IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

VISA, INC.,

Petitioner,

v.

CORTEX MCP, INC.,

Patent Owner.

IPR2024-00489

PATENT NO. 10,749,859

DECLARATION OF MICHAEL IAN SHAMOS, PH.D., J.D.

VISA EXHIBIT - 1005
Visa Inc. v. Cortex MCP, Inc.

TABLE OF CONTENTS

I. INTRODUCTION AND QUALIFICATIONS 1
II. MATERIALS CONSIDERED 5
III. SUMMARY OF OPINIONS 8
IV. LEGAL PRINCIPLES 9
V. THE CHALLENGED PATENT 15
VI. LEVEL OF ORDINARY SKILL IN THE ART 25
VII. CLAIM CONSTRUCTION 27
A. "officially verifiable electronic representation"/"OVER" file 27
B. "…verified by an issuing agency…" 32
VIII. BACKGROUND OF THE PRIOR ART 33
A. Secure Credentials 33
B. Tokens 38
C. QR Codes 72
D. Near-Field Communication 77
E. Credential Identifiers 80
F. Device Identifiers 81
G. Status Indicators 83
H. Reason for Invalid Credential 84
IX. Ground 1: Claims 1-2, 4-10, 13-14, AND 16-21 were Obvious over Oborne 86
A. Claim 1 87
1. Preamble 87
2. Limitation 1.1 87
3. Limitation 1.2 90
4. Limitation 1.3 93
5. Limitation 1.4 96
6. Limitation 1.5 97
7. Limitation 1.6 100
8. Limitation 1.7 102

B. Claim 2 104
C. Claim 4 106
D. Claim 5 108
E. Claim 6 109
F. Claim 7 110
G. Claim 8 111
H. Claim 9 112
1. Preamble 113
2. Limitations 9.1 and 9.2 113
3. Limitations 9.3-9.7 114
i. Limitation 9.8 114
I. Claim 10 117
J. Claim 13 117
K. Claim 14 117
L. Claim 16 117
M. Claim 17 118
N. Claim 18 118
O. Claim 19 119
P. Claim 20 119
1. Limitations 20.6-20.7 119
2. Limitation 20.8 119
Q. Claim 21 120
X. Ground 2: Claims 3, 11-12, and 15 were Obvious over Oborne in view of Purves 120
A. Overview and Reasons to Combine 120
B. Claims 3 and 11 121
C. Claim 12 122
D. Claim 15 125
XI. Ground 3: Claims 1, 3-4, 6-9, 11-12, and 14-17 were Obvious over Stafford IN VIEW OF Purves 127
A. Overview and Rationale to Combine 127

B. Claim 1 129
1. Preamble 129
2. Limitation 1.1 130
3. Limitation 1.2 132
4. Limitation 1.3 134
5. Limitation 1.4 137
6. Limitation 1.5 137
7. Limitation 1.6 140
8. Limitation 1.7 142
C. Claim 3 143
D. Claim 4 145
E. Claim 6 146
F. Claim 7 147
G. Claim 8 148
H. Claim 9 148
1. Preamble 148
2. Limitations 9.1 and 9.2 149
3. Limitations 9.3-9.7 151
4. Limitation 9.8 151
I. Claim 11 154
J. Claim 12 154
K. Claim 14 157
L. Claim 15 157
M. Claim 16 157
N. Claim 17 158
XII. Ground 4: Claims 2, 5, 10, 13, and 18-21 were Obvious over Stafford in view of Purves further in view of NEAFSEY 158
A. Overview and Rationale to Combine 158
B. Claim 18 160
1. Limitations 18.1-18.4 160
2. Limitations 18.5-18.7 161

C. Claim 20 161
1. Limitations 20.6-20.7 161
2. Limitation 20.8 162
D. Claims 2, 5, 10, 13, 19, and 21 162
XIII. CONCLUDING STATEMENT 164
XIV. JURAT 164

I, Michael I. Shamos, declare as follows.

I. INTRODUCTION AND QUALIFICATIONS

1. I have been retained by Wilson Sonsini Goodrich & Rosati Professional Corporation on behalf of Petitioner Visa Inc. ("Visa") to provide my opinions concerning the validity of claims 1-21 (the "Challenged Claims"), constituting all claims of U.S. Patent No. 10,749,959 ("'859 Patent," or the "Patent," EX1003) in support of Petitioner's Petition for *Inter Partes* Review of the '859 Patent (the "Petition").

2. I have been retained as an independent expert consultant in this proceeding before the United States Patent and Trademark Office. Although I am being compensated at my rate of $600.00 per hour for the time I spend on this matter, no part of my compensation depends on the outcome of this proceeding, and I have no other interest in this proceeding, any of the parties, or the subject patent.

