oborne describes the entire invention as the "Payment Privacy Tokenization Apparatuses, Methods, and Systems (hereinafter 'PPT')." *Id*. at 30–31 (citing Ex. 1001 ¶ 22, code (57)). Patent Owner also asserts that Petitioner improperly points to different components of Oborne's PPT system to teach different claim limitations. *Id*. at 31–34. For example, Patent Owner argues that the Petition improperly points to the "merchant server" of Oborne's PPT apparatus to satisfy the "OVER file third-party client verifying device" (limitation 1.5), while at the same time relying on the PPT apparatus to satisfy the OVER engine of limitation 1.1. *Id.* According to Patent Owner, pointing to the same "PPT apparatus" to satisfy separate claim limitations is improper. *Id.* at 33–34 (citing cases). Patent Owner also contends that Dr. Shamos fails to identify the OVER engine in Oborne. *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 that the Petition sufficiently identified the token server as the relevant portion of the PPT that embodies the OVER engine. Pet. Reply 8. In this regard, Petitioner argues that the Petition's argument for limitation [1.1] specifically referenced the Petition's later discussions of limitations [1.3] and [1.6], and that these later sections made clear that Petitioner was relying on the PPT's token server to satisfy the OVER engine limitation. *Id.* (citing Pet. 17, 20, 27–29). In its Sur-

reply, Patent Owner argues that Petitioner's Reply argument fails because the Petition relies on the PPT's token database 406a, rather than the PPT's token server 405, to teach certain elements of the OVER engine. PO Sur-reply 8–10.

We have reviewed the full trial record, and find that Petitioner has sufficiently proven that Oborne teaches limitation [1.1]. We also find that Petitioner has sufficiently identified Oborne's PPT token server and token database as the OVER engine. The Petition 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. Pet. 17 (referencing the arguments for limitations [1.3] and [1.6]). These portions of the Petition make clear that Petitioner is relying on the token server to carry out the functions of the OVER engine. *Id.* at 20 (asserting that Oborne's "token server . . . generate[s] a date record and data structure for a token *(OVER file)*"), 26 (referring to "the OVER engine (token server)"), 26–27 (explaining that Oborne's token server processes the token arbitration request triggered by the NFC communication). As for Patent Owner's argument that Petitioner also pointed to the token database in its Reply, Oborne 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 Oborne's token server (including a token database that can be integrated with the token server) as the OVER engine.

Consequently, Petitioner has sufficiently proven that Oborne 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 Oborne 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. 18 (citing Ex. 1011 ¶ 35). According to Petitioner, "[i]f the user desires to use tokenization, the client 'may generate a comp[l]eted application form, and provide, e.g., 424, the token application to the token server (either directly or via the merchant server).'" *Id.* at 18–19 (citing Ex. 1011 ¶ 40).

Petitioner also argues that Oborne 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 Oborne's PPT apparatus." Pet. 19–20 (citing Ex. 1011 ¶ 40). The token server, according to Petitioner, "uses values extracted from the form when generating a token record." *Id.* at 20 (citing Ex. 1011 ¶ 41). Therefore, Petitioner contends, the request is "based on information associated with the credential," as limitation [1.2] requires. *Id.* (citing Ex. 1005 ¶¶ 207–208).

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 Oborne 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 "Oborne 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. 20 (citing Ex. 1011 ¶¶ 47–48, Fig. 5; Ex. 1005 ¶ 209). Petitioner argues that "the token is a virtual representation of a credential, such as a credit card," as shown in Figure 1B of Oborne, reproduced below.

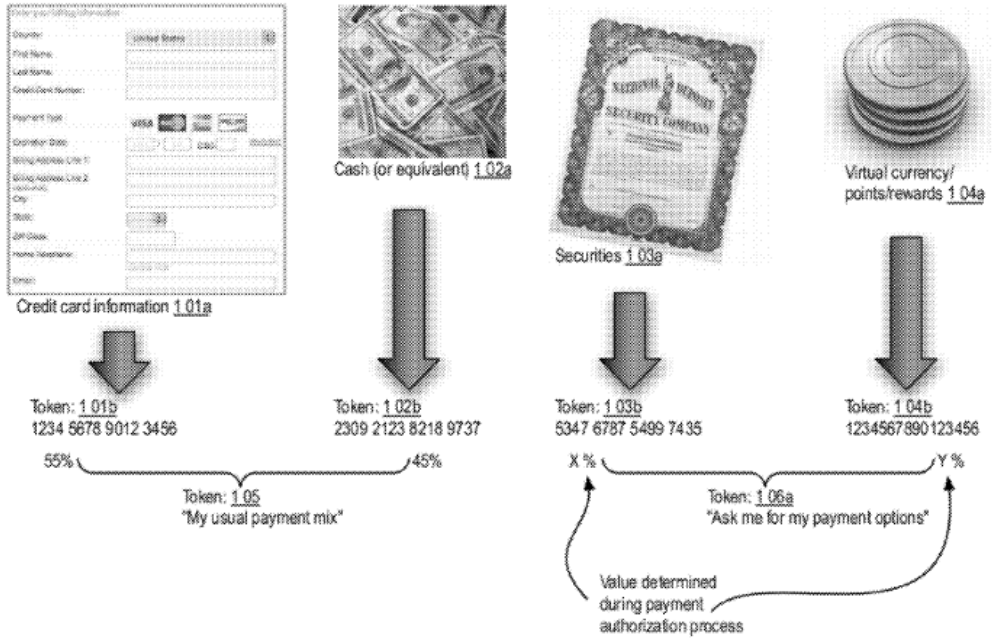

FIGURE 1B Example: Payment Tokenization

Oborne's Figure 1B is a block diagram illustrating aspects of payment tokenization in some embodiments of the PPT. Pet. 20–21; Ex. 1011, Fig. 1B.

