Trials@uspto.gov
571-272-7822

Paper: 31
Date: July 22, 2025

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

VISA, INC.,
Petitioner,

v.

CORTEX MCP, INC.,
Patent Owner.

IPR2024-00488
Patent 9,954,854 B2

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

SZPONDOWSKI, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining No Challenged Claims Unpatentable
35 U.S.C. § 318(a)

I. INTRODUCTION

We instituted an *inter partes* review of claims 1–17 of U.S. Patent 9,954,854 B2, issued on April 24, 2018 (Ex. 1002, "the '854 patent"), in response to a Petition (Paper 2, "Pet.") filed by Visa Inc. ("Petitioner"). Paper 7 ("Inst. Dec."). During trial, Cortex MCP, Inc. ("Patent Owner") filed a Response to the Petition (Paper 12, "PO Resp."), Petitioner filed a Reply (Paper 16, "Reply"), and Patent Owner filed a Sur-reply (Paper 25, "Sur-reply").

We held an oral hearing in this proceeding[1] on May 6, 2025 and a copy of the transcript is entered into the record. Paper 30 ("Tr.").

We have jurisdiction under 35 U.S.C. § 6 (2018). This Decision is a Final Written Decision under 35 U.S.C. § 318(a) as to the patentability of the claims on which we instituted trial. Petitioner has the burden of proving unpatentability of a claim by a preponderance of the evidence. 35 U.S.C. § 316(e).

Based on the complete record, Petitioner has not shown, by a preponderance of the evidence, that claims 1–17 of the '854 patent are unpatentable.

II. BACKGROUND

A. Real Parties-in-Interest

Petitioner identifies itself as the real party-in-interest. Pet. 79; Paper 17, 1 (Petitioner's Updated Mandatory Notices). Patent Owner also identifies itself as the real party-in-interest. Paper 4, 1 (Patent Owner's

[1] The hearing was a combined hearing for IPR2024-00486, -00488, -00489, and -00490.

Mandatory Notices); Paper 18, 1 (Patent Owner's Updated Mandatory Notices); Paper 27, 1 (Patent Owner's Updated Mandatory Notices).

B. Related Matters

The parties identify *Cortex MCP, Inc. v. Visa, Inc.*, Case No. 5-23-cv-05720 (N.D. Cal.) (originally filed as Case No. 6-23-cv-00048 (W.D. Tex.)) as a related case. Pet. 79; Paper 4, 1. Petitioner has also concurrently filed petitions against three related patents in IPR2024-00486, IPR2024-00487, IPR2024-00489, and IPR2024-00490. Pet. 79.

C. The '854 Patent (Ex. 1002)

The '854 patent is titled "File Format and Platform for Storage and Verification of Credentials" and is generally directed to "a computer-implemented method for generating and verifying officially variable electronic representations [OVER files]" of user credentials. Ex. 1002, codes (54), (57). The method comprises a credential database receiving a request for credential action, where "[t]he credential database may be configured to store one or more credentials comprising a status indicator." *Id.* at code (57). The credential database may then determine "a response to the credential action based on the . . . user credentials stored in the credential database" and transmit "the response to a client device." *Id.* at code (57).

Figure 1, reproduced below, illustrates an embodiment of invention identified as the OVER File management platform. Ex. 1002, 2:41–32, 3:60–62.

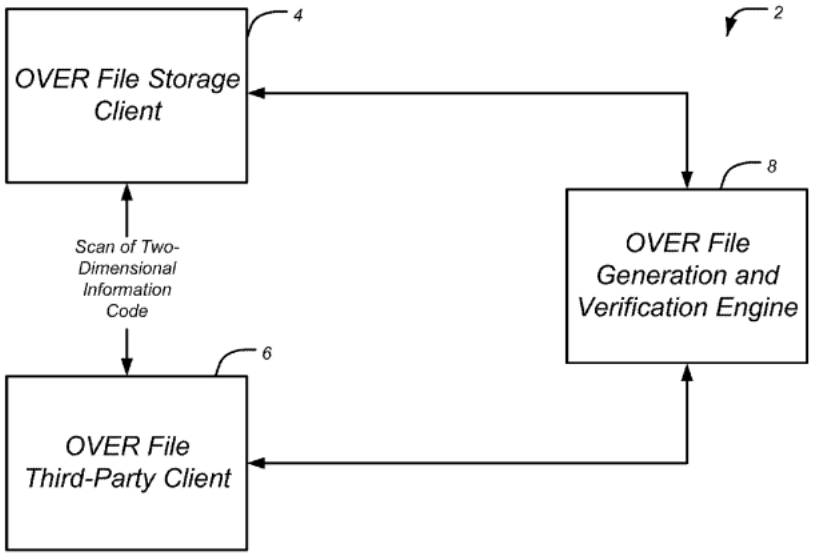

Fig. 1

Figure 1, above, depicts the components of the OVER File management platform, including OVER File storage client 4, OVER File third party client 6, and OVER File generation and authorization engine 8. *Id*. at 3:60–64.

The ’854 patent describes that OVER File storage client 4 stores “generated OVER Files representative of the user’s credentials.” Ex. 1002, 3:64–67. “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” or “privately issued credentials.” *Id.* at 4:5–14. The ’854 patent further describes that “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.” *Id.* at 4:15–18. In addition, an embodiment of process 100 for generating and storing an OVER File credential, which may be performed by Over File generation and

authorization engine 8, is described. Ex. 1002, 4:51–7:43, Fig. 2. The '854 patent also describes an embodiment of an OVER File verification process. *Id.* at 7:44–9:63, Fig. 3.

D. Illustrative Claim

Independent claim 1 is reproduced below, with Petitioner's identifiers in brackets.

> 1. [Preamble] A computer-implemented method comprising:
>
> [1.1] accessing, by an officially verifiable electronic representation (OVER) file verifying device, a first OVER file stored on a first OVER file client device, the first OVER file comprising:
>
> a first virtual representation of an original credential of a user that has been verified by an issuing agency to be a first official representation of the original credential of the user for proving the user's identity or qualifications, based on information associated with the original credential of the user, wherein the first OVER file is itself a first new credential of the user;
>
> the first OVER file generated by an OVER engine configured to:
>
> store the information associated with the original credential of the user; and
>
> transmit the first generated OVER file to the first OVER file client device;
>
> [1.2] transmitting, by the OVER file verifying device, to the OVER engine, a first verifying request to verify that the first OVER file accessed from the first OVER file client device authenticates the user;

> [1.3] receiving, by the OVER file verifying device, a first authentication message comprising a first indication of whether a first scan associated with the first OVER file on the first OVER file client device of the user corresponds to the information associated with the original credential of the user that is stored in the OVER engine;
>
> [1.4] outputting a first status indicator expressing whether the first OVER file authenticates the user;
>
> [1.5] accessing, by the OVER file verifying device, a second OVER file stored on a second OVER file client device of the user, the second OVER file comprising a second virtual representation of the original credential that has been verified by the issuing agency to be a second official representation of the original credential that is invalid for use in the first OVER file client device for authenticating the user, wherein the second OVER file is itself a second new credential over the first OVER file and the original credential;
>
> [1.6] transmitting, by the OVER file verifying device, to the OVER engine, a second verifying request to verify that the second OVER file scanned at the second client device authenticates the user;
>
> [1.7] receiving, by the OVER file verifying device, a second authentication message comprising a second indication of whether the second scan associated with the second OVER file on the device of the user corresponds to the information associated with the original credential of the user that is stored in the OVER engine; and
>
> [1.8] outputting a second status indicator expressing whether the second OVER file authenticates the user.

Ex. 1002, 21:46–22:30. Claims 8 and 15 are also independent, and recite similar limitations. *Id.* at 22:57–23:47, 24:4–55.