3. A detailed description of my professional qualifications, including a listing of my specialties/expertise and professional activities and publications, is contained in my curriculum vitae, a copy of which is provided as EX1006. Below is a short summary of my professional qualifications.

4. I received an A.B. (1968) from Princeton University in Physics; a M.A. (1970) from Vassar College in Physics; a M.S. (1972) from American University in Technology of Management, a field that covers quantitative tools used in managing

organizations, such as statistics, operations research and cost-benefit analysis; a M.S. (1973), and M.Phil. (1974) and a Ph.D. (1974) from Yale University in Computer Science; and a J.D. (1981) from Duquesne University.

5. I currently hold the title of Distinguished Career Professor in the School of Computer Science at Carnegie Mellon University in Pittsburgh, Pennsylvania. I am a member of two departments in that School, the Software and Societal Systems Department and the Language Technologies Institute. I was a founder and Co-Director of the Institute for eCommerce at Carnegie Mellon from 1998-2004 and from 2004-2018 was Director of the eBusiness Technology graduate program in the Carnegie Mellon University School of Computer Science. Since 2018, I have been Director of the M.S. in Artificial Intelligence and Innovation degree program at Carnegie Mellon.

6. I have taught graduate courses at Carnegie Mellon in Electronic Commerce, including eCommerce Technology, Electronic Payment Systems, Electronic Voting, Internet of Things, Electronic Payment Systems and eCommerce Law and Regulation, as well as Analysis of Algorithms. Since 2007 I have taught an annual course in Law of Computer Technology. I currently also teach Artificial Intelligence and Future Markets.

7. I am the author and lecturer in a 24-hour video course on Internet protocols and have taught computer networking, wireless communication, and Internet architecture since 1999.

8. From 2001-2021, I was a Visiting Professor at the University of Hong Kong, where I taught an annual course in Electronic Payment Systems. This is one of only a handful of graduate courses taught on this subject in the world.

9. I was the Director of Carnegie Mellon's graduate degree program in eBusiness Technology from 1999-2018 and am now a faculty member in the Privacy Engineering degree program at Carnegie Mellon. My course on Law of Computer Technology is required for all students in that program, the M.S. in Artificial Intelligence and Innovation program and in the Societal Computing Ph.D. program.

10. From 1979-1987, I was the founder and president of two computer software development companies in Pittsburgh, Pennsylvania, Unilogic, Ltd. and Lexeme Corporation.

11. I am an attorney admitted to practice in Pennsylvania and have been admitted to the Bar of the U.S. Patent and Trademark Office since 1981. I have been asked to render opinions in this Declaration as a technical expert. I have not been asked to offer any opinions on patent law in this proceeding.

12. I am a named co-inventor on the following six issued patents relating to electronic commerce: U.S. Patent Nos. 7,330,839, 7,421,278, 7,747,465, 8,195,197, 8,280,773, and 9,456,299.

13. I have previously served as an expert in over 375 cases concerning computer technology. In particular, I have been involved in at least 40 cases involving electronic payments.

14. I am aware of contemporaneous litigation involving the parties in a case styled *Cortex MCP. Inc. v. Visa Inc.*, 6:23-cv-00048-FB (W.D. Texas) (the "Litigation").

15. The Petition involves the '859 Patent. Its ancestor, U.S. Patent 9,251,531 (the "'531 Patent") claims priority to U.S. Provisional Patent Application 71/740,731 (the "'731 Provisional"), filed December 21, 2012. At least three other patents descend from the '531 Patent. U.S. Patent 9,954,854 (the "'854 Patent," EX1002) is a continuation of the '531 Patent, and also claims priority to December 21, 2012. The '859 Patent," is a continuation of the '854 Patent and further claims priority to December 21, 2012. U.S. Patent 11,329,973 (the "'973 Patent," EX1004) is a continuation of the '859 Patent and likewise claims priority to December 21, 2012. I refer to these four patents collectively as the "Cortex Patents." I understand that IPR petitions have been concurrently filed on this day challenging all four Cortex Patents. I am providing supporting declarations those IPR proceedings.

16. I have been asked to assume, for purposes of these IPR proceedings only, and without offering an opinion on the point, that the claims of the four listed patents are all entitled to a Priority Date of December 21, 2012.

17. I have no financial interest in Patent Owner or the Cortex Patents. It is conceivable that I may own mutual funds whose portfolios include stock in Petitioner. If this is the case, the value of such holding would not constitute a material part of my net worth.

18. The statements made and opinions provided in this Declaration are based on my own personal knowledge and, if called as a witness, I could and would testify in a manner consistent with this Declaration.

19. In this Declaration, all emphasis has been added unless otherwise noted.

II. MATERIALS CONSIDERED

20. In forming my opinions, I have reviewed and am familiar with the '859 patent and its prosecution history, the materials cited herein, and the following exhibits to the Petition.