Petitioner also points to Oborne's disclosure that the token is "linked to credit card information" and used "in lieu of payment information" such as "card information." *Id.* at 21 (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 ¶ 210).

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. 21. 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.* at 21–22 (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 22 (citing Ex. 1005 ¶¶ 211–212). 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 Oborne does not teach or make obvious issuing agency verification of an OVER file. PO Resp. 11–30; PO Sur-reply 3–4. First, Patent Owner argues that Petitioner "does not point to a disclosure of any such verification by an issuing agency in Oborne." *Id.* at 13. In this regard, Patent Owner argues that Oborne'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 Oborne'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 Oborne's standard Figure 5 process, which shows no verification step whatsoever." *Id.* at 15 (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 Oborne's token server (no matter who operates it) generates a token without any verification step." *Id.* at 16 (emphasis omitted). Finally, Patent Owner argues that Petitioner failed to prove that issuing agency verification would have been obvious over Oborne. *Id.* at 17–30.

In its Reply, Petitioner argues that "Oborne teaches checking credential data for pre-funded tokens." Pet. Reply 4. More specifically, Petitioner contends that Oborne's paragraph 47 teaches tokens that are "'pre-authorized' by having the token source obtain 'assurance' that funds have been allocated 'from the source to which the token points' (i.e., from an

issuing agency)." Pet. Reply 4 (citing Ex. 1011 ¶ 47). "Confirming funds in an account," Petitioner avers, "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. 13). 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 Oborne 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 preliminarily construed the term "OVER file." *See* § II.B.1, *supra*. 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>
```

Id. ¶ 47.

We also find that Oborne 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 explained 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* § II.B.2, *supra*. Oborne 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 ¶ 211.

We also find that Oborne 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, Oborne 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.* at ¶ 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 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 Oborne'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, Oborne 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 Oborne's paragraph 47 quoted above in either its Patent Owner Response or Sur-reply. *See* PO Resp. 11–17; 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. 2028, 11; Ex. 2027, 27:18–28:2.

We disagree with these assertions. As we explain above, Oborne discloses more than simply verifying in the abstract that credential data supplied by the user is correct. Oborne 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 Oborne'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, Oborne 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 Oborne to meet the "verified by an issuing agency" language in limitation 1.3. Pet. 20, 21–22. 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.

Consequently, we find that Petitioner has sufficiently proven that Oborne discloses 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 "Oborne 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. 23 (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, Oborne "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 ¶ 214).

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 Oborne 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 a Near-Field Communication (NFC) protocol-based communication 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 an NFC protocol-based communication*)." Pet. 24. "Beginning with the NFC communication 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.* at 24–25 (citing Ex. 1011 ¶¶ 35, 49, 93). According to Petitioner, "[t]his NFC interaction 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.* at 25 (citing Ex. 1011 ¶ 50). Thus, Petitioner contends, "Oborne's NFC activation triggers the purchase to be performed with the token between the user's and merchant's devices," and is therefore "an *(NFC) 'protocol-based*

communication associated with the OVER file on the OVER file storage client device of the user.'" *Id.* at 25 (citing Ex. 1005 ¶ 215).

Petitioner also argues that, "[t]o process the purchase order request, the merchant sever sends a 'token arbitration request . . . to a token server,'" which reads on the "verifying request" of limitation [1.5]. Pet. 25 (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's paragraph 52, which references a token_id field representing a token. *Id.* at 25–26 (citing Ex. 1005 ¶ 216). 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, Oborne "teaches that the *OVER engine* (token server) receives the recited verifying request from a third-party device based on the recited NFC communication." *Id.* (citing Ex. 1005 ¶ 216).

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 NFC protocol-based communication 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;"

Petitioner argues that "Oborne teaches that the token server processes the token arbitration request triggered by the NFC communication 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 the database 'using the payment token as a search term in the query.'" Pet. 27 (internal citation omitted) (citing Ex. 1011 ¶ 53). "In response," 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 Oborne. *Id.* at 27–28 (citing Ex. 1001 ¶ 53). Additionally, Petitioner asserts, the "token server may determine whether the user token is authenticated." *Id.* at 28 (citing Ex. 1011 ¶¶ 54, 69). "[F]or example," Petitioner contends, if "'no XML data is available associated with the payment token,' this indicates that the 'user has not signed up for payment tokenization services.'" *Id.* "In other words," according to Petitioner, "the query determines whether the NFC communication '*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 ¶ 217).

Additionally, Petitioner argues, Oborne 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, "Oborne teaches that an NFC communication's correspondence with the user's credential information may be verified using various complementary techniques." *Id.* (citing Ex. 1005 ¶ 218).

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 Oborne 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 NFC protocol-based communication 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 Oborne "teaches sending an authenticating message comprising an indicator" of whether the user token has been authenticated. Pet. 29–30. "For example," Petitioner asserts, Oborne 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.* at 30 (citing Ex. 1011 ¶ 69, Fig. 7A). According to Petitioner, "[t]his is an indication that the NFC communication is not associated with the stored user data." *Id.* (citing Ex. 1005 ¶ 220). "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, 63, 70, Figs. 7B–7C). "Any of these messages," according to Petitioner, "is an indicator that the token was authenticated, and thus that the NFC communication

corresponded to the stored user credential information." *Id.* (citing Ex. 1005 ¶ 221).