E. Prior Art and Asserted Challenges to Patentability

Petitioner asserts that claims 1–17 are unpatentable based on the following challenges (Pet. 10):

Claims Challenged	35 U.S.C. §[2]	Basis/References
1–17	103(a)	Oborne[3]
1–17	103(a)	Oborne, Neafsey[4]
1–17	103(a)	Stafford,[5] Purves,[6] Neafsey

In support of its proposed challenges, Petitioner relies on the Declarations of Michael Ian Shamos, Ph.D, J.D. *See* Exs. 1005, 1048. Patent Owner relies on the Declaration of Sam Malek. *See* Ex. 2009. Deposition transcripts have been submitted to the record for Dr. Shamos (Exs. 2016, 2027) and Dr. Malek (Ex. 1047).

---

[2] Because the earliest possible effective filing date of the '854 patent is before March 16, 2013, patentability is governed by the version of 35 U.S.C. § 103 preceding the Leahy-Smith America Invents Act ("AIA"), Pub L. No. 112–29, 125 Stat. 284 (2011). *See* Pet. 4.

[3] Oborne, US 2012/0316992 A1, published Dec. 13, 2012 (Ex. 1011). Petitioner contends Oborne is prior art under 35 U.S.C. §§ 102(a) and (e). Pet. 10, n.1.

[4] Neafsey, US 2013/0212248 A1, published Aug. 15, 2013 (Ex. 1015). Petitioner contends Neafsey is prior art under 35 U.S.C. § 102(e). Pet. 10 n.2, 11 (relying on Neafsey, US Provisional Patent App. No. 61/598,219 (Ex. 1016)).

[5] Stafford., US 2009/0271321 A1, published Oct. 29, 2009 (Ex. 1012) ("Stafford"). Petitioner contends Stafford is prior art under 35 U.S.C. §§ 102(a), (b), and (e). Pet. 10 n.3.

[6] Purves, US 2013/0054454 A1, published Feb. 28, 2013 (Ex. 1013). Petitioner contends Purves is prior art under 35 U.S.C. § 102(e). Pet. 10 n.4.

III. ANALYSIS

A. Legal Standards

A claim is unpatentable under 35 U.S.C. § 103(a) 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) objective evidence of nonobviousness, i.e., secondary considerations.[7] *See Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

A patent claim "is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007). An obviousness determination based on a combination of references requires finding "both 'that a skilled artisan would have been motivated to combine the teachings of the prior art references to achieve the claimed invention, and that the skilled artisan would have had a reasonable expectation of success in doing so.'" *Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1367–68 (Fed. Cir. 2016) (citation omitted); *see KSR*, 550 U.S. at 418. Further, an assertion of obviousness "cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning

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

with some rational underpinning to support the legal conclusion of obviousness." *KSR*, 550 U.S. at 418; *In re NuVasive, Inc.*, 842 F.3d 1376, 1383 (Fed. Cir. 2016) (a finding of a motivation to combine "must be supported by a 'reasoned explanation.)'"

In an *inter partes* review, a petitioner bears the burden of persuasion to prove "unpatentability by a preponderance of the evidence." *Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015) (quoting 35 U.S.C. § 316(e)). This burden of persuasion never shifts to Patent Owner. *Dynamic Drinkware*, 800 F.3d at 1378 (citing *Tech. Licensing Corp. v. Videotek, Inc.*, 545 F.3d 1316, 1326–1327 (Fed. Cir. 2008). Petitioner must explain with particularity how the prior art would have rendered the challenged claims unpatentable. 35 U.S.C. § 312(a)(3); 37 C.F.R. § 42.104(b)(4) (2024) ("The petition must specify where each element of the claim is found in the prior art patents or printed publications relied upon.").

B. Level of Ordinary Skill in the Art

Petitioner contends a person of ordinary skill in the art "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. Petitioner further asserts that a person of ordinary skill in the art "could have less education but significant professional experience in one or more of these fields." *Id.* (citing Ex. 1005 ¶¶ 74–79).

Patent Owner "agrees with [Petitioner's proposed] definition of the level of ordinary skill in the art." PO Resp. 10 (citing Ex. 2009 ¶¶ 37–41).

In the Institution Decision, we found Petitioner's proposed level of ordinary skill in the art to be reasonable and consistent with the problems and solutions disclosed in the prior art of record. Inst. Dec. 8. Given that Patent Owner does not dispute Petitioner's proposed level of ordinary skill in the art, we continue to apply Petitioner's proposed level of ordinary skill in the art for purposes of this Decision.

C. 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) (2024). Petitioner identifies three claim terms for construction: "officially verifiable electronic representation (OVER) file," "scan," and "verified by an issuing agency." Pet. 11–14. Patent Owner "maintains that claim construction is unnecessary to confirm patentability of the claims here." PO Resp. 10.

1. "Officially Verifiable Electronic Representation (OVER) file"

Petitioner argues that "[t]he specification [of the '854 patent] 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." Pet. 12 (citing Ex. 1002, 6:33–35, 6:67–7:3, 12:23–26). Petitioner additionally argues that the "'OVER file credential' may include an image from an issuing agency, such as a logo or a card image, and the OVER file may also include a scannable code, like a QR (quick response) code." *Id.* (citing Ex. 1002, 9:26–30, 14:19–29, Fig. 11; Ex. 1005 ¶¶ 83–85). Petitioner asserts that "[t]he '854 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 (citing Ex. 1018, 4, 9, 16–17; Ex. 1005 ¶ 86). "Accordingly," Petitioner applies "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 ground 3), but also encompassing a file comprising a virtual representation in the form of a token (as asserted in Patent Owner's infringement complaint and addressed in grounds 1–2)." *Id.* at 13 (citing Ex. 1005 ¶¶ 83–88).

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. 9–13 (referring to the '854 patent Specification, the language of claim 1, and Dr. Shamos's testimony). However, we did not determine whether an "OVER file" included "tokens" as a general matter, or further elaborate on what additional characteristics might be required to qualify as an "OVER file," because it was not necessary for purposes of Institution. *Id.* Moreover, we determined that Petitioner had made a sufficient showing that Oborne's tokens qualified as "OVER files." *Id.* at 11, 24–31.

Patent Owner argues that no construction is required, but, regardless, "the claims may be confirmed under the Board's construction." PO Resp. 11; Sur-reply 1. Petitioner also does not dispute our preliminary construction. Reply 1.

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." Reply 1–2 (citing PO Resp. 49–50). "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. "Scan"

Petitioner argues that "[t]he specification [of the '854 patent] describes that an OVER file can include an 'information code,' and a third-party device can 'scan 220 the information code displayed on the user device'" and this "'scannable code' can be 'for example, a barcode or a QR code.'" Pet. 13 (citing Ex. 1002, 7:65–8:16, 14:19–29, 5:16–35). According to Petitioner, "[t]he specification [of the '854 patent] also refers to using information codes involving radio and electronic transmissions or interactions like Near Field Communication (NFC), Bluetooth, or sensor readings," but "it does not specify that such interactions involve scans and describes these embodiments as alternatives to other embodiments that use scans." *Id.* (citing Ex. 1002, 5:16–35, 12:17–50). Therefore, Petitioner contends, "the specification uses 'scan' to refer to an optical scan, but it does not use 'scan' to refer to other types of interactions like electronic interactions." *Id.* (citing Ex. 1005 ¶¶ 89–94).

Petitioner states that "Patent Owner has asserted in its complaint that a proximity-payment request (e.g., an NFC interaction) constitutes a scan." Pet. 14 (citing Ex. 1018, 10, 36). "Accordingly," Petitioner "applies an interpretation of 'scan' that encompasses an optical scan" as addressed in Ground 1, "while also encompassing an NFC interaction" as addressed in Grounds 2–3 and asserted in the complaint. *Id.* (citing Ex. 1005 ¶¶ 89–86).