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
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	Oborne U.S. Patent Pub. No. 2012/0316992("Oborne")
1012	Stafford U.S. Patent Pub. No. 2009/0271321 ("Stafford")
1013	Purves et al. U.S. Patent Pub. No. 2013/0054454("Purves")
1014	Harris et al. U.S. Patent Pub. No. 2012/0310838 ("Harris")
1015	Neafsey et al. U.S. Patent Pub. No. 2013/0212248 ("Neafsey")
1016	U.S. Provisional Patent Application No. 61/598,219 ("Neafsey Provisional")
1017	Morin et al. U.S. Patent Publication No. 2008/0270166 ("Morin")
1018	First Amended Complaint (Dkt. No. 25) *Cortex MCP, Inc. v. Visa Inc.*, No. 5-23-cv-05720 (N.D. Cal.), *as filed in* No. 6-23-cv-00048 (W.D. Tex) (Apr. 10, 2023) ("Complaint")
1019	Steiner et al., "Kerberos: An Authentication Service for Open Network Systems." *Usenix Winter* (1988) ("Steiner")
1020	Cross River, "Tokenization in Card Networks" (May 2023) ("Cross River")
1021	U.S. Patent No. 7,014,107 to 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. *PCI Compliance for Dummies* (2009) ("Thakar")
1026	Ben Jackson. "Token Gestures." *Digital Transactions* (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	Mattson U.S. Patent Pub. No. 2009/0249082 ("Mattson")
1029	Leach U.S. Patent Pub. No. 2010/0070754 ("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	Shader et al. U.S. Patent Pub. No. 2011/0258122 ("Shader")
1037	Randazza et al. U.S. Patent Pub. No. 2011/0320316 ("Randazza")

1038	Tim Horton et al. "A Primer on Payment Security Technologies: Encryption and Tokenization." (2011) ("First Data 2011")
1039	Smith et al. U.S. Patent Pub. No. 2012/0016731 ("Smith")
1040	Langley U.S. Patent Pub. No. 2012/0150669 ("Langley")
1041	Guenther Starnberger et al. "QR-TAN: Secure Mobile Transaction Authentication." *2009 International Conference on Availability, Reliability and Security*. IEEE. (2009) ("Starnberger")
1042	Laracey U.S. Patent Pub. No. US 2011/0251892 ("Laracey")
1043	Hammad et al. U.S. Patent Pub. No. 2012/0209749 ("Hammad")
1044	Adams U.S. Patent Pub. No. 2009/0113543 ("Adams")

21. I have also relied on my education, skill, training, and experience in the relevant fields of technology. I have further considered the viewpoint of a person of ordinary skill in the art ("POSITA") in the subject matter of the '859 Patent as of December 21, 2012.

22. I reserve the right to supplement my opinions as expressed in this Declaration to address any new information obtained in the course of this proceeding, or based on any new positions taken by Patent Owner.

III. SUMMARY OF OPINIONS

23. It is my understanding that the following table summarizes the grounds of challenge ("Grounds") raised in the Petitions:

Grd.	Sec.	References	Challenged Claims
1	103	Oborne	1-2, 4-10, 13-14, 16-21

2	103	Oborne, Purves	3, 11-12, 15
3	103	Stafford, Purves	1, 3-4, 6-9, 11-12, 14-17
4	103	Stafford, Purves, Neafsey	Stafford, Purves, Neafsey

24. After a review of the '859 Patent and the prior art asserted by Petitioner, it is my opinion that the Challenged Claims are invalid under the respective Grounds. My opinions, and the bases therefor, are detailed throughout this Declaration.

IV. LEGAL PRINCIPLES

25. Counsel for Patent Owner has informed me of the legal principles that apply in this proceeding.

26. I understand that for a claim to be anticipated under 35 U.S.C. § 102, each claim element must be disclosed, either expressly or inherently, in a single item of prior art, and the claimed arrangement or combination of those elements in the claim must also be disclosed, either expressly or inherently, in that same item of prior art.

27. A prior art reference can disclose a limitation that is not expressly disclosed in the reference if it is "inherently present" in the reference. I further understand that to be "inherently present," the missing disclosure must necessarily and inevitably be present in the element or process described in the reference. It is my understanding that a limitation is not disclosed by inherency if the missing limitation is only probably present or if there is merely a possibility that it is present.

28. Material not explicitly contained in a single prior art document may still be considered for purposes of anticipation if that material is incorporated by reference into the document. I understand that incorporation by reference provides a method for integrating material from various documents into a host document—a patent or printed publication in an anticipation determination—by citing such material in a manner that makes clear to one of ordinary skill in the art that the material is effectively part of the host document as if explicitly contained therein.