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 Oborne teaches limitation [1.7].

i) [1.8]: "requesting, by the processor of the OVER engine to the issuing agency, an agency authentication to validate the credential, wherein the issuing agency issued the credential of the user;"

[1.9]: "receiving, by the OVER engine, a status indicator and credential information associated with the credential; and"

[1.10]: "storing, by the OVER engine, the status indicator."

Petitioner argues that Oborne teaches requesting authentication and receiving a status indicator in at least two ways. Pet. 31. First, Petitioner asserts, "when adding a user's card to a wallet for Oborne's system, Oborne teaches verifying the pay card's information 1252 (such as name, account number, etc.), including 'contacting the issuer of the pay card for confirmation of the decoded information 1252 and any other relevant information.'" *Id.* at 31–32 (citing Ex. 1011 ¶ 108). "In light of this teaching," Petitioner contends, one of ordinary skill "would have found it obvious for the OVER engine to request authentication from a credential's issuing agency and receive a status indicator from the agency indicating whether the credential is valid, along with other relevant credential information." *Id.* at 32 (citing Ex. 1005 ¶ 222).

Second, according to Petitioner, "Oborne teaches that, when a tokenized transaction is performed, the token or pay network server contacts

'issuer server(s) corresponding to the payment token,'" and the issuer server "determine[s] whether the user can pay for the transaction using funds available in the account" and provides either an "authorization fail" message or a "notification of successful authorization." Pet. 32 (citing Ex. 1011 ¶¶ 57–58, 61–63). Petitioner asserts that these authorization success or fail messages would be "status indicators (e.g., indication of a valid credential) and credential information associated with the credential (e.g., conformation of sufficient funds), received based on a validation request to validate the credential's coverage of a transaction[]." *Id.* (citing Ex. 1005 ¶ 223). Relying on Dr. Shamos, Petitioner contends that one of ordinary skill "would have employed such an arrangement even if the token server and issue server were operated by the same party," because "such authorization and responses correspond to standard procedures used for transaction processing in a payment network, allowing Oborne's system to be integrated into a system for traditional payment processing in a straightforward and predictable way." *Id.* at 32–33 (citing Ex. 1005 ¶ 223).

Additionally, Petitioner argues that storing the status indicator would have been obvious because "Oborne teaches generating 'a transaction data record' for the pay network server to 'store the details of the transaction and authorization,'" and that "the token server may be . . . a pay network server." Pet. 33 (citing Ex. 1011 ¶¶ 39, 62). According to Petitioner, one of ordinary skill "would view these teachings as suggesting that the token server can store a received status indicator." *Id.* As a practical matter, Petitioner contends, "to properly use a received status indicator (e.g., an indication that a transaction for a credential was authorized or not authorized, or an indication that an issuer did or did not validate a new credential)," one of

ordinary skill "routinely would have stored the status indicator during normal token server operations." *Id.* (citing Ex. 1005 ¶ 224).

Patent Owner does not present arguments specific to these limitations. *See generally* PO Resp.

We have reviewed Petitioner's arguments and evidence on the teaching of limitations [1.8]–[1.10]. On this complete record, we agree with Petitioner that Oborne teaches limitations [1.8]–[1.10].

j) 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 Oborne.

3. Analysis of Dependent Claims 2 and 17

Dependent claim 2 recites as follows:

> 2. The computer-implemented method of claim 1, wherein the OVER file is a first OVER file, the OVER file storage client device of the user is a first OVER file storage client device of the user, the virtual representation is a first virtual representation, the official representation is a first official representation, and the method further comprises:
>
> [2.1] receiving from a second OVER file storage client device of the user, a second OVER file generation request to provide authentication of the user based on the information associated with the credential;
>
> [2.2] generating, by the processor, a second OVER file comprising a second virtual representation of the credential that has been verified by the issuing agency to be a second official representation of the credential that is invalid for use in the first OVER file storage client device for authenticating the user; and

> [2.3] transmitting, to the second OVER file storage client device of the user, the second OVER file in response to the second OVER file generation request.

Ex. 1003, 22:35–53. Claim 17 is dependent on independent claim 16, and includes essentially the same limitations as claim 2. *Id.* at 25:11–29.

Petitioner argues that claim 2 "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 invalid for use in the first OVER file storage client device for authenticating the user.'" Pet. 33–34. Petitioner contends that "the first two of these aspects of claim 2 are satisfied by a user having two devices and receiving respective OVER files on each device." Pet. 34. According to Petitioner, a person of ordinary skill in the art "would have expected users to use multiple devices," and "Oborne teaches that the token server may keep a device table with various identifiers for a user's devices, such as 'device_ID,' 'device_name,' 'device_MAC (referring to a MAC address), etc." *Id.* at 34 (citing Ex. 1011 ¶ 148; Ex. 1005 ¶¶ 226–227).

Petitioner also argues that "[t]he third aspect of claim 2—that the second OVER file (i.e., for the second device) is invalid for use in the first device—would also have been obvious to a [person of ordinary skill in the art] based on Oborne's disclosure. Pet. 34. Petitioner relies on Oborne's teaching of using "device fingerprinting" to provide "additional security" for Oborne's tokens, as well as Oborne's example token data structure that includes a "client_fingerprint" field with device-identifying information like the client's MAC address. *Id.* (citing Ex. 1011 ¶¶ 26, 47). "To obtain the additional security taught by Oborne," Petitioner contends, one of ordinary

skill would have been "motivated to employ Oborne'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). *Id.* at 34–35 (citing Ex. 1005 ¶ 228).