In our Institution Decision, we preliminarily determined that the term "scan" encompassed an optical scan as well as an NFC interaction. Inst. Dec. 15. Patent Owner argues that no construction is necessary, but that "scan" should be given its plain and ordinary meaning, which is that "scan" encompasses optical scans, NFC, and Bluetooth. PO Resp. 11.

On the full record, we see no reason to depart from our preliminary construction. Moreover, no further construction is required. *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) ("[O]nly those terms need be construed that are in controversy, and only to the extent necessary to resolve the controversy.")

3. "Verified by an issuing agency"

Petitioner states that "[e]ach independent claim recites an OVER file comprising "a virtual representation of the credential that has been verified by an issuing agency to be an official representation of the credential." Pet. 14. Petitioner argues that "[d]uring prosecution of the ['531] parent application, Applicants 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 ¶¶ 97–100).

In our Institution Decision, we preliminary agreed with Petitioner's construction. Inst. Dec. 15–16.

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 'a first official representation of the original credential.'" PO Resp. 11–12.

In its Reply, Petitioner points to Patent Owner's reliance on an example in the '854 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. Reply 2 (citing PO Resp. 14–16; Ex. 1002, 6:35–39, 6:54–65). 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 the credential may be 'verified by an issuing agency' by checking credential data against an issuing agency database." *Id.* (citing Ex. 1047, 37:24–41:1, 41:2–22). In its Sur-reply, Patent Owner argues that Petitioner misinterprets its discussion of the DMV example, and contends that what Patent Owner was actually arguing based on that example is that the "credential" (the "OVER file") is verified, not that "credential data" is verified. PO Sur-reply 1–3.

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 a credential." Inst. Dec. 15–16. 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.

D. Ground 1: Alleged Obviousness Over Oborne

Petitioner contends claims 1–17 would have been obvious over Oborne. Pet. 15–46. Patent Owner disputes Petitioner's contentions. PO Resp. 12–43. Specifically, Patent Owner argues that Petitioner has not shown that Oborne teaches an OVER file "verified by an issuing agency" and a "second OVER file," which are required by all challenged claims. *Id.* at 12. We agree with Patent Owner that Petitioner has not sufficiently shown that Oborne teaches a "second OVER file" as recited in limitation [1.5].

1. Oborne (Ex. 1011)

Oborne is titled "Payment Privacy Tokenization Apparatuses, Methods and Systems" and generally describes a payment privacy tokenization (PPT) system that transforms payment token-based purchase orders into multi-issuer purchase payment funds transfers. Ex. 1011, codes (54), (57), ¶ 22. Figure 1A, reproduced below, depicts diagrams illustrating aspects of the payment tokenization in some embodiments of the invention. *Id.* ¶ 7.

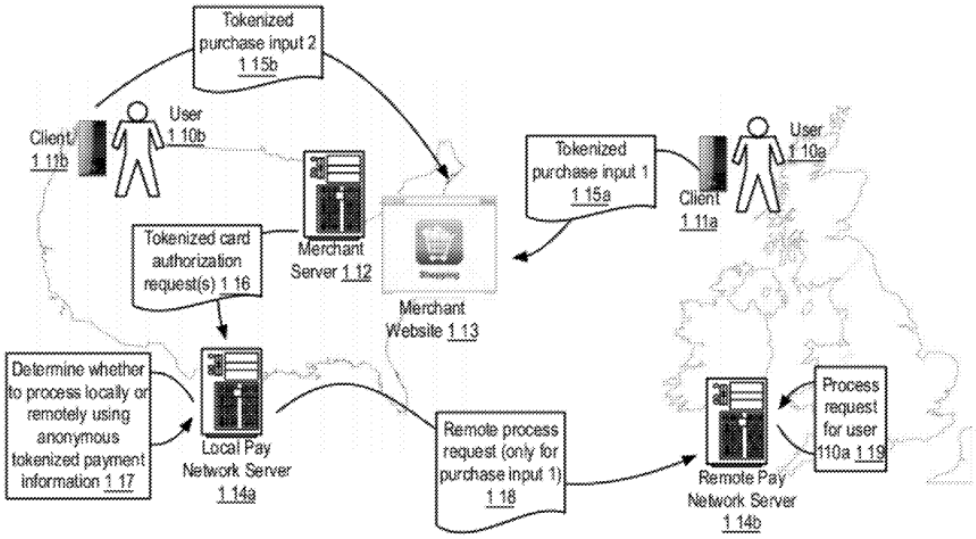

FIGURE 1A Example: Payment Tokenization

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

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

and values from the form to generate a token data record." *Id.* ¶ 41. The token server may store the data extracted from the application form to a token database. *Id.* ¶ 44.

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

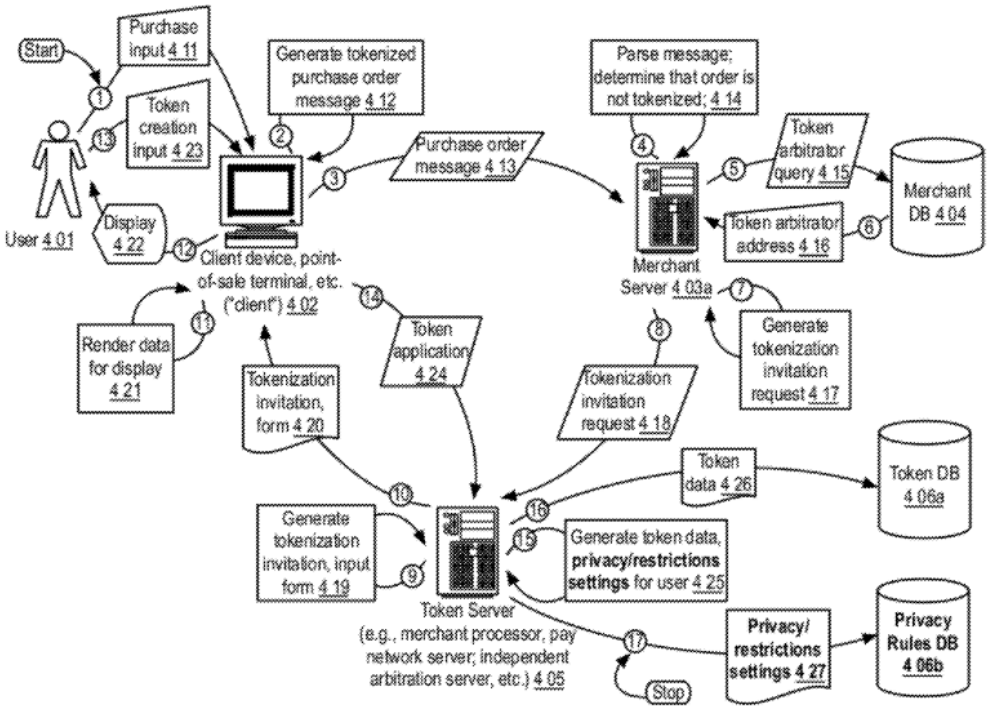

FIGURE 4 Example: Token-Based Purchase Enrollment

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

2. Analysis of Independent Claim 1

Petitioner contends that Oborne teaches or suggests each limitation of independent claim 1. Pet. 16–35. Patent Owner disputes Petitioner's contentions. PO Resp. 12–43. Having considered the arguments and evidence before us, we determine that Petitioner has not shown, by a preponderance of the evidence, that Oborne teaches or suggests limitation [1.5]. Although our analysis focuses on limitation [1.5], we begin with Petitioner's contentions for limitation [1.1], i.e., the first OVER file, which are pertinent to limitation [1.5], i.e., the second OVER file.

a) Limitation [1.1]

Limitation [1.1] recites in part, "the first OVER file comprising: a first virtual representation of an original credential of a user that has been verified by an issuing agency to be a first official representation of the original credential of the user for proving the user's identity or qualifications, based on information associated with the original credential of the user, wherein the first OVER file is itself a first new credential of the user." Ex. 1002, 21:47–63.