29. I understand that a claim is unpatentable for obviousness under 35 U.S.C. § 103 "if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains." Obviousness may be based upon a combination of references. Obviousness may also be based on a single reference combined with the knowledge of a person of ordinary skill in the art ("POSITA") at the time the filing of the application that led to patent.

30. For a claim to be obvious in view of a combination of known elements, there must be some apparent reason to combine the known elements in the fashion of the claim at issue by considering the teachings of prior art references, the effects of demands known to people working in the field or present in the marketplace, and the background knowledge possessed by a POSITA. Identifying a reason the

elements should be combined is important because inventions in many instances rely upon building blocks long since uncovered, and claimed discoveries almost of necessity will be combinations of what, in some sense, was already known. The prior art references themselves may provide a suggestion, motivation, or reason to combine, but the nexus linking two or more prior art references is sometimes simple common sense.

31. An obviousness inquiry requires consideration of the following factors: (1) the scope and content of the prior art; (2) the differences between the claims and the prior art; (3) the level of ordinary skill in the pertinent art; and (4) any objective indicia of non-obviousness, such as commercial success, long-felt but unresolved need, failure of others, industry recognition, copying, and unexpected results.

32. Such secondary considerations include: (a) commercial success of a product due to the merits of the claimed invention; (b) a long-felt, but unmet need for the invention; (c) failure of others to find the solution provided by the claimed invention; (d) deliberate copying of the invention by others; (e) unexpected results achieved by the invention; (f) praise of the invention by others skilled in the art; (g) the taking of licenses under the patent by others and (h) the patentee proceeded contrary to the accepted wisdom of the prior art. Secondary considerations are relevant where there is a connection, or nexus, between the evidence and the claimed

invention. I am not aware of any such objective evidence of non-obviousness of the Challenged Claims at this time.

33. In addition, I understand that the obviousness inquiry should not be done in hindsight, but must be done using the perspective of a person of ordinary skill in the relevant art as of the effective filing date of the patent claims.

34. Obviousness may also be shown by demonstrating that it would have been obvious to modify what is taught in a single piece of prior art to create the patented invention. Obviousness may be shown by establishing that it would have been obvious to combine the teachings of more than one item of prior art. In determining whether a piece of prior art could have been combined with other prior art or with other information within the knowledge of one of ordinary skill in the art, the following are examples of approaches and rationales that may be considered:
(A) Combining prior art elements according to known methods to yield predictable results; (B) Simple substitution of one known element for another to obtain predictable results; (C) Use of a known technique to improve similar devices (methods, or products) in the same way; (D) Applying a known technique to a known device (method, or product) ready for improvement to yield predictable results; (E) Applying a technique or approach that would have been "obvious to try" (i.e., choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success); (F) Known work in one field of endeavor may prompt

variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations would have been predictable to one of ordinary skill in the art; or (G) Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention. I also understand this suggestion or motivation may come from such sources as explicit statements in the prior art, or from the knowledge or common sense of one of ordinary skill in the art.

35. I understand that an invention that might be considered an obvious variation or modification of the prior art may be considered non-obvious if one or more prior art references discourages or lead away from the line of inquiry disclosed in the reference(s). A reference does not "teach away" from an invention simply because the reference suggests that another embodiment of the invention is better or preferred. My understanding is that for a reference to teach away the reference must clearly indicate that the combination should not be attempted (e.g., because it would not work or explicit statement saying the combination should not be made).

36. I further understand that obviousness must be determined in light of all of the facts, and that there is no rule that if a reference teaches away a finding of nonobviousness is mandated. I understand this to be the rule because, for example, a given course of action often has simultaneous advantages and disadvantages, and

thus teaching away does not necessarily obviate motivation to combine. Thus, I understand that where the prior art contains apparently conflicting teachings (for example, where some references teach the combination and others teach away from it) each reference must be considered for its power to suggest solutions to a POSITA considering the degree to which one reference might accurately discredit another. I am informed that the degree of teaching away depends upon the particular facts of each circumstance and that rigid rules that prevent the application of common sense are not mandated.

37. I further understand that obviousness also requires that a POSITA would have perceived that the proposed combination would have had a reasonable expectation of success. I am informed that reasonable expectation of success does not mean certainty of success. If a technique has been used to improve one device, and a person of ordinary skill at the time of invention would have recognized that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond their skill.

38. Practical and common-sense considerations should guide a proper obviousness analysis, because familiar items may have obvious uses beyond their primary purposes. A POSITA looking to overcome a problem will often be able to fit together the teachings of multiple prior art references. An obviousness analysis

therefore takes into account the inferences and creative steps that a person of ordinary skill would have employed at the time of invention.

39. A proper obviousness analysis focuses on what was known or obvious to a POSITA at the time of invention, not to the patentee. Accordingly, any need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed.

