

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. IPR2024-00489
Patent No. 10,749,859

**PETITION FOR INTER PARTES REVIEW OF
U.S. PATENT NO. 10,749,859**

TABLE OF CONTENTS

	<u>Page</u>
I. Introduction.....	1
A. The '859 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. “...verified by an issuing agency...”	13
IV. Ground 1: Claims 1-2, 4-10, 13-14, and 16-21 were Obvious over Oborne	14
A. Overview of Ground.....	14
B. Claim 1	14
C. Claim 2	30
D. Claim 4	32
E. Claim 5	34
F. Claim 6	34
G. Claim 7	35
H. Claim 8	36
I. Claim 9	37
J. Claims 10, 13, 14, and 16.....	41
K. Claim 17	41
L. Claim 18	42
M. Claim 20	42
V. Ground 2: Claims 3, 11-12, and 15 were Obvious over Osborne and Purves.....	43
A. Overview of Ground and Rationale to Combine	43

B.	Claims 3 and 11	44
C.	Claim 12	44
D.	Claim 15	47
VI.	Ground 3: Claims 1, 3-4, 6-9, 11-12, and 14-17 were Obvious over Stafford and Purves.....	48
A.	Overview and Rationale to Combine	48
B.	Claim 1	51
C.	Claim 3	63
D.	Claim 4	64
E.	Claim 6	64
F.	Claim 7	65
G.	Claim 8	66
H.	Claim 9	66
I.	Claim 11	71
J.	Claim 12	71
K.	Claim 14	74
L.	Claim 15	74
M.	Claim 16	74
N.	Claim 17	75
VII.	Ground 4: Claims 2, 5, 10, 13, and 18-21 were Obvious over Stafford, Purves, and Neafsey.....	75
A.	Overview and Rationale to Combine	75
B.	Claim 18	77
C.	Claim 20	78
D.	Claims 2, 5, 10, 13, 19, and 21	78
VIII.	Discretionary Denial is Not Warranted	80
IX.	Grounds for Standing.....	81
X.	Conclusion	81
XI.	Mandatory Notices under 37 C.F.R. §42.8.....	82

XII. Payment of Fees under 37 C.F.R. §§42.15(a) and 42.103	84
XIII. Certificate of Compliance.....	85
XIV. Appendix – List of Exhibits.....	85

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, wherein said information is used to prove 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, wherein the OVER file storage client device of the user is a first Near Field Communication (NFC) enabled device;

[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 that is a second NFC enabled device, a verifying request to verify that the OVER file transmitted to the user authenticates the user, based on a Near Field Communication (NFC) protocol-based communication associated with the OVER file on the OVER file storage client device of the user being transmitted to the OVER file third-party client verifying device via an NFC protocol;

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

[1.7] transmitting, to the OVER file third-party client verifying device, an authentication message comprising an indication of whether the NFC protocol-based communication associated with the OVER file on the OVER

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

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 after the processor determines that no credential of the user is stored.

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

5. 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.

6. 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.

7. 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.

8. The computer-implemented method of claim 7, wherein the OVER file comprises a portion of the stored credential.

9.[preamble] An apparatus comprising:

[9.1] a processor;

[9.2] a memory unit operatively coupled to the processor, the memory unit configured to store information associated with a credential of a user and a plurality of instructions, wherein said information is used to prove the user's identity or qualifications, wherein the instructions are configured to program the processor to:

[9.3] receive, from an officially verifiable electronic representation (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, wherein the OVER file storage client device of the user is a first Near Field Communication (NFC) enabled device;

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

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

[9.6] receive, from an OVER file third-party client verifying device that is a second NFC enabled device, a verifying request to verify that the OVER file transmitted to the OVER file storage client device of the user authenticates the user, based on a Near Field Communication (NFC) protocol-based

communication associated with the OVER file on the OVER file storage client device of the user being transmitted to the OVER file third-party client verifying device via an NFC protocol;

[9.7] verify that the NFC protocol-based communication associated with the OVER file corresponds with the information associated with the credential of the user, in response to the verifying request; and

[9.8] transmit, to the OVER file third-party client verifying device, an authentication message comprising a status indicator indicating whether the OVER file corresponds to the credential of the user.

10. The apparatus of claim 9, 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 instructions are further configured to program the processor to:

[10.1] receive, 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;

[10.2] generate 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

[10.3] transmit, to the second OVER file storage client device of the user, the second OVER file in response to the second OVER file generation request.

11. The apparatus of claim 9, wherein the instructions further program the processor to generate the credential, wherein the credential is generated after the processor determines that no matching credential is stored.

12. The apparatus of claim 9, wherein the instructions are further configured to program the processor to: request the credential from the issuing agency, wherein the issuing agency stores credentials issued by the issuing agency; receive the status indicator and credential information associated with the

credential transmitted by the issuing agency; and store the credential and a status indicator.

13. The apparatus of claim 9, wherein the instructions are further configured to program the processor to generate a device identifier for the credential, wherein the device identifier limits the credential to the client device.

14. The apparatus of claim 9, wherein the instructions are further configured to program the processor to generate 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.

15. The apparatus of claim 9, wherein the instructions are further configured to program the processor to check a stored status indicator of a stored credential, wherein the status indicator comprises the stored status indicator.

16. The apparatus of claim 9, wherein the instructions are further configured to program the processor to check 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

17. The apparatus of claim 9, wherein the instructions are further configured to program the processor to check a status indicator of a stored credential, and the authentication message comprises the status indicator of the stored credential.

18.[preamble] A computer-implemented method comprising:

[18.1] 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, wherein said information is used to prove the user's identity or qualifications;

[18.2] 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, wherein the OVER file storage client device of the user is a first Near Field Communication (NFC) enabled device;

[18.3] 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;

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

[18.5] receiving, from an OVER file third-party client verifying device that is a second NFC enabled device, a verifying request to verify that the OVER file transmitted to the user authenticates the user, based on a Bluetooth protocol-based communication associated with the OVER file on the OVER file storage client device of the user being transmitted to the OVER file third-party client verifying device via an NFC protocol;

[18.6] verifying that the Bluetooth protocol-based communication associated with the OVER file corresponds with the information associated with the credential of the user that is stored in the OVER engine, in response to the verifying request; and

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

19. The computer-implemented method of claim 18, 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:

[19.1] 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;

[19.2] 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

[19.3] 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.

20.[preamble] An apparatus comprising:

[20.1] a processor;

[20.2] a memory unit operatively coupled to the processor, the memory unit configured to store information associated with a credential of a user and a plurality of instructions, wherein said information is used to prove the user's identity or qualifications, wherein the instructions are configured to program the processor to:

[20.3] receive, from an officially verifiable electronic representation (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, wherein the OVER file storage client device of the user is a first Near Field Communication (NFC) enabled device;

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

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

[20.6] receive, from an OVER file third-party client verifying device that is a second NFC enabled device, a verifying request to verify that the OVER file transmitted to the OVER file storage client device of the user authenticates the user, based on a Bluetooth protocol-based communication associated with the OVER file on the OVER file storage client device of the user being transmitted to the OVER file third-party client verifying device via an NFC protocol;

[20.7] verify that the Bluetooth protocol-based communication associated with the OVER file corresponds with the information associated with the credential of the user, in response to the verifying request; and

[20.8] transmit, to the OVER file third-party client verifying device, an authentication message comprising a status indicator indicating whether the OVER file corresponds to the credential of the user.

21. The apparatus of claim 20, 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 instructions are further configured to program the processor to:

[21.1] receive, 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;

[21.2] generate 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

[21.3] transmit, to the second OVER file storage client device of the user, the second OVER file in response to the second OVER file generation request.

Visa Inc., (“Petitioner” or “Visa”) requests review of U.S. Patent No. 10,749,859 (“the ’859 patent,” EX1003), currently assigned to Cortex MCP, Inc. (“Patent Owner”). This petition demonstrates by a preponderance of the evidence that claims 1-21 (“Challenged Claims”) of the ’859 patent are unpatentable as obvious.

I. INTRODUCTION

The ’859 patent purports to have invented a method for storing and verifying credentials. However, the claims of the ’859 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 transmitted and verified by third parties. These virtual representations can be transmitted as needed to third parties via a Near Field Communication (NFC) or Bluetooth-based protocol communication as proof a user’s identity or qualification. In its complaint (EX1018), Patent Owner has interpreted the claim terms broadly, mapping 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 1-21 of the ’859 patent should be found unpatentable and cancelled.

A. The '859 Patent

The '859 patent is entitled “File Format and Platform for Storage and Verification of Credentials.” EX1003, Title. The '859 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.” EX1003, Abstract, 3:62-65. The '859 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. EX1003, 6:56-8:24, 10:4-9, 10:46-65, 12:43-48, Figs. 2-3.

The independent claims 1 and 18 recite computer-implemented methods and claims 9 and 20 recite an apparatus comprising instructions to program a processor; all of these claims involve use of “officially verifiable electronic representation (OVER)” files that are associated with user credentials, as well as reciting steps involving engines, clients, and third-party devices that deal with such files. The use of OVER files involves interactions between three parties, as shown in Fig. 1 (below).

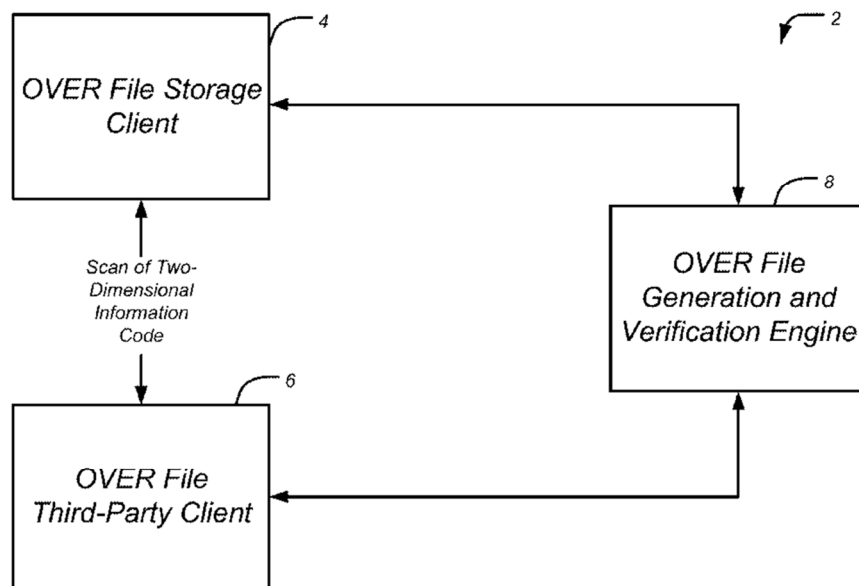


Fig. 1

EX1003, Fig. 1. The OVER file engine (corresponding to the apparatus and processor recited in claim 9) stores credential information for a user and generates an OVER file, providing it to the OVER file storage client of the user's device.