Patent Owner argues that Oborne does not teach or suggest a "second OVER file" that is "invalid for use" in the first device, as claimed. PO Resp. 36–44. According to Patent Owner, claim 2 "require[s] 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 37–38 (citing Ex. 1004, 22:41–53, 23:61–24:6, 25:17–29; Ex. 2009 ¶¶ 100–102). Specifically, Patent Owner argues that Petitioner has not shown that it would have been obvious for Oborne 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 storage client device." *Id.* at 38.

Claim 2 requires Petitioner to show that Oborne teaches the generation of a second OVER file which comprises a second virtual representation of the credential that has been verified by the issuing agency to be a second official representation of the 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 Oborne teaches or suggests all of the limitations of claim 2. First, we consider whether Petitioner has shown that Oborne teaches or suggests generating "a second OVER file comprising a *second virtual*

representation of the credential that has been verified by the issuing agency to be a second official representation of the credential." Patent Owner contends that the "Petition does not explain why one of skill would have been motivated to adapt Oborne's system to allow a user to receive tokens on multiple devices." PO Resp. 39. Patent Owner also argues that Petitioner "does not show that a user receiving an OVER file on two devices meets the claimed 'generating' a '***second*** OVER file comprising a ***second*** virtual representation' of the same credential for the user's second device." *Id.* at 40 (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 credential that had already been created and stored. *Id.* at 40–41 (citing Ex. 1004, 22:35–50; Ex. 1005 ¶ 58; 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. 34. But it is not enough that there is a second token used for a second device, or a "device-specific token." *See* Pet. Reply 12–13. Petitioner fails to explain how Oborne teaches that the second OVER file (i.e., second token) is "a second virtual representation of the credential that has been verified by the issuing agency to be a second official representation of the credential." Rather, Petitioner refers to its contentions and Dr. Shamos's testimony, which do not address, for example, how the second token is a *second virtual representation of the credential*. *Id.*; *see* PO Sur-reply 12 (arguing that "Oborne does not teach two devices with distinct OVER files representing the same credential"); *see* PO Resp. 38–41. 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 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. 38–41.

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 Oborne, a [person of ordinary skill in the art] would have been motivated to employ Oborne'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. 34–35 (citing Ex. 1005 ¶ 228). 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 ¶ 228. Dr. Shamos refers to Oborne'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 and Dr. Shamos's testimony in light of Oborne's disclosure, but find Patent Owner's arguments and Dr. Malek's responsive testimony to be more persuasive. We agree with Dr. Malek that, in Oborne, "device fingerprinting simply refers to identifying a device and the user associated with that device." Ex. 2009 ¶ 111. Specifically, paragraph 26 of Oborne (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 fingering for determining the device identity in order to authenticate a user is corroborated by the disclosures in paragraph 47 of Oborne 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 Oborne that "device fingerprinting" ties a *token* to a particular device. *See,* Ex. 1011 ¶¶ 26, 47. Rather, Oborne'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.

Moreover, Petitioner (and Dr. Shamos's) statement that "the first device's fingerprint would not match" the fingerprint for the second device merely provides a possible outcome of device fingerprinting, but does not explain ***why*** one of ordinary skill would be motivated to use device

fingerprinting to make the "second device's token . . . invalid in the first device," or make the "token for the second device . . . a new credential," or point to disclosures in Oborne that would support such a motivation. *See* Pet. 34–35; Ex. 1005 ¶ 228. Thus, we find that Petitioner's contentions as to this limitation lack sufficient specificity to explain how Oborne teaches the limitation. *See Netflix, Inc. v. DivX, LLC*, 84 F.4th 1371, 1377 (Fed. Cir. 2023) ("Ultimately, it is the petitioner's burden to present a clear argument."); *Intelligent Bio-Sys. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1369 ("It is of the utmost importance that petitioners in the IPR proceedings adhere to the requirement that the initial petition identify 'with particularity' the 'evidence that supports the grounds for the challenge to each claim.' " (quoting 35 U.S.C. § 312(a)(3))).

We further agree with Patent Owner that Oborne's disclosure of "device fingerprinting" is limited, and does not describe how it would be implemented for a user with two devices. *See* PO Resp. 41–42. Therefore, Dr. Shamos's cited Declaration testimony is "conclusory, adds little to the conclusory assertion for which it is offered to support, and is entitled to little weight." *Xerox Corp. v. Bytemark, Inc.*, IPR2022-00624, Paper 9 at 15 (PTAB August 24, 2022) (precedential); *see also* 37 C.F.R. § 42.65(a) ("Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight.").

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 Oborne.

As noted above, claim 17 is dependent on claim 16, respectively, and includes essentially the same limitations as claim 2. The Petition asserts that Oborne teaches claim 17 for similar reasons as claim 2. Pet. 39. We find that claim 17 is not unpatentable for the same reasons as claim 2.

4. Analysis of Dependent Claim 5

Claim 5 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. 1004, 22:63–67.

Petitioner asserts that Oborne teaches storing information associated with a credential in a database. Pet. 36 (citing Ex. 1011 ¶¶ 47, 133, 148 (listing fields such as "account_number," "routing_number.")). Dr. Shamos testifies that Oborne teaches that its systems may store data objects locally or in "remote storage facilities through a communications network." Ex.1005 ¶ 233 (citing Ex. 1011 ¶ 133). In Reply, Petitioner notes Oborne's discussion of distributed databases. Pet. Reply 15 (citing Ex. 1011 ¶¶ 147–150, Fig. 15).