40. Prior art teachings are properly combined if one of ordinary skill, having the understanding and knowledge reflected in the prior art and motivated by the general problem facing the inventor, would have been led to make the combination of elements recited in the claims. Under this analysis, the prior art references themselves, or any need or problem known in the field of endeavor at the time of the invention, can provide a reason for combining the elements of multiple prior art references in the claimed manner.

41. I understand that in an *inter partes* review, the petitioner shall have the burden of proving a proposition of unpatentability, including a proposition of obviousness, by a preponderance of the evidence.

V. THE CHALLENGED PATENT

42. I understand that Petitioner is challenging all claims (1-21) of the ’859 Patent the Petition.

43. The Patent asserts a need for secure electronic credentials:

> *Additionally, as more users move to a digital transaction model, the need for digital identification also increases. As fewer users carry wallets or traditional payment forms, traditional forms of ID will become less common. Current platforms are insecure and carrying digital credentials increases the risk of identity theft or fraud in transactions. What is needed is secure system for storing and displaying user credentials.* EX1003, 1:43-49

44. The Patent purports to solve this problem in a conventional manner through the following steps in claim 1:

45. [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." That is, a first party stores credential information for a user, the credential being used to verify (prove) the qualification or identity of the user. In other words, the credential is a conventional credential, such as a driver's license, which proves the identity of the user (through a name and photograph) and the qualifications of the user (*i.e.*, qualifications to drive, which is the very purpose of a driver's license).

46. [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." That

is, the user has a user device capable of NFC communication and uses the device to ask for a verifiable form of the credential from the first party.

47. [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." That is, the first party (who has stored the credential) creates an electronic "representation" of the credential.

48. [1.4] "transmitting, to the OVER file storage client device of the user, the OVER file in response to the OVER file generation request." That is, the electronic representation of the credential is sent to the user device.

49. [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." That is, the user has presented themselves to a third party, the third party asks the first party whether the user is authenticated based on a scan associated with the file containing the electronic representation of the credential, the communication occurring using NFC.

50. [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." That is, the first party verifies that the information in the scan matches information in the credential communicated via NFC.

51. [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." That is, using NFC, the first party transmits a message to the third party that the scan matches information in the credential. Presumably, based on this authentication message, the third party will trust that the user is really the person named in the credential.

52. The reason I say that this process was conventional is that it was commonly used before the Patent in credit card transactions performed on a mobile device using NFC, as will be explained in detail below.

53. All of the Challenged Claims recite merely conventional steps using conventional mechanisms for their commonly intended purpose. Immediately below I offer a high-level explanation why this is true for each of the remaining Challenged Claims. Detailed explanation is given later in discussion of the relevant Grounds.

54. Claim 2 depends from claim 1 and adds that a user may have a second OVER file storage client and may request a second credential for that device that is invalid for use on the first OVER file storage client. Such a limitation was conventional because multiple prior art references disclosed the use of device-dependent credentials allowing a user to store different credential on different devices, each such credential being unique to its device.

55. Claim 3 depends from claim 1, but adds that a credential is only generated if no credential is already stored in the OVER engine. I note that the language of claim 3 is confusing because it refers to "wherein the credential is generated" but claim 1 does not recite a step of generating any credential. Claim 1 instead recites "generating … an OVER file comprising a virtual representation of the credential." I believe that a POSITA would understand the addition step of claim 3 to mean "generating, by the processor of the OVER engine, the virtual representation of the credential, wherein the credential is generated when the processor determines that no virtual representation of the credential of the user is stored." That is, if the virtual representation has already been generated and stored, do not generate it again. It was conventional to not to repeat generating a representation of a credential if the representation had previously been generated and stored. It is simply logical not to waste resources generating something that has already been generated.

56. I note further that the substitution of the term "credential" for "virtual representation of the credential" also affects claims 5, 11, and 13. In each of these claims, I have understood "credential," when used alone, to actually mean "virtual representation of the credential."

57. Claim 4 depends from claim 1 and adds that the issuing agency is requested to verify the credential and provide a status indicator. This was purely conventional. In a standard credit card transaction, long predating the Patent, the bank issuing the credit card was asked in real-time whether the card was valid or not. If the card was not valid, the transaction would be declined.

58. Claim 5 depends from claim 1, and adds that a device identifier is generated limiting the credential to the OVER file storage client device. This was also conventional. As discussed below, it was conventional to use a device identifier to limit the use of a credential to a particular device for security purposes. That is, a wrongdoer or eavesdropper who somehow obtained the credential representation would be unable to use it except on the device of the authorized user.

