

Filed on behalf of: Visa Inc.

By: Matthew A. Argenti (margenti@wsgr.com)
Michael T. Rosato (mrosato@wsgr.com)
Patrick M. Medley (pmedley@wsgr.com)
Joseph M. Baillargeon (jbaillargeon@wsgr.com)
WILSON SONSINI GOODRICH & ROSATI

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

VISA INC.,
Petitioner,

v.

CORTEX MCP, INC.,
Patent Owner.

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

**PETITION FOR INTER PARTES REVIEW OF
U.S. PATENT NO. 9,251,531**

TABLE OF CONTENTS

	<u>Page</u>
I. Introduction.....	1
A. The '531 Patent	2
B. Prosecution History	4
C. Background and State of the Art.....	5
D. Level of Skill in the Art.....	9
II. Statement of the Precise Relief Requested for Each Claim Challenged	9
III. Claim Construction.....	11
A. “OVER file”	12
B. “scan”	13
C. “...verified by an issuing agency...”	14
IV. Ground 1: Claims 1-2 and 4-14 are Obvious over Osborne	15
A. Overview of Ground.....	15
B. Claim 1	16
C. Claim 2	31
D. Claim 4	33
E. Claim 5	35
F. Claim 6	35
G. Claim 7	36
H. Claim 8	37
I. Claims 9-10	37
J. Claim 11	38
K. Claim 12	39
L. Claim 13	40
M. Claim 14	40
V. Ground 2: Claim 3 is Obvious over Osborne and Purves.....	42
VI. Ground 3: Claims 1-2, 4-18 and 20 are Obvious over Osborne and Neafsey	43

A.	Overview and Rationale to Combine	43
B.	Claims 1-2 and 4-14	44
C.	Claim 15	45
D.	Claim 16	49
E.	Claim 17	49
F.	Claim 18	50
G.	Claim 20	52
VII.	Ground 4: Claims 3 and 19 are Obvious over Osborne, Purves, and Neafsey	52
A.	Claim 3	52
B.	Claim 19	53
VIII.	Ground 5: Claims 1, 3-5, 7-16, and 18-20 are Obvious over Stafford and Purves.....	54
A.	Overview and Rationale to Combine	54
B.	Claim 1	57
C.	Claim 3	70
D.	Claim 4	71
E.	Claim 5	72
F.	Claim 7	72
G.	Claim 8	73
H.	Claims 9-10	73
I.	Claim 11	73
J.	Claim 12	74
K.	Claim 13	75
L.	Claim 14	75
M.	Claim 15	76
N.	Claim 16	77
O.	Claim 18	78
P.	Claim 19	78

Q.	Claim 20	78
IX.	Ground 6: Claims 2, 6, and 17 are Obvious over Stafford, Purves, and Neafsey	79
X.	Discretionary Denial is Not Warranted	81
XI.	Grounds for Standing.....	82
XII.	Conclusion	82
XIII.	Mandatory Notices under 37 C.F.R. §42.8.....	83
XIV.	Payment of Fees under 37 C.F.R. §§42.15(a) and 42.103	84
XV.	Certificate of Compliance.....	85
XVI.	Appendix – List of Exhibits.....	86

LISTING OF CHALLENGED CLAIMS

1.[Preamble] A computer-implemented method comprising:

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

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

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

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

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

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

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

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.

3. The computer-implemented method of claim 1, further comprising generating, by the processor of the OVER engine, the credential, wherein the credential is generated when the processor determines that no credential of the user is stored.

4. The computer-implemented method of claim 1, further comprising:

[4.1] 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;

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

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

5. The computer-implemented method of claim 4, wherein the status indicator indicates the credential is valid.

6. The computer-implemented method of claim 1, further comprising generating, by the OVER engine, a device identifier for the credential, wherein the device identifier limits the credential to the OVER file storage client device.

7. The computer-implemented method of claim 4, wherein the status indicator indicates an invalid credential and the credential information indicates a reason for the invalid credential.

8. The computer-implemented method of claim 1, 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.

9. The computer-implemented method of claim 1, further comprising storing, by the OVER engine, user-specific information.

10. The computer-implemented method of claim 9, wherein the user specific-information comprises at least one of:

biometric information, location information, a password, or a device identifier.

11. The computer-implemented method of claim 1, further comprising checking, by the OVER engine, a status indicator of a stored credential, wherein the OVER file generation request comprises a credential identifier for specifying which credential among a plurality of credentials of the user is officially represented by the OVER file.

12. The computer-implemented method of claim 11, wherein verifying that the scan of the OVER file corresponds with the credential of the user comprises comparing the credential identifier with one or more stored credentials.

13. The computer-implemented method of claim 12, wherein the authentication message comprises the status indicator of the stored credential when the credential identifier matches a stored credential.

14. The computer-implemented method of claim 1, wherein the OVER file comprises a portion of the stored credential.

15.[Preamble] A computer-implemented method comprising:

[15.1] transmitting, from an officially verifiable electronic represent (OVER) file storage client device of a user to an OVER file generation and verification engine, an OVER file generation request to provide authentication of the user based on information associated

with a credential of the user, the credential proving the user's identity or qualifications;

[15.2] receiving, at the OVER file storage client device of the user, an OVER file in response to the OVER file generation request, the 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;

[15.3] displaying a portion of the OVER file to an OVER file third-party client verifying device to authenticate the user; and

[15.4] receiving, at the OVER file storage client device of the user, an authentication message comprising a status indicator indicating whether the OVER file corresponds to the credential of the user.

16. The computer-implemented method of claim 15, wherein the displayed portion of the OVER file is scanned as part of authenticating the user.

17. The computer-implemented method of claim 15, wherein the OVER file comprises a device identifier, wherein the device identifier limits the validity of the OVER file to the device of the user.

18. The computer-implemented method of claim 15, further comprising:

collecting, by the device, user-specific information; and

transmitting, by the device, the user-specific information to a credential engine, wherein the user-specific information is included in the OVER file.

19. The computer-implemented method of claim 15, wherein when the OVER file comprises a credential image.

20. The computer-implemented method of claim 15, wherein when the status indicator indicates an invalid credential, and the authentication message comprises a reason for the invalid credential.

Visa Inc., (“Petitioner” or “Visa”) requests review of U.S. Patent No. 9,251,531 (“the ’531 patent,” EX1001), currently assigned to Cortex MCP, Inc. (“Patent Owner”). This petition demonstrates by a preponderance of the evidence that claims 1-20 (“Challenged Claims”) of the ’531 patent are unpatentable as obvious.

I. INTRODUCTION

The ’531 patent purports to have invented a method for storing and verifying credentials. However, the claims of the ’531 patent merely recite known methods for online credential management without adding anything new or non-obvious.

The Challenged Claims recite generating files called “officially verifiable electronic representation” (OVER) files, which include representations of credentials such as a driver’s license and which can provide virtual credentials to be scanned and verified by third parties. In its complaint (EX1018), Patent Owner has interpreted the claim terms broadly, mapping digital tokens to the claimed “OVER files.” However, as explained herein, tokenization and systems for management and verification of electronic credentials were well-known before the alleged invention of the challenged patent.

Claims 1-20 of the ’531 patent should be found unpatentable and cancelled.

A. The '531 Patent

The '531 patent is entitled “File Format and Platform for Storage and Verification of Credentials.” EX1001, Title. The '531 patent describes methods to generate and verify a credential using an “Officially Verifiable Electronic Representation (OVER) File,” which “may provide a secure file format and platform for the storage and verification of key user or consumer credentials.” EX1001, Abstract, 3:50-53. The '531 patent describes that OVER files may be generated, sent to user devices, and presented to third parties in place of a traditional credential, such as a driver’s license, insurance credentials, electronic coupons, loyalty cards, discount cards, and credit cards. EX1001, 6:37-8:3, 9:48-53, 10:21-39, Figs. 2-3.

The independent claims 1 and 15 recite computer-implemented methods involving the use of OVER files that are associated with user credentials, as well as reciting steps involving engines and client devices that deal with such files. The use of OVER files involves interactions between three parties, as shown in Fig. 1 (below).

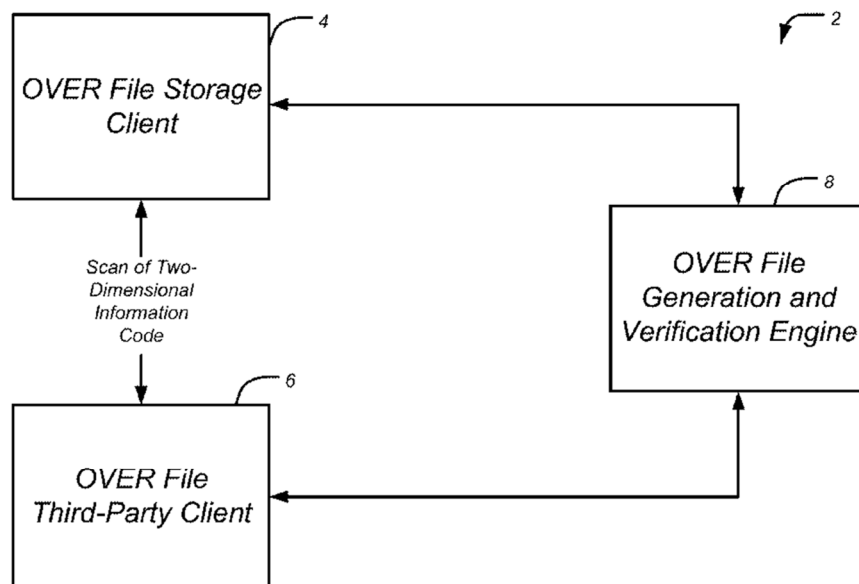


Fig. 1

EX1001, Fig. 1. The OVER file engine stores credential information for a user and generates an OVER file, providing it to the OVER file storage client of the user’s device. EX1001, 4:7-24. The user presents the OVER file to a third party (e.g., a merchant) as though it were a credential, and, based on a scan associated with the OVER file, the third party sends a message to the OVER file engine seeking verification of the OVER file. *Id.* The engine can respond by confirming whether the OVER file is valid. EX1001, 8:4-40.

Claim 1 is generally written from the perspective of an “OVER engine” and includes steps of storing credential information, receiving a request to generate an

OVER file, generating such a file, transmitting it to a user device, receiving a verifying request from a third-party device, verifying a scan associated with the OVER file, and transmitting an authentication message to the third-party device.

Claim 15 recites similar limitations from the perspective of the user client device. It includes steps of transmitting a request for an OVER file, receiving the OVER file, displaying a portion of the OVER file, and receiving an authentication message at the client device.

As to the remaining challenged claims, none adds anything beyond steps conventionally known in the art. EX1005, ¶¶42-75.

B. Prosecution History

The '531 patent was filed as U.S. Application No. 13/794,878 (“the '878 application”) on March 12, 2013, claiming priority to Provisional Application No. 61/740,731, filed December 21, 2012. EX1001, Face. For purposes of this petition only, Visa assumes a priority date of December 21, 2012.

During prosecution, the Examiner issued two office actions, rejecting the pending claims over the prior art. EX1007, 128-49 (citing U.S. Patent Publication No. 2007/0208665 to Ohara and U.S. Patent No. 7,290,146 to Ekers), 62-90 (citing Ohara and U.S. Patent Publication No. 2007/0208665 to Chu). Applicant amended the claims significantly in response. EX1007, 30-48, 105-20. None of the prior art at issue in this proceeding was raised during prosecution.

Among the amendments, Applicant amended claim 1 to no longer require a scan of the OVER file, but to more broadly recite a scan that is “associated with the OVER file.” *Id.* The Examiner responded by allowing the claims. EX1007, 19. In the Notice of Allowance, the Examiner highlighted a single basis for allowance, namely, that Ohara and Chu did not teach the recited step of “generating 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.” *Id.*

C. Background and State of the Art

This petition is supported by the Declaration of Dr. Michael I. Shamos, a Professor in the Carnegie Mellon Department of Computer Science. EX1005, ¶¶1-22; EX1006. As Dr. Shamos explains and as addressed in further detail below, the Challenged Claims would not have been considered new or non-obvious to a person of ordinary skill in the art (“POSA”) at the relevant time.

The brief background described below provides an overview of some important elements of credential storage and verification that Dr. Shamos explains are relevant to a POSA’s understanding as of the ’531 patent’s priority date. EX1005, ¶¶116-227.

1. Credential verification systems

Credential verification systems were well known, including those involving a user, a credential manager, and a third party seeking verification of a credential. For example, U.S. Patent Publication No. 2009/0271321 (“Stafford,” EX1012) taught such a system “for storing, validating and disseminating credential information about an entity.” EX1012, Abstract. Stafford’s system receives and stores credential information, including scans of credentials, and distributes sensitive credential information to third parties using key signatures to unlock their release. EX1012, ¶¶10, 62, 73-75, 93-97, 107-25, Figs. 2-3. The techniques employed by Stafford were not unique to it, but rather represented well-understood and broadly-applied techniques to those skilled in the art. EX1005, ¶¶117-23 (citing EX1019).

One well-established method to facilitate transactions was to use electronic tokens, in a process called “tokenization.” In tokenization, a digital “token” is used as a substitute for a credential such as a credit card. The token could be limited to a single device or transaction, so that if an eavesdropper or malicious third party obtained the token, it could not be used. A credit card number, by contrast, could be used by an unauthorized party. Systems employing electronic tokens would store users’ credential information remotely, associating them with tokens distributed to the users. By providing such a token in a transaction with a third

party, a user would be able to conduct a transaction with the stored credential.

EX1005, ¶¶124-58, 168-90 (citing EX1011-EX1017, EX1020-EX1040).

An example system employing tokenization technology is provided by U.S. Patent Publication No. 2012/0316992 (“Oborne,” EX1011). Oborne is a Visa patent publication teaching a “payment privacy tokenization” (PPT) apparatus that facilitates methods in which users sign up for tokenized transactions, user credentials are associated with a token issued to the user, and the token’s authenticity is verified when used for transactions with third parties. EX1011, ¶¶22, 35, 40-54, Figs. 4-7F. The tokenization techniques employed by Oborne were well-understood by the POSA and similar technologies had been employed in various related applications. EX1005, ¶176-82. *See generally id.*, §VIII.B.

2. Formats used for virtual credentials

When using remote credential verification systems to facilitate transactions, it was recognized to be useful for users to employ virtual representations of credentials to replace mechanisms traditionally provided by physical credentials. EX1005, ¶¶117-23. For example, when using a mobile device to employ credential management systems like virtual wallets, it was convenient to provide visual indications of available credentials. EX1005, ¶¶183-86. For example, U.S. Patent Publication No. 2013/0054454 (“Purves,” EX1013) is a Visa patent publication disclosing methods for enrollment of payment accounts in users’ electronic wallets.

EX1013, Abstract. Purves teaches that a user's accounts may be illustrated using images of credentials such as credit cards. EX1013, ¶85. This type of representation would help users by providing a simple method to choose a credential for a transaction. EX1005, ¶¶183-86.

3. Mechanisms to convey virtual credential information

Various mechanisms were known to initiate a transaction with a third party. In one example, Osborne teaches that various types of interaction could trigger tokenized transactions, such as a Near Field Communication (NFC) interaction. EX1011, ¶49. Similarly, Purves teaches that a QR code may be used to trigger a wallet connection, such as connecting to a merchant. EX1013, ¶64; EX1005, ¶¶186, 191-99 (citing EX1041-1043).

There were also well-known ways of conveying information associated with credential files from a user to a third party. For example, U.S. Patent Publication No. 2013/0212248 ("Neafsey," EX1015) discloses methods of credential management, including systems for disseminating virtual credentials in multiple different formats, including scannable codes like optical codes. EX1015, ¶61; EX1016, 12.