We have reviewed Petitioner's arguments and evidence and we agree with Petitioner that Oborne teaches the limitations of claim 5.

Patent Owner asserts that Oborne 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. 45 (citing Pet. 36; Ex. 1011 ¶ 133). Patent Owner contends that "Oborne distinguishes between 'program and/or database components and/or data,' indicating that Oborne was not teaching that 'data

objects' could be stored remotely as the Petition asserts." *Id*. (emphasis omitted).

We find that Petitioner has provided sufficient evidence that Oborne teaches the limitations of claim 5. Oborne discloses that the memory may contain a "collection of programs and/or database components and/or data" "such as" "a component collection." 1011 ¶ 133. Oborne 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 Oborne 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 Oborne's disclosure concerning distributed databases, which states that databases may be distributed "over several computer systemizations and/or storage devices," which supports that Oborne teaches that data, such as credentials, may be stored remotely. Pet. Reply 15; Ex. 1011 ¶ 150. Although Patent Owner argues that Petitioner's reference to paragraph 150 of Oborne in Reply is a new theory (PO Sur-reply 14), 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 Oborne 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 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 14 (citing Ex. 1011 ¶ 150). Patent Owner asks too much; Oborne'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 5 would have been obvious over Oborne.

5. Analysis of Independent Claim 16

Independent claim 16 includes similar limitations as claim 1. Ex. 1004, 24:35–25:10. Petitioner relies on similar arguments and evidence for claim 16 as it did for claim 1, and Patent Owner does not argue claim 16 separately from claim 1. Pet. 38–39; PO Resp. 11–46. We find that Petitioner has proven by preponderance of the evidence that claim 16 would have been obvious over Oborne for the reasons discussed above with respect to claim 1. *See* § II.D.2, *supra*.

6. Dependent Claims 4, 6, and 7

Petitioner asserts that Oborne teaches the limitations of claims 4, 6, and 7. Pet. 35, 36–38. Patent Owner does not present arguments specifically directed to these dependent claims in this ground. PO Resp. 11–46. 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, and 7 would have been obvious over Oborne.

E. Ground 2: Obviousness of Claims 3 and 8–15 Over Oborne in View of Purves

Petitioner presents arguments that claims 3 and 8–15 would have been obvious over the combination of Oborne and Purves. Pet. 10, 40–51. Patent

Owner presents arguments in response directed to claims 8–15. PO Resp. 34–36. We begin with a brief summary of Purves and then address the argument and evidence presented.

1. Overview of 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 of Independent Claim 8

Claim 8 is similar in many respects to claim 1, but also includes the limitation that the processor is programmed to "request the credential from the issuing agency, wherein the issuing agency stores credentials issued by the issuing agency" ("limitation [8.9]"). Ex. 1004, 23:47–49. Patent Owner argues that Petitioner fails to carry its burden as to this limitation because it does not provide a reason to combine Purves's payment account retrieval with Oborne. PO Resp. 34–36.

Petitioner asserts that Purves teaches the generation of new credentials like a gift card or prepaid card. Pet. 46 (citing Ex. 1013 ¶ 85). 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, 107, 108; Ex. 1005 ¶ 261). Petitioner argues that Oborne teaches receiving a 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*. at 46–47 (citing Ex. 1011 ¶¶ 60–63; Ex. 1005 ¶ 262).

Petitioner asserts that a person of ordinary skill in the art "would have been motivated to combine Oborne and Purves" because "[b]oth 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 Oborne's digital wallet." Pet. 40 (citing Ex. 1005 ¶¶ 250). According to Petitioner, "[t]his combination would be a predictable combination of known, related technologies, to produce a predictable result (a wallet system capable of engaging in tokenized transactions and of adding new credentials as needed)." *Id.* at 40–41.

Patent Owner notes that claim 8 "requires the 'processor[]' to 'request the credential from the issuing agency,'" and contends that Petitioner fails to teach a rationale to combine Purves's payment account retrieval with Oborne. PO Resp. 34 (citing Ex. 1004 at 23:17, 23:47). Patent Owner contends that, although Petitioner argues that Purves teaches the claimed

"request" by "retriev[ing] the user's 'payment account information from the payment account issuer,'" Petitioner "does not specifically argue that it would be obvious to combine this feature of Purves with Oborne," or "explain 'how or why' one of skill would have combined the relied-on teachings in a manner that meets the claims." *Id*. at 34–35 (citing Pet. 46). Patent Owner also asserts that Petitioner's argument that it would have been obvious to combine the references because they are directed to similar applications is not enough to demonstrate a motivation to combine. *Id*. at 35 (citing Pet. 40; *Securus Techs. v. Glob. Tel*Link*, 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 Oborne's digital wallet," but does not explain why the specific addition of Purves's alleged "request [for] the credential from the issuing agency" would be useful to the specific embodiment in Oborne that Petitioner relies on for this claim. PO Resp. 35 (citing *Sisvel Int'l v. Sierra Wireless*, 82 F.4th 1355, 1364 (Fed. Cir. 2023)). Patent Owner further argues that Dr. Shamos's testimony does not provide any evidentiary support. *Id*. at 36 (citing Pet. 40; Ex. 1005 ¶¶ 248–250, 261–266).[4]

Petitioner has provided sufficient articulated reasoning to support the rationale for the combination of Oborne and Purves for the teaching of the limitation requiring "requesting the credential." The Petition explains that a person of ordinary skill in the art would have been motivated to combine

[4] We note that Patent Owner does not assert that there would be any security concerns with the combination of Oborne 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. 34–36.