59. Claim 6 depends from claim 1 and adds that the OVER engine generates a representation of a "remotely stored credential." A POSITA would have understood that "remotely stored" means stored somewhere other than the OVER engine itself. This was conventional, as credentials themselves, for security purposes, would be stored in a location separate from the place where the

representation would be generated. This was the method of operation of the Kerberos system from the 1980s, described below beginning at ¶100.

60. Claim 7 depends from claim 1 and adds two unrelated limitations. First, the OVER engine checks a status indicator of a stored credential. This was conventional. If a credential had expired, for example, it would be invalid, and there would be no point in generating an OVER file from it. Second, the OVER file generation request contains a credential identifier "for specifying which credential among a plurality of credentials of the user is officially represented by the OVER file." This was also conventional. Clearly it would be necessary to distinguish, for example, between a driver's license, a credit card and a passport. There is no point in generating a virtual representation of a credential if the recipient cannot determine what type of credential it is.

61. Claim 8 depends from claim 1 and adds that that "the OVER file comprises a portion of the stored credential." This was also conventional, as it is difficult to imagine a virtual representation of a credential that would include no portion of the credential itself.

62. the OVER engine generates a representation of a "remotely stored credential." A POSITA would have understood that "remote stored" means stored somewhere other than the OVER engine itself. This was conventional, as credentials themselves, for security purposes, would be stored in a location separate from the

place where the representation would be generated. This was the method of operation of the Kerberos system from the 1980s, described below beginning at ¶100.

63. Claim 9 is an independent apparatus claim corresponding to method claim 1, and was conventional for the same reasons.

64. Claim 10 depends from claim 9 and corresponds to method claim 2, and was conventional for the same reasons given for claim 2.

65. Claim 11 depends from claim 9 and corresponds closely to method claim 3, except that the claim 3 term "no credential of the user is stored" has been replaced with "no matching credential is stored." This limitation is puzzling to a degree because the specification seems clear that credentials "match" if they have the same "credential identifier." *See* EX1003, 9:20-29, 9:45-55, 18:26-30. However, parent claim 9 does not recite any "credential identifier." Nevertheless, even assuming a credential identifier is somehow present, it was conventional not to generate another representation of a credential if a credential with the same identifier was already stored.

66. Claim 12 depends from claim 9, is a method form of claim 4, and was conventional for the same reasons given for claim 4.

67. Claim 13 depends from claim 9, is a method form of claim 5, and was conventional for the same reasons given for claim 5.

68. Claim 14 depends from claim 9, is a method form of claim 6, and was conventional for the same reasons given for claim 6.

69. Claim 15 depends from claim 9, is a method form of a portion of claim 7 (checking a status indicator of a stored credential), and was conventional for the same reasons given for claim 7.

70. Claim 16 depends from claim 9, is a method form of the whole of claim 7, and was conventional for the same reasons given for claim 7.

71. Claim 17 depends from claim 16 and is confusingly written: "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." I believe a POSITA would understand this claim as "17. The apparatus of claim 16, wherein when the credential identifier matches the stored credential, and **wherein** the authentication message comprises the status indicator of the stored credential." This claim was conventional, as authentication messages (e.g., in credit cards transactions), on finding a matching credential (credit card) would include an indication whether the card was valid or not.

72. Independent claim 18 unsuccessfully attempts to mirror independent claim 1, but with "Bluetooth" substituted for "NFC." It fails to do so. The preamble and limitations 18.1-18.4 are literally identical, respectively to the preamble of claim 1 and limitations 1.1.-1.4. The first difference appears in limitation 18.5, which

recites: "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." The substitution of "Bluetooth" for "NFC" was made by Examiner's amendment is the Notice of Allowance and was erroneous. It is literally impossible for a "Bluetooth protocol-based communication" to be transmitted "via an NFC protocol." The two protocols are incompatible. As written, claim 18 is inoperable. If "NFC" were retained in place of the substitution of "Bluetooth," claim 18 would be identical claim 1 and would thereby be invalid for double patenting. The logical resolution, in the eye of a POSITA, is that applicant intended "Bluetooth" to substitute for "NFC" throughout claim 18, so limitation 18.2 should be understood as "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)~~ **Bluetooth** enabled device" and limitation 18.5 should be understood as "receiving, from an OVER file third-party client verifying device that is a second ~~NFC~~ **Bluetooth** 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)~~ **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~~ a **Bluetooth** protocol." With that understanding, claim 18 parallels claim 1 with "Bluetooth" substituted for "NFC" throughout, and claim 18 was conventional because Bluetooth was a conventional substitute for NFC.

73. The language of claim 19 is literally identical to that of claim 2, except that claim 19 depends from claim 18 instead of from claim 1. Claim 19 was conventional for the same reasons as claim 2.