EX1003, 4:21-38. The user presents the OVER file to a third party (e.g., a merchant) as though it were a credential, and based on an NFC and/or Bluetooth protocol-based communication 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. EX1003, 8:24-61.

Claims 1 are 9 are 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 an NFC enabled user device, receiving a verifying request from an NFC enabled third-party device, verifying an NFC or Bluetooth protocol-based communication associated with the OVER file, and transmitting an authentication message to the third-party device.

Claims 18 and 20 are directed to an apparatus with instructions configured to program a processor to perform similar limitations to claims 1 and 9 but utilize both Bluetooth and NFC protocol-based communications.

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

B. Prosecution History

The '859 patent was filed as U.S. Application No. 16/422,715 (“the '715 application”) on May 24, 2019, which is a continuation of Application No. 15/887,873, which is now abandoned, which is a continuation of Patent No. 9,954,854, which is a continuation of Patent No. 9,251,531, which claims priority to Provisional Application No. 61/740,731, filed on Dec. 21 , 2012. EX1003, Face. For purposes of this petition only, Visa assumes a priority date of December 21, 2012.

During prosecution, the Examiner issued a single office action, rejecting the pending claims over two prior art references. EX1009, 64-96 (citing U.S. Patent Publication No. 2009/0307756 to Kang and U.S. Patent Publication No. 2012/0240204 to Bhatnagar). None of the prior art at issue in this proceeding was raised during prosecution.

To secure allowance, Applicant agreed to an Examiner's Amendment to all independent claims requiring (1) the OVER file storage client device and third-party verifying devices are first and second NFC enabled devices, and (2) the NFC communication was "transmitted to the OVER file third-party client verifying device via an NFC protocol." EX1009, 12-13, 15-16, 18-21.

The Examiner referred to the amendments and Applicant's arguments in lieu of providing reasons for allowance, although the Applicant's arguments had not addressed the subject matter added in the Examiner's Amendment. *See* EX1009, 22, 42-46.

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, ¶¶1-19; 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 a concise overview of some important elements of credential storage and verification that Dr. Shamos explains are relevant to a POSA's understanding as of the '859 patent's priority date. EX1005, ¶¶95-205.

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, ¶¶96-102 (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, ¶¶103-37, 147-69 (citing EX1011-EX1017, EX1020-EX1040).

An example system employing tokenization technology is provided by U.S. Patent Publication No. 2012/0316992 ("Osborne," EX1011). Osborne 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 Osborne were well-understood by the POSA and similar technologies had been employed in various related applications. EX1005, ¶155-61. *See generally id.*, §IV.I.

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, ¶¶96-102. 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, ¶¶162-65. 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, ¶¶162-65.

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 NFC or Bluetooth. EX1011, ¶49, 80. Similarly, Purves teaches that an NFC ‘tap’ may be used to trigger a wallet connection, such as connecting to a merchant. EX1013, ¶64; EX1005, ¶¶165, 170-85 (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. 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, ¶¶147-48. Such use of device identifiers to tie electronic representations to particular devices was well-known. EX1005, ¶¶192-97. 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, ¶193. 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, ¶¶96-102.

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, ¶¶76-81.

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

Visa requests review of claims 1-21 of the '859 patent under 35 U.S.C. §311 and AIA §6. The grounds for relief are as follows:

Ground	Claims	Description
1	1-2, 4-10, 13-14, 16-21	35 U.S.C. §103: obvious over Osborne ¹
2	3, 11-12, 15	35 U.S.C. §103: obvious over Osborne and Purves ²
3	1, 3-4, 6-9, 11- 12, 14-17	35 U.S.C. §103: obvious over Stafford ³ and Purves
4	2, 5, 10, 13, 18- 21	35 U.S.C. §103: obvious over Stafford, Purves, and Neafsey ⁴

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 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).

⁴ 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 (the “Neafsey Provisional,” EX1016), filed February 13, 2012. As discussed below, Neafsey is available as prior art as of its provisional filing date.

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, ¶¶137-46.

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.” EX1003, 2:38-40. The specification describes that an OVER file may contain “credential information.” EX1003, 6:39-41, 7:6-9. 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. EX1003, 12:30-33. This “OVER file credential” may include an image from an issuing agency, such as a logo or a card image. EX1003, 9:33-37, 14:25-35; EX1005, ¶¶85-87. In some embodiments, an OVER File storage client (e.g., a client device) generates an information code in the form of a networked or radio transmission such as an NFC or Bluetooth communication to verify the user’s credential to third parties. EX1003, Abstract, 12:34-42; EX1005, ¶¶178-86.

The ’859 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 based on 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 3-4), but also encompassing a file comprising a token (as asserted in Patent Owner’s infringement complaint and addressed in grounds 1-2). EX1005, ¶¶85-90.

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

Each independent claim recites an OVER file comprising “a virtual representation of the credential that has been verified by an issuing agency to be an official representation of the credential.” During prosecution of the ’531 parent application, 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, ¶¶91-94.

IV. GROUND 1: CLAIMS 1-2, 4-10, 13-14, AND 16-21 WERE OBVIOUS OVER OBORNE

A. Overview of Ground

As discussed below, Osborne discloses or suggests each and every element of claims 1, 2, 4-10, 13-14, and 16-21, 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* consistent with Patent Owner's district court complaint (i.e., encompassing use of a token). *See supra* §§III.A; EX1005, ¶207.

Osborne teaches or at least suggests that its token server may be operated by the issuer of a user's credentials. It would at minimum have been obvious that the token would be an issuer-verified official representation, since the issuer issues the token as well as the credential. EX1005, ¶208; *see infra* §IV.B.4.

The discussion of the claims 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, ¶¶208-29.

1. Preamble

1. A computer-implemented method comprising:

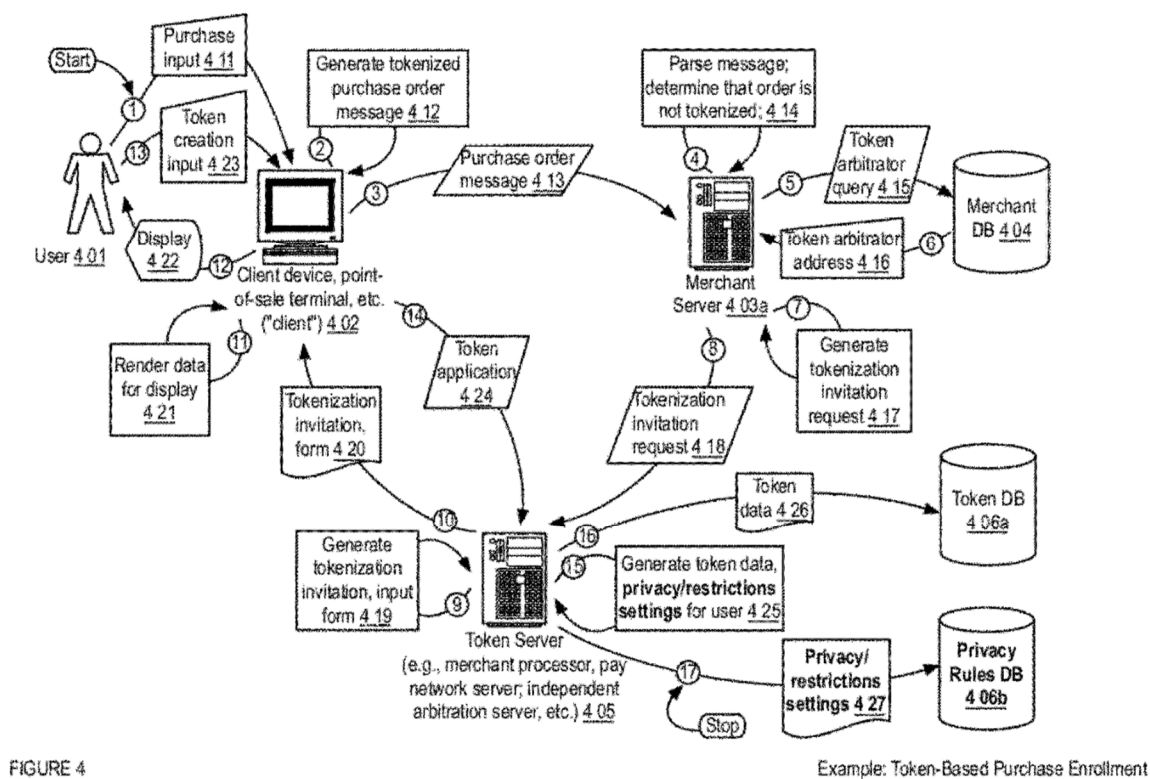
Osborne teaches a computer-implemented method. *See, e.g.*, EX1011, ¶¶114-22 (describing computerized system used to perform Osborne's methods); EX1005, ¶209-229.