Oborne and Purves because "the teachings of Purves would be recognized as useful to add new credentials to the Oborne's digital wallet," and that this would have been "a predictable combination of known, related technologies, to produce a predictable result (a wallet system capable of engaging in tokenized transactions and of adding new credentials as needed)." Pet. 40–41 (citing Ex. 1005 ¶ 250). Dr. Shamos testifies that the credential that Purves teaches is a new gift card or reloadable prepaid card. Ex. 1005 ¶¶ 253, 261 (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. Pet. 46 (citing Ex. 1013 ¶ 83). Dr. Shamos testifies that when "the processor determines that no credential of the user is stored" it would have been obvious "to generate the new credential" because "the purpose of Oborne's tokens is to represent a credential" and "by generating the new credential, the user is able to benefit from Oborne's tokenization system." Ex. 1005 ¶ 253. 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 have been natural for the issuer to store such new credentials, at least until being sent to the recipient, and more practically for as long as they remained valid, so that the issuer's systems could confirm their existence." *Id*. ¶ 264.

Patent Owner does not present any arguments challenging the sufficiency of Petitioner's showing as to claim 3. As explained for claim 3, 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 Oborne, and Patent Owner does not dispute this rationale. Pet. 41; *see generally* PO Resp. As Petitioner also explains, a user would

want to store credentials like a gift card or reloadable prepaid card in Oborne'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." Pet. 47. As Dr. Shamos testifies, this is taught by Purves's 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 ¶ 261 (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 Oborne and Purves for requesting the credential in order to have the desired storage of a credential.

Other than limitation [8.9], Patent Owner does not separately argue any other limitations of claim 8. PO Resp. 34–36

Thus, we find that based on the evidence and analysis above, as well as the analysis presented above for claim 1, Petitioner has demonstrated that the combination of Oborne and Purves teaches the limitations of claim 8 with articulated reasoning to support the rationale for the combination.

3. Analysis of Dependent Claim 9

Dependent claim 9 includes substantially the same limitations as dependent claim 2. As discussed above, we find that Petitioner has failed to prove by a preponderance of the evidence that claim 2 is unpatentable. *See* § II.D.3, *supra*. Petitioner relies on the same arguments for claim 9 as it does for claim 2. Pet. 48. We find that Petitioner has failed to prove by a

preponderance of the evidence that claim 9 is unpatentable for the same reasons discussed above with respect to claim 2.

4. Dependent Claims 3 and 10–15

Petitioner asserts that Oborne teaches the limitations of claims 3 and 10–15. Pet. 41, 49–51. Patent Owner does not present arguments specifically directed dependent claim 3 in this ground, and relies on its arguments for claim 8 for dependent claims 9–15. PO Resp. 11–46. 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 and 10–15 would have been obvious over Oborne.

F. Grounds 3 and 4: Obviousness of Claims 1, 3, 5–8, 10, and 12–15 over Stafford and Purves and Obviousness of Claims 2, 4, 9, 11, 16, and 17 Over Stafford, Purves, and Neafsky

Petitioner contends that claims 1, 3, 5–8, 10, and 12–15 would have been obvious over the combination of Stafford and Purves. Pet. 51–75. Petitioner also contends that claims 2, 4, 9, 11, 16, and 17 would have been obvious over Stafford, Purves, and Neafsky. Pet. 75–80. 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. Pet. 51–80. Patent Owner asserts that the claims are not obvious under these grounds. PO Resp. 46–60. In particular, Patent Owner alleges that the combination of Stafford and Purves fails to teach certain claim limitations and that Petitioner fails to establish a rationale to combine the references. *Id.*

1. Overview of 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.

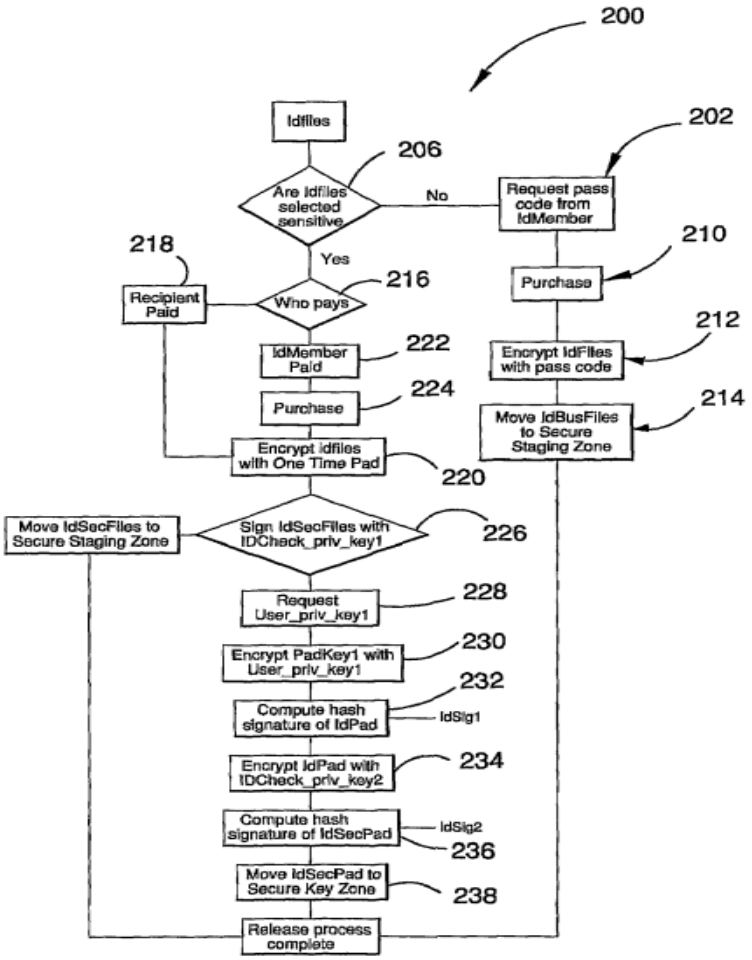

FIGURE 2

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.