74. Independent claim 20 appears to be an attempt at an apparatus form of claim 18, but suffers from the same NFC/Bluetooth confusion and is therefore inoperable. I believe that a POSITA would understand the intent of claim 20 to be for "Bluetooth" to substitute for "NFC" throughout. With that understanding, claim 18 was conventional for the same reasons that claim 18 was conventional.

75. Claim 21 depends from claim 20 and is an apparatus form of claim 19. It was therefore conventional for the same reasons that claim 19 was conventional.

VI. LEVEL OF ORDINARY SKILL IN THE ART

76. I understand that the Board will be asked to characterize a person having ordinary skill in the art ("POSITA") at the time the purported invention was made. To make that determination, it is my understanding that the Board considers

the following factors: (i) the educational level of active workers in the field, (ii) the type of problems encountered in the art, (iii) the prior art solutions to those problems, the rapidity with which innovations are made, and (v) the sophistication of the technology in the art. It is my understanding that the importance of each factor varies from case to case.

77. The ’859 Patent defines its field of invention as follows:

> *The present disclosure relates to electronic transactions, and more particularly to systems, methods, and apparatuses for securely storing and displaying user credentials.* EX1003, 1:27-29.

78. The Specification of the ’859 Patent (“Specification”) discloses the use of electronic credentials for virtual wallets and payment platforms for e.g., credit card payments. EX1003, 10:4-12.

79. The claims of the ’859 Patent are drawn to generating verifiable representations of authentical credentials, transmitting the representations to a client device, and validating the representations.

80. In my opinion, in order to understand the Specification and make and use the claimed invention without undue experimentation as of December 21, 2012, one of ordinary skill in the art of the ’859 Patent would have been someone with (1) a bachelor’s degree in computer science or computer engineering or equivalent

experience; and (2) two years' experience with electronic payment systems and/or network authentication systems involving electronic credentials.

81. I had at least the background of such a POSITA at least as early as December 21, 2012.

VII. CLAIM CONSTRUCTION

82. I understand that, in the absence of an express definition or disclaimer, claim terms are given their ordinary and customary meaning, as would have been understood by a POSITA at the time of the alleged invention.

83. In considering the meaning of the claims, however, I understand that one must consider the language of the claims in light of the remainder of the specification, the prosecution history, and extrinsic evidence concerning relevant scientific principles, the meaning of technical terms, and the state of the art.

84. I provide below my understanding of the plain and ordinary meaning to a POSITA of certain terms used in the Challenged Claims.

A. "officially verifiable electronic representation"/"OVER" file

85. The term "officially verifiable electronic representation" is not a term of art. It was devised purely for use in the Cortex Patents. A Google search I conducted on January 2, 2024, for the string "officially verifiable electronic representation" produced exactly five hits (out of 400 billion documents in Google's

index[1]). All five hits relate to the Cortex Patents. The term has never appeared in the technical literature, or any other place to my knowledge.

86. Each independent claim of the ’859 Patent recites an OVER file and uses the term “OVER” or “OVER file” to characterize other elements, such as an “OVER file generation request” (a request to generate an OVER file), an “OVER file storage client device” (a device that stores an OVER file), and an “OVER file generation and verification engine” (a device that generates OVER files and responds to verification requests regarding those files).

87. The specification of the ’859 Patent describes that an OVER file may contain “credential information.” EX1003, 6:39-41 (“OVER file containing the entered credential information”), 7:6-9 (same). 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 (“OVER File credential representative of the user’s driver’s license”). 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 a Near Field Communication (NFC) and/or Bluetooth

[1] See “Google’s Index Size Revealed: 400 Billion Docs (& Changing),” available at https://zyppy.com/seo/google-index-size/

communication for verification of the user's credential by a third party. EX1003, Abstract, 12:34-42.

88. The '859 patent does not discuss tokens or describe that tokens may be either an OVER file or a part of an OVER file (such as a representation of a credential). However, in the "First Amended Complaint for Patent Infringement and Jury Demand" (EX1018, "Amended Complaint"), Patent Owner made the following allegations:

> *The OVER File platform allows consumers to store credit card data and associated personal identifying information on a mobile device without the associated risk if this data is accessed by hackers. Each OVER File is a token that is unique to the user and device. The OVER File is also encrypted, which prevents the use or manipulation of data even if a hacker gains access to the device or to the file. When a customer presents an OVER File identification at a point of sale, the merchant can validate the user's credentials through an authentication application designed to interact with the token. Importantly, the technology is compatible not only with all major smartphones but also with the existing point-of-sale infrastructure used by merchants.*
>
> *…*
>
> *Visa makes, uses, offers for sale, and/or sells certain products ("'859 Accused Products"), including within this Judicial District, such as VTS. Visa's infringing use of the '859 Accused*

Products includes its internal use and testing of the '859 Accused Products.

...