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, wherein said information is used to prove 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

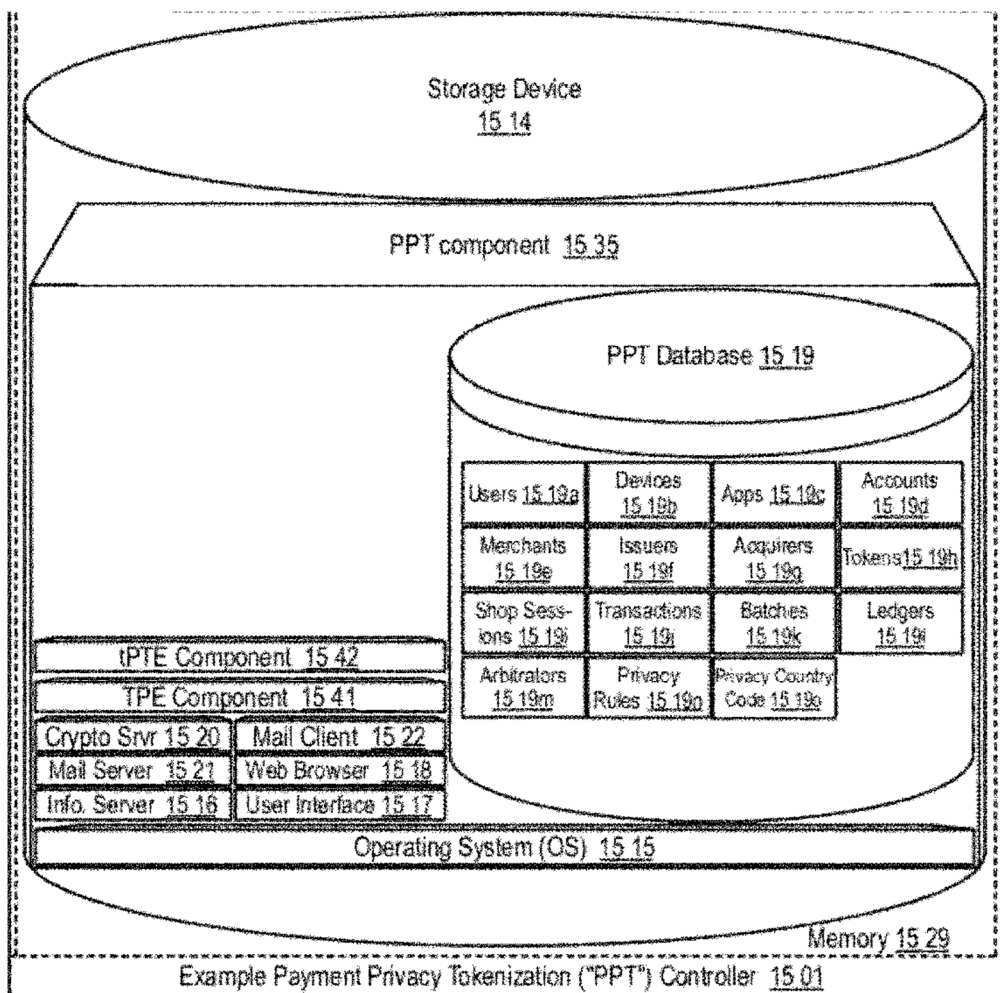
source”), ¶29 (user may obtain token from funding source). Osborne depicts the general arrangement of customers, parties, and the pay network server (which can include the PPT apparatus) in Fig. 4, reproduced below:



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, ¶¶210-211.

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 useful for proving the user’s identity or qualifications*. *See* EX1011, ¶147. Osborne teaches that a user “desir[ing] to utilize a card” may use “tokens in lieu of payment information” (thus, *to prove the user’s identity or qualifications*). EX1011, ¶25; EX1005, ¶212.

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, wherein the OVER file storage client device of the user is a first Near Field Communication (NFC) enabled device;

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. In particular, the user may communicate with a merchant server to purchase a product via the client by “activating a RFID/NFC enabled hardware device” (*OVER file storage client device of the user is a first NFC enabled device*) EX1011, ¶¶35, 49, 93. If the user desires to use tokenization, the client “may generate a completed application form, and provide, e.g., 424, the token application to the token server (either directly or via the merchant server).” 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, ¶213.

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> /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. 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, ¶¶214-15.

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, ¶216.

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

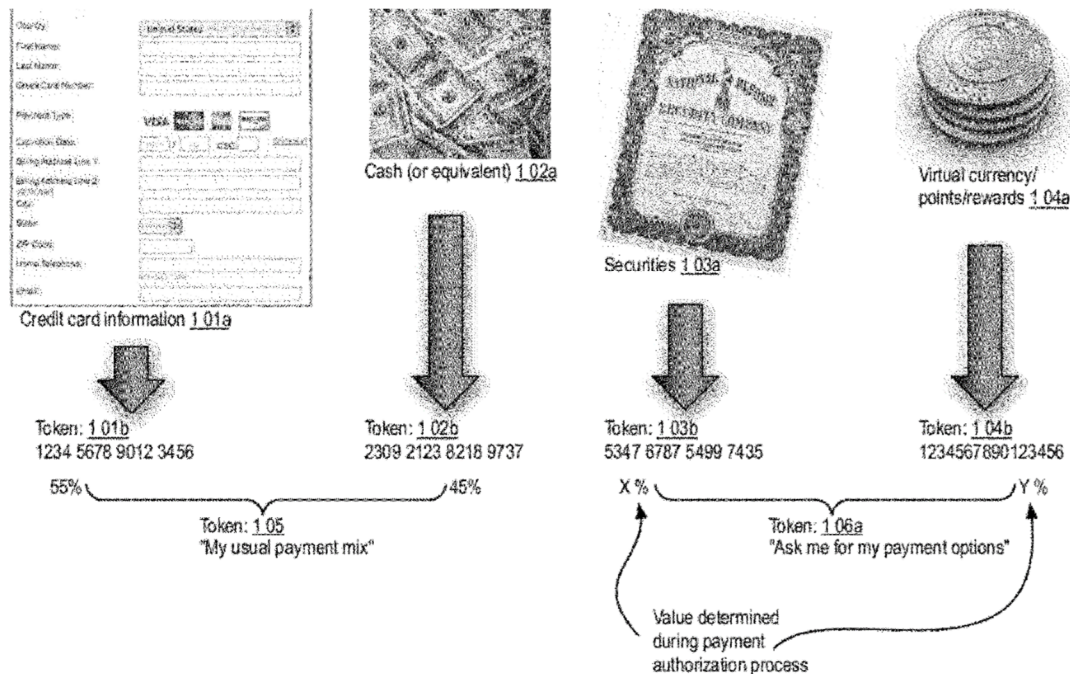


FIGURE 1B

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 generated based on the information associated with the credential*. EX1005, ¶217.

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, ¶¶218-20.

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 issuer verify the credential, rather than the token, 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, ¶221.

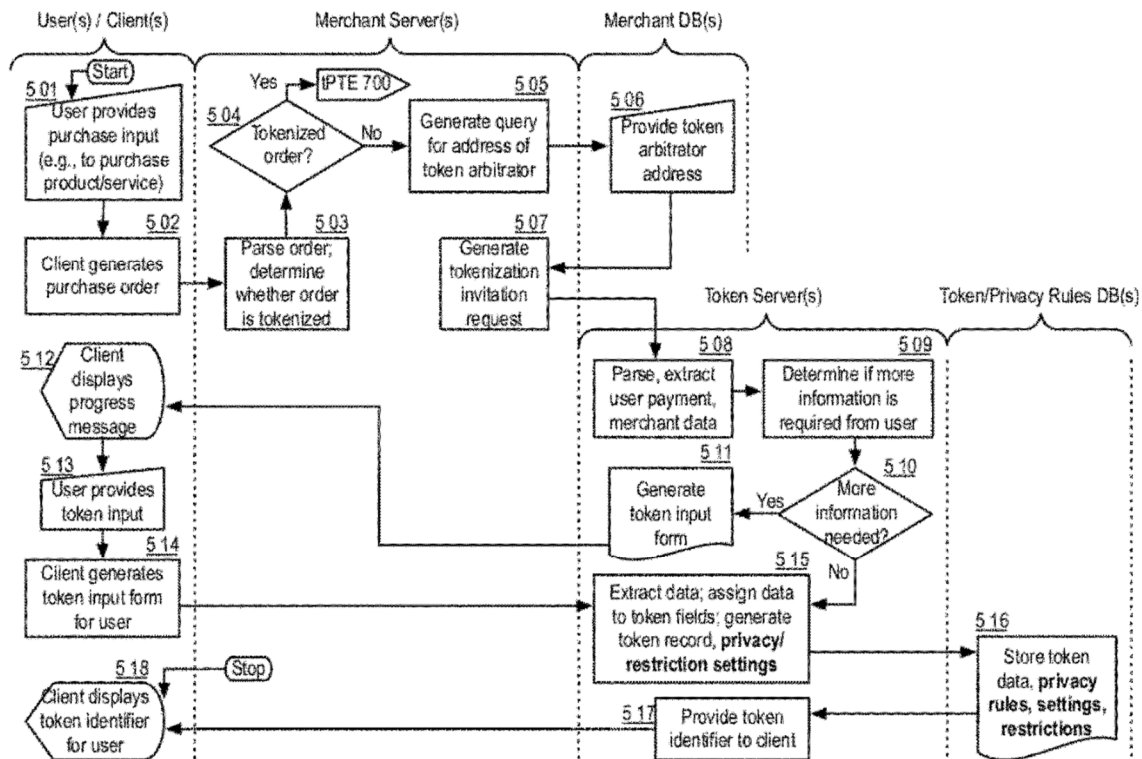


FIGURE 5

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 that is a second NFC enabled device, a verifying request to verify that the OVER file transmitted to the user authenticates the user, based on a Near Field Communication (NFC) protocol-based communication associated with the OVER file on the OVER file storage client device of the user being transmitted to the OVER file third-party client verifying device via an NFC protocol;

Osborne teaches this element as part of a merchant's token arbitration request (*verifying request*) triggered by a purchase order request from a user (*based on an NFC protocol-based communication*). Beginning with the NFC communication 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, ¶¶35, 49, 93. This NFC interaction triggers a tokenized purchase with the merchant, via a *third-party client verifying device that is a second NFC enabled 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"). Osborne's RFID/NFC activation triggers the purchase to be performed with the token and is therefore, an (*NFC*) *protocol-based communication associated with the OVER file on the OVER file storage client device of the user being transmitted*

to the OVER file third-party client verifying device via an NFC protocol. EX1005, ¶222.

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, ¶223. 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.”). Osborne thus teaches that the *OVER engine* (token server) receives the recited verifying request from a third-party device based on the recited NFC communication. EX1005, ¶223.

Osborne thus teaches element 1.5.

7. Element 1.6

verifying that the NFC protocol-based communication associated with the OVER file corresponds with the information associated with the credential of the user that is stored in the OVER engine, in response to the verifying request; and

Osborne teaches that the token server processes the token arbitration request triggered by the NFC communication (*supra* §IV.B.6) by looking up the account number in a token database. The token server “extract[s] the payment token from the message,” then issues a database query “using the payment token as a search term.” EX1011, ¶53. The database responds with “instructions for the token server on how to proceed with payment processing.” *Id.* This includes credential information such as user account numbers, as shown highlighted 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 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, ¶224.

Oborne 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, Oborne teaches verifying an NFC communication's correspondence with the user's credential using various complementary techniques. EX1005, ¶225.

Oborne thus teaches element 1.6.