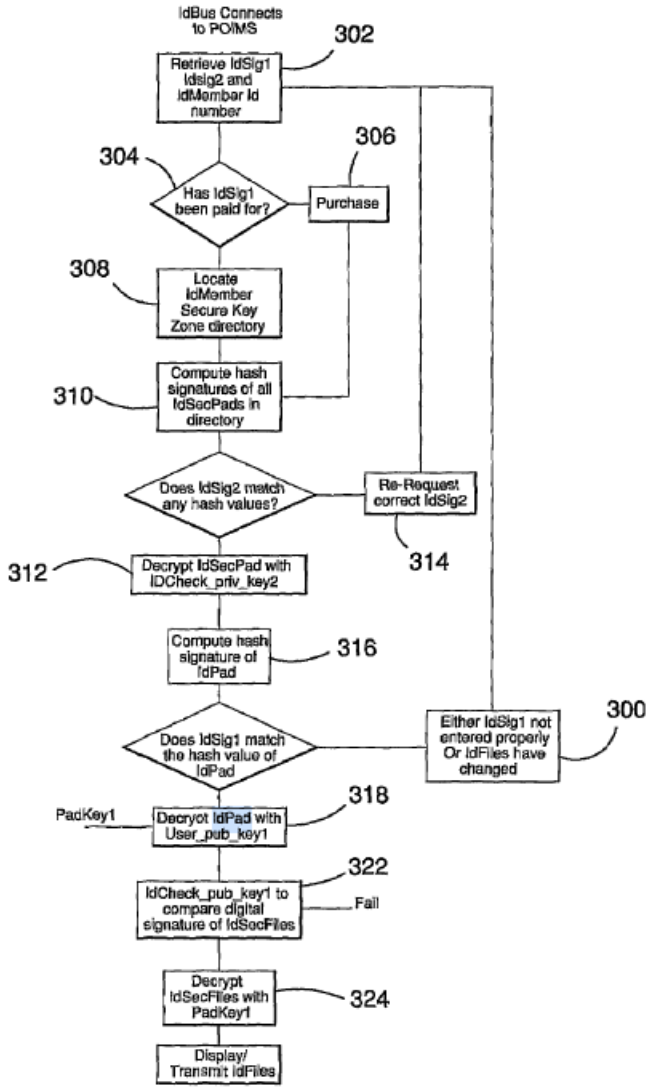

FIGURE 3

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

2. 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. 58 (citing Ex. 1005 ¶ 295). 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 ¶ 295.

Pet. 58 (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. 58–59 (citing Ex. 1012 ¶¶ 62, 65, 67). "However," Petitioner asserts, "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 59 (citing Ex. 1005 ¶ 296).

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. 59 (citing Ex. 1013 ¶¶ 102, 108–109, 122). This card image, according to Petitioner, 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 ¶ 297).

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. 59. Petitioner argues that providing an image of the user's 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.* at 59–60 (citing Ex. 1013 ¶¶ 85, 122). According to Petitioner, this image would be "a virtual representation verified by the issuer as being an official representation of the credential." *Id.* at 60 (citing Ex. 1005 ¶ 298).

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 that "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. 53–54 (citing Ex. 1005 ¶ 286).

Petitioner further argues that one of ordinary skill "would have viewed Purves's NFC communication 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." Pet. 54. "By adapting Stafford's credential management system to transmit key signatures using an NFC communication," Petitioner contends, one of

ordinary skill "would reasonably have expected to achieve these benefits for users." *Id.* (citing Ex. 1005 ¶ 287).

b) Analysis

Limitation [1.3] recites "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." Ex. 1004, 22:1–5.

Petitioner relies on Stafford to teach the "OVER engine" which uses its system to generate a "virtual representation of the credential." Pet. 54–60. 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. 56–58. 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. 58 (citing Ex. 1005 ¶ 295).

As an initial matter, we do not find that Stafford teaches that its OVER engine generates a "virtual representation the credential." As discussed in the Institution Decision (Inst. Dec. 40–41), 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. 48–50 (citing Ex. 1012 ¶¶ 47–48, 94–103, Fig. 2; Ex. 2009 ¶¶ 131–148); PO Sur-reply 15–17.

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 16–17 (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*. at 17 (citing Ex. 1048 ¶¶ 9–10). Petitioner further asserts that Stafford's key signatures are generated based on information associated with the 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 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 credential, that is, as the claim recites, it must be a "virtual representation of the credential." *See* Ex. 1004, 22:1–5. 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 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 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 16. 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. *See* PO Sur-reply 17; 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 the credential . . . based on information associated with the credential of the user."[5]

---

[5] In Reply, Petitioner argues that Purves "credential image" should be considered to teaches the "virtual representation" that is "based on information associated with the credential of the user." Pet. Reply 16. We agree with Patent Owner that the Petition relies on Stafford to teach a "virtual representation" that is "based on information associated with the credential of the user" and on Purves to teach a "virtual representation" that has been "verified by an issuing agency." PO Sur-reply 15; Pet. 58–60.