The '859 Accused Products generate a token to act in place of a primary account number ("PAN") and then uses the token to verify the identity of the cardholder before a transaction is processed by a merchant. The "officially verifiable electronic representation (OVER) generation and verification engine" is the Visa Network that implements the Visa Token Service. The PAN (and potentially other cardholder information) is stored in Visa's digital Token Vault— the repository for maintaining tokens. The "credential" is the user's Visa credit card, which proves the user's identity and qualification to make a purchase.

...

Additionally, the method practiced by the '859 Accused Products involves generation, by a processor of an OVER engine of an OVER file comprising a virtual representation of the credential that has been verified by an issuing agency to be an official representation of the credential, based on the information associated with the credential of the user. When a consumer initiates a digital payment through a digital wallet, the digital payment service provider requests a payment token (associated with the PAN, i.e., the information associated with the credential of the user) from Visa for the enrolled account. The Visa Network then generates a token and shares it with the credit card issuer

> *for approval. The token is the "virtual representation of the credential that has been verified by an issuing agency to be an official representation of the credential."*

EX1018, ¶¶9, 60, 62, 64.

89. When describing related U.S. Patent No. 9,954,854, which is a grandparent of the '859 Patent, the Amended Complaint further equates a token to an OVER file, as well as asserting that it acts as a virtual representation of the user's credentials:

> *The '854 Accused Products also involve a first OVER file comprising a first virtual representation of an original credential that has been verified by an issuing agency to be a first official representation of the original credential of a user for proving the user's identity or qualifications, based on information associated with the original credential of the user, wherein the first OVER file is itself a first credential of the user. The token (i.e., "first OVER file") acts a first virtual representation of the user's credentials, such as the user's PAN.*

EX1018, ¶40.

90. In light of the claim language and the disclosure in the specification of the '859 Patent, as well as Patent Owners allegations in the Amended Complaint, I interpret an OVER file as encompassing a file comprising a virtual representation

in the form of an image of (or associated with) the credential, but also encompassing a file comprising a virtual representation in the form of a token.

B. <u>"…verified by an issuing agency…"</u>

91. 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 of representation the credential."[2] During prosecution of the '531 Patent, an ancestor sharing the same specification, the 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 (arguing that there "is no discussion of how [prior art] electronic documents are verified by an issuing agency to be an official representation of the credential of the user").

92. The Applicant also quoted several parts of the specification to support the meaning of this phrase. *See also id.* 40 (citing material appearing at EX1003, 3:50-4:6, 4:25-41, 5:7-25, 6:12-36). I have reproduced the passages quoted below:

> *"An OVER File generation and authorization engine 8 may generate OVER File credentials in response to request from an OVER File storage client 4 or an OVER File third party client 6," at [0027]. OVER Files are "representative of the user's credentials"; the "OVER File may also comprise ... any other*

[2] Claim 20 appears to have a typographical error, omitting the word "of" between "official representation" and "the credential."

> *credential that may be electronically verified by an issuing agency," at [0025]. Also, the "issuing agency database 130" may be used "for verification of the credential," at [0030]. Also, the "issuing agency datastore" may be used "to verify the information contained in the OVER File generation request and to obtain additional credential information stored by the issuing agency database 130," at [0033].*

Id.

93. In light of the specification and the statements by the Applicant during prosecution, a POSITA would interpret "a virtual representation of the credential that has been verified by an issuing agency to be an official of representation the credential" to require that an issuing agency have verified a *virtual representation* in an OVER file as being an official representation of a credential.

94. I have accorded all of the claim terms their plain and ordinary meaning to a POSITA.

VIII. BACKGROUND OF THE PRIOR ART

95. In this section, I discuss the state of the art prior to the alleged invention with respect to certain technologies relevant to the subject matter of the '859 Patent as of December 21, 2012. As a POSITA is presumed to have been familiar with all relevant prior art, a POSITA would have been familiar with the material in this section.

A. Secure Credentials

96. Credentials in the physical world, sometimes referred to as identity documents, such as driver's licenses, passports and credit cards are physical objects designed to be difficult to forge or alter. Their legitimacy stems from the fact that the authority issuing them can be readily recognized by inspecting the credential itself. They also carry information to be used in verifying the identity of the person presenting the credential by means of a "challenge." For example, passports and driver's licenses carry a photograph of authorized holder. The "challenge" consists of having the holder exhibit their face. If the face matches the photograph on the credential, then the presenter is known to be the authorized holder. A credit card carries the signature of the authorized holder. In the case of a credit card, the "challenge" is requiring the presenter to sign a receipt. If the signature on the receipt matches the signature on the credit card, the presenter is believed to be the authorized cardholder.

97. Creating identity documents in the digital world was challenging for several reasons: (1) it was not easy to determine if a digital credential was issued by a recognized authority; (2) a digital credential can