Further, Neafsey teaches that credentials may be generated for different user devices based on device identifiers unique to each device. EX1015, ¶¶48-49; EX1016, 10; EX1005, ¶¶168-69. Such use of device identifiers to tie electronic

representations to particular devices was well-known. EX1005, ¶¶213-18. For example, Osborne teaches including device identifiers such as MAC addresses in its token data when distributing tokens to user devices and using techniques of device fingerprinting to tie its tokens to such devices. EX1011, ¶¶26, 47, 148; EX1005, ¶214. A known benefit of tying a token to a particular device is that an eavesdropper who somehow obtains the token cannot use it on any other device. EX1005, ¶¶117-23.

D. Level of Skill in the Art

As Dr. Shamos explains, a person of ordinary skill in the art (POSA) by December 21, 2012, 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. A POSA could have less education but significant professional experience in one or more of these fields. *See* EX1005, ¶¶89-94.

II. STATEMENT OF THE PRECISE RELIEF REQUESTED FOR EACH CLAIM CHALLENGED

Visa requests review of claims 1-20 of the '531 patent under 35 U.S.C. §311 and AIA §6. The grounds for relief are as follows:

Ground	Claims	Description
1	1-2, 4-14	35 U.S.C. §103: obvious over Osborne ¹
2	3	35 U.S.C. §103: obvious over Osborne and Purves ²
3	1-2, 4-18, 20	35 U.S.C. §103: obvious over Osborne and Neafsey ³
4	3, 19	35 U.S.C. §103: obvious over Osborne, Neafsey, and Purves
5	1, 3-5, 7-16, 18-20	35 U.S.C. §103: obvious over Stafford ⁴ and Purves
6	2, 6, 17	35 U.S.C. §103: obvious over Stafford, Purves,

¹ Osborne was filed on June 7, 2012, and published on December 13, 2012.

Osborne is prior art under pre-AIA 35 U.S.C. §§102(a) and (e).

² Purves was filed on September 21, 2012, and published on February 28, 2013.

Purves is prior art under pre-AIA 35 U.S.C. §102(e).

³ Neafsey was filed on February 13, 2013, and published on August 15, 2013.

Neafsey claims priority to U.S. Provisional Patent Application No. 61/598,219 (“Neafsey Provisional,” EX1016), filed February 13, 2012. As discussed below, Neafsey is available as prior art as of its provisional filing date.

⁴ Stafford was filed on May 31, 2007, and published on October 29, 2009.

Stafford is prior art under pre-AIA 35 U.S.C. §§102(a), (b), and (e).

		and Neafsey
--	--	-------------

This petition provides parallel citations to both Neafsey and corresponding disclosure in Neafsey Provisional, demonstrating that all matter relied on is found in both documents. Under *Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375 (Fed. Cir. 2015), Neafsey is available as prior art under pre-AIA 35 U.S.C. §102(e) as of February 13, 2012, as illustrated by the chart below illustrating exemplary support in Neafsey Provisional for claim 1 of Neafsey. *See* EX1005, ¶¶158-67.

US20130212248	US61/598,219
1. A method comprising:	EX1016, 2, claims 1-14, 18.
providing, with at least one server, a cloud credential management service including generating credentials of at least two different types;	EX1016, 11-12, Figs. 1, 9.
receiving, with the server, a credential request from a customer computer to assign a virtual credential to a mobile device; and	EX1016, 4, 8, 12.
transmitting, with the server, the virtual credential to the mobile device.	EX1016, 4, 12, Fig. 9.

III. CLAIM CONSTRUCTION

Claim terms should be given their ordinary and customary meaning as would be understood by a POSA in light of the specification. 37 C.F.R.

§42.100(b); *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312-13 (Fed. Cir. 2005) (en

banc). Unless otherwise stated, this petition applies the ordinary and customary meaning of the claim terms. The following terms warrant discussion.

A. “OVER file”

Each independent claim recites an “officially verifiable electronic representation (OVER)” file. The claims also use “OVER” or “OVER file” to characterize other claim elements relating to the OVER file (e.g., “OVER engine,” “OVER file generation request”). Like the claims, the specification uses the term “OVER” to refer to an “Officially Verifiable Electronic Representation.” EX1001, 2:28-30. The specification describes that an OVER file may contain “credential information.” EX1001, 6:20-22, 6:54-56. An OVER file may also contain or act as a credential, which may in turn be representative of another credential, such as a driver’s license. EX1001, 12:3-6. This “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 code. EX1001, 9:11-15, 13:61-14:4, Fig. 11; EX1005, ¶¶98-100.

The ’531 patent does not describe that tokens may be either an OVER file or a part of one (such as a representation of a credential). However, Patent Owner’s complaint expressly identifies tokens as OVER files. *See, e.g.*, EX1018, 4 (“Each OVER File is a token....”), 9 (for an “OVER file comprising a virtual representation,” “[t]he token is the ‘virtual representation’”), 16-17 (“The token

(i.e., ‘first OVER file’) acts a first virtual representation of the user’s credentials....” (for related patent)). For the purposes of this petition, Visa applies a construction that includes Patent Owner’s interpretation of this term.

Accordingly, this petition 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 grounds 5-6), but also encompassing a file comprising a token (as asserted in Patent Owner’s infringement complaint and addressed in grounds 1-4). EX1005, ¶¶98-103.

B. “scan”

Claim 1 recites a “scan associated with the OVER file,” and claim 16 recites that a displayed portion of the OVER file is “scanned.” The specification 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.” EX1001, 7:51-8:2. The “scannable code” can be “for example, a barcode or a QR code.” EX1001, 13:61-14:4; *see also id.*, 5:7-25. The specification also refers to using information codes involving radio and electronic transmissions or interactions like Near Field Communication (NFC), Bluetooth, or sensor readings; however, it does not specify that such interactions involve scans and describes these embodiments as alternatives to other embodiments that use scans. EX1001, 5:7-25, 11:64-12:29. Thus, the specification uses the term “scan” to refer to an optical scan, but it does

not use “scan” to refer to other types of interactions like electronic interactions. EX1005, ¶¶104-09.

Nonetheless, Patent Owner has asserted in its complaint that a proximity-payment request (e.g., an NFC interaction) constitutes a scan. EX1018, 10 (“proximity-payment request (i.e., scan associated with the OVER file)”); 36 (“scan the OVER file...such as through an NFC or a card reader” (for related patent)). Accordingly, this petition applies an interpretation of “scan” that encompasses an optical scan (as addressed in Grounds 3-6), while also encompassing an NFC interaction (as addressed in Grounds 1-2 and asserted in the complaint). EX1005, ¶¶104-11.

C. “...verified by an issuing agency...”

Claims 1 and 15 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.” During prosecution, Applicant argued that this phrase requires that the issuing agency verify that the *virtual representation* is an official representation of the credential. *See* EX1007, 44-45; *see also id.*, 40 (pointing to disclosure found at EX1001, 3:50-4:6, 4:25-41, 5:7-25, 6:12-36). Accordingly, 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. EX1005, ¶¶112-15.

IV. GROUND 1: CLAIMS 1-2 AND 4-14 ARE OBVIOUS OVER OBOURNE

A. Overview of Ground

As discussed below, Osborne discloses or suggests each and every element of claims 1-2 and 4-14, arranged as in those claims. In particular, Osborne teaches the use of tokens representative of credentials such as credit cards to perform transactions with third parties, in a manner that meets or renders obvious each element of these claims. This ground applies interpretations of *OVER file* and *scan* consistent with Patent Owner's district court complaint (i.e., encompassing use of a token and an NFC interaction, respectively). *See supra* §§III.A-B; EX1005, ¶228.

As addressed below for element 1.3's requirement that the OVER file's *virtual representation* (mapped here to a token) must be verified as an official representation of a credential by an issuer, Osborne teaches or at least suggests that its token server may be operated by the issuer of a user's credentials. In such a system, it would at minimum have been obvious that the OVER file comprising a virtual representation of the credential has been verified by the issuer as an official representation, since the issuer is the entity issuing the token as well as the credential. As Dr. Shamos explains, such an arrangement was common among issuers of credit cards, who issue both cards and tokens representing the cards. EX1005, ¶229; *see infra* §IV.B.4 (discussing this for element 1.3).

The discussion of claims 1-2 and 4-14 below provides further detail regarding POSAs' rationale to apply Osborne's teachings to arrive at the claimed invention with a reasonable expectation of success.

B. Claim 1

Osborne teaches or suggests each element of claim 1, as discussed below. EX1005, ¶¶230-251.

1. Preamble

1. A computer-implemented method comprising:

Osborne teaches a computer-implemented method. *See, e.g.*, EX1011, ¶¶114-22 (describing computerized system used to perform Osborne's methods); EX1005, ¶231.

2. Element 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;

Osborne teaches an *OVER generation and verification engine (OVER engine)*. Osborne teaches a "payment privacy tokenization apparatus" or "PPT" apparatus to "transform payment token-based purchase orders, via PPT components, into multi-issuer purchase payment funds transfers." EX1011, ¶¶22, 166. This system includes a "token server," also referred to as a "token arbitrator,"

that may be any entity involved in the PPT, such as “a pay network server.”

EX1011, ¶53. Osborne also notes that the “the source of the token” may be the

“issuer” (e.g., a funding source for the user’s account). EX1011, ¶47; *see also id.*,

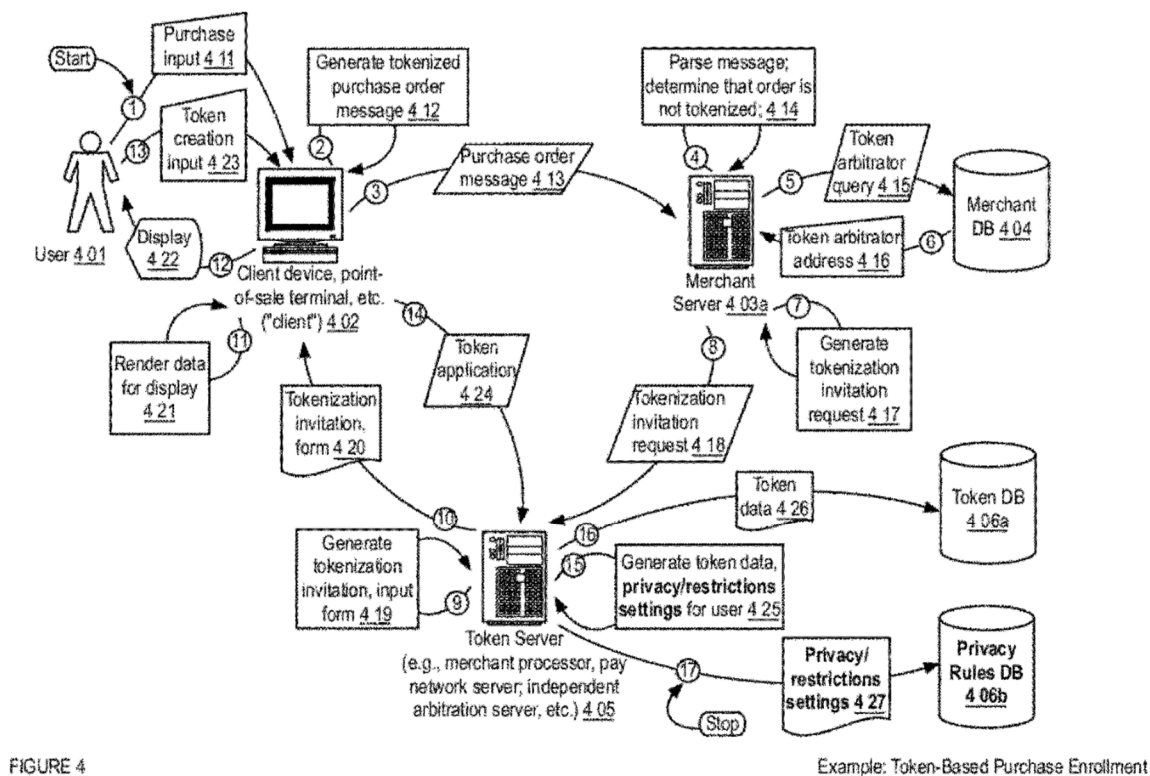
¶48 (noting in XML comments that the token administrator may be the funding

source, or that “alternatively token administrator may be different from funding

source”), ¶29 (user may obtain token from funding source). Osborne depicts the

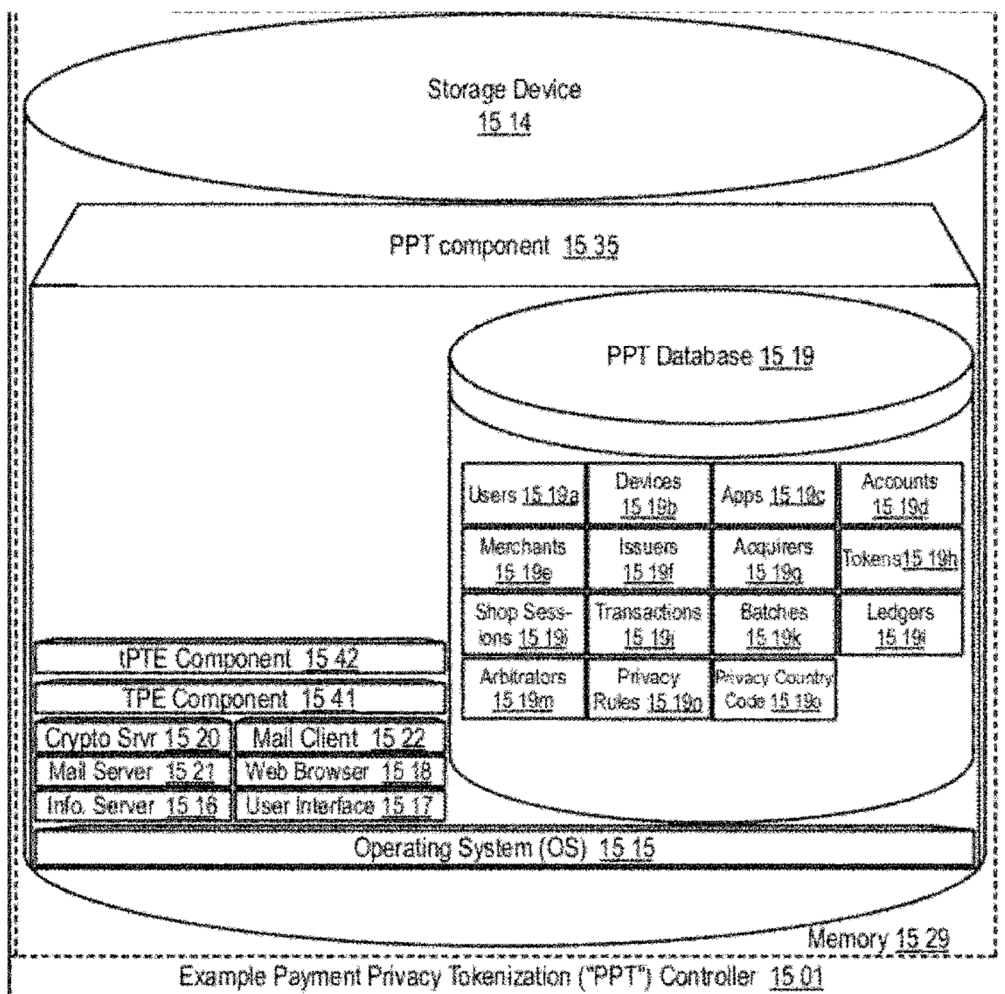
general arrangement of customers, parties, and the pay network server (which can

include the PPT apparatus) in Fig. 4, reproduced below:



EX1011, Fig. 4. As addressed in more detail below for elements 1.3 and 1.6, this apparatus generates and verifies OVER files. *Infra* §§IV.B.4, IV.B.7. Osborne thus discloses the recited OVER engine. EX1005, ¶¶232-33.