8. Element 1.7

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

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

determining whether the recited NFC communication corresponds to the recited stored information. EX1005, ¶226.

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*).

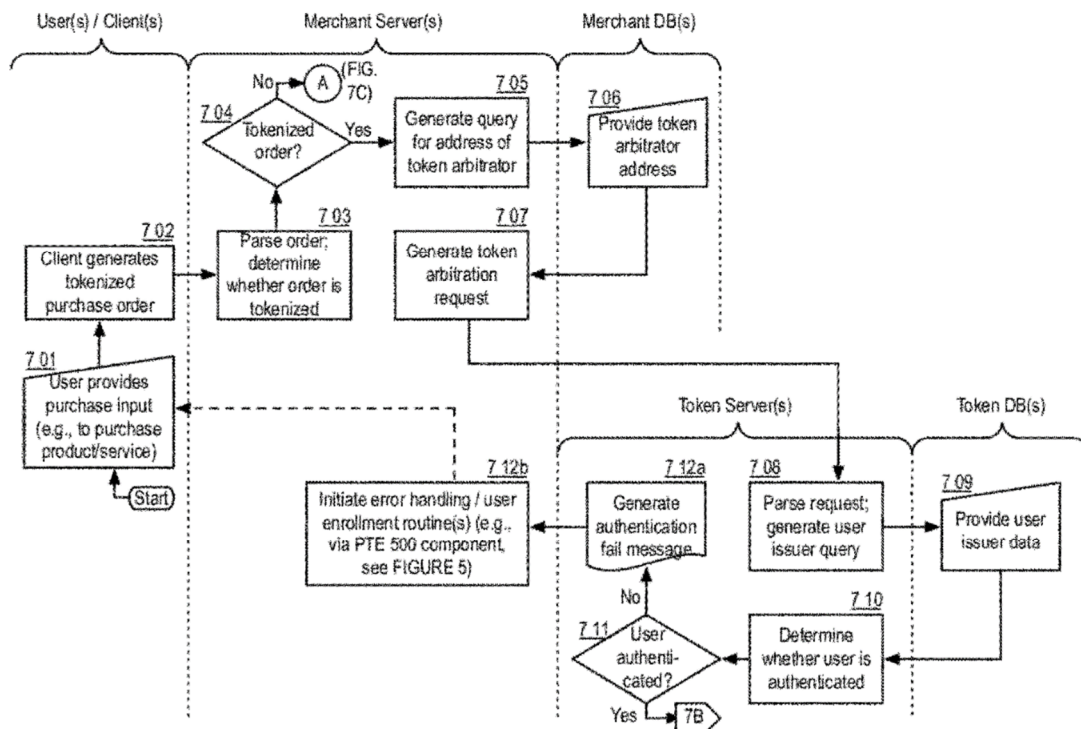


FIGURE 7A

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

EX1011, ¶69, Fig. 7A. This is an indication that the NFC communication is not associated with the stored user data. EX1005, ¶227.

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 NFC communication corresponded to the stored user credential information. EX1005, ¶228.

Osborne thus teaches element 1.7.

Accordingly, claim 1 was obvious over Osborne. EX1005, ¶¶208-229.

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.” Osborne 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, ¶230-31.

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, ¶232-33.

Accordingly, claim 2 was obvious over Osborne.

D. Claim 4

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

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 and credential information, 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, ¶234.

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, ¶235. 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, ¶¶236-37.

Accordingly, claim 4 was obvious over Osborne.

E. Claim 5

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 5 obvious. EX1005, ¶¶238-39.

F. Claim 6

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, ¶¶240-42.

Oborne thus renders claim 6 obvious.

G. Claim 7

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, ¶¶243.

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

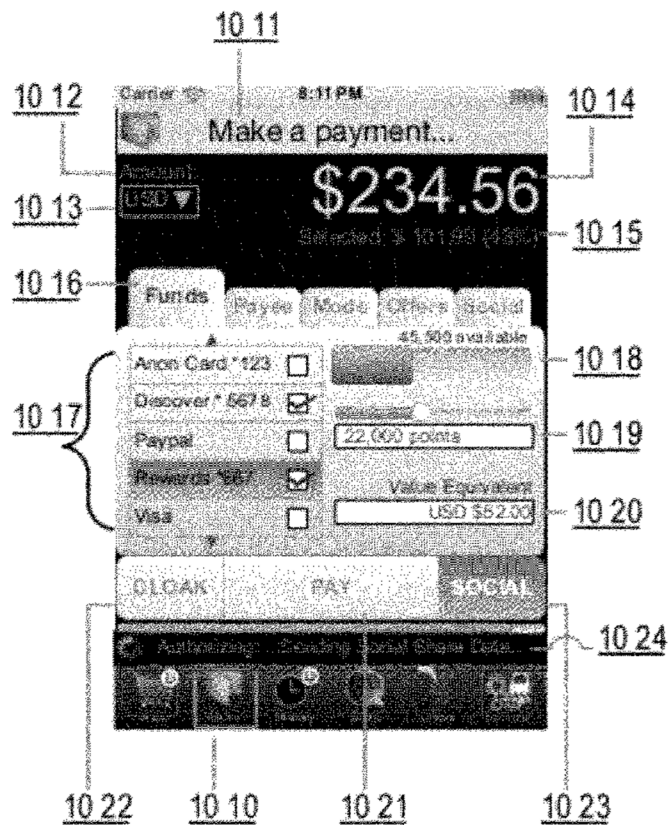
stored when creating a token, with the token data structure indicating which account number(s) correspond to a given token. *See* EX1011, ¶¶40, 47 (identifying by account numbers of user's credentials associated with token); *see also id.*, ¶25, Fig. 1B (token may indicate mix of one or more specified credentials via token indicators). EX1005, ¶¶244-45.

Accordingly, claim 7 was obvious over Osborne.

H. Claim 8

The computer-implemented method of claim 7, 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, ¶¶246-48.

Osborne thus renders claim 8 obvious.

I. Claim 9

1. Preamble

An apparatus comprising:

Oborne teaches an apparatus. *See, e.g.*, EX1011, Abstract (describing “PAYMENT PRIVACY TOKENIZATION APPARATUSES”), ¶¶114-22 (describing a computerized apparatus used to perform Oborne’s methods); EX1005, ¶¶249-250.

2. Elements 9.1-9.2

a processor;

a memory unit operatively coupled to the processor, the memory unit configured to store information associated with a credential of a user and a plurality of instructions, wherein said information is used to prove the user’s identity or qualifications, wherein the instructions are configured to program the processor to:

Oborne teaches a “PPT apparatus with a token server that stores credential information as discussed above. *Supra* §IV.B.2. This includes a processor and memory unit storing the data and instructions to perform the steps discussed for claim 1, and recited in elements 9.3-9.7. *See* EX1011, ¶¶115, 135, 146, Fig. 15; EX1005, ¶¶251-53.

Accordingly, Oborne teaches elements 9.1-9.2.

3. Elements 9.3-9.7

Oborne teaches elements 9.3-9.7 for similar reasons to elements 1.2-1.6. *See supra* §§IV.B.3-7; EX1005, ¶254.

4. Element 9.8

transmit, to the OVER file third-party client verifying device, 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's token server determines whether the user token is authenticated (e.g., EX1011, ¶¶54, 69), which corresponds to determining whether the OVER file corresponds to the user's credential. EX1005, ¶255.

Osborne further teaches sending an authentication message comprising a *status indicator* indicating 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*).

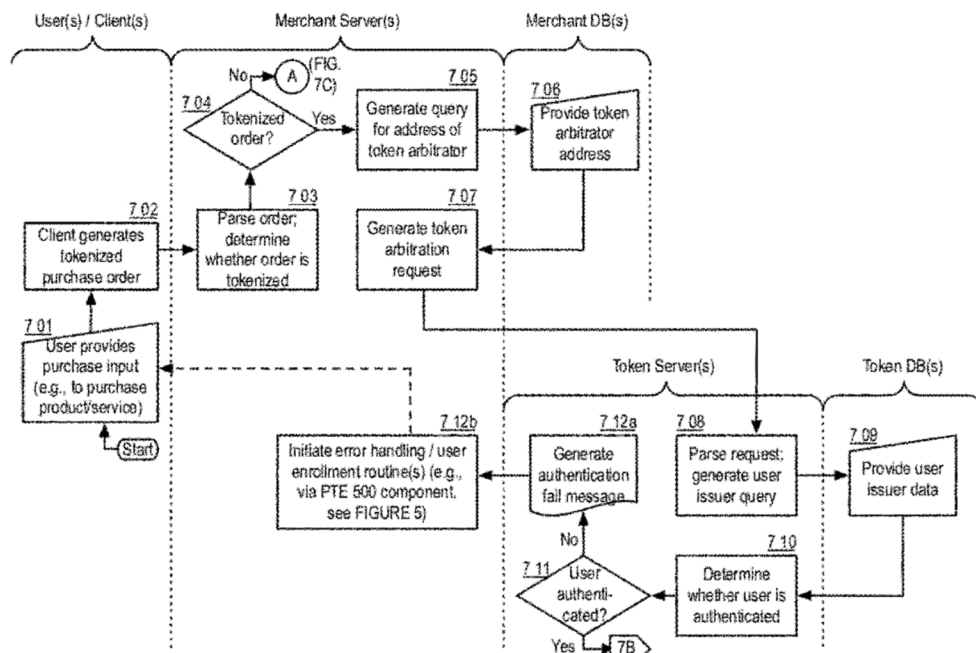


FIGURE 7A

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

EX1011, ¶69, Fig. 7A. This is a status indicator indicating that the OVER file does not correspond to the user's credential. EX1005, ¶256.

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 a *status indicator* indicating that the token was

authenticated, and thus that the OVER file corresponds to the user's credential. EX1005, ¶257.

Osborne thus teaches element 9.8.

Accordingly, claim 9 was obvious over Osborne. EX1005, ¶¶255-58.

J. Claims 10, 13, 14, and 16

Osborne teaches claims 10, 13, 14, and 16 for similar reasons to claims 2, 5, 6, and 7, respectively. *See supra* §§IV.C, IV.E-G; EX1005, ¶¶259-666.

K. Claim 17

The apparatus of claim 16, wherein when the credential identifier matches the stored credential, and the authentication message comprises the status indicator of the stored credential.