Petitioner contends Oborne's tokens used for transactions that are generated and verified by the PPT apparatus teach the recited *OVER file*. Pet. 19 (citing Ex. 1011 ¶ 25; Ex. 1005 ¶¶ 220–221). Petitioner contends that the token is a *virtual representation of a credential*, such as a credit card. *Id.* at 22 (citing Ex. 1011 ¶ 25, Fig. 1B). Petitioner contends that Oborne's token application form provides *information associated with the original credential of the user* that the PPT stores in a database, such as account number, type, billing address, etc., for the user's credit cards. *Id.* at 20; *see id.* at 21 (citing Ex. 1011 Fig. 15). Therefore, Petitioner contends

that Oborne's "token is a *virtual representation of an original credential of a user* that is generated based on information associated with the credential." Pet. 22 (citing Ex. 1005 ¶ 223). Petitioner contends that the token is a first new credential used for proving the user's identity or qualifications, by standing in for an original credential because a user may use tokens in lieu of payment information." *Id.* at 22–23 (Ex. 1011 ¶ 25; Ex. 1005 ¶ 223).

Petitioner contends that "Oborne teaches or at least suggests that the token would be verified by the issuing agency as an official representation." Pet. 23. According to Petitioner, "any entity can operate as the token server," for example, the "credential's 'funding source' – that is, by the agency that issued the credential." *Id.* (citing Ex. 1011 ¶¶ 29, 47, 48, 53, 58). According to Petitioner "[b]y generating the token and providing it to the user to represent the credential it has issued, the issuer would be verifying it to be an official representation of the credential." *Id.* (citing Ex. 1005 ¶ 224).

Petitioner also contends that a person of ordinary skill in the art "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, since 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." Pet. 23–24 (citing Ex. 1005 ¶ 225).

b) Limitation [1.5]

Petitioner contends that limitations [1.5] through [1.8] repeat limitations [1.1] through [1.4] with several modifications, including, for

example, reciting a "second" OVER file and "second" OVER file client device (limitations [1.5]–[1.8]) and requiring that the second OVER file be a "second new credential" that is "invalid for use in the first OVER file client device for authenticating the user" (limitation [1.5]). Pet. 33. In addition, Petitioner contends that "it is not specified whether the OVER engine generates the second OVER file." *Id.*

Petitioner contends that "[t]he existence and use of a second OVER file is satisfied by a user having two devices and receiving respective OVER files to be used on each device." Pet. 33. 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." *Id.* at 33–34 (citing Ex. 1011 ¶ 148; Ex. 1005 ¶ 237).

Petitioner argues that it would have been obvious to a person of ordinary skill in the art in light of Oborne's disclosure that the second OVER file be a new, device-specific credential that is invalid on the first OVER file client device. Pet. 34. Petitioner relies on Oborne's teaching of using device fingerprinting to provide additional security of Oborne's tokens, as well as Oborne's example token data structure that includes a "client_fingerprint." *Id.* at 34–35 (citing Ex. 1011 ¶¶ 26, 47). According to Petitioner, 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 a new credential, different from the first token (with both being different credentials from the original credential), with the second device's token being invalid in the first

device (since the first device's fingerprint would not match)." *Id.* at 35 (citing Ex. 1005 ¶ 239).

Patent Owner argues that Oborne does not teach or suggest a "second OVER file" as claimed.[8] PO Resp. 31. According to Patent Owner, "all '854 Patent claims require a user with two devices ('first'/'second' device), each storing 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 32 (citing Ex. 1002, 21:47–50, 22:9–11, 22:66–67, 23:27–28, 24:7–8, 24:35–36; 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 client device," as recited in limitation [1.5]. PO Resp. 33.

c) Analysis

We agree with Patent Owner that Petitioner has not met its burden to establish that Oborne teaches or suggests limitation [1.5]. First, we consider whether Petitioner has shown that Oborne teaches or suggests "the second OVER file comprises a *second virtual representation of the original credential* that has been verified by the issuing agency to be a second official representation of the original credential." Ex. 1002, 22:9–19 (emphasis

[8] Patent Owner presents a number of arguments as to Petitioner's contentions for claim 1. PO Resp. 12–43. Because we determine that Petitioner has not met its burden for limitation [1.5], we do not address Patent Owner's additional arguments.

added). 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. 33. Patent Owner argues that Petitioner "does not show that a user receiving an OVER file on two devices meets the claimed '***second*** OVER file comprising a ***second*** virtual representation' of the same credential for the user's second device." *Id.* at 34 (citing Ex. 2009 ¶¶ 106–109). According to Patent Owner, the "logical" and "conventional" option would be to use the first OVER file comprising the first virtual representation of the original credential that had already been created and stored. *Id.* at 34–35 (citing Ex. 1002, 22:66–23:1; Ex. 2026 ¶ 55; Ex. 2009 ¶¶ 108–109).

We agree with Patent Owner. The basis of Petitioner's contentions for limitation [1.5] is that the user has two devices and receives respective OVER files (i.e., tokens) to be used on each device. *See* Pet. 33. But it is not enough that there is a second token used for a second device,[9] or a "device-specific token." *See* Reply 8–9. Petitioner fails to explain how Oborne teaches that the second OVER file (i.e., second token) is "a second virtual representation of the original credential that has been verified by the issuing agency to be a second official representation of the original credential." Rather, Petitioner simply refers back to the contentions for limitation [1.1], which do not address, for example, how the second token is a *second virtual representation of the original credential*. *Id.*; *see* Sur-reply 8 (arguing that "Oborne does not teach two devices with distinct OVER files representing the same credential"); *see* PO Resp. 32–34. We find persuasive

[9] We note that there is no dispute that Oborne teaches use of multiple user devices. *See* Ex. 1011 ¶ 148; Reply 8–9; Ex. 1047, 9:13–10:24; Sur-reply 8.

Dr. Malek's testimony that Petitioner hasn't shown why a person of ordinary skill in the art would choose to generate a new token that is a virtual representation of the original credential when a user requested a token on a second device, rather than simply re-using the original token that is a virtual representation of the same credential. *See* Ex. 2009 ¶ 108; *see* PO Resp. 34.

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" and "is itself a second new credential over the first OVER file and the original credential."

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:

> 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 the second device would be a new credential, different from the first token with both being different credentials from the original credential), with the second device's token being invalid in the first device (since the first device's fingerprint would not match).

Id. at. 34–35 (citing Ex. 1005 ¶ 239).

Although we agree with Petitioner that Oborne teaches that "'device fingerprinting may be utilized' to provide 'additional security' for use of Oborne's tokens," Pet. 34 (citing Ex. 1011 ¶ 26 (emphasis added)), we do not agree with Petitioner's arguments related to "device fingerprinting." Petitioner also relies on testimony from Dr. Shamos to support its position. However, Dr. Shamos's cited testimony in paragraph 239 merely repeats what is stated in the Petition, does not provide citation to any other evidence of record, and does not provide any further explanation as to why one of ordinary skill would have been motivated to use device fingerprinting to tie a given token to a given device such that the token for the second device would be invalid in the first device. Ex. 1005 ¶ 239. 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 in light of Oborne's disclosure, but find 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 "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 a second device . . . a new credential," or point to disclosures in Oborne that would support such a motivation. *Id.* 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.*, 821 F.3d at 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. 36–37. Therefore, Dr. Shamos's cited declaration testimony is "conclusory and unsupported, 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 are lacking for limitation [1.5], and we, therefore, determine that Petitioner has not demonstrated by a preponderance of the evidence that claim 1 is unpatentable over Oborne.