Osborne's PPT apparatus stores information associated with a credential of a user for proving the user's identity or qualifications. Osborne's PPT apparatus includes a storage device storing account information in a database, as shown in Fig. 15, excerpted below.



EX1011, Fig. 15; *see id.*, ¶¶114, 146-51. The database’s “Accounts table 1519d,” includes fields with *information associated with a credential* (e.g., information about the user’s credit cards) and useful *for proving the user’s identity or qualifications*, such as “account_number,” “issuer_name,” “account_address,” “routing_number,” etc. EX1011, ¶147. Osborne 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, *proving the user’s identity or qualifications*). EX1011, ¶25; EX1005, ¶234.

Osborne thus teaches element 1.1.

3. Element 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;

To generate token information, the user in Osborne communicates “via a client such as, but not limited to: a personal computer, mobile device, television, point-of-sale terminal, kiosk, ATM, and/or the like,” providing input “indicating the user’s desire to purchase the product.” EX1011, ¶35; *see also id.*, ¶25. If the user desires to use tokenization, the client “may generate a comp[li]eted application form, and provide, e.g., 424, the token application to the token server (either directly or via the merchant server).” EX1011, ¶40; *see also id.*, ¶¶40-47

(describing process of generating and using token), 54 (token authentication). This token application is an *OVER file generation request*. EX1005, ¶235.

Osborne provides an example encoding of a tokenization application form, shown below:

```
POST /purchase.php HTTP/1.1
Host: www.merchant.com
Content-Type: Application/XML
Content-Length: 1306
<?XML version = "1.0" encoding = "UTF-8"?>
<token_application_form>
  <provisional_token_ID>4NFU4RG94</provisional_token_ID>
  <timestamp>2011-02-22 15:22:43</timestamp>
  <user_ID>john.q.public@gmail.com</user_ID>
  <client_details>
    <client_IP>192.168.23.126</client_IP>
    <client_type>smartphone</client_type>
    <client_model>HTC Hero</client_model>
    <OS>Android 2.2</OS>
    <app_installed_flag>true</app_installed_flag>
  </client_details>
  <account_params>
    <account_name> John Q. Public </account_name>
    <account_type> credit </account_type>
    <account_num>123456789012345</account_num>
    <billing_address> 123 Green St., City, ST 12345
    </billing_address>
    <phone> 123-456-7890 </phone>
    <sign> /jpg/ </sign>
    <confirm_type> CVV2 456 </confirm_type>
    <contact_info> SAME AS BILLING </contact_info>
    <country> UK </country>
    <privacy_restriction_type> EU DEFAULT
    </privacy_restriction_type>
  </account_params>
  <shipping_info>
    <shipping_adress> 123 Green St., City, ST 12345
    </shipping_address>
    <ship_type> Express </ship_type>
    <ship_carrier> FedEx </ship_carrier>
    <ship_account> 0908765432 </ship_account>
    <tracking_flag> ON </tracking_flag>
    <sign_flag> ON </sign_flag>
  </shipping_info>
</token_application_form>
```

EX1011, ¶40. This form includes *information associated with the credential*, such as account number, type, billing address, etc., which are stored by Osborne’s PPT apparatus. *Supra* §IV.B.2. The token server uses values extracted from the form when generating a token record. EX1011, ¶41. The request is thus *based on the information associated with the credential*. EX1005, ¶¶236-37.

Osborne thus teaches element 1.2.

4. Element 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;

Osborne teaches that the token server “parse[s] the form to extract data fields and values from the form” to generate a data record and data structure for a token (*OVER file*), as well as a “token identifier” representing the token, which is provided to the user. EX1011, ¶¶47-48, Fig. 5 (showing process); EX1005, ¶238.

As depicted in Fig. 1B (below), the token is a virtual representation of a credential, such as a credit card.

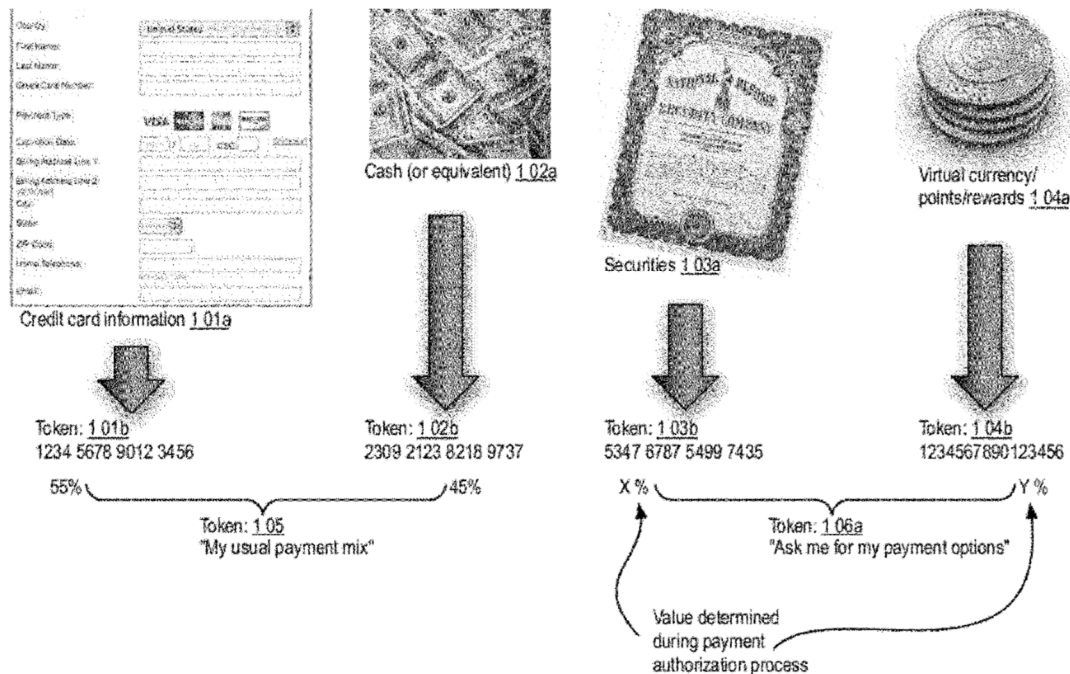


FIGURE 1B

Example: Payment Tokenization

EX1011, Fig. 1B; *see also id.*, ¶25 (confirming that token is “linked to credit card information” and used “in lieu of...card information”). Thus, the token is a *virtual representation of the credential* that is generated *based on the information associated with the credential*. EX1005, ¶239.

Further, Osborne teaches or at least suggests that the token would be verified by the issuing agency as an official representation. As discussed above for element 1.1, Osborne 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. EX1011, ¶¶29, 47-48, 53; *see also id.*, ¶58 (“Issuer server(s)...may maintain details of the user’s account

linked to the payment token.”). By 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. EX1005, ¶¶240-42.

Moreover, as Dr. Shamos explains, a POSA 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 the 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. *Id.*

Finally, to the extent Patent Owner argues that the claim requires that the credential, rather than the token, be verified by the issuer, a POSA would have found it obvious that a credential is verified by virtue of being issued by an official issuer. Indeed, since the purpose of a credential is to be an official representation from the issuer, an issuer would make such a verification as a matter of course when issuing the credential. *Id.*

Osborne thus teaches element 1.3.

5. Element 1.4

transmitting, to the OVER file storage client device of the user, the OVER file in response to the OVER file generation request;

Osborne teaches that a “token may be provided as a data structure via HTTP(S) POST, as a file, as an attachment (e.g. via email), and/or provided to the client device for later use.” EX1011, ¶48. This 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). See EX1011, ¶¶40-41, 46-47, Fig. 5 (below). Osborne thus 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*. EX1005, ¶243.

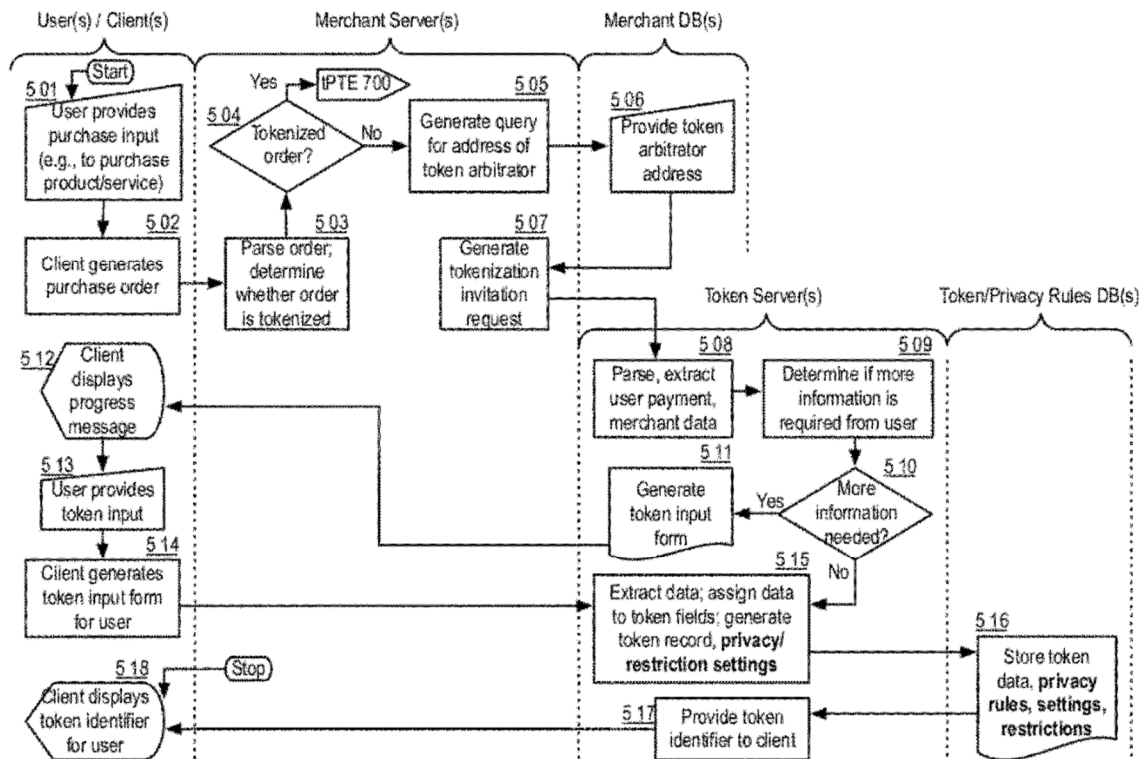


FIGURE 5

Example: Token-Based Purchase Enrollment ("TPE") component 500

Osborne thus teaches element 1.4.

6. Element 1.5

receiving, from an OVER file third-party client verifying device, a verifying request to verify that the OVER file transmitted to the user authenticates the user based on a scan associated with the OVER file on the OVER file storage client device of the user;

Oborne teaches this element as part of a merchant's token arbitration request (*verifying request*) triggered by a purchase order request from a user (*based on a scan*). Beginning with the scan aspect, 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" EX1011, ¶49. This 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). EX1011, ¶50 (client provides "tokenized purchase order message to the merchant server"). As discussed above in §III.B, Patent Owner has argued in district court that transmitting NFC-based payment requests constitutes a scan under the '531 patent. Applying this interpretation to Oborne, since Oborne's RFID/NFC activation triggers the purchase to be performed with the token, the RFID/NFC activation would be a *scan associated with the OVER file on the OVER file storage client device of the user*. EX1005, ¶244.

To process the purchase order request, the merchant server sends a "token arbitration request...to a token server." EX1011, ¶¶51-52. This is the verifying

request of element 1.5. EX1005, ¶245. An example of an encoding of such a request, which includes a token_id field representing a token, is reproduced below.

```
GET /purchase.php HTTP/1.1
Host: www.merchant.com
Content-Type: Application/XML
Content-Length: 1306
<?XML version = "1.0" encoding = "UTF-8"?>
<purchase_order>
  <order_ID>4NFU4RG94</order_ID>
  <timestamp>2011-02-22 15:22:43</timestamp>
  <user_ID>john.q.public@gmail.com</user_ID>
  <client_details>
    <client_IP>192.168.23.126</client_IP>
    <client_type>smartphone</client_type>
    <client_model>HTC Hero</client_model>
    <OS>Android 2.2</OS>
    <app_installed_flag>true</app_installed_flag>
  </client_details>
  <merchant_params>
    <merchant_id>3FBCR4INC</merchant_id>
    <merchant_name>Books & Things, Inc.</merchant_name>
    <merchant_auth_key>1NNF484MCP59CHB27365</merchant_auth_key>
  </merchant_params>
  <purchase_details>
    <num_products>1</num_products>
    <product>
      <product_type>book</product_type>
      <product_params>
        <product_title>XML for dummies</product_title>
        <ISBN>938-2-14-168710-0</ISBN>
        <edition>2nd ed.</edition>
        <cover>hardbound</cover>
        <seller>bestbuybooks</seller>
      </product_params>
      <quantity>1</quantity>
    </product>
  </purchase_details>
  <account_params>
    <token_id>1234567890123456</token_id>
  </account_params>
  <shipping_info>
```

Id. As further addressed below for element 1.6, Osborne teaches that the “token server may parse the token arbitration request message” and “determine whether the user token is authenticated.” EX1011, ¶¶53-55; *see also id.*, ¶25 (“[U]pon receiving a payment token from the user, the merchant may pass the token to a transaction arbitrator.”). Applying Patent Owner’s interpretation of “scan,” Osborne

thus teaches that the OVER engine (token server) receives the recited verifying request from a third-party device based on the recited scan. EX1005, ¶245.

Osborne thus teaches element 1.5.

7. Element 1.6

verifying that the scan associated with the OVER file corresponds with the information associated with the credential of the user that is stored in the OVER engine, in response to the verifying request;

Osborne teaches that the token server processes the token arbitration request triggered by the scan (discussed above for element 1.5) by looking up the account number in a token database. In particular, the token server “extract[s] the payment token from the message,” then issues a query to a database “using the payment token as a search term in the query.” EX1011, ¶53. In response, the database provides “instructions for the token server on how to proceed with payment processing.” *Id.* This includes credential information such as user account numbers, as shown in the highlighted XML example reproduced below:

```

<?XML version = "1.0" encoding = "UTF-8"?>
<issuer_data>
  <auto_default>false</auto_default>
  <user_contact>in-app</user_contact>
  <device_id>B17BP927</device_id>
  <default>
    <issuer>
      <issuer_id>A12345</issuer_id>
      <issuer_name>Bank de Tolkien</issuer_name>
      <issuer_IP>123.45.67.891</issuer_IP>
      <account_type>token</account_type>
      <account_number>1234567890123456</account_number>
      <percentage>65</percentage>
    </issuer>
    <issuer>
      <issuer_id>B12345</issuer_id>
      <issuer_name>ABC Credit Union</issuer_name>
      <issuer_IP>223.25.67.091</issuer_IP>
      <account_type>token</account_type>
      <account_number>6543210987654321</account_number>
      <percentage>25</percentage>
    </issuer>
    <issuer>
      <issuer_id>C67890</issuer_id>
      <issuer_name>BNR Bank</issuer_name>
      <issuer_IP>153.65.87.231</issuer_IP>
      <account_type>token</account_type>
      <account_number>1234567890123456</account_number>
      <percentage>10</percentage>
    </issuer>
  </default>
</issuer_data>

```

Id. Osborne further teaches that the “token server may determine whether the user token is authenticated,” for example, where “no XML data is available associated with the payment token,” this indicates that the “user has not signed up for payment tokenization services.” EX1011, ¶54; *see also id.*, ¶69 (determining “whether the user token is authenticated”). In other words, the query determines whether the *scan* (RFID/NFC interaction) *associated with the OVER file* (token) *corresponds with the information associated with the credential of the user stored*

in the OVER engine (whether the database query for the token returns the user's account details or not), thereby performing the recited step of verifying. EX1005, ¶246.