As described above, the credential identifier matching the stored credential corresponds to the account number associated with the token matching an account number of the user (e.g., an account with sufficient funds). *See supra* §IV.I.4. In such a case, *the authentication message comprises the status indicator*—that is, it indicates that the user's credential is authorized by the issuer. *See* EX1011, ¶¶61-63; EX1005, ¶¶267-68.

Accordingly, claim 17 was obvious over Osborne.

L. Claim 18

Osborne teaches a computer implemented method and elements 18.1-18.4 for reasons similar to elements 1.1-1.4 and the claim 1 preamble. EX1005, ¶269; *supra* §IV.B.1-5.

Osborne also teaches elements 18.5-18.7 for reasons similar to elements 1.5-1.7. *See supra* §§VI.B.6-8; EX1005, ¶¶269-70. Elements 18.5-18.7 substitute using NFC with using Bluetooth. Using both types of communication would have been obvious over Osborne, which teaches utilizing Bluetooth in the same manner as NFC. EX1011, ¶¶26 (communication “via Bluetooth...RFID...and/or the like”), 80 (“payment via near field communication 917e, Bluetooth 917f and email”), 127 (I/O devices may use Bluetooth). A POSA would thus be motivated to employ Bluetooth communications to transmit OVER file data. The arguments for using NFC in elements 1.5-1.7 thus similarly hold for using Bluetooth. EX1005, ¶¶269-70.

M. Claim 20

Osborne teaches an apparatus as shown for claim 9’s preamble, elements 20.1-20.5 as shown for elements 9.1-9.5, elements 20.6-20.7 as shown for elements 18.5-18.7, and element 20.8 as shown for element 9.8. EX1005, ¶¶379-81; *supra* §§IV.H.1-4, IV.L.

Thus, claim 20 was obvious over Osborne.

Accordingly, claims 1-2, 4-10, and 12-21 were obvious over Osborne.

EX1005, ¶¶206-277.

V. GROUND 2: CLAIMS 3, 11-12, AND 15 WERE OBVIOUS OVER OSBORNE AND PURVES

A. Overview of Ground and Rationale to Combine

Claim 3 depends from claim 1 and claims 11-12 and 15 depend from claim 9. As discussed below, each of these claims were obvious over Osborne and Purves.

Osborne teaches providing “user interface elements to generate new tokens” for accounts by providing a funding source and relevant information. EX1011, ¶29. Osborne’s PPT also “keeps track of all generated tokens via token identifiers,” ensuring that each such token is “unique.” EX1011, ¶47; EX1005, ¶278.

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 the use of virtual wallets and credentials, and the teachings of Purves would be recognized as useful to add new credentials to the digital wallet of Osborne’s PPT apparatus. EX1005, ¶¶279-80. 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.*

The discussion below shows how each element of claims 3, 11-12, and 15 is taught by Osborne and Purves. EX1005, ¶¶281-96.

B. Claims 3 and 11

As discussed above, Osborne teaches providing “user interface elements to generate new tokens” for accounts and “keep[ing] track of all generated tokens via token identifiers,” ensuring that each such token is “unique.” EX1011, ¶47; EX1005, ¶¶281-82.

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 (open loop or closed loop) or a reloadable prepaid card.” EX1013, ¶83; *see also id.*, ¶83 (discussing personalization of “the new card”). It would have been common sense to generate the new credential *after the processor determines that no credential of the user is stored*, since the purpose of Osborne’s tokens is to represent a credential; by generating the new credential, the user becomes able to benefit from Osborne’s tokenization system. EX1005, ¶283.

Accordingly, claims 3 and 11 were obvious over Osborne and Purves. EX1005, ¶¶281-284.

C. Claim 12

The apparatus of claim 9, wherein the instructions are further configured to program the processor to:

request the credential from the issuing agency, wherein the issuing agency stores credentials issued by the issuing agency;

receive the status indicator and credential information associated with the credential transmitted by the issuing agency; and

store the credential and a status indicator.

As discussed above for claim 11, Purves teaches generation of new credentials, such as a gift card or prepaid card. EX1013, ¶83. Purves further teaches that the system may, with user consent, retrieve the user's "payment account information from the payment account issuer." EX1013, ¶107. The issuer responds by providing the user's account information, including "user, user account, user financial account, and/or similar data for use in establishing a virtual wallet account, prepaid account, enrolling a payment account in a virtual wallet." EX1013, ¶108 (also showing XML including address, ZIP, etc.). Thus, Purves teaches requesting the credential from the issuing agency and receiving the credential information transmitted by the issuing agency. EX1005, ¶285.

Further, as discussed above for claim 9, Osborne teaches receiving the status indicator from the issuer. For example, in response to a request for authorization, an issuer queries a database to determine whether the account number sent for the token matches an account of the issuer with available funds for the transaction. *See* EX1011, ¶¶60-61; EX1005, ¶286. The issuer then sends a message indicating authorization success or failure, either of which is a status indicator received by the token server from the issuer. EX1011, ¶¶61-63; EX1005, ¶286.

It would also have been obvious both that the issuer would store credentials and that the received credential and status indicator would be stored by the PPT apparatus. EX1005, ¶287.

With regard to the issuer storing credentials, this storage of credentials would allow the issuer to provide the appropriate credential information upon request, as taught by Purves. *See* EX1013, ¶¶107-08. Moreover, when new credentials were generated upon user request, such as the gift and prepaid cards taught by Purves (EX1013, ¶83), it would be natural for the issuer to store such new credentials, at least until being sent to the recipient, and more practically for as long as they remained valid, so that the issuer's systems could confirm their existence. EX1005, ¶288. Consistent with this, Osborne teaches that the "user profile database" of the issuer can store "data associated with an account linked to the user's payment token." EX1011, ¶60. This would naturally include storing a credential, such as the new credential taught by Purves. *See* EX1005, ¶288.

Regarding storing the status indicator and credential in the PPT apparatus, this would also be obvious in view of Osborne and Purves. When receiving a credential, such as the new gift or prepaid card taught by Purves, it would be natural that it would be stored by Osborne's system for use with a token similar to how other credentials, such as regular credit cards, are stored in Osborne. *See*

EX1011, ¶45-48 (storing credentials in token data record and token data structure); EX1005, ¶289.

Likewise, Osborne teaches or suggests storing status indicators. 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 received status indicators, a POSA would have routinely stored them during normal token server operations. EX1005, ¶290.

Accordingly, claim 12 was obvious over Osborne and Purves. EX1005, ¶¶285-91.

D. Claim 15

Osborne teaches receiving and storing various status indicators, each of which leads to different processing steps. A POSA would have found it obvious to accomplish the different processing in response to different statuses (e.g., success, failed, insufficient funds, etc.) by checking the received status indicator. This would include checking the stored status indicator for a stored credential like those addressed in claim 12 for similar reasons as discussed for claim 16. EX1005, ¶¶292-93.

Osborne teaches storing a credential identifier for a given token, indicating which account number(s) correspond to a given token, via a database operation when creating a token. *See* EX1011, ¶47; *see also id.* (“[T]he token server keeps track of all generated tokens via token identifiers....For example, a serial series of token identifiers may be created....”); EX1005, ¶294.

Accordingly, claim 15 was obvious over Osborne and Purves.

Therefore, claims 3, 11-12, and 15 were obvious over Osborne and Purves. EX1005, ¶¶278-96.

VI. GROUND 3: CLAIMS 1, 3-4, 6-9, 11-12, AND 14-17 WERE OBVIOUS OVER STAFFORD AND PURVES

A. Overview and Rationale to Combine

The combination of Stafford and Purves renders each of claims 1, 3-4, 6-9, 11-12, and 14-17 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; EX1005, ¶297.

Stafford discloses methods for providing credentials to third parties that parallel the methods in the '973 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, ¶298.

Stafford teaches providing key signatures and other information to a third party "online or in person," and "delivery process may vary." EX1012, ¶¶106-13. Stafford thus expressly suggests including other information with its key signatures and employing various known delivery processes. EX1005, ¶299. These would include using an optical scan for delivery and including an image as a virtual credential representation in an OVER file, both of which are taught by Purves. In particular, Purves teaches providing issuer-verified representations of credentials and triggering transactions using near-field communications (NFC). EX1003, ¶64. It would have been obvious to use these features as part of Stafford's credential-distribution system to provide user devices convenient images of the credentials they are sharing and to use the well-known NFC communication-based protocol to transfer Stafford's key signatures to the third party. EX1005, ¶299.

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, ¶300. Further, incorporating features such as credential images and NFC protocol-based communication functionality 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, ¶301.

Similarly, a POSA would have viewed Purves's NFC communication as a convenient way to convey key signatures to third parties in a more efficient and reliable manner than reading or typing a code manually, both of which are slow and error-prone. By adapting Stafford's credential management system to transmit key signatures using an NFC communication, a POSA would reasonably have expected to achieve these benefits for users. EX1005, ¶302; *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, ¶303.

B. Claim 1

1. Preamble

Stafford and Purves teach a computer-implemented method. *See, e.g.*, EX1012, ¶54, Fig. 1; EX1005, ¶305.

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).

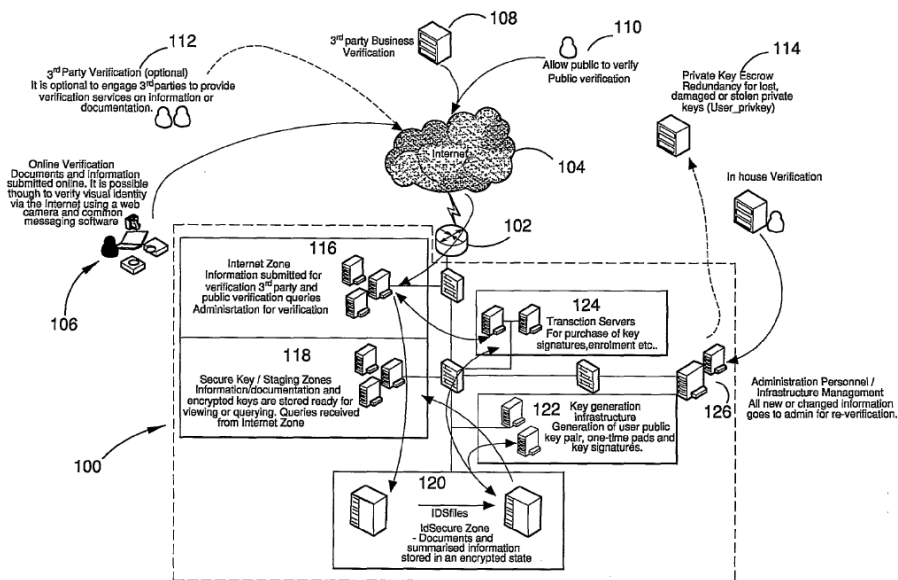


FIGURE 1

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, ¶306; *see also infra* §§VI.B.4, VI.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* §VI.B.3; EX1005, ¶307.