Petitioner has also not shown that Stafford teaches "a virtual representation of an credential that has been verified by an issuing agency." As discussed above in Section II.B.2, the claim language requires that the issuing agency has verified the OVER file comprising a virtual representation of the 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. 61–62 (citing Ex. 1012 ¶¶ 119–122; Ex. 1005 ¶ 303). 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 58–59 (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. 58–59. 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 with Purves. *See id*. at 59 (arguing that "to the extent that Stafford does not expressly teach that the key signature files sent to the user include a virtual

---

However, even assuming Petitioner relies on the 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.

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. 55–60; PO Sur-reply 21–25. 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. 51–54, 58–60. "Ultimately, it is the petitioner's burden to present a clear argument." *See Netflix, ,* 84 F.4th at 1377; *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. 59–60. 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." *Id.* (citing Ex. 1013 ¶¶ 85, 122;

Ex. 1005 ¶ 298); *see also* Pet. 53–54 (citing Ex. 1005 ¶ 286) (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").

Therefore, Petitioner proposes providing the user with Stafford's key signatures, 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 and an image of the credential. *See* Pet. 55 ("[a] hash value . . . acts as a virtual representation of the stored credential"), 53 (stating that "Purves teaches providing issuer-verified representations of credentials"), 59 (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*, 550 U.S. at 415. 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) (internal quotations omitted). 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. 60. 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. Although proof of physical or bodily 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. 52 (citing Ex. 1012 ¶¶ 106–113; 1005 ¶ 284); Pet. Reply 21–22 (citing Pet. 52–53, 62; Ex. 1005 ¶¶ 284–285; 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 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 ¶¶ 284–285.

Petitioner argues that the combination provides images of the credentials and allows "quick selection" of the credential. Pet. 59–60 (citing Ex. 1005 ¶ 298). 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. 56–57; PO Sur-reply 21; *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 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.[6] *See* Ex. 1048 ¶ 33; Ex. 1012 ¶¶ 74, 118. However, as discussed above, and further discussed herein, we find Petitioner lacks sufficient

[6] It is undisputed that Stafford's key signatures are used only one time. Pet. 56–58, 58–59; PO Resp. 48–49; PO Sur-reply 15–16; Ex. 2027, 14:9–13.

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 add this teaching to Stafford, 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 Werner 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 22 (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 NFC (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."). 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. 58 (citing Ex. 1012 ¶¶ 75, 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. 57–60; Pet.

Reply 24–26; PO Sur-reply 23–25. Patent Owner generally argues that sending card images "introduces security vulnerabilities that would only defeat the purpose of using Stafford's key signature-based security system." PO Resp. 58 (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 59 (citing Ex. 1005 ¶ 298; 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 60 (citing Ex. 2009 ¶¶ 167–170). Petitioner, on the other hand, generally argues that using representative images "was commonplace and 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 24–25 (citing, e.g., Ex. 1048 ¶¶ 34–35; Ex. 1013 ¶ 122).

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. 57–60; *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 26 (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 26 (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. 59–60; Ex. 1005 ¶ 298; 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 and 8 are unpatentable over Stafford and Purves. We determine that Petitioner has not demonstrated by a preponderance of the evidence that claims 3, 5–7, 10, and 12–15, which depend from claims 1 and 8, are unpatentable over Stafford and Purves.

Further, we have reviewed Petitioner's showing for the obviousness of claims 2, 4, 9, 11, and 16–17 over Stafford, Purves, and Neafsey (Pet. 75–80). Independent claim 16 includes similar limitations as claim 1, and Petitioner relies on the same arguments and combination of Stafford and Purves for the common limitations of these claims. Pet. 77–78. Petitioner

adds Neafsky to the combination because claim 16 "requires the use of Bluetooth instead of NFC protocol-based communications" and "Neafsky teaches using Bluetooth protocol-based communications in the same manner as NFC." *Id.* at 76 (citing Ex. 1015 ¶ 21; Ex. 1016, 6). Petitioner's reliance on Neafsky's Bluetooth disclosures does not cure the deficiencies in the Stafford-Purves combination relied on for the other limitations of claim 16. Accordingly, Petitioner has not demonstrated by a preponderance of the evidence that independent claim 16 is unpatentable over Stafford, Purves, and Neafsky. Petitioner has also failed to demonstrate by a preponderance of the evidence that claims 2, 4, 9, 11, and 17, which are dependent on claims 1, 8, and 16, are unpatentable over Stafford, Purves, and Neafsky.

III. CONCLUSION[7]

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

[7] 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, 4–7, 16–17	103(a)	Oborne	1, 4–7, 16	2, 17
3, 8–15	103(a)	Oborne, Purves	3, 8, 10–15	9
1, 3, 5–8, 10, 12–15	103(a)	Stafford, Purves		1, 3, 5–8, 10, 12–15
2, 4, 9, 11, 16–17	103(a)	Stafford, Purves, Neafsey		2, 4, 9, 11, 16–17
Overall Outcome			1, 3–8, 10–16	2, 9, 17

IV. ORDER

Accordingly, it is:

ORDERED that claims 1, 3–8, and 10–16 of the ’973 patent have been shown to be unpatentable and claims 2, 9, and 17 of the ’973 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.

PETITIONER:

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

PATENT OWNER:

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