3. Claims 2–17

Independent claims 8 and 15 likewise, both recite a "second OVER file comprising a second virtual representation of the original credential that has been verified by the issuing agency to be a second official representation of the original credential that is invalid for use in the first OVER file client device for authenticating the user, wherein the second OVER file is itself a second new credential over the first OVER file and the original credential." Ex. 1002, 23:28–36, 24:36–44. For this limitation, Petitioner refers back to the arguments for claim 1. Pet. 38–39. Accordingly, for the same reasons as claim 1, we determine that Petitioner has not demonstrated by a preponderance of the evidence that claims 8 and 15 are unpatentable over Oborne. Similarly, we determine that Petitioner has not demonstrated by a preponderance of the evidence that claims 2–7, 9–14, and 16, and 17, which depend from claims 1, 8, and 15, are unpatentable over Oborne.

E. Ground 2: Alleged Obviousness over Oborne and Neafsey

Petitioner contends that claims 1–17 would have been obvious over the combination of Oborne and Neafsey. Pet. 47–48.

1. Neafsey (Ex. 1015)

Neafsey is titled "Credential Management System" and is generally directed to a system where a server may generate a credential, transmit the credential to a mobile device for use in an access control system, payment system, transit system, vending system, or the like. Ex. 1015, codes (54), (57). Neafsey describes, for example, virtual credentials that "can be generated by the cloud credential management service . . . in multiple formats," including optical, bar code, or Quick Response (QR) code. *Id.* ¶¶ 49, 61.

2. Analysis

This challenge is identical to the challenge over Oborne, except that Petitioner applies the alternative construction of "scan," that is, an optical scan. Pet. 47–48. Therefore, rather than relying on Oborne's NFC interactions to teach "scan," as recited in limitations [1.3] and [1.6], Petitioner relies on Neafsey's optical scan. *Id.* Petitioner does not rely on Neafsey to teach limitation [1.5]. *Id.* at 47–48. Accordingly, for the same reasons as set forth in the Oborne ground, we determine that Petitioner has not demonstrated by a preponderance of the evidence that claims 1–17 are unpatentable over Oborne and Neafsey.

F. Ground 3: Alleged Obviousness Over Stafford, Purves, and Neafsey

Petitioner contends claims 1–17 would have been obvious over the combination of Stafford, Purves, and Neafsey. Pet. 48–76. Patent Owner disputes Petitioner's contentions. PO Resp. 43–59. In particular, Patent Owner alleges that the combination of Stafford and Purves fails to teach limitation [1.1] and Petitioner fails to establish a rationale to combine Stafford and Purves. *Id.* We agree with Patent Owner that Petitioner has not

shown that the combination of Stafford and Purves teaches limitation [1.1] and has not provided sufficient articulated reasoning, with rational underpinning, to combine the teachings of Stafford and Purves.

1. Stafford (Ex. 1012)

Stafford is directed to "a system [] for storing, validating and disseminating credential information about an entity." Ex. 1012, code (57). Stafford's system "generates data representing at least part of the credential information and a data representation of at least part of a document supporting that information and stores the credential information and data representation in a database . . . in an encrypted form." *Id.*

Stafford's system has several different subsystems, including an Internet Zone, Secure Staging Zone, Secure Zone, Key Generation Infrastructure, Transaction Servers, and Administration Sub-System. Ex. 1012 ¶¶ 55–62. The Secure Staging Zone "includes a data store including a database of encrypted credential information which has been released by an entity for collection by an information user." *Id.* ¶ 57. The Secure Staging Zone "store[s] encrypted released information and security key data which is used during the data transmission process" and "store[s] submitted information by the entity for the purposes of collection and verification of the system." *Id.* The Secure Zone "includes a series of databases storing all credential information . . . and other associated data." *Id.* ¶ 58. "All credential information stored in the" Secure Zone "is encrypted by the IdMember's public key." *Id.*

Prior to using Stafford's system, an entity needs to enroll in the system, i.e., "become an IdMember." Ex. 1012 ¶ 63. To enroll, the entity submits their credential information or documentation to the system, where

it is then verified. *Id.* ¶ 64. Once verified, the original documents are electronically scanned, digitally signed, encrypted, and stored in the Secure Zone. *Id.* ¶ 67. The unencrypted documents are referred to as IdFiles. *Id.* The encryption process begins with generating an asymmetric or public key pair for the entity (i.e., User_pub_key1, User_priv_key1). *Id.* ¶ 68. The system digitally signs the IdFiles, and then encrypts the IdFiles with user_pub_key1 to create IdSecFiles1 and submits IdSecfiles1 to the Secure Zone. *Id.* ¶ 69–70. Then, if an entity wants to provide that information to a third party, the information needs to be moved to the Secure Staging Zone to allow collection or transmission of the information. *Id.* ¶ 72.

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.

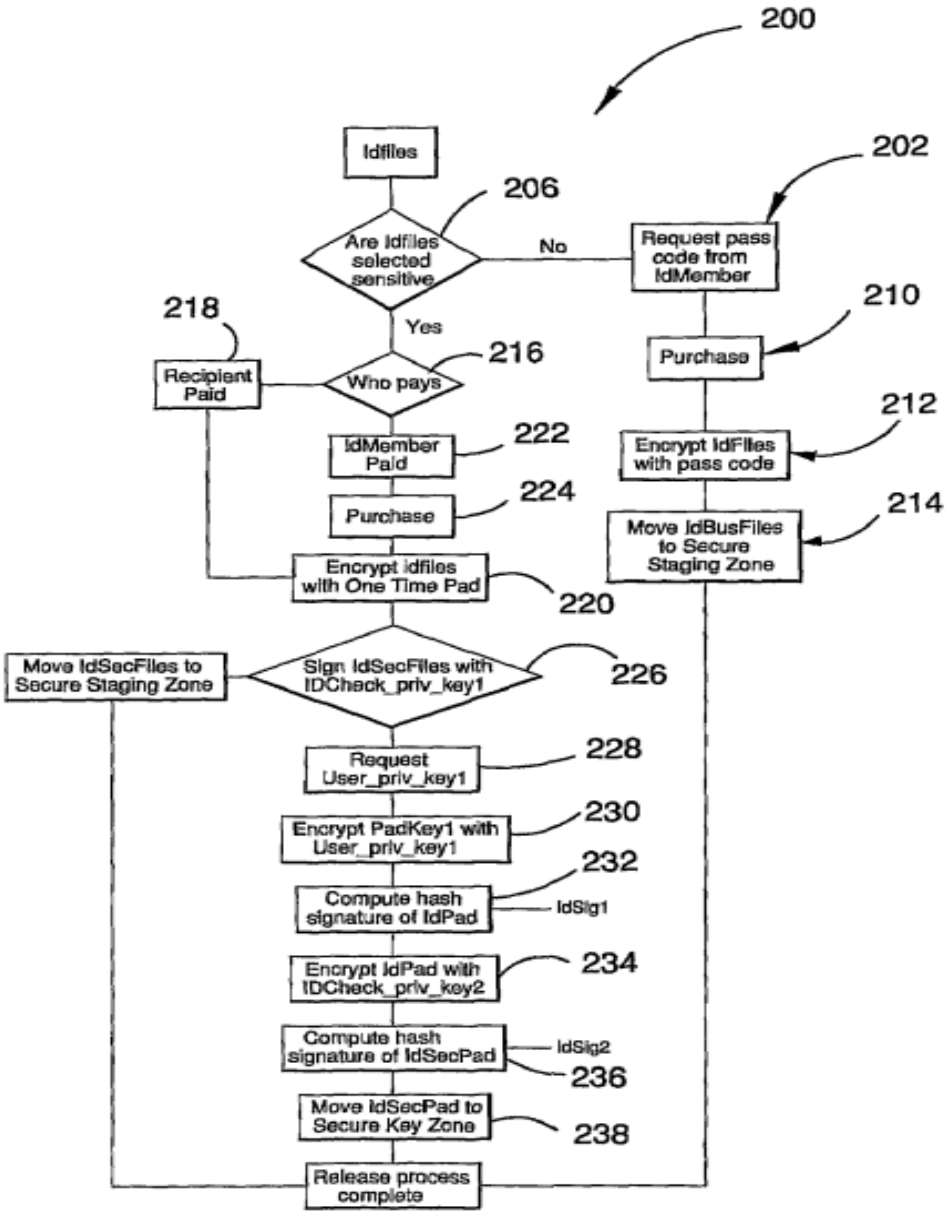

FIGURE 2

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 (206 through 238) 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, 84–106.