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.

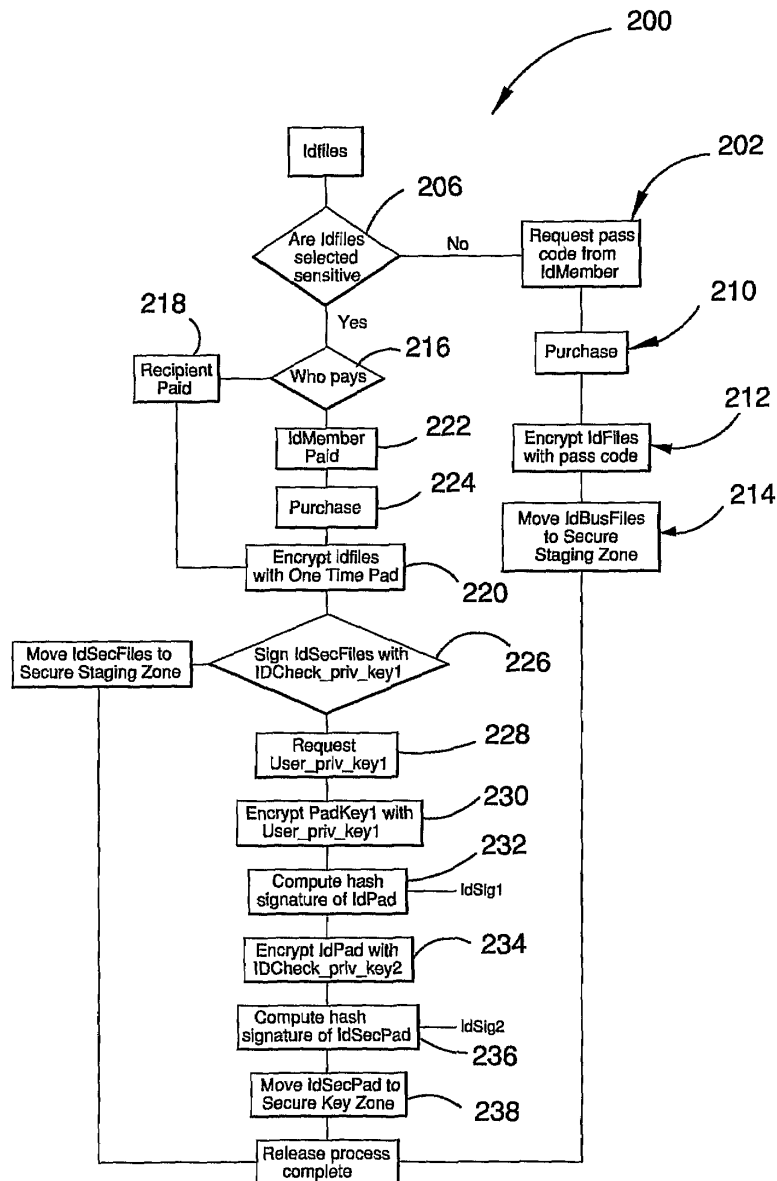


FIGURE 2

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, ¶308.

Purves teaches the user may communicate with a merchant server to purchase a product via the client by “activating a RFID/NFC enabled hardware device” (*the OVER file storage client device*) EX1011, ¶¶35, 49, 93; EX1005, ¶309. As is described in greater detail below with respect to element 1.5 below, Purves’s teaching renders obvious using an NFC interaction in place of other credential interactions, and thus an NFC-enabled user device, to transmit Stafford’s key signature, as doing so would allow the user to more easily transmit the key signature to a third party. EX1005, ¶309; *see infra* §VI.B.6.

Thus, Stafford and Purves teach element 1.2. EX1005, ¶310.

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, ¶311.

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, ¶312.

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, ¶313.

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, ¶314.

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, ¶315.

Stafford and Purves thus teach element 1.3. *Id.*, ¶¶311-16.

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). *Supra* §IV.B.4. 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* §VI.B.3; EX1012, ¶¶93-105, Fig. 2. Thus, Stafford and Purves teach element 1.4. EX1005, ¶¶317-18.

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).

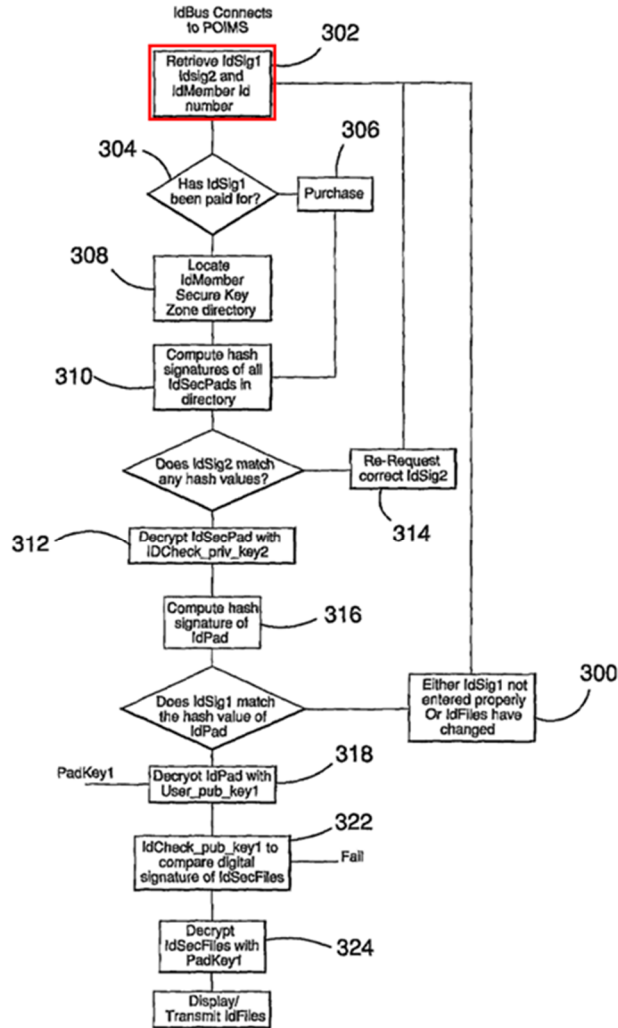


FIGURE 3

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, ¶319.

Purves teaches that an NFC interaction may be used to “trigger a wallet connection or login,” in place of a card swipe. EX1013, ¶64. Consistent with Purves’s teaching that an NFC interaction could be used to in place of a physical

credential swipe, and as discussed below in Ground 4, it was known that an NFC communication associated with an OVER file could be used to verify the OVER file transmitted to the user authenticates the user. *Supra* §I.C.3; EX1015, ¶61; EX1016, 12; EX1005, ¶320.

In light of Purves's teaching to use an NFC interaction in place of other credential interactions such as card swipes, it would have been obvious to use an NFC communication to transmit Stafford's key signature, as doing so would allow the user to more easily transmit the key signature to a third party. EX1005, ¶321. This NFC communication would be used to transmit the key signatures to the third-party verification device in step 302 of Stafford's Fig. 3. EX1005, ¶321. Thus, the verifying request would be *based on* the recited *NFC protocol-based communication associated with the OVER file* and the third-party device would be an *NFC enabled device*. Stafford and Purves thus teach element 1.5. EX1005, ¶321.

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 NFC communication. Stafford's system responds to this request (and thus the associated NFC communication of Stafford and Purves) by comparing the encoded hash

values IdSig1 and IdSig2 of the key signature. EX1012, ¶115-21, Fig. 3 (marked up below).

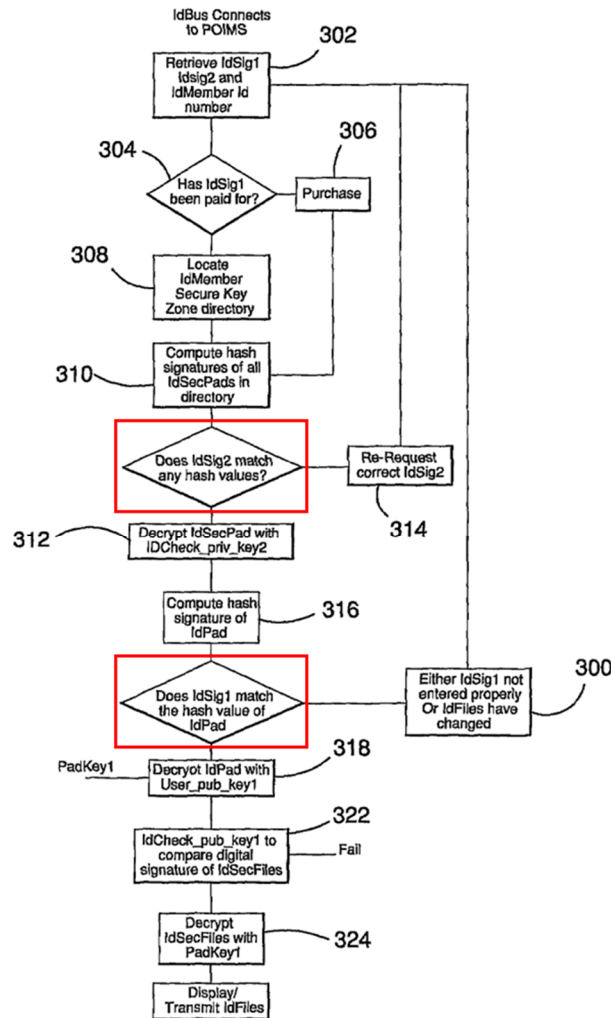


FIGURE 3

Checking the key signatures verifies that the NFC communication providing the key signatures 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); EX1005, ¶¶322-24. Thus, Stafford and Purves teach element 1.6. *Id.*

8. Element 1.7

Stafford teaches sending an authenticating message to the third-party device indicating whether the NFC communication corresponds to the information associated with the credential of the user. 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. Fig. 3 (marked-up below). 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, ¶¶325-326; EX1012, Fig. 3.