Osborne also teaches that further verification may optionally be performed. For example, the token server may verify using biometric identification or may request a "user name and password to enable the token for payment processing." EX1011, ¶54. Other verification options include using an authentication chip communicating in proximity with the user's card via RFID or similar technology. EX1011, ¶26. Thus, Osborne teaches that a scan's correspondence with the user's credential information may be verified using various complementary techniques. EX1005, ¶247.

Osborne thus teaches element 1.6.

8. Element 1.7

transmitting, to the OVER file third-party client verifying device, an authenticating message comprising an indicator of whether the scan associated with the OVER file on the device of the user corresponds to the information associated with the credential of the user that is stored in the OVER engine.

As discussed for element 1.6, Osborne's token server determines whether the user token is authenticated (e.g., EX1011, ¶¶54, 69), which corresponds to

determining whether the recited scan corresponds to the recited stored information.

EX1005, ¶248.

Osborne further teaches sending *an authenticating message comprising an indicator* of this determination. For example, 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.’” EX1011, ¶69. As shown in Fig. 7A, steps 712a-b, this message is sent to the merchant server (*third-party client verifying device*).

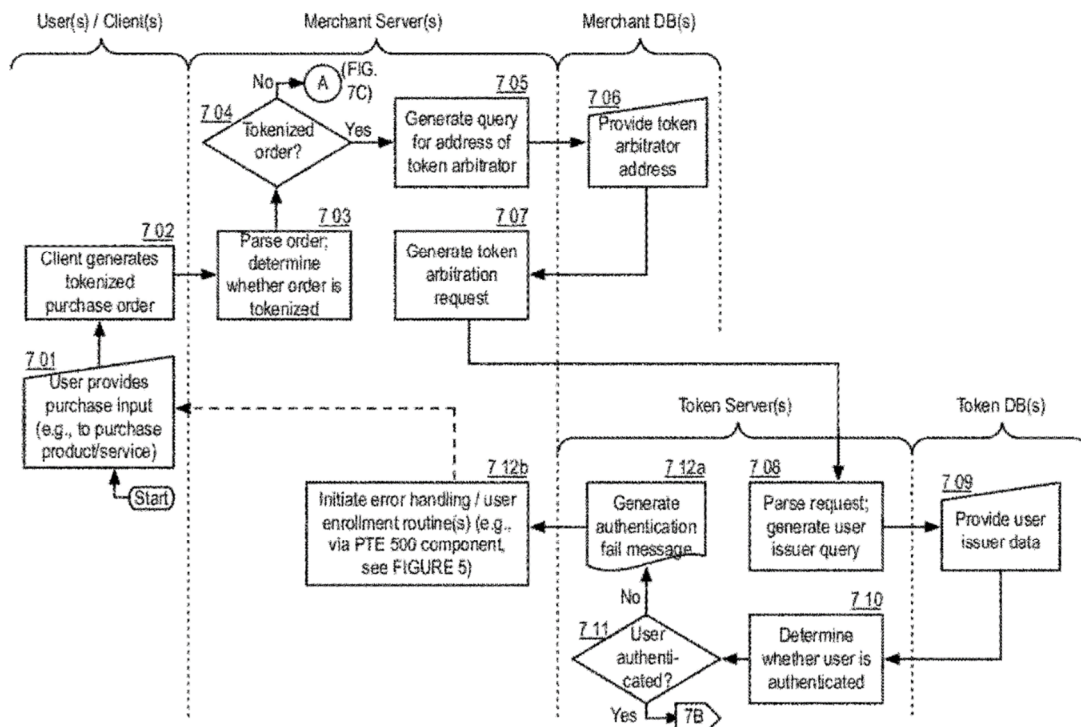


FIGURE 7A

Example: Token-Based Purchase Transaction Execution ("PTE") component 700

EX1011, ¶69, Fig. 7A. This is an indication that the scan is not associated with the stored user data. EX1005, ¶249.

On the other hand, if the user token is authenticated, then the “token server may continue processing.” EX1011, ¶¶69. The stored user account information is then used to procure payment authorization, and a message is sent to the merchant server indicating the result. EX1011, ¶¶63 (“token server...may in turn forward the authorization success message, e.g., 647, to the merchant server”), 61 (“‘authorization fail’ message”), 70 (“authorization in progress” message), Figs. 7B-C. Any of these messages is an indicator that the token was authenticated, and thus that the scan corresponded to the stored user credential information. EX1005, ¶¶250-51.

Oberne thus teaches element 1.7.

Accordingly, claim 1 was obvious over Oberne. EX1005, ¶¶230-251.

C. Claim 2

Claim 2 depends from claim 1 adds the word “first” before each of claim 1’s OVER file, OVER file storage client device, virtual representation, and official representation. Claim 2 then recites three elements identical to elements 1.2-1.4, except that (1) the word “second” is applied instead of the word “first”; (2) the generation copied from element 1.3 need not be “based on the information associated with the credential of the user”; and (3) the second OVER file is “is invalid for use in the first OVER file storage client device for authenticating the user.” Oberne teaches these elements.

The first two of these aspects of claim 2 are satisfied by a user having two devices and receiving OVER files on each device. This would have been obvious in view of Osborne. A POSA would have expected users to use multiple devices; indeed, Osborne 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. EX1011, ¶148; EX1005, ¶252-53.

The 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 the POSA based on Osborne's disclosure. For example, Osborne teaches that "device fingerprinting may be utilized" to provide "additional security" for use of Osborne's tokens. EX1011, ¶26. Similarly, Osborne provides an example token data structure including a "client_fingerprint" field with device-identifying information like the client's MAC address. EX1011, ¶47. To obtain the additional security taught by Osborne, a POSA would be motivated to employ Osborne's device fingerprinting to tie a given token to a given device, such that the token for a second device would be invalid in a first device (since the device's fingerprint would not match). EX1005, ¶¶254-55.

Accordingly, claim 2 was obvious over Osborne.

D. Claim 4

Claim 4 depends from claim 1 and further recites three additional steps:

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;

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

storing, by the OVER engine, the status indicator.

Regarding requesting authentication and receiving a status indicator, Osborne meets these limitations in at least two ways. First, when adding a user's card to a wallet for Osborne's system, Osborne teaches verifying the pay card's information (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." EX1011, ¶108. In light of this teaching, a POSA 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. EX1005, ¶¶219-21 (citing EX1044), 256.

Second, Osborne teaches that, when a tokenized transaction is performed, the token or pay network server contacts "issuer server(s) corresponding to the

payment token.” EX1011, ¶¶57-58. The issuer server “determine[s] whether the user can pay for the transaction using funds available in the account.” EX1011, ¶¶60-61. The issuer then provides a response, either an “authorization fail” message or “notification of successful authorization.” EX1011, ¶¶61-63. Such authorization success or fail messages would also be status indicators (e.g., indication of a valid credential) and credential information associated with the credential (e.g., confirmation of sufficient funds), received based on a request to validate the credential’s coverage of a transaction. EX1005, ¶257. As Dr. Shamos explains, a POSA would have employed such an arrangement even if the token server and issuer server were operated by the same party, since such authorization and responses correspond to standard procedures used for transaction processing in a payment network, allowing Osborne’s system to be integrated into a system for traditional payment processing in a straightforward and predictable manner. *Id.*

Storing the status indicator would also have been obvious in view of Osborne. For example, Osborne teaches generating “a transaction data record” for the pay network server to “store the details of the transaction and authorization.” EX1011, ¶62. Osborne also teaches that “the token server may be...a pay network server.” EX1011, ¶39. A POSA would view these teachings as suggesting that the token server can store a received status indicator. More practically, 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), a POSA routinely would have stored the status indicator during normal token server operations. EX1005, ¶¶258-59.

Accordingly, claim 4 was obvious over Osborne.

E. Claim 5

The computer-implemented method of claim 4, wherein the status indicator indicates the credential is valid.

As discussed for claim 4, Osborne teaches receiving various status indicators including receiving a verification response from an issuer when adding a new credential and an authorization message approving a transaction. *See* EX1011, ¶¶57-63, 108. Either such message would indicate that the credential was valid. EX1005, ¶260-61. Osborne thus renders claim 5 obvious.

F. Claim 6

The computer-implemented method of claim 1, further comprising generating, by the OVER engine, a device identifier for the credential, wherein the device identifier limits the credential to the OVER file storage client device.

As discussed for claim 2, Osborne teaches using “device fingerprinting” to provide “additional security.” EX1011, ¶26. Osborne’s “token data structure” thus includes a “client_fingerprint” with device information such as a MAC address. EX1011, ¶¶47-48, 148 (identifying devices using device_ID, device_MAC, etc.).

As explained for claim 2, applying the device fingerprinting taught by Osborne would limit the token (and thus the credential) to the device having a given fingerprint. Osborne thus renders claim 6 obvious. EX1005, ¶¶213-18, 262-63.

G. Claim 7

The computer-implemented method of claim 4, wherein the status indicator indicates an invalid credential and the credential information indicates a reason for the invalid credential.

As discussed for claim 4, Osborne teaches status indicators indicating whether a credential is valid (e.g., a verification and/or authorization response). A negative response for either indicator would indicate an invalid credential. EX1005, ¶262. Moreover, it would be obvious for the credential information to indicate a reason for invalidity; for example, if the information provided for the credential did not match the issuer's information, it would be routine to indicate this mismatch in a rejection response. Further, where a credential was not valid for a given transaction, Osborne expressly teaches indicating the reason for invalidation. For example, an issuer response can indicate lack of funds, or indicate that a "number of failed authorization attempts exceeds a threshold" by sending a "transaction terminated" message. EX1011, ¶72. Each of these messages indicates a reason that the credential is invalid. EX1005, ¶¶264-65.

Thus, claim 7 was obvious over Osborne.

H. Claim 8

The computer-implemented method of claim 1, 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.

Oborne teaches that its systems may store data objects locally or in “remote storage facilities.” EX1011, ¶133. As discussed for element 1.1, Oborne teaches storing information associated with a credential in a database. *See* EX1011, ¶148 (listing fields such as “account_number,” “routing_number,” etc.); *see also id.*, ¶47 (token data structure includes account_num field). These fields are references to a credential, and in light of Oborne’s teaching that data may be stored remotely, it would have been obvious to store the credential referred to by the fields remotely. EX1005, ¶¶266-68.

Oborne thus renders claim 8 obvious.

I. Claims 9-10

9. The computer-implemented method of claim 1, further comprising storing, by the OVER engine, user-specific information.

10. The computer-implemented method of claim 9, wherein the user specific-information comprises at least one of:

biometric information, location information, a password, or a device identifier.

Oborne teaches the elements of claims 9 and 10. As recited in claim 9, Oborne teaches that its PPT system stores user-specific information in a “Users table,” including, for example, the user’s “state, address firstline, address secondline, zipcode,” etc. EX1011, ¶148; *see id.*, Fig. 15, ¶47 (token server stores user’s address). These entries include at least location information (e.g., address, zip code, ...) about the user, as recited in claim 10. EX1011, ¶¶148 (also storing “device_ID,” “device_GPS,” “password”), 30 (biometric and/or like recognition). Oborne thus renders claims 9 and 10 obvious. EX1005, ¶¶269-71.

J. Claim 11

The computer-implemented method of claim 1, further comprising checking, by the OVER engine, a status indicator of a stored credential, wherein the OVER file generation request comprises a credential identifier for specifying which credential among a plurality of credentials of the user is officially represented by the OVER file.

As discussed for claim 4, Oborne teaches receiving and storing various status indicators. A POSA would have found it obvious to accomplish the disclosed different processing in response to different statuses (e.g., success, failed, insufficient funds, etc.) by checking the received status indicator. EX1005, ¶¶219-21, 272.

Regarding a credential identifier, Oborne teaches that the token application identifies a user credential by a credential identifier (account_num field), which is

stored when creating a token, with the token data structure indicating which account number(s) correspond to a given token. *See* EX1011, ¶¶40, 47 (identifying by account numbers of user's credentials associated with token); *see also id.*, ¶25, Fig. 1B (token may indicate mix of one or more specified credentials via token indicators). EX1005, ¶¶208-12, 273-74.

Accordingly, claim 11 was obvious over Osborne.

K. Claim 12

The computer-implemented method of claim 11, wherein verifying that the scan of the OVER file corresponds with the credential of the user comprises comparing the credential identifier with one or more stored credentials.

When a token arbitration request is processed, the token server generates a query to retrieve token data. EX1011, ¶69. The stored token data includes one or more stored credentials. *See* EX1011, ¶¶47 (listing account numbers and other details), 148 (accounts table stores credential data including account numbers, routing numbers, etc.). By using the token identifier to query a database and retrieve stored credentials (e.g., cards' account numbers), Osborne is comparing the credential identifier with the stored credentials. EX1005, ¶¶275-76.

Accordingly, claim 12 was obvious over Osborne.

L. Claim 13

The computer-implemented method of claim 12, wherein the authentication message comprises the status indicator of the stored credential when the credential identifier matches a stored credential.

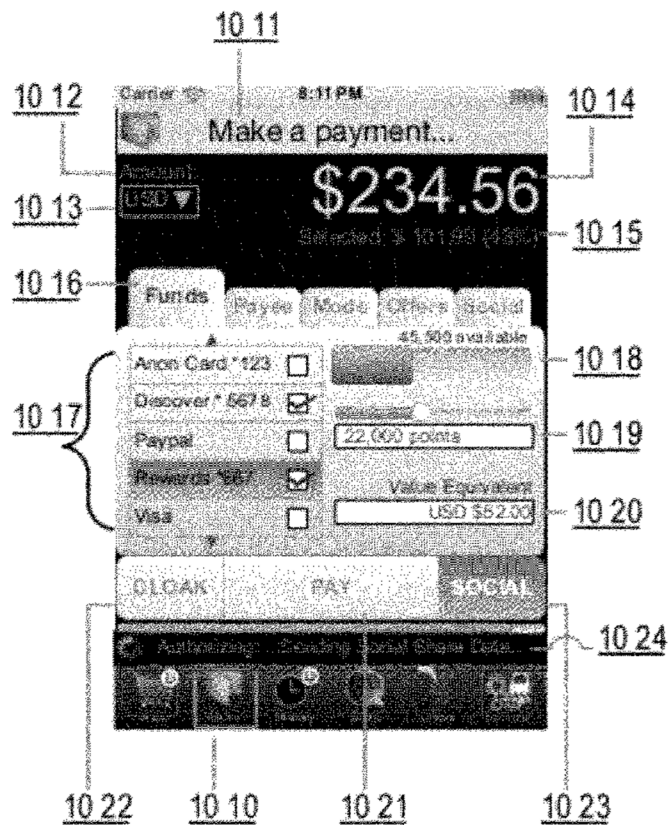
As discussed for claim 4, Osborne teaches that when a transaction for a given account is approved, a “notification of successful authorization” is sent to the token server. EX1011, ¶¶61-63. This constitutes an authentication message comprising the status indicator. EX1005, ¶277. Further, this is sent “when the credential identifier matches a stored credential” because, as discussed for claim 12, the accounts are identified by using the credential identifier (token ID) as a database query to retrieve stored account information (matching identifier to stored credentials). *See* EX1011, ¶69.

Osborne thus renders claim 13 obvious. EX1005, ¶¶277-78.

M. Claim 14

The computer-implemented method of claim 1, wherein the OVER file comprises a portion of the stored credential.

Osborne teaches that various credential details including account numbers are stored in a token data structure. *See* EX1011, ¶54. Osborne further teaches that the user device may include interface diagrams displaying a portion of a credential, such as a part of an account number. EX1011, ¶85; *see id.*, Fig. 10A (excerpted below).



In view of this disclosure, a POSA would have found it obvious to include a portion of the stored credential (e.g., part of an account number) in the OVER file in order to achieve the disclosed display of portions of credentials. EX1005, ¶¶279-81.

Osborne thus renders claim 14 obvious. *Id.*

Accordingly, claims 1-2 and 4-14 were obvious over Osborne. EX1005, ¶¶228-81.

V. GROUND 2: CLAIM 3 IS OBVIOUS OVER OBERNE AND PURVES

Claim 3 depends from claim 1 and recites “generating, by the processor of the OVER engine, the credential, wherein the credential is generated when the processor determines that no credential of the user is stored.” Osborne and Purves teach this element.

Osborne teaches providing “user interface elements to generate new tokens” by providing a funding source and relevant information. EX1011, ¶29. Osborne’s PPT also uses “token identifiers,” to ensure that each token is “unique.” EX1011, ¶47; EX1005, ¶¶292-93.

To the extent Osborne does not expressly disclose that this process includes generating *the credential*, doing so would be obvious in view of Purves. Purves teaches that a customer with a wallet account “may obtain a new gift card...or a reloadable prepaid card.” EX1013, ¶83 (discussing “new card” personalization); EX1005, ¶294.

A POSA would have been motivated to combine Osborne and Purves with a reasonable expectation of success to arrive at the claimed invention. Both references are directed to similar applications, including virtual wallets and credentials, and the teachings of Purves would be recognized as useful to add new credentials to Osborne’s digital wallet. EX1005, ¶¶295-96. It would have been common sense to generate the new credential *when the processor determines that*

no credential of the user is stored, since the purpose of Osborne’s tokens is to represent a credential; generating the new credential increases the benefit of Osborne’s tokenization system. *Id.* This 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.*

Accordingly, claim 3 was obvious over Osborne and Purves. EX1005, ¶¶292-96.

VI. GROUND 3: CLAIMS 1-2, 4-18 AND 20 ARE OBVIOUS OVER OBORNE AND NEAFSEY

A. Overview and Rationale to Combine

As discussed for Ground 1, Osborne teaches or suggests each element of claims 1-2 and 4-14. Claims 15-16 and 18-20 include similar limitations, but with elements recited from the perspective of the user device. For elements 1.5-1.6, Ground 1 applied a construction of “scan” encompassing NFC interactions. However, an optical scan would also have been obvious, as exemplified by Neafsey. Similarly, element 15.3 recites a step of “displaying a portion of the OVER file,” which Neafsey also teaches.

In particular, Neafsey teaches various formats of virtual credentials for conducting transactions. Among these are optically-scannable codes, such as QR and bar codes. EX1015, ¶61; EX1016, 12; *see* EX1011, ¶32 (QR and barcodes may

be scanned with camera). A POSA would have been motivated to incorporate an optically-scannable code into an OVER file to be used to trigger the use of tokens to purchase goods, in a manner similar to Osborne’s disclosure of using NFC or mag stripe interactions, as Neafsey teaches that optically-scannable codes would serve similar roles. The combination would thus be a simple substitution of known elements to achieve predictable results. EX1005, ¶¶317-18; *see KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 416-17 (2007). Doing so would provide greater flexibility to users, increasing convenience and allowing a greater range of mobile devices to be employed. EX1005, ¶318.

A POSA would also have a reasonable expectation of success in this combination. Indeed, Osborne expressly teaches the use of QR and bar codes in conjunction with similar transactions. *See* EX1011, ¶¶80 (QR code for money transfer), 93 (payment via “user-obtained QR code” alternative to NFC). Thus, a POSA would expect success in using optically-scannable codes to stand in for credentials (e.g., as a scannable part of an OVER file) to trigger a tokenized transaction as taught by Osborne. EX1005, ¶319; *see supra* §I.C.3.

B. Claims 1-2 and 4-14

As discussed for Ground 1, Osborne teaches or suggests each element of claim 1 including a *scan* as recited in elements 1.5-1.6. It would also have been obvious to use an optically-scannable code (e.g., a QR code) in place of an NFC or

similar interaction to trigger a tokenized purchase in Osborne. As discussed in §VI.A, a POSA would be motivated to use such codes in view of Osborne and Neafsey. In this combination, scanning an optically-scannable code would replace the use of NFC or mag stripe interactions in Osborne, invoking token use in a similar way. The remaining claim elements for claims 1-2 and 4-14 would be obvious for the same reasons discussed above for Ground 1. *See supra* §IV. Accordingly, claims 1-2 and 4-14 were obvious over Osborne and Neafsey.

EX1005, ¶320.

C. Claim 15

Osborne and Neafsey teach each element of claim 15, as discussed below.

EX1005, ¶¶321-29.

1. Preamble

15. A computer-implemented method comprising:

Osborne teaches a computer-implemented method. EX1005, ¶322; *see supra* §IV.B.1.

2. Element 15.1

transmitting, from an officially verifiable electronic represent (OVER) file storage client device of a user to an OVER file generation and verification engine, an OVER file generation request to provide authentication of the user based on information associated with a

credential of the user, the credential proving the user's identity or qualifications;

Element 15.1 includes aspects from elements 1.1 and 1.2, written from the perspective of the user's device. Thus, Osborne in view of Neafsey teaches element 15.1 for similar reasons. *See supra* §§IV.B.2-3; EX1011, ¶¶22, 25, 29, 40-47, 166 (OVER file generation request sent to OVER engine), 114, 146-51 (based on information associated with credential proving the user's identity or qualifications); EX1005, ¶323.

3. Element 15.2

receiving, at the OVER file storage client device of the user, an OVER file in response to the OVER file generation request, the 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;

Element 15.2 includes aspects from elements 1.3 and 1.4, written from the perspective of the user's device. Thus, Osborne in view of Neafsey teaches element 15.2 for similar reasons. *See supra* §§IV.B.4-5; EX1011, ¶¶25, 29, 41, 46-48, 53, 58, Figs. 1B, 5; EX1005, ¶324.

4. Element 15.3

displaying a portion of the OVER file to an OVER file third-party client verifying device to authenticate the user; and

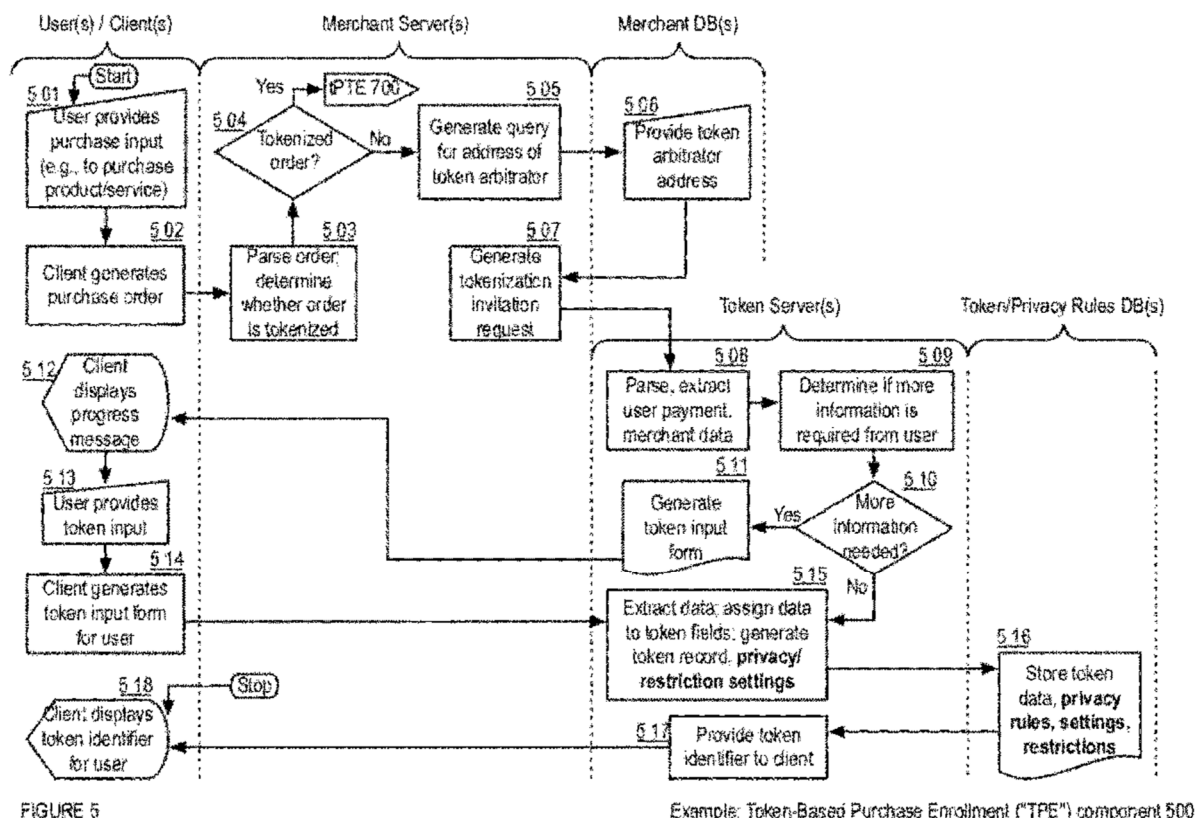
As discussed for element 1.5, Osborne teaches “activating a RFID/NFC” device to initiate a transaction using a token (OVER file). EX1011, ¶49. Neafsey teaches generating “virtual credentials” in “multiple formats,” including optical credentials. EX1015, ¶61; EX1016, 12. As discussed in §VI.A, a POSA would have been motivated to incorporate an optically-scannable credential (e.g., a bar or QR code) into an OVER file to trigger tokenized transactions, thereby providing greater flexibility to users. The process of using such a scannable code would naturally involve *displaying a portion of the OVER file* to a third-party client verifying device to authenticate the user, similar to how Osborne’s RFID/NFC activation is used to trigger authentication. EX1005, ¶¶325-26. Osborne and Neafsey thus teach element 15.3.

5. Element 15.4

receiving, at the OVER file storage client device of the user, an authentication message comprising a status indicator indicating whether the OVER file corresponds to the credential of the user.

As discussed for element 1.7, Osborne teaches sending a status indicator indicating whether the user is authenticated for use of the credential associated with the token (i.e., *OVER file corresponds to the credential of the user*). Where the authentication fails, the PPT can “initiate an error-handling routine and/or a user enrollment routine,” as depicted in Fig. 5. EX1011, ¶69. This includes sending

a message to the user to set up tokenization (such as a progress message showing a token input form 512 or a token identifier 518). EX1011, ¶¶46-48, Fig. 5 (below).



Such messages comprise *a status indicator indicating whether the OVER file corresponds to the credential of the user* because the token input form indicates that the user's credential does not correspond to the credential, and the token identifier indicates that it now does. EX1005, ¶327. Likewise, when token authentication is successful, the "token server may continue processing," which includes sending an authorization message to the user. EX1011, ¶¶61, 63, 69-70. Such messages (whether indicating successful or unsuccessful authorization)

include status messages indicating that the OVER file corresponds to the user's credential, because they are sent based on successful authentication. EX1005, ¶¶327-28; *see also supra* §§IV.D, IV.J, (discussing further status indicators).

Oborne and Neafsey thus teach element 15.4, and claim 15 was obvious over Oborne and Neafsey. EX1005, ¶¶328-29.

D. Claim 16

The computer-implemented method of claim 15, wherein the displayed portion of the OVER file is scanned as part of authenticating the user.

As discussed for claim 15, it would have been obvious to use an optically-scannable code as taught by Neafsey as part of an OVER file sent to the user in order to trigger a tokenized transaction, in a manner similar to Oborne's NFC/RFID activation. *Supra* §VI.C.5. Use of such a code would involve scanning it, as that is how optical codes typically function. EX1005, ¶¶330-31.

Thus, claim 16 was obvious over Oborne and Neafsey.

E. Claim 17

The computer-implemented method of claim 15, wherein the OVER file comprises a device identifier, wherein the device identifier limits the validity of the OVER file to the device of the user.

As discussed for claim 6, Oborne teaches or suggests including a device identifier in an OVER file, which limits the OVER file's validity to the user's

device. *Supra* §IV.F. Claim 17 would have been obvious over Osborne and Neafsey for the same reasons. EX1005, ¶332.

F. Claim 18

The computer-implemented method of claim 15, further comprising:

collecting, by the device, user-specific information; and

transmitting, by the device, the user-specific information to a credential engine, wherein the user-specific information is included in the OVER file.

Osborne teaches collecting user-specific information by a user device. For example, an application form is provided to a user device and used for token generation. EX1011, ¶¶40, 46-47. This form includes user-specific information (account number, address, name, etc.), as illustrated below.

```

POST /purchase.php HTTP/1.1
Host: www.merchant.com
Content-Type: Application/XML
Content-Length: 1306
<?XML version = "1.0" encoding = "UTF-8"?>
<token_application_form>
  <provisional_token_ID>4NFU4RG94</provisional_token_ID>
  <timestamp>2011-02-22 15:22:43</timestamp>
  <user_ID>john.q.public@gmail.com</user_ID>
  <client_details>
    <client_IP>192.168.23.126</client_IP>
    <client_type>smartphone</client_type>
    <client_model>HTC Hero</client_model>
    <OS>Android 2.2</OS>
    <app_installed_flag>true</app_installed_flag>
  </client_details>
  <account_params>
    <account_name> John Q. Public </account_name>
    <account_type> credit </account_type>
    <account_num>123456789012345</account_num>
    <billing_address> 123 Green St., City, ST 12345
    </billing_address>
    <phone> 123-456-7890 </phone>
    <sign> /jqp/ </sign>
    <confirm_type> CVV2 456 </confirm_type>
    <contact_info> SAME AS BILLING </contact_info>
    <country> UK </country>
    <privacy_restriction_type> EU DEFAULT
    </privacy_restriction_type>
  </account_params>
  <shipping_info>
    <shipping_address> 123 Green St., City, ST 12345
    </shipping_address>
    <ship_type> Express </ship_type>
    <ship_carrier> FedEx </ship_carrier>
    <ship_account> 0908765432 </ship_account>
    <tracking_flag> ON </tracking_flag>
    <sign_flag> ON </sign_flag>
  </shipping_info>
</token_application_form>

```

EX1011, ¶40. Osborne thus teaches the first element of claim 18. EX1005, ¶333.

Oborne further teaches sending this form to a token server, and extracting its data fields to generate the token data record. EX1011, ¶47. Thus, Oborne also teaches the second element of claim 18. EX1005, ¶¶334-35.

Claim 18 was thus obvious over Oborne and Neafsey.

G. Claim 20

The computer-implemented method of claim 15, wherein when the status indicator indicates an invalid credential, and the authentication message comprises a reason for the invalid credential.

Claim 20 contains limitations paralleling claim 7. As discussed for claim 7, Oborne teaches these limitations. *Supra* §IV.G; EX1005, ¶¶336-38.

Accordingly, claims 15-18 and 20 were obvious over Oborne and Neafsey. EX1005, ¶¶317-38.

VII. GROUND 4: CLAIMS 3 AND 19 ARE OBVIOUS OVER OBORNE, PURVES, AND NEAFSEY

A. Claim 3

Claim 3 depends from claim 1. As discussed in Ground 2, claim 3 would have been obvious in view of Oborne and Purves. And as discussed in Ground 3, it would have been obvious in view of Neafsey to use an optically-scannable virtual credential in combination with Oborne's token system. In conjunction, a POSA would have been motivated to include both Neafsey's optically-scannable virtual credentials and Purves's teachings to generate new credentials with Oborne's

system to arrive at the subject matter of claim 3, as a POSA would have viewed the three references as compatible and the reasons for combining discussed in Grounds 2 and 3 would have consistently applied to lead to this combination. EX1005, ¶¶339-41.

B. Claim 19

Claim 19 depends from claim 15, reciting “The computer-implemented method of claim 15, wherein when the OVER file comprises a credential image.” As discussed above for Ground 3, Osborne and Neafsey render claim 15 obvious. The further combination with Purves renders claim 19 obvious.

Purves teaches that a virtual wallet “panel 1210 may display an image of the card (e.g., from the issuer),” providing the customer with a helpful image representative of the credential. EX1013, ¶85; *see id.*, ¶39 (describing “automatically retriev[ing] an image of the payment account”). In some examples, the credential image may be a card image including account information (or a virtual simulation of such an image), optionally with sensitive information obscured. EX1013, ¶108 (transmitting “card_image” in XML file), ¶112; EX1005, ¶¶73-74, 342-44.

Osborne, Purves, and Neafsey each provide complementary teachings regarding virtual credentials. EX1005, ¶345. A POSA would have been motivated to combine Purves’s disclosure regarding providing credential images with Osborne

and Neafsey’s virtual credentials to include a credential image as part of an OVER file also including a token as taught by Osborne and a scannable code as taught by Neafsey to provide an improved interface for users with a simple visual indication of the credentials to be invoked in a tokenized transaction. EX1005, ¶¶345-46.

Accordingly, claims 3 and 19 were obvious over Osborne, Neafsey, and Purves.

VIII. GROUND 5: CLAIMS 1, 3-5, 7-16, AND 18-20 ARE OBVIOUS OVER STAFFORD AND PURVES

A. Overview and Rationale to Combine

The combination of Stafford and Purves renders claims 1, 3-5, 7-16, and 18-20 obvious.

In particular, Stafford teaches a system for “validating and disseminating credential information” that meets almost all elements of the independent claims as well as many dependent claim limitations. EX1012, Abstract. Instead of tokens, Stafford’s system uses key signatures (e.g., hash values for encrypted files) to verify users’ identity and provide credential information to a third party. *See* EX1012, Fig. 3, ¶¶107-21.

Stafford discloses methods for providing credentials to third parties that parallel the methods in the ’531 patent. Stafford’s system stores credential information for a user (“entity”) in a credential database, provides users key signatures representing those credentials, and allows a third party (“IdBus1”) with

which the user has shared the key signatures to receive credential verification. *See* EX1012, ¶¶10, 97-102, 108, 115, 118-26, Figs. 2-3; EX1005, ¶¶350-52.

Stafford teaches that the key signatures and other information may be provided to a third party “online or in person,” and that the “delivery process may vary” based on the information provided and the recipient. EX1012, ¶¶106-13. Stafford thus expressly suggests including other information with its key signatures and employing various known delivery processes. EX1005, ¶353. Such known processes and information would include using an optical scan for delivery and including an image as a virtual representation of a credential in an OVER file, both of which are taught by Purves. In particular, Purves teaches providing issuer-verified representations of credentials (such as credit card images), as well as triggering transactions using QR codes. EX1003, ¶73. It would have been obvious to use these features as part of Stafford’s credential-distribution system (1) to provide user devices convenient images of the credentials they are sharing with third parties and (2) to use the well-known QR code format to transfer Stafford’s key signatures to the third party by providing QR-encoded key signatures to the user. EX1005, ¶353.

A POSA would have been motivated to combine Stafford and Purves with a reasonable expectation of success to arrive at the claimed invention. Both references are directed to similar applications (electronic use of credentials

replacing physical credentials typically carried in physical wallets, such as driver's licenses and credit cards). EX1005, ¶354. Further, incorporating features such as credential images and QR codes into a credential management system like Stafford's would have been straightforward, as the use of these features would have been familiar to the POSA and their application would have been predictable. *Id.*; *supra* §I.C.2-3.

A POSA would have recognized various benefits from incorporating Purves's credential images into Stafford's system. For example, 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. EX1005, ¶355.

Similarly, a POSA would have viewed Purves's QR codes as a convenient way to convey key signatures to third parties in a more efficient and reliable manner than reading or typing a code manually, both of which are slow and error-prone. By adapting Stafford's credential management system to provide QR-encoded key signatures, a POSA would reasonably have expected to achieve these benefits for users. EX1005, ¶356; *supra* §I.C.3.

The claim discussion below provides further detail regarding POSAs' rationale to combine Stafford and Purves to arrive at the claimed invention with a reasonable expectation of success. EX1005, ¶357.

B. Claim 1

Stafford and Purves teach each element of claim 1, as discussed below.

EX1005, ¶¶358-80.

1. Preamble

Stafford and Purves teach a computer-implemented method. *See, e.g.*, EX1012, ¶54, Fig. 1; EX1013, ¶¶130-46; EX1005, ¶359.

2. Element 1.1

Stafford teaches element 1.1, as illustrated in Fig. 1 (below), which depicts a system (*OVER engine*) that stores credential information for proving users' identity or qualifications. EX1012, ¶54 ("FIG. 1 illustrates a system 100 for storing, validating and disseminating credential information about an entity."), Fig. 1; *see also id.*, claim 1 ("method of compiling a credential database including" receiving and verifying credential information, generating data representations of credential information and document, and storing them in encrypted form).

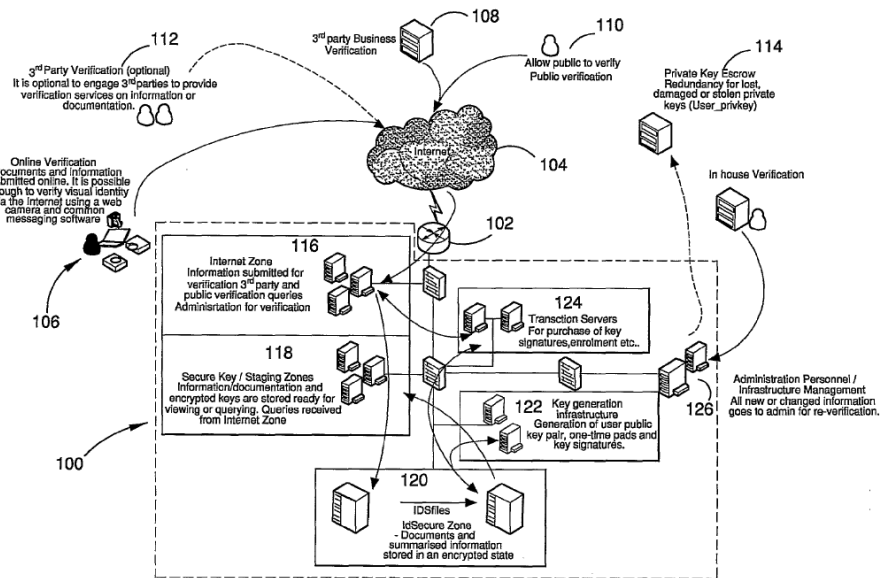


FIGURE 1

Stafford uses the terms “entity” or “IDMember” to refer to the user whose credentials are stored. Stafford’s system stores “credential information,” such as “name, address, date or birth, as well other information.” EX1012, ¶¶53-54. This includes memory (a “data store”) hosting a “database of encrypted credential information.” EX1012, ¶57. Credential information is encrypted and securely stored. EX1012, ¶¶58, 71, 88. Stafford’s example credentials include driver’s licenses, professional memberships, a degree (such as Ph.D.), etc. EX1012, ¶¶4, 65, 131, 139. Stafford thus teaches element 1.1. EX1005, ¶360; *see also infra* §§IV.B.4, IV.B.7 (addressing the generation and verification functions for elements 1.3 and 1.6).

3. Element 1.2

Stafford teaches that an entity client terminal (*OVER file storage client device*) operated by an entity/IdMember communicates with Stafford's system to store credentials, and the entity/IdMember sets the sensitivity of credential information. EX1012, ¶¶54, 81. Sensitive credential information requires use of "highly secure symmetric or similar encryption process e.g. a one time pad" when being released. EX1012, ¶88; *see id.*, ¶¶73-74, Fig. 2 (showing credential release process). As discussed below for element 1.3, Stafford's process for using such encryption involves generation of an OVER file. *Infra* §IV.B.4; EX1005, ¶361.

Stafford teaches users can request release of sensitive credentials. *See* EX1012, ¶74 ("To release data,...the entity (IdMember)...elects to 'release' information using the appropriate interface."). The request/release process is shown in Fig. 2, reproduced below.

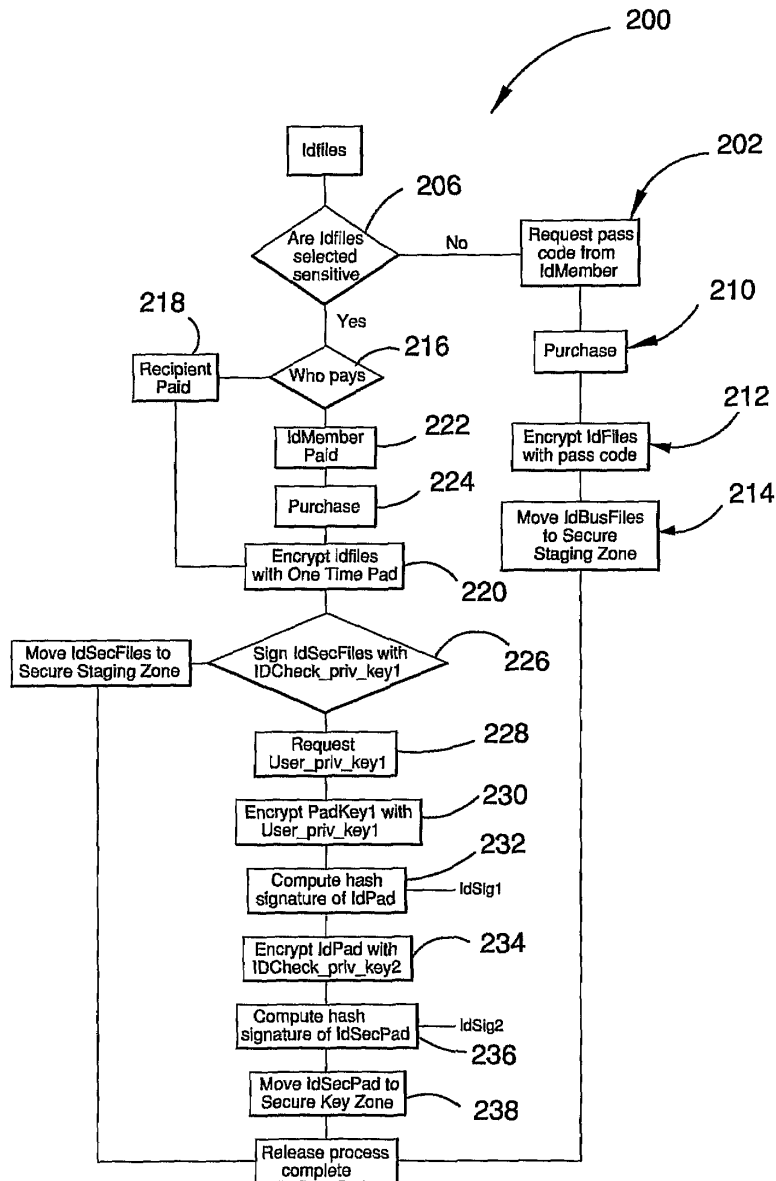


FIGURE 2

EX1012, Fig. 2. As shown, when sensitive files are selected for release, the recipient or IdMember purchases a “key signature” that includes “a hash value or similarly secured...encrypted passwords or one-time pads” that identify and authorize release of encrypted credentials (IdFiles). EX1012, ¶¶75-79; *see id.*,

¶¶38, 88, 93-95. As discussed below for element 1.3, the key signatures taught by Stafford correspond to the recited OVER files; accordingly, the request to release sensitive credential information (as well as the user's purchase of key signatures) is a received request to generate an OVER file. EX1005, ¶¶362-63.

Thus, Stafford teaches element 1.2.

4. Element 1.3

The key signatures Stafford's system generates to release sensitive files can comprise hash values (IdSig1 and IdSig2) provided to the user. EX1012, ¶¶97-99.

The 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. EX1012, ¶¶116-22.

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. *Id.*; 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. EX1005, ¶364.

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). EX1012, ¶¶62, 65, 67. However, 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. EX1005, ¶365.

Purves teaches that a user device (e.g., a device implementing a digital wallet) may be sent an image of a credential such as a credit card, to conveniently represent a real credential. EX1013, ¶¶102, 108-09. The card image may be “from an issuer.” EX1013, ¶85. The server may also generate an image of the credential, optionally with “confidential information...obscured.” EX1013, ¶122; *see also id.*, ¶¶111-12 (“multiple versions of the card” may be used in various formats). A 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. EX1005, ¶366.

In light 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. For example, the system would provide 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 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. *See* EX1013, ¶¶85, 122. Such an image would be a virtual

representation verified by the issuer as being an official representation of the credential. EX1005, ¶367.

To the extent Patent Owner argues that the claim requires that the credential itself be verified by the issuer, this would also have been obvious, as Stafford expressly teaches contacting an issuer to verify a credential. *See* EX1012, ¶65; EX1005, ¶368.

As explained in §VIII.A, it would also have been obvious to generate a QR code to convey at least the key signature. Purves teaches that a QR code scan may be used to “trigger a wallet connection or login,” in place of a card swipe or NFC interaction. EX1013, ¶64. Consistent with Purves’s teaching that a QR code scan could be used to in place of a physical credential swipe or interaction, and as discussed above in Ground 3, it was known that QR codes could be used as a virtual stand-in for a credential. *Supra* §I.C.3; EX1015, ¶61; EX1016, 12; EX1005, ¶369.

In light of Purves’s teaching to use QR codes in place of other credential interactions such as NFC activations or card swipes, it would have been obvious to use a QR code to encode Stafford’s key signature, as doing so would allow the user to more easily transmit the key signature to a third party using a QR code scan. EX1005, ¶369; *see supra* §VIII.A.

Stafford and Purves thus teach element 1.3.

5. Element 1.4

Stafford and Purves teach element 1.4. Stafford teaches that the key signatures generated by its system can be sent to the user electronically (e.g., by email or by sending to a user's display to be copied). EX1012, ¶¶97-99. As discussed for element 1.3, it would have been obvious to send an OVER file comprising a virtual representation (e.g., an issuer-verified credential image) and the key signatures encoded as a scannable QR code. *Supra* §VIII.A. Thus, Stafford and Purves teach the recited transmitting step of element 1.4. Further, this transmission is performed in response to the request discussed for element 1.2 (i.e., in response to the identification of the files as sensitive and the request for release with accompanying purchase of key signatures). *See supra* §VIII.B.3; EX1012, ¶¶93-105, Fig. 2. Thus, Stafford and Purves teach element 1.4. EX1005, ¶¶370-71.

6. Element 1.5

Stafford and Purves teach element 1.5. As illustrated in Fig. 3, Stafford teaches that a third-party client verifying device (referred to as IdBus1, *see* EX1012, ¶108) sends a request for release of information to the credential-database system. EX1012, ¶115; Fig. 3 (marked-up below).

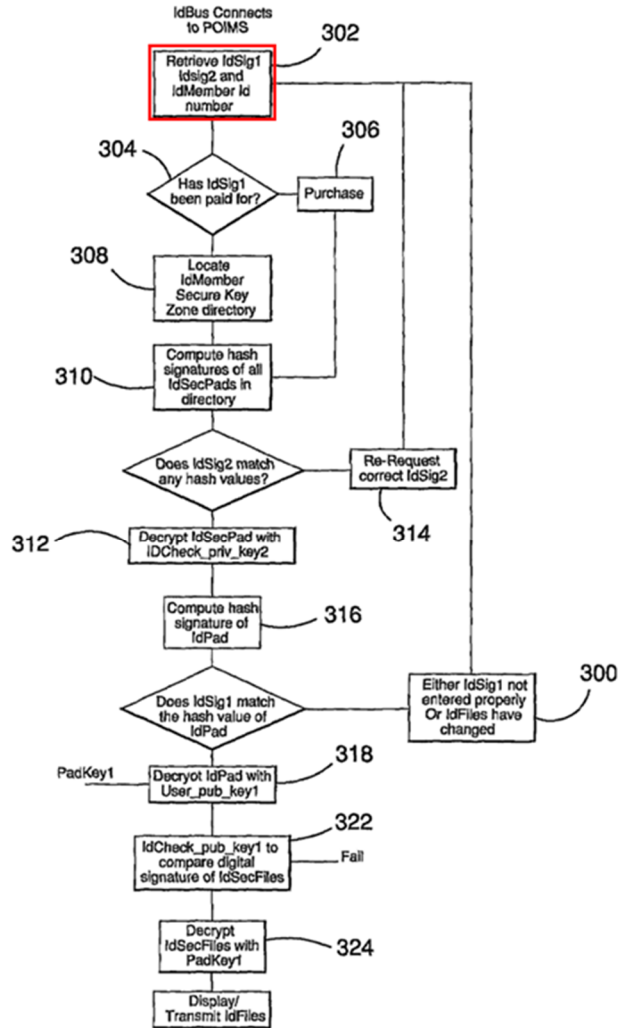


FIGURE 3

The request includes the key signatures IdSig1 and IdSig2, which are used to verify that the 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. *See* EX1012, ¶119-22; EX1005, ¶372.

As explained for element 1.3, in view of Purves’s teachings the key signatures would have been conveyed by a scannable code. This code would be scanned by the third-party device to provide the key signatures used in step 302 of

Stafford's Fig. 3. Thus, the verifying request would be "based on" the recited "scan associated with the OVER file." Stafford and Purves thus teach element 1.5.

EX1005, ¶¶373-74.

7. Element 1.6

Stafford and Purves teach this element. As discussed for element 1.5, Stafford and Purves teach sending a verifying request based on the recited scan. Stafford's system responds to this request (and thus the associated scan) by comparing the encoded hash values IdSig1 and IdSig2 of the key signature. EX1012, ¶¶115-21, Fig. 3 (marked up below).

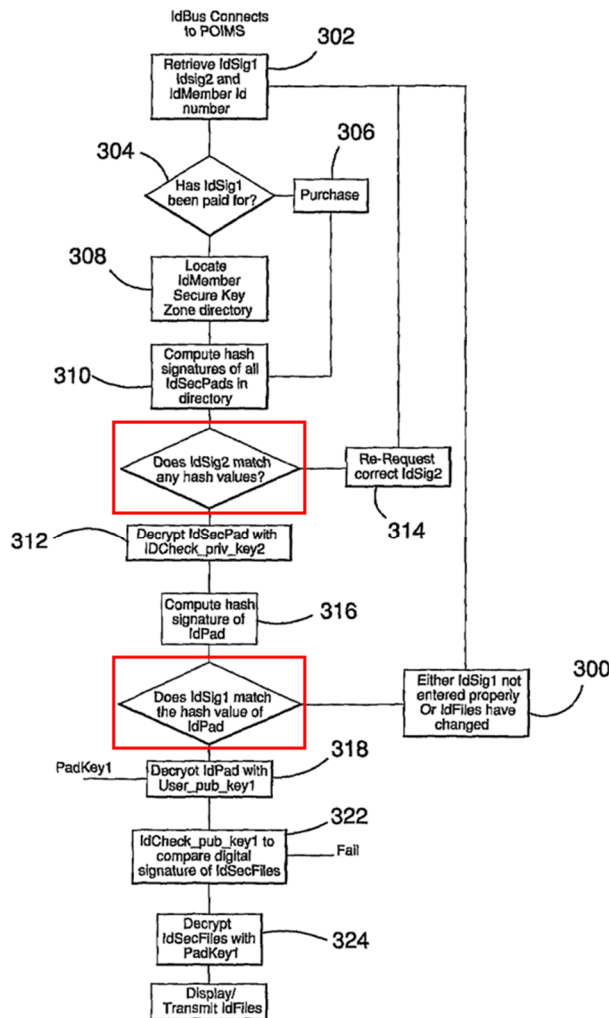


FIGURE 3

Checking the key signatures verifies that the scan providing them corresponds with the information associated with the credential (since it matches the encrypted credential's hash values). See EX1012, ¶¶93 (IdFiles (credentials) encrypted with one-time pad) 115-22 (hash values match credential's one-time pad). Thus, Stafford and Purves teach element 1.6. EX1005, ¶¶375-77.

8. Element 1.7

Stafford teaches sending an authenticating message to the third-party device indicating whether the scan corresponds to the OVER file. For example, where either key signature fails to match, an appropriate message is sent to re-request the non-matching hash value. EX1012, ¶¶120-22. On the other hand, where the key signatures match, a decrypted copy of the IdFiles is transmitted to the third-party device. EX1012, ¶¶120-26. These alternatives, indicated in Fig. 3 (marked-up below) both correspond to the recited authenticating message. EX1005, ¶¶278-80.

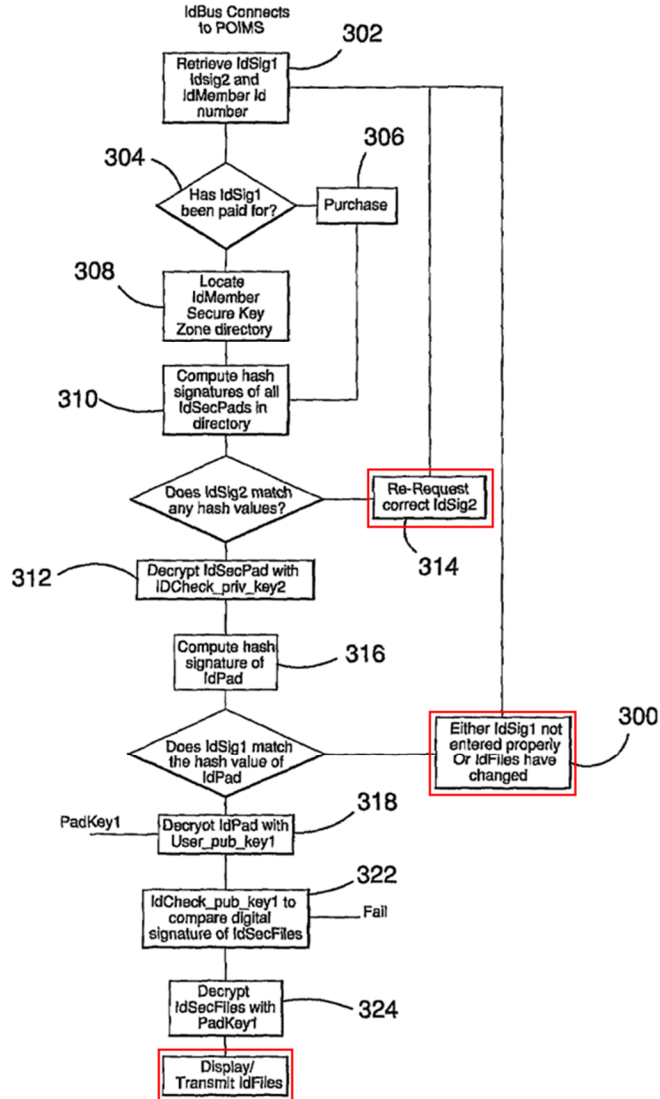


FIGURE 3

Stafford in view of Purves thus teaches element 1.7.

Accordingly, claim 1 was obvious over Stafford and Purves. EX1005,

¶¶358-80.

C. Claim 3

Stafford teaches that, when compiling a database, a document with credential information is received and a representation of the document is created. EX1012, ¶10; ¶24 (documents “attesting to one or more characteristics of the entity”). An administrative sub-system is used to “scan or upload hard copy documents into the system.” EX1012, ¶62; *see id.*, ¶67 (“original documents are also electronically scanned...and then encrypted”). EX1012, ¶24. Stafford thus teaches generating, by the processor, an electronic credential, such as a scanned original credential document. EX1005, ¶381.

Further, it would have been common sense that the processor would determine that no credential is stored when a document is first scanned and uploaded. EX1005, ¶¶382-83. When a document is received but not yet scanned, no credential would be stored, and Stafford’s database would reflect this. *Id.* It would have been obvious for the processor to make a determination that no credential was stored, so that the document could be scanned and added to the database; otherwise, the newly-scanned credential would needlessly overwrite the previously stored credential. *Id.*

Accordingly, claim 3 was obvious over Stafford and Purves.

D. Claim 4

Stafford teaches “automated verification” of its credentials, including “verification...with a document’s issuing body.” EX1012, ¶65. For example, Stafford describes requesting a university to “verify that IdMember has a PhD.” *Id.* The issuer thus provides status indicator (e.g., valid or invalid), as well as additional credential information. *See* EX1012, ¶65 (verifying authenticity of credential’s data), 4 (driver’s license credential may also supply name and license number). Purves further teaches issuers can provide various credential information. *See* EX1013, ¶108 (XML file containing data from issuer such as account number, address, ZIP, etc.). Thus, Stafford and Purves teach the requesting and receiving steps of claim 4. EX1005, ¶384.

The system can also assign a confidence rating to a credential based on the issuer’s reliability. EX1012, ¶65. The recipient can use these ratings to determine a credential’s validity. *Id.* Storing the received indicators would have been obvious so that these confidence ratings could be applied to assess the credential information’s reliability. EX1005, ¶¶385-86.

Accordingly, claim 4 was obvious over Stafford and Purves.

E. Claim 5

Stafford teaches that the issuer can indicate that the credential is valid. *See* EX1012, ¶65 (verifying PhD credential as valid). Thus, claim 5 was obvious over Stafford and Purves. EX1005, ¶387.

F. Claim 7

Stafford teaches that a status indicator may indicate the credential is not valid and that the credential information may reflect a reason for the invalidity. For example, Stafford teaches that certain information “has a validity date associated” and “remains current only for a pre-determined set of time.” EX1012, ¶135; *see also* EX1013, ¶108 (“Card Expiry”). Where the status indicator indicates invalidity and the date of expiration (credential information) is in the past, it would indicate that the credential was invalid, with the reason being expiration. EX1005, ¶388.

Further, other types of status indicators could also indicate an invalid credential. For example, a POSA considering Stafford’s discussion of a university validating a PhD would immediately envision the alternative, in which the university did *not* validate the credential. EX1005, ¶¶389-90. The reason could also be reflected in issuer-provided credential information. For example, Stafford teaches that documents may include watermarks for validation, so the reason for invalidity may be a missing watermark. *See id.*; EX1012, ¶5.

Thus, claim 7 was obvious over Stafford and Purves.

G. Claim 8

Stafford teaches storage of credentials in a remote system. *See* EX1012, ¶62, Fig. 1 (showing remote computers storing credentials). Stafford also teaches that the system can be connected to “other data storage services” for “storage of certain information outside the system 100.” EX1012, ¶54. Applying these teachings, a POSA would have understood that remotely stored data was typically accessed via a reference to that data (e.g., a pointer, virtual address, remote API call, etc.). EX1005, ¶391. Indeed, Stafford expressly teaches generating references which locate a remotely-stored credential by matching hashes of its associated one-time pads stored in Stafford’s system. *See* EX1012, ¶¶33, 119-22, Fig. 3. Accordingly, claim 8 was obvious over Stafford and Purves. EX1005, ¶¶391-92.

H. Claims 9-10

Stafford teaches storing user-specific information, including the specific categories listed in claim 10. For example, Stafford stores location information (addresses) as well as encrypting a private key that is stored “using a biometric such as a fingerprint or password.” EX1012, ¶53, 71. Thus, claims 9 and 10 were obvious over Stafford and Purves. EX1005, ¶¶393-94.

I. Claim 11

Claim 11 requires checking a status indicator and that the OVER file generation request includes a credential identifier to specify the credential

represented by the OVER file. Stafford teaches storing a status indicator, as discussed for claim 4. *Supra* §VIII.D. Stafford also discloses checking the status indicator, as Stafford teaches conditioning release of information on having verification to a particular confidence level for a credential. EX1012, ¶65 (The “user may choose not to release information to a recipient unless their confidence level is over a certain threshold.”). A POSA would have implemented this by checking the status indicator to determine whether the credential was validated and what the confidence level was based on the validator. EX1005, ¶395.

Stafford also teaches that a user may specify which credentials from a list of the user’s stored credentials are to be released. EX1012, ¶22 (The authorization “includes an indication which credential data is to be provided.”); *see id.*, ¶¶75-79 (authorization provided by “entity”). As discussed for claim 1, Stafford and Purves teach using an OVER file to release credentials. *Supra* §IV.B. The indication taught by Stafford would constitute the *credential identifier*, as it identifies the credential to be released, and thus represented. EX1005, ¶¶396-97.

Thus, claim 11 was obvious over Stafford and Purves.

J. Claim 12

Stafford teaches that the verifying step includes comparing the credential identifier (key signature) with stored credentials, as discussed for elements 1.6-1.7.

Supra §§VIII.B.7-8; EX1012, ¶¶115-21, Fig. 3; EX1005, ¶¶398-99. Accordingly, Stafford and Purves render claim 12 obvious.

K. Claim 13

As discussed for element 1.7, Stafford teaches sending an authentication message, and, as discussed for claims 4-5 and 11, Stafford teaches sending a status indicator when key signatures match, indicating a credential's validity, including a confidence level. *Supra* §§VIII.D-E, VIII.I. A POSA would have found it obvious to include the status indicator in the authentication message, as including verification and/or a confidence level with a credential would provide useful information to the third party about credential validity. EX1005, ¶¶400-01.

Accordingly, claim 13 was obvious over Stafford and Purves.

L. Claim 14

Stafford teaches storing scans of a credential, as discussed for claim 3. EX1012, ¶¶62, 67; *supra* §VIII.C. And as discussed for claim 1, it would have been obvious in view of Purves to include an image of a portion of a stored credential in an OVER file. *Supra* §VIII.B; EX1013, ¶122 (partially obscured credential image). Accordingly, claim 14 was obvious over Stafford and Purves. EX1005, ¶¶402-03.

M. Claim 15

1. Preamble

Stafford teaches a computer-implemented method. EX1005, ¶404; *see supra* §VIII.B.1.

2. Element 15.1

Stafford teaches element 15.1 for similar reasons to elements 1.1 and 1.2. *See supra* §§VIII.B.2-3; EX1012, ¶¶53-54, 57-58, 71, 75-79, 81, 88, 93-95, Figs. 1-2, claim 1; EX1005, ¶405.

3. Element 15.2

Stafford and Purves teach element 15.2 for similar reasons to elements 1.3 and 1.4. *See supra* §§VIII.B.4-5; EX1012, ¶¶62, 65-67, 85, 93-112, 116-22; EX1013, ¶¶64, 85, 122; EX1005, ¶406.

4. Element 15.3

As discussed for elements 1.5-1.6, Stafford and Purves suggest that a third party scan a QR code in an OVER file. *Supra* §§VIII.B.6-7; EX1012, ¶¶105, 115-22, Fig. 3; EX1013, ¶¶64, 85, 112. This would include displaying the code (portion of an OVER file) to a third party. EX1005, ¶407-08. Thus, Stafford and Purves teach element 15.3.

5. Element 15.4

As discussed for element 1.7, Stafford in view of Purves teaches sending the recited authentication message to the third party device. *Supra* §VIII.B.8. This

authentication message can be displaying the credential (where authentication succeeds) or requesting re-entry of the key signatures (where authentication fails). EX1012, ¶¶120-22, Fig. 3. The entry of key signatures is performed by the user (EX1012, ¶113), so a POSA would have found it obvious for the user to receive the request for re-entry (i.e., the authentication message indicating lack of correspondence to the credential). EX1005, ¶409. Further, on success, Stafford teaches that a credential image may be compared manually to an original document held by the user. EX1012, ¶131. In this case, too, it would have been obvious for the user to receive the authentication message (e.g., by showing it to the user on a display to allow side-by-side comparison to a physical credential). EX1005, ¶¶409-10.

Thus, Stafford and Purves teach element 15.4. *Id.*

Accordingly, claim 15 was obvious over Stafford and Purves. EX1005, ¶¶404-11.

N. Claim 16

As discussed for element 1.5, scanning the displayed portion of the OVER file (QR code) would have been obvious over Stafford and Purves. *Supra* §VIII.B.6; EX1012, ¶¶105, 115-22, Fig. 3; EX1013, ¶¶64, 85, 112. Thus, claim 16 was obvious over Stafford and Purves. EX1005, ¶¶412-13.

O. Claim 18

Stafford teaches collecting user-specific information via a user device and transmitting the information to a credential engine. *See* EX1012, ¶64 (The user “submits their credential information or documentation to the system....over the Internet.”); Fig. 1 (client device 106 connected over internet). This process is conducted to store the user-specific information. EX1012, ¶¶63, 70; EX1005, ¶¶414-15. Thus, claim 18 was obvious over Stafford and Purves.

P. Claim 19

As discussed for claim 14 and element 1.3, it would have been obvious in view of Stafford and Purves to include an image of a credential as part of an OVER file. *Supra* §§VIII.B.4, VIII.L. Accordingly, Stafford and Purves render claim 19 obvious. EX1005, ¶¶416-17.

Q. Claim 20

Claim 20 contains limitations paralleling claim 7. As discussed for claim 7, Stafford in view of Purves teaches these limitations. *Supra* §VIII.F. Thus, claim 20 would have been obvious over Stafford and Purves for similar reasons. EX1005, ¶418.

Accordingly, claims 1, 3-5, 7-16, 18-20 were obvious over Stafford and Purves. EX1005, ¶¶350-418.

IX. GROUND 6: CLAIMS 2, 6, AND 17 ARE OBVIOUS OVER STAFFORD, PURVES, AND NEAFSEY

Claims 2, 6, and 17 add limitations regarding (for claims 6 and 17) a device identifier limiting the credential to the client device, or (for claim 2) generating and transmitting a requested second OVER file to a second client device that is invalid for use on a first client device. These limitations are taught by Stafford, Purves, and Neafsey. EX1005, ¶¶448-49.

For example, Neafsey teaches that clients may have different devices, and that credentials may be provided in different formats appropriate to a particular device. EX1015, ¶61; EX1016, 12. Neafsey further teaches that these different credentials may be generated based on a “unique device ID” of the recipient device. EX1015, ¶49; EX1016, 10. As Dr. Shamos explains, a POSA would have been motivated in light of these teachings to provide OVER files (such as files comprising the hash codes and credential representation of Stafford and Purves) to client devices in formats appropriate to each client device, e.g., by tying the OVER files to a given device’s unique device ID. EX1005, ¶450. In particular, a POSA would understand different client devices would sometimes require using different formats appropriate to each device. For example, while a smartphone could display an optical code, a typical smartcard could not. EX1005, ¶451; *see* EX1015, ¶61 (device may be smartphone or smartcard); EX1016, 12.

Applying these teachings, each of claims 2, 6, and 17 was obvious over Stafford, Purves, and Neafsey.

Claims 6 and 17 recite that the OVER file contains a device identifier limiting the validity of the OVER file to the device of the user. Neafsey teaches using a device identifier unique to a particular device to generate credentials that take on different formats specific to each particular device. EX1015, ¶¶49, 61; EX1016, 10-12. In combination, a POSA would have found it obvious to use device identifiers to limit an OVER file to a specific user device and as appropriate for its format, as taught by Neafsey, such that a particular OVER file would be limited in validity to a specific user device. EX1005, ¶¶453-54.

As to claim 2, it repeats elements 1.2-1.4 as applied to a second OVER file, with the second OVER file being invalid for use in the first user device. Applying the same teachings of Neafsey, an OVER file would be specific to a particular device, and thus the second OVER file (matched to the second device) would not be valid in the first device, as its device identifier would not match. EX1005, ¶¶455-56. Thus, Stafford, Purves, and Neafsey teach the elements of claim 2 for similar reasons as they teach the elements of claims 6 and 17. *Id.*

A POSA would have reasonably expected success in combining Stafford, Purves, and Neafsey as described above. EX1005, ¶¶451-52. The references involve well-understood and related technologies for electronic credentials and

transactions, each of which would function predictably in combination. *Id.*; *supra* §I.C.

Accordingly, claims 2, 6, and 17 were obvious over Stafford, Purves, and Neafsey. EX1005, ¶¶448-56.

X. DISCRETIONARY DENIAL IS NOT WARRANTED

This petition does not implicate the Board’s discretion according to *Fintiv*. *Apple Inc., v. Fintiv, Inc.*, IPR2020-00019, Paper 11. *See generally* Memorandum on Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation (June 21, 2022) (*Fintiv* Memo). Patent Owner filed its district court complaint in the Western District of Texas on January 26, 2023, asserting four patents including the ’531 patent. The court granted a motion to transfer the case to the Northern District of California on November 3, 2023, and the case was transferred on November 7, 2023. As of the filing of this petition, a trial date has not been set but is reasonably expected to be after issuance of a final written decision here. *See* EX1045; EX1046, 66 (37 month average time to trial in N.D.Cal.).

This petition also does not implicate §325(d). The petition presents new art and argument, as none of the asserted references was disclosed or considered during examination. *Supra* §I.B. *See generally* EX1007. Nor are the references relied on in the petition cumulative to the references applied during examination,

as the Examiner allowed the claims on the basis that no asserted prior art taught including, in an OVER file, a “virtual representation of the credential that has been verified by an issuing agency to be an official representation” based on information associated with the credential. EX1007, 20. Finally, the discussion in the grounds above explains in detail why the claims of the ’531 patent were obvious over the prior art, confirming that their allowance constituted material error.

XI. GROUNDS FOR STANDING

Visa certifies that, under 37 C.F.R. §42.104(a), the ’531 patent is available for *inter partes* review, and Visa is not barred or estopped from requesting *inter partes* review of the ’531 patent on the grounds identified.

XII. CONCLUSION

For the reasons set forth above, claims 1-20 of the ’531 patent are unpatentable. Visa therefore requests that an *inter partes* review of these claims be instituted.

Respectfully submitted,

Dated: January 25, 2024

/Matthew A. Argenti/
Matthew A. Argenti, Lead Counsel
Reg. No. 61,836

XIII. MANDATORY NOTICES UNDER 37 C.F.R. §42.8

Real Party-in-Interest (37 C.F.R. §42.8(b)(1)): Visa Inc. is the real party-in-interest.

Related Matters (37 C.F.R. §42.8(b)(2)): Patent Owner has asserted the '531 patent against Petitioner in a case originally filed in the United States District Court in the Western District of Texas (6-23-cv-00048), which was transferred and is currently pending in the United States District Court in the Northern District of California (5-23-cv-05720). Concurrently, Petitioner is filing another petition against the '531 patent (IPR2024-00487). Petitioner is also filing petitions against three related patents: U.S. Patent No. 9,954,854 (IPR2024-00488); U.S. Patent No. 10,749,859 (IPR2024-00489); and U.S. Patent No. 11,329,973 (IPR2024-00490).

Lead and Back-Up Counsel (37 C.F.R. §42.8(b)(3))

Lead Counsel: Matthew A. Argenti (Reg. No. 61,836)

Back-Up Counsel: Michael T. Rosato (Reg. No. 52,182); Patrick M. Medley (Reg. No. 74,735); Joseph M. Baillargeon (Reg. No. 79,685)

Service Information – 37 C.F.R. §42.8(b)(4). Petitioner hereby consents to electronic service.

Email: margenti@wsgr.com; mrosato@wsgr.com; pmedley@wsgr.com;
jbaillargeon@wsgr.com

Post: Wilson Sonsini Goodrich & Rosati, 650 Page Mill Rd., Palo Alto, CA
94304

Tel.: 650-354-4154

Fax: 650-493-6811

XIV. PAYMENT OF FEES UNDER 37 C.F.R. §§42.15(A) AND 42.103

The required fees are submitted herewith. If any additional fees are due at any time during this proceeding, the Office is authorized to charge such fees to Deposit Account No. 23-2415.

XV. CERTIFICATE OF COMPLIANCE

Pursuant to 37 C.F.R. §42.24(d), the undersigned certifies that this Petition complies with the type-volume limitation of 37 C.F.R. §42.24(a). The word count application of the word processing program used to prepare this Petition indicates that the Petition contains 13,970 words, excluding the parts of the brief exempted by 37 C.F.R. §42.24(a).

Respectfully submitted,

Dated: January 25, 2024

/Matthew A. Argenti/
Matthew A. Argenti, Lead Counsel
Reg. No. 61,836

XVI. APPENDIX – LIST OF EXHIBITS

Exhibit No.	Description
1001	U.S. Patent No. 9,251,531 to Shaunt M. Sarkissian
1002	U.S. Patent No. 9,954,854 to Shaunt M. Sarkissian
1003	U.S. Patent No. 10,749,859 to Shaunt M. Sarkissian
1004	U.S. Patent No. 11,329,973 to Shaunt M. Sarkissian
1005	Declaration of Michael I. Shamos, Ph.D., J.D.
1006	Curriculum vitae of Michael I. Shamos
1007	U.S. Patent Application No. 13/794,878 File History
1008	U.S. Patent Application No. 14/982,981 File History
1009	U.S. Patent Application No. 16/422,715 File History
1010	U.S. Patent Application No. 16/893,023 File History
1011	U.S. Patent Pub. No. 2012/0316992 to Timothy W. Osborne (“Osborne”)
1012	U.S. Patent Pub. No. 2009/0271321 to Grant Stafford (“Stafford”)
1013	U.S. Patent Pub. No. 2013/0054454 to Thomas Purves et al. (“Purves”)
1014	U.S. Patent Pub. No. 2012/0310838 to Theodore Harris et al. (“Harris”)
1015	U.S. Patent Pub. No. 2013/0212248 to Jeffrey Scott Neafsey et al. (“Neafsey”)
1016	U.S. Provisional Patent Application No. 61/598,219 (“Neafsey Provisional”)
1017	U.S. Patent Publication No. 2008/0270166 to Duane Morin et al. (“Morin”)

1018	First Amended Complaint (Dkt. No. 25) <i>Cortex MCP, Inc. v. Visa, Inc.</i> , No. 5-23-cv-05720 (N.D. Cal.), <i>as filed in</i> No. 6-23-cv-00048 (W.D. Tex) (Apr. 10, 2023) (“Complaint”)
1019	Steiner et al., “Kerberos: An Authentication Service for Open Network Systems.” <i>Usenix Winter</i> (1988) (“Steiner”)
1020	Cross River, “Tokenization in Card Networks” (May 2023) (“Cross River”)
1021	U.S. Patent No. 7,014,107 to Irek Singer et al. (“Singer”)
1022	Heather Mark. “Shift4: Secure Payment Processing” (2006) (“Shift4”)
1023	Tom Arnold. “Credit Card Information Surrogate: A Method and System for using surrogates to integrate PCI-level security for legacy information systems.” (2007) (“Arnold”)
1024	Brown et al. “Microsoft Code Name ‘Geneva’ Framework Whitepaper for Developers” (2008) (“Brown”)
1025	Thakar et al. <i>PCI Compliance for Dummies</i> (2009) (“Thakar”)
1026	Ben Jackson. “Token Gestures.” <i>Digital Transactions</i> (2009) (“Jackson”)
1027	First Data. “Data Encryption and Tokenization: An Innovative One-Two Punch to Increase Data Security and Reduce the Challenges of PCI DSS Compliance.” (2009) (“First Data 2009”)
1028	U.S. Patent Pub. No. 2009/0249082 to Ulf Mattson (“Mattson”)
1029	U.S. Patent Pub. No. 2010/0070754 to Nathan P. Leach (“Leach”)
1030	Propay Press Release. “ProPay Adds Automated Clearing House (ACH) Data Encryption And Tokenization To Its Suite Of ProtectPay Services.” (May 10, 2010) (“Propay”)
1031	Richard J. Sullivan. “The Changing Nature of U.S. Card Payment Fraud: Issues for Industry and Public Policy.” (2010) (“Sullivan”)

1032	CyberSource. “CyberSource Electronic Check Services Implementation Guide” (2010) (“CyberSource”)
1033	Visa. “Visa Best Practices for Tokenization Version 1.0.” (2010) (“Visa Best Practices”)
1034	U.S. Patent No. 8,458,487 to Gary Palgon et al. (“Palgon”)
1035	PCI Security Standards Council. “PCI DSS Tokenization Guidelines.” (2011) (“Tokenization Guidelines”)
1036	U.S. Patent Pub. No. 2011/0258122 to Daniel Jeffrey Shader et al. (“Shader”)
1037	U.S. Patent Pub. No. 2011/0320316 to Joseph R. Randazza et al. (“Randazza”)
1038	Tim Horton et al. “A Primer on Payment Security Technologies: Encryption and Tokenization.” (2011) (“First Data 2011”)
1039	U.S. Patent Pub. No. 2012/0016731 to Randy Smith et al. (“Smith”)
1040	U.S. Patent Pub. No. 2012/0150669 to Garrett S. Langley et al. (“Langley”)
1041	Guenther Starnberger et al. “QR-TAN: Secure Mobile Transaction Authentication.” <i>2009 International Conference on Availability, Reliability and Security</i> . IEEE. (2009) (“Starnberger”)
1042	U.S. Patent Pub. No. US 2011/0251892 to Kevin Laracey (“Laracey”)
1043	U.S. Patent Pub. No. 2012/0209749 to Ayman Hammad et al. (“Hammad”)
1044	U.S. Patent Pub. No. 2009/0113543 to Neil P. Adams et al. (“Adams”)
1045	Patent Scheduling Order (Dkt. No. 73) <i>Cortex MCP, Inc. v. Visa, Inc.</i> , No. 5-23-cv-05720 (N.D. Cal.) (Jan. 3, 2024) (“Scheduling Order”)
1046	United States District Courts — National Judicial Caseload Profile, https://www.uscourts.gov/sites/default/files/data_tables/fcms_na_distpro file0331.2023.pdf (March 2023)

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§42.6(e) and 42.105(a), this is to certify that I caused to be served a true and correct copy of the foregoing Petition for Inter Partes Review of U.S. Patent No. 9,251,531 (and accompanying Exhibits 1001-1046 by overnight courier (Federal Express or UPS), on this 25th day of January, 2024, on the Patent Owner at the correspondence address of the Patent Owner as follows:

K&L Gates LLP-Pittsburgh
210 Sixth Avenue
Pittsburgh, PA 15222-2613

Dated: January 25, 2024

/Matthew A. Argenti/
Matthew A. Argenti, Lead Counsel
Reg. No. 61,836