The process starts with the user (IdMember) selecting files or information (i.e., the IdFiles) for release. Ex. 1012 ¶ 84. 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. In this scenario, "the selected information to be released is identified from within IdSecFiles1, the unencrypted IdFiles . . . are symmetrically encrypted using One Time Pad . . . to create IdSecFiles2." *Id.* ¶ 94 (steps 206, 220). IdSecFiles2 are digitally signed and moved to the Secure Staging Zone. *Id.* (step 226). In step 230, "[t]he key or pad (PadKey1) used for the One Time Pad is encrypted with User_priv_key1, requested in Step 228, to create IdPad in step 230." *Id.* ¶ 95. In step 232, "a hash value of IdPad is created, called IdSig1," which "represents a first key signature component that is required by a recipient to collect/obtain the released information." *Id.* ¶ 97. In step 234, IdPad is encrypted to generate IdSecPad. *Id.* ¶ 99. In step 236, a hash value of IdSecPad is created, called IdSig2. *Id*. In step 238, IdSecPad is moved to Secure Key Zone. *Id.* ¶ 100.

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

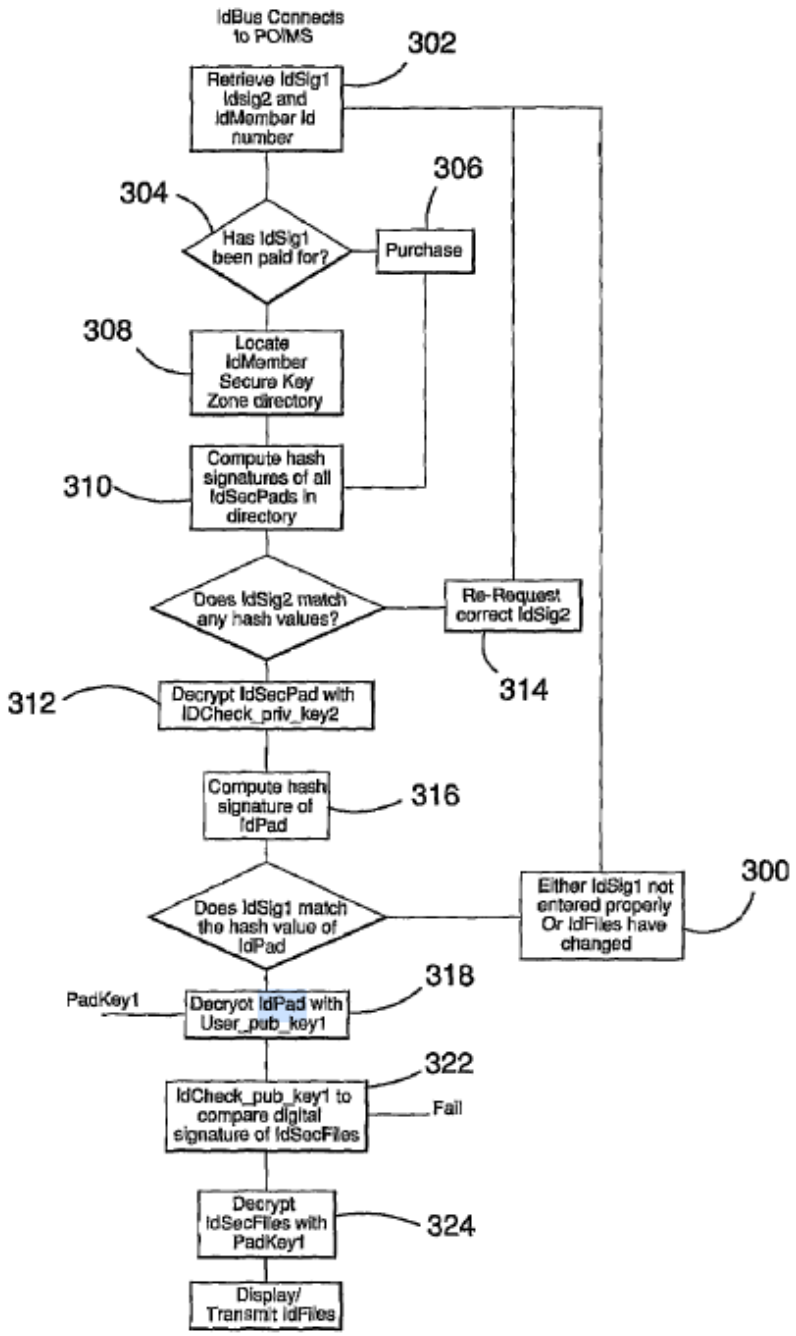

FIGURE 3

Figure 3, above, shows the steps for allowing a third party (e.g., IdBus) to obtain secured credentials. Ex. 1012 ¶¶ 107–125. Generally, the process begins with IdMember filling out an online application form, and providing

IdSig1, IdSig2, and MIN.[10] *Id.* ¶ 107, 113. IdBus then requests release of information from IdMember's profile, which includes IdSig1, IdSig2, and MIN. *Id.* ¶ 115 (step 302). The system "creates a hash against all the IdSecPad's in the [IdMember's] directory until a match against IdSig2 is found." *Id.* ¶ 119 (step 310). When a match is found, IdSecPad is decrypted to retrieve IdPad. *Id.* ¶ 120 (step 312). Then, a hash value of IdPad is created and compared with IdSig1. *Id.* ¶ 121 (step 316). When a match is found, IdPad is decrypted to retrieve PadKey1. *Id.* (step 318). Next, PadKey1 is sent to Secure Staging Zone. *Id.* ¶ 123. The system then computes hash values of the IdSecFiles2 stored in the Secure Staging Zone, and if there is a match between IdSecFiles 2 and IdSig1, then the digital signature is decrypted and compared to the hash value of IdSecFiles2. *Id.* ¶ 124. Finally, PadKey1 is used to decrypt IdSecFiles2 to retrieve the IdFiles. *Id.* ¶ 125 (step 324). Therefore, "[t]he decrypted and released IdFiles can then be transmitted or displayed to IdBus1 for use in the necessary data comparison and credential verification." *Id.* ¶ 126.

2. 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*. 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

[10] MIN is a member identification number, which is assigned during enrollment. Ex. 1012 ¶ 69.

WSEP may also be configured to facilitate the creation and funding of pre-paid accounts in a consumer's virtual wallet." *Id*. In one embodiment, a payment methods panel may list one or more payment methods that are present in the wallet, including displaying "an image of the card (e.g., from the issuer), a nickname for the card, card identifier, card brand, and/or the like." *Id.* ¶ 85. A QR code scan may be used to trigger a wallet account connection or login during a point-of-sale interaction. *Id*. ¶ 64.