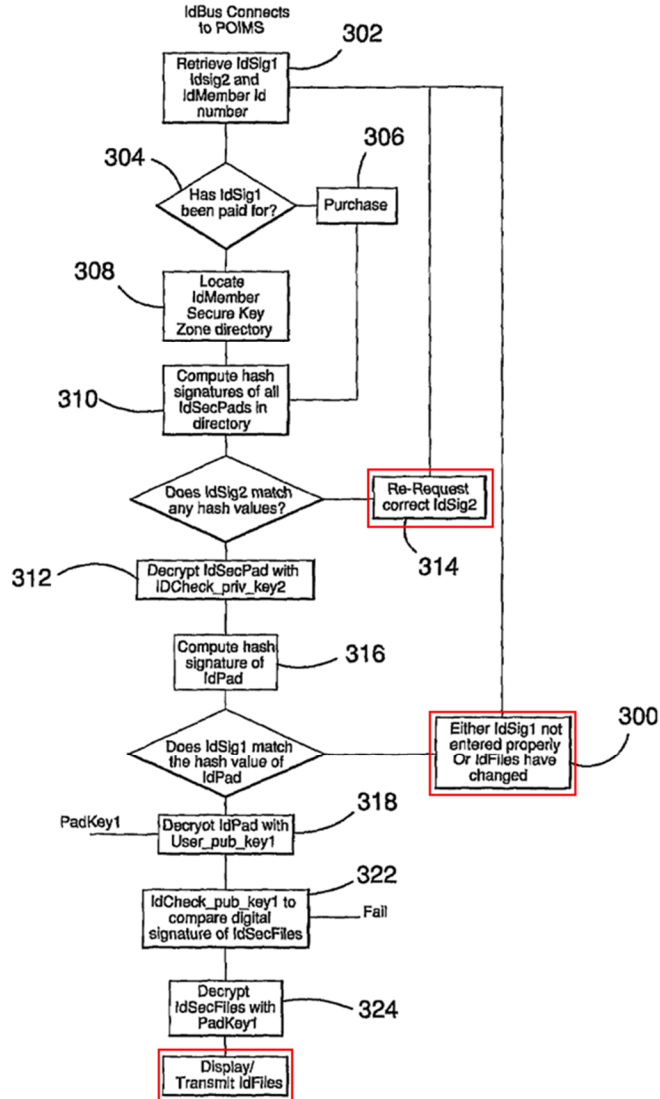


FIGURE 3

Stafford and Purves thus teach element 1.7.

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

¶¶304-27.

C. Claim 3

Stafford teaches that, after 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, ¶328.

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, ¶¶329-30. After 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 a 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, ¶331.

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, ¶¶332-33.

Accordingly, claim 4 was obvious over Stafford and Purves.

E. Claim 6

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, ¶334. 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 6 was obvious over Stafford and Purves. EX1005, ¶¶334-35.

F. Claim 7

Claim 7 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* §VI.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, ¶336.

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, ¶¶337-38.

Thus, claim 7 was obvious over Stafford and Purves. *Id.*

G. Claim 8

Stafford teaches storing scans of a credential, as discussed for claim 3. EX1012, ¶¶62, 67; *supra* §VI.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* §VI.B; EX1013, ¶122 (partially obscured credential image). Accordingly, claim 8 was obvious over Stafford and Purves. EX1005, ¶¶339-40

H. Claim 9

1. Preamble

Stafford and Purves teach an apparatus. *See, e.g.*, EX1012, ¶54, Fig. 1 (computerized system 100 and accompanying components); EX1013, Abstract, ¶¶130-46; EX1005, ¶341.

2. Element 9.1 and 9.2

Stafford and Purves teach *a processor* and an operatively-coupled *memory unit* that stores instructions and information about a user's credential, as recited in elements 9.1 and 9.2. EX1005, ¶342.

Stafford discloses a computer-implemented "system 100 for storing, validating and disseminating credential information about an entity," which may be connected "to a computer network such as the Internet." EX1012, ¶54; *see id.*, Fig. 1 (depicting system 100 as a system comprising computers). Thus, Stafford discloses a computer apparatus that stores credential information. EX1005, ¶343. A POSA would have understood that such a system would include a processor coupled to a memory unit storing instructions and the user's credential information. *Id.*

Purves confirms this arrangement, teaching that "computers employ processors to process information," which "may be referred to as central processing units (CPU)" operating on "instructions and data in various processor accessible and operable areas of memory." EX1013, ¶127; *see also id.*, ¶132 (CPU "execute[s] stored instructions (i.e., program code) according to conventional data processing techniques"). Purves details components present in typical computer systems, including CPUs and memory to store information and instructions. EX1013, ¶¶131-49; EX1005, ¶344.

The information stored in Stafford's system includes *information associated with a credential of a user*, as recited in element 9.2. EX1005, ¶345.

Fig. 1 (below), which depicts a system that stores credential information. 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).

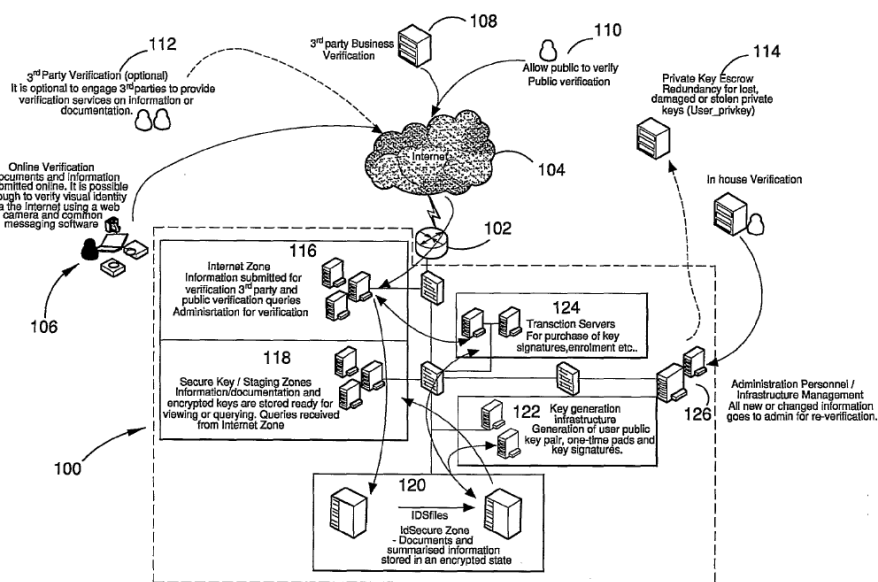


FIGURE 1

Stafford uses the terms “entity” (as well as the term “IDMember”) to refer to the user whose credentials are stored. EX1005, ¶360. 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 (e.g., Ph.D.), etc. EX1012, ¶¶4, 65, 131, 139. Stafford thus stores information associated with a user’s credential. EX1005, ¶¶346-47.

Thus, Stafford and Purves teach elements 9.1-9.2.

3. Elements 9.3-9.7

Stafford and Purves teach elements 9.3-9.7 for similar reasons to elements 1.2-1.6. *See supra* §§VI.B.3-7; EX1005, ¶348.

4. Element 9.8

Stafford teaches sending an authentication message to the third-party device indicating whether the scan corresponds to the OVER file. Where either key signature fails to match, an appropriate message is sent to re-request the non-matching hash value. EX1012, ¶¶120-22. Where they 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 comprising a status indicator, since a re-request message is an indicator of a lack of correspondence and the sending of the IdFiles is an indicator of a successful correspondence between the credential and the OVER file. EX1005, ¶349; EX1012, Fig. 3.

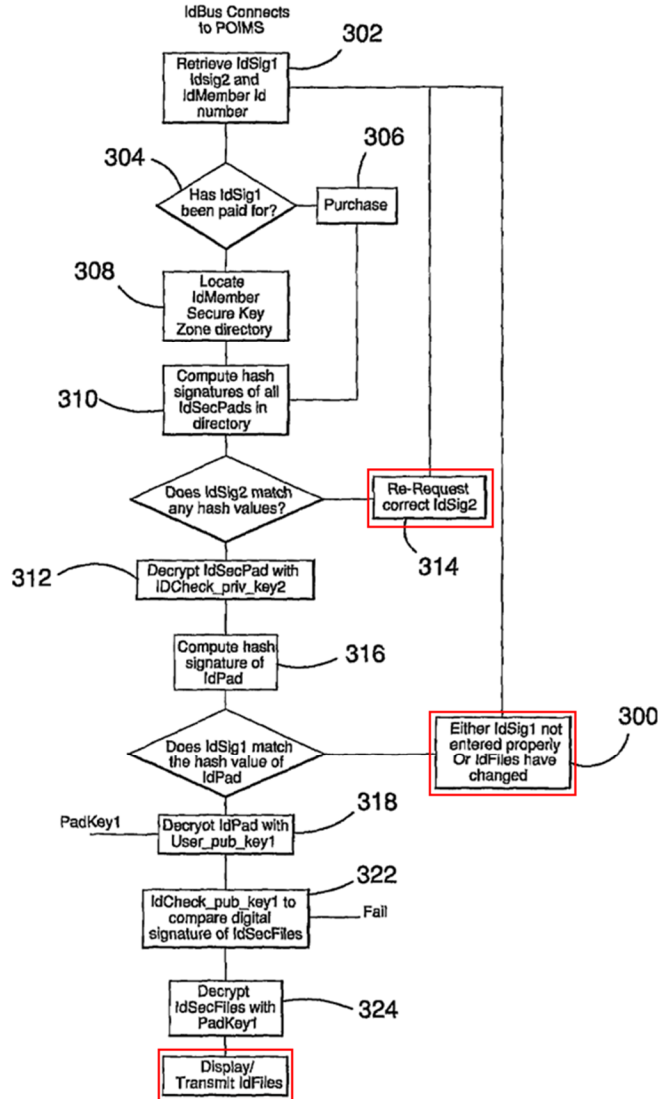


FIGURE 3

Stafford's system can assign a confidence rating to a credential based on the issuer's reliability. EX1012, ¶65. Stafford teaches that the "rating can be used by recipients in their assessment of the weight to be given to an IdMembers' credential information." *Id.* The inclusion of an indication that a credential was (or was not) verified, as well as the rating for the verifying issuer, when sending

credentials to a recipient would be a further example of a *status indicator* as recited. For example, a credential verified by a trusted issuer would indicate that the OVER file corresponds to an actual credential of the user. EX1005, ¶350.

Stafford and Purves thus teach element 9.8.

Accordingly, claim 9 was obvious over Stafford and Purves. EX1005, ¶¶341-52.