3. Petitioner's Contentions

Petitioner contends that limitation [1.1] is taught by the combination of Stafford, Purves, and Neafsey. Pet. 53. Petitioner contends that Stafford's system teaches an OVER engine that stores credential information for proving users' identity or qualifications. Pet. 53 (citing Ex. 1012 ¶ 54, Fig. 1, claim 1). Petitioner argues that "Stafford's system generates key signatures to release sensitive files" which "can comprise hash values (IdSig1 and IdSig2), which can either be displayed to the user or transmitted electronically to the user's device." Pet. 58 (citing Ex. 1012 ¶¶ 97–99). Petitioner contends that "[t]he credential to be released is stored in an encrypted format using one-time pads (IdSecPad and IDPad), and IdSig1 and IdSig2 are hash values of the credential's one-time pads, thereby identifying the encrypted credential." *Id.* (citing Ex. 1012 ¶¶ 116–122). Petitioner further contends that:

> The release of the credential is authorized by comparing the hash values to the IdSecPad and IdPad corresponding to the credential, with a match indicating that release is authorized. [Ex. 1012 ¶¶ 116–122]; Ex. 1005 ¶ 293. *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 ¶ 293.

Id. (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. 59 (citing Ex. 1012 ¶¶ 62, 65, 67). Petitioner asserts, however, that to the extent that Stafford does not expressly teach that the key signature files include a virtual representation *verified by the issuing agency*, Purves teaches verification by the issuing agency. *Id*. (citing Ex. 1005 ¶ 294).

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, 111, 112, 122). Petitioner asserts that this card image is from an issuer. *Id*. (citing Ex. 1013 ¶ 85). Petitioner argues that the "representative image provided 'from an issuer' would be *verified by the issuing agency to be an official representation*, as would an image produced from an actual credential, since an actual credential naturally represents itself." *Id*. (citing Ex. 1005 ¶ 295).

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 (e.g., a generally-representative, issuer-provided image or a real image of the credential with optionally-obscured confidential information), along with the encoded key signature," would "remind users which credential the key signature

represents and enable quick selection from among a plurality of options available on the user's device." *Id*. at 59–60 (citing Ex. 1013 ¶¶ 85, 122; Ex. 1005 ¶ 296). Petitioner contends that 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 ¶ 296).

Petitioner additionally argues that a person of ordinary skill in the art "would have been motivated to incorporate such representations with Stafford's key signatures to provide user devices convenient images of the credentials that may be selected by the user." *Id.* at 49–50 (citing Ex. 1005 ¶ 277). According to Petitioner, a person of ordinary skill in the art "would have recognized various benefits from incorporating Purves's credential images into Stafford's system," such as "the images would improve ease-of-use and reduce user error by providing users images matching the credentials the user seeks to provide to third parties." *Id.* at 52 (citing Ex. 1005 ¶ 282).

Petitioner also argues that Stafford "expressly suggests including other information with its key signatures and employing various known delivery processes," to the recipient (e.g., IdBus1), including "using an optical scan in the delivery process, as taught by Neafsey, in addition to the virtual representation of a credential taught by Purves." Pet. 59–60 (citing Ex. 1012 ¶¶ 106–113; 1005 ¶ 297). Further, Petitioner argues that optical codes, as taught by Neafsey and Purves, may be used to convey virtual credential information. *Id.* at 50 (citing, e.g., Ex. 1016, 4, 12 (optical code); Ex. 1013 ¶¶ 64 (QR code may trigger wallet connection), 95 (QR code)). Petitioner contends that "it would have been obvious to use such optically-scannable codes to encode Stafford's key signatures, allowing them to be transferred to the recipient (IdBus1) in a simple, reliable manner." *Id.* at 60–

61 (citing Ex. 1005 ¶ 297); *see also id.* at 51 (stating that it would have been obvious "to use the scannable code formats such as QR and bar codes to transfer Stafford's key signatures to the third party by providing device-specific, encoded key signatures to the user").

4. Analysis

Limitation [1.1] recites a "first OVER file" comprising:

> a first virtual representation of an original credential of a user that has been verified by an issuing agency to be a first official representation of the original credential of the user for proving the user's identity or qualifications, based on information associated with the original credential of the user, wherein the first OVER file is itself a first new credential of the user;
>
> the first OVER file generated by an OVER engine configured to:
>
> store the information associated with the original credential of the user; and
>
> transmit the first generated OVER file to the first OVER file client device.

Ex. 1002, 21:49–63.[11]

Petitioner relies on Stafford alone to teach the "OVER engine" which uses its system to generate a "virtual representation of the original credential." Pet. 53–58. 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

[11] Independent claims 8 and 15 recite the same limitation. *See* Ex. 1002, 22:67–23:14, 24:8–22. Therefore, our analysis for claim 1 also applies to claims 8 and 15.

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. 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 ¶ 293).

As an initial matter, we do not find that Stafford teaches that its OVER engine generates a "virtual representation of the original credential." As discussed in the Institution Decision (Inst. Dec. 45–46), 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. 45–46 (citing Ex. 1012 ¶¶ 47–48, 94–103, Fig. 2; Ex. 2009 ¶¶ 147–148); Sur-reply 12–15.

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. Reply 13–14 (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 14 (citing Ex. 1048 ¶¶ 9–10). Petitioner further asserts that Stafford's key signatures are generated based on information associated with the original credential because "[t]hey are derived as a result of a request to release the credential information" and are "tied to the credential information and facilitate its release." *Id*. at 15. 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 15–16.

Although we agree with Petitioner that "the virtual representation of the credential" does not have to have certain formatting or be a visual representation of the credential itself, the virtual representation nevertheless has to be based on information associated with the original credential, that is, as the claim recites, it must be a "virtual representation of an original credential" and the OVER engine is configured to "store the information associated with the original credential." *See* Ex. 1002, 21:51–61. We do not agree with Petitioner's arguments that Stafford's key signatures "represent" a credential like a coat check ticket "represents" a coat or, alternatively, that key signatures are representative of the original credential by virtue of being derived as a result of a request. As discussed above, a key signature is developed independently from the credential (i.e., is a hash value of a One Time Pad), and although it allows a user to release a stored credential, like a coat check ticket allows a user to retrieve a coat, there is nothing in the key signatures in Stafford that is based on information associated with the

original credential. We find more persuasive Patent Owner's comparison of the key signatures to a stamp on an envelope, where the stamp is not based on anything inside the envelope. *See* Sur-reply 14. 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 14–15; Ex. 1012 ¶ 68–69, 94. Dr. Shamos agrees with this. *See* Ex. 2027, 9:12–22, 18:4–7; 33:22–33:9. Accordingly, Petitioner has not carried its burden to demonstrate that Stafford teaches an OVER engine that generates a "virtual representation of an original credential . . . based on information associated with the original credential of the user."[12]

Petitioner has also not shown that Stafford teaches "a virtual representation of an original credential that has been verified by an issuing agency." As discussed above in Section III.C.3, the claim language requires that the issuing agency has verified the OVER file comprising a virtual representation of the original credential, not the original credential itself. Petitioner asserts that Stafford's "request [third-party OVER file verifying device request for the release of information] includes the key signatures that

[12] In Reply, Petitioner argues that Purves teaches a "virtual representation" that is "based on information associated with the original credential of the user." Reply 12–13, 15. We agree with Patent Owner that the Petition relied on Stafford to teach a "virtual representation" that is "based on information associated with the original credential of the user" and on Purves to teach a "virtual representation" that has been "verified by an issuing agency." Sur-reply 12; Pet. 58–60. However, even assuming Petitioner relied 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.

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. 58 (citing Ex. 1012 ¶¶ 119–122; Ex. 1005 ¶ 292). 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 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. 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*. (arguing that "to the extent that Stafford does not expressly teach that the key signature files sent to the user include a virtual representation verified by the issuing agency, this aspect of the claim is met by Purves").

We agree with Patent Owner that Petitioner has not sufficiently established that a person of ordinary skill in the art would have been motivated to combine Stafford and Purves. *See* PO Resp. 52–58; Sur-reply 18–23. 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 Int'l. S.A. v. Sierra Wireless, Inc.*, 82 F. 4th 1355 (Fed. Cir. 2023) (stating "we cannot fault the Board for being at a loss in trying to decipher Cross-Appellants kitchen-sink of unclear and confusing motivation-to-combine arguments"); Pet. 48–50, 59–60. "Ultimately, it is the petitioner's burden to present a clear argument." *See Netflix,* 84 F.4th at 1377; *see also Intelligent Bio-Sys.*, 821 F.3d at 1369. 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. 58–60. 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." Pet. 59–60 (citing Ex. 1013 ¶¶ 85, 122; Ex. 1005 ¶ 296); *see also* Pet. 52 (citing Ex. 1005 ¶ 282) (arguing 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"). Additionally, Petitioner also modifies Stafford's system to use scannable code formats such as QR and bar codes (as taught in Purves and Neafsey) to transfer Stafford's key signatures to the third party by providing device-specific, encoded key signatures to the user. Pet. 51 (citing Ex. 1005 ¶ 280), 62. Petitioner argues that this would have been obvious because it would "allow[] [the key signatures] to be transferred to the

recipient (IdBus1) in a simple, reliable manner." *Id.* at 60–61 (citing Ex. 1005 ¶ 297), 62–63.

Therefore, Petitioner proposes providing the user with Stafford's key signatures in a scannable format, such as a QR code, and also providing the user with an image of the credential associated with the key signatures. In other words, under Petitioner's apparent theory, the user would be provided with two virtual representations of the credential, i.e., key signatures in a scannable code format and an image of the credential. *See* Pet. 58 ("[a] hash value thus acts as a virtual credential representation of the stored credential"), 49 (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. 59–60. Nor does Petitioner address whether the QR code would be provided to the user in a similar manner. *See* PO Resp. 58. 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.[13] 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

[13] Dr. Shamos' testimony that "[t]he user then presents the QR code image to the third-party recipient for scanning . . . according to well-known QR-code-scanning techniques" appears inconsistent with the ecommerce example relied upon in Stafford. Ex. 1048 ¶ 43; *see* Ex. 1012 ¶ 74 ("In the exemplary embodiment, the system 100 has a web interface through which entities and recipients of data may interact with the system to store, administer, release and obtain verified credential data"), ¶ 106 ("ecommerce related activities"), ¶ 107 (stating that the example in Figure 3 "is applicable to situations such as when an IdMember (the entity) is using an online application form, such as an on-line loan application"); *see* Pet. 60, 62; Reply 23–24.

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. 49 (citing Ex. 1012 ¶¶ 106–13); Reply 18 (citing Pet. 49–51, 60–63; Ex. 1005 ¶¶ 276–277, 297, 301; 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 ¶¶ 276–277, 297, 301.

Petitioner argues that the combination "provide[s] user devices convenient images of the credentials that may be selected by the user." Pet. 50 (citing Ex. 1005 ¶ 277) (emphasis added). 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. 53; Sur-reply 18; *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); Reply 19–20. 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.[14] *See* Ex. 1048 ¶ 33; Ex. 1012 ¶¶ 74, 118. However, as discussed above, and further discussed herein, we find Petitioner lacks sufficient explanation as to the proposed combination, e.g., a user selecting or providing key signatures through the use of a credential image.

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

[14] It is undisputed that Stafford's key signatures are used only one time. Pet. 56, 58; PO Resp. 53; Sur-reply 14; Ex. 2027, 14:9–13.

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 user 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* Reply 18 (stating that a person of ordinary skill in the art "would have been motivated to obtain known benefits from using credential images (e.g., convenience and error-reduction) and QR codes (e.g., convenience, efficiency, and reliability)"). However, we are not persuaded that these generic benefits would have motivated a person of ordinary skill in the art to make these modifications to Stafford. *See Belden Inc. v. Berk-Tek LLC*, 805 F.3d 1064, 1073 (Fed. Cir. 2015) ("[O]bviousness concerns whether a skilled artisan not only *could have made* but *would have been motivated to make* the combinations or modifications of prior art to arrive at the claimed invention."). 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. 54–55 (citing Ex. 1012 ¶¶ 81, 93–106). For example, Stafford explains that "[a]dvantageously, embodiments of a key signature purchase process involves multiple controls to ensure that the release of sensitive information is intentional, secure and ensures data is delivered to the intended recipient." Ex. 1012 ¶ 81.

The parties dispute whether the modifications to Stafford in view of Purves would compromise Stafford's security. *E.g.*, PO Resp. 54–54; Reply 20–25; Sur-reply 20–23. Patent Owner generally argues that sending cards and QR codes "would open vulnerabilities in Stafford's system . . . defeating the purpose of using Stafford's key signatures in the first place." PO Resp. 54 (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 55 (citing Ex. 1005 ¶ 296; 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 56 (citing Ex. 2009 ¶¶ 167–170). Additionally, Patent Owner argues that neither of Stafford's delivery mechanisms for IdSig1 and IdSig2 (i.e., email or copying from the display) "would work with a QR code." *Id.* at 58 (citing, e.g., Ex. 2009 ¶¶ 173–174).

Petitioner, on the other hand, generally argues that "using representative images was commonplace and viewed as sufficiently secure," that Purves "teaches using an obscured image for sensitive credentials like credit cards," and that "virtual wallets routinely displayed partially obscured account information and that irrecoverable image-obscuring was commonplace and readily achieved." Reply 21–22 (citing, e.g., Ex. 1048

¶¶ 34–36, Ex. 1013 ¶ 122). Petitioner further argues that "storing QR-encoded key signatures is just as secure as storing non-QR-encoded key signatures," and that "QR codes are [ ] simply a different way of encoding data." Reply 23 (citing e.g., Ex. 1048 ¶¶ 40, 50–51). In addition, Petitioner argues that QR-code-mediated transfer of key signatures is more secure than manual entry of the key-signature characters, and that "Purves itself demonstrates that QR codes are sufficiently secure in this context since it teaches using them for payment transactions." *Id.* (citing e.g., Ex. 1048 ¶¶ 41, 52, 53; Ex. 1013 ¶ 64).

On balance, Petitioner's generic benefits do not outweigh Patent Owner's concerns as to the introduction of security vulnerabilities to Stafford's system. PO Resp. 55–58; *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 "significant benefits easily outweigh any corresponding security risk." Reply 25 (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 ¶¶ 166–168; Ex. 1048 ¶¶ 35–38; Reply 25 (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 ¶ 296; 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. Relatedly, 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 proffered through Dr. Shamos, as explained above. Therefore, Petitioner has not established by a preponderance of the evidence that the claims 1, 8, and 15 are unpatentable over Stafford, Purves, and Neafsey. Similarly, we determine that Petitioner has not demonstrated by a preponderance of the evidence that claims 2–7, 9–14, and 16, and 17, which depend from claims 1, 8, and 15, are unpatentable over Stafford, Purves, and Neafsey.

IV. CONCLUSION

For the foregoing reasons, we are not persuaded that Petitioner has established by a preponderance of the evidence that claims 1–17 of the '854 patent are unpatentable.

Claims	**35 U.S.C. §**	**References/Basis**	**Claims Shown Unpatentable**	**Claims Not Shown Unpatentable**
1–17	103(a)	Oborne		1–17
1–17	103(a)	Oborne, Neafsey		1–17
1–17	103(a)	Stafford, Purves, Neafsey		1–17
Overall Outcome				1–17

V. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that claims 1–17 of the ’854 patent have not been shown to be unpatentable; and

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

IPR2024-00488
Patent 9,954,854 B2

For PETITIONER:

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

For PATENT OWNER:

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