I. Claim 11

Stafford and Purves teach claim 11 for similar reasons to claim 3. *See supra* §VI.C; EX1005, ¶¶353-54.

J. Claim 12

Stafford teaches “automated verification” of users’ credentials, including “verification...with a document’s issuing body.” EX1012, ¶¶64-65. For example, Stafford describes requesting a university to “verify that IdMember has a PhD.” *Id.* The issuer thus provides a 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.); EX1005, ¶¶355; *see also id.*, ¶¶331-32.

As discussed for element 9.8, the system can also assign a confidence rating to a credential based on the issuer's reliability, which may be used by recipients to judge whether a credential has been sufficiently verified as genuine. *See* EX1012, ¶65. When Stafford's system receives a verification from an issuer and applies its reliability assessment to it, it is *receiv[ing] the status indicator* (e.g., a status of *verified* ("IdMember has a PhD") or *not verified*). Stafford's system would also be receiving *credential information associated with the credential transmitted by the issuing agency*, as Stafford teaches that the issuer provides "Verification of the information conveyed by the documentation," through "verification of document or data authenticity with a document's issuing body." EX1012, ¶65. This verification would include both a status of valid or invalid and verify particular details (such as the name for the credential, and information such as associated numbers). EX1005, ¶356; *see* EX1012, ¶¶4 (information for driver's license includes "number on the drivers license used for identification" and "name on the license"), 62 (documentation information can include scans of an entire credential document); *see also* EX1013, ¶108 (issuer-provided XML file including various information associated with a credential, e.g., address and ZIP). Stafford stores the credential (EX1012, ¶67), and a POSA would also have found it natural to store the indicator received from the issuing agency so that the issuer's verification (or

failure to verify) could be provided to recipients and to apply confidence ratings when deciding the reliability of the credential information. EX1005, ¶356.

A POSA would have expected that an issuer would store the issued credentials as a matter of course. For example, as discussed in Ground 2, Purves teaches generating new credentials by issuers, (*see* EX1013, ¶83). It would be natural for the issuer to store such new credentials, at least until being sent to the recipient, and more practically for as long as they remained valid, so that the issuer's systems could confirm their existence. EX1005, ¶357. This accords with Stafford's teaching that an issuer is to be contacted to verify a credential (*see* EX1012, ¶65), as storing the credential would allow the issuer to verify its authenticity. EX1005, ¶357. For example, Stafford describes a scenario involving verification of an academic degree (EX1012, ¶65), and a POSA would have understood that it was common practice for academic institutions to store credentials such as academic transcripts in electronic databases to allow their production to interested parties. EX1017, ¶¶89-90 ("The information system 14 of the first institution typically includes a database with the relevant transcript data....Specifically, the transcript information can be encoded in a structured document format. One suitable format is Xtensible Markup Language (XML)."); EX1005, ¶¶357-58.

Accordingly, claim 12 was obvious over Stafford and Purves.

K. Claim 14

Stafford and Purves teach claim 14 for similar reasons to claim 6. *See supra* §VI.E; EX1005, ¶¶359-60.

L. Claim 15

Claim 15 requires checking the stored status indicator. Stafford teaches storing a status indicator, as discussed for claim 12. *Supra* §VI.J. 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.”); *see also id.*, (also teaching providing confidence ratings to credential recipients, which would include checking the stored status indicator to indicate the confidence level to the recipient). A POSA would have implemented this process by checking the status indicator (a verification from an issuer) along with the issuer’s confidence rating to determine whether the credential was validated and what the confidence level was. EX1005, ¶¶361-62.

Thus, claim 15 was obvious over Stafford and Purves.

M. Claim 16

Stafford and Purves teach claim 16 for similar reasons to claim 7. *See supra* §VI.F; EX1005, ¶¶363-64.

N. Claim 17

Stafford teaches or suggests sending a *status indicator* as part of the authentication message *when the credential identifier* (key signature) *matches the stored credential*. For example, the status indicator can include the credential and indicate whether the issuer has verified the credential, as well as indicating the issuer's reliability. *See supra* §VI.B.7; EX1012, ¶¶65 (confidence rating for verification sent with verified credential), 120-26, Fig. 3 (credential sent upon matching key signatures); EX1005, ¶¶365-66.

Accordingly, claim 17 was obvious over Stafford and Purves.

Accordingly, claims 1, 3-4, 6-9, 11-12, and 14-17 were obvious over Stafford and Purves. EX1005, ¶¶297-67

VII. GROUND 4: CLAIMS 2, 5, 10, 13, AND 18-21 WERE OBVIOUS OVER STAFFORD, PURVES, AND NEAFSEY

A. Overview and Rationale to Combine

The combination of Stafford, Purves, and Neafsey renders claim 2, 5, 10, 13, and 18-21 obvious.

As described above in Ground 3, Stafford and Purves render the computer-implemented methods of claims 1 and 9 obvious. *See supra* §VI. Claims 18 and 20 differ from claims 9 and 1, respectively, only in that, properly understood, they require using Bluetooth in place of NFC. Purves teaches using Bluetooth transceivers as part of its virtual wallet computer system. EX1013, ¶¶131, 139.

Neafsey teaches using both Bluetooth and NFC protocol-based communications. EX1015, ¶31; EX1016, 6. Should Patent Owner argue that claims 18 and 20 should be understood as written (that is, to require both NFC and Bluetooth), this would have been obvious in light of the disclosures of Neafsey.

A POSA would have been motivated to incorporate the Bluetooth communication module of Neafsey into the device of Osborne and Purves to be used to trigger the use of tokens to purchase goods because the Bluetooth communication would serve a similar role as NFC. The combination would thus be a simple substitution of known elements to achieve predictable results. EX1005, ¶371; *see KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 416-17 (2007).

Introducing Bluetooth would enhance flexibility, increase convenience, and support more mobile device types. A POSA would reasonably have expected to achieve these benefits when transmitting key signatures using Bluetooth at least because Bluetooth was a well-known technology and would require only a one-to-one substitution with NFC. EX1005, ¶¶372-73.

Neafsey is drawn to a credential management system for managing tokens and is in the same field of endeavor as Stafford and Purves. All three references relate to the creation and management of credentials, including tokens. EX1005, ¶368.

A POSA would have reasonably expected success in combining Stafford, Purves, and Neafsey. The references involve well-understood and related networking technologies for managing electronic credentials and conducting transactions, each of which would function predictably in combination. Combining these references does not result in contravening the method of operation of any of them. EX1005, ¶369.

Applying these teachings, each of claims 2, 5, 10, 13, and 18-21 was obvious over the combination of Stafford, Purves, and Neafsey.

B. Claim 18

Stafford and Purves teach a computer implemented method and elements 18.1-18.4 for similar reasons elements 1.1-1.4 and the claim 1 preamble. EX1005, ¶¶374-75; *supra* §VI.B.1-5.

Stafford and Purves also teach elements 18.5-18.7 for similar reasons to elements 1.5-1.7. *See supra* §§VI.B.6-8; EX1005, ¶376. Elements 18.5-18.7 require using a Bluetooth protocol-based communication in an NFC-enabled device. Using both types of communication would have been obvious over Stafford, Purves, and Neafsey. For example, Neafsey teaches utilizing Bluetooth in the same manner as NFC. EX1015, ¶31; EX1016, 6 (input/output system using Bluetooth or NFC, optionally using “more than one system”). A POSA would thus be motivated to employ Bluetooth communications to transmit OVER file data.

The arguments for using NFC in elements 1.5-1.7 thus similarly hold for using Bluetooth. EX1005, ¶¶374-78.

C. Claim 20

Stafford, Purves, and Neafsey teach an apparatus as shown for claim 9's preamble, elements 20.1-20.5 as shown for elements 9.1-9.5, elements 20.6-20.7 as shown for elements 18.5-18.7, and element 20.8 as shown for element 9.8.

EX1005, ¶¶279, 379-81; *supra* §§VI.H.1-4, VII.B.

Thus, claim 20 was obvious over Stafford and Purves.

D. Claims 2, 5, 10, 13, 19, and 21

Claims 2, 5, 10, 13, 19, and 21 add limitations regarding (for claims 5 and 13) a device identifier limiting the credential to the client device, or (for claims 2, 10, 19, and 21) a 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, ¶383.

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 different credential representations 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, ¶384. In particular, a POSA would understand different client devices would sometimes require using different formats appropriate to each device, as certain formats could not be used on certain devices. EX1005, ¶384; *see* EX1015, ¶61 (device may be smartphone or smartcard); EX1016, 11.

Applying these teachings, each of claims 2, 5, 10, 13, 19, and 21 was obvious over Stafford, Purves, and Neafsey.

Claims 5 and 13 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, ¶385.

As to claims 2, 10, 19, and 21, each claim 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, ¶386. Thus, Stafford, Purves, and Neafsey teach the elements of claims 2, 10, 19, and 21 for similar reasons as they teach the elements of claims 5 and 13. *Id.*

Accordingly, claims 2, 5, 10, 13, 19, and 21 were obvious over Stafford, Purves, and Neafsey. *Id.*, ¶¶383-88

VIII. 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 ’859 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, nor are the references relied on in the petition cumulative to the references applied during examination. *Supra* §I.B. *See generally* EX1009. Indeed, the discussion in the grounds above explains in detail why the claims of the '859 patent were obvious over the prior art, confirming that their allowance constituted material error.

IX. GROUNDS FOR STANDING

Visa certifies that, under 37 C.F.R. §42.104(a), the '859 patent is available for *inter partes* review, and Visa is not barred or estopped from requesting *inter partes* review of the '859 patent on the grounds identified.

X. CONCLUSION

For the reasons set forth above, claims 1-21 of the '859 patent are unpatentable. Visa therefore requests that an *inter partes* review of these claims be instituted.

Respectfully submitted,

Dated: January 26, 2024

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

XI. 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 '859 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 petitions against three related patents: U.S. Patent No. 9,251,531 (IPR2024-00486 and IPR2024-00487); U.S. Patent No. 9,954,854 (IPR2024-00488); and U.S. Patent No. 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

XII. 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.

XIII. 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 13,998 words, excluding the parts of the brief exempted by 37 C.F.R. §42.24(a).

Respectfully submitted,

Dated: January 26, 2024

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

XIV. 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_distprofile0331.2023.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. 10,749,859 (and accompanying Exhibits 1001-1046) by overnight courier (Federal Express or UPS), on this 26th 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 26, 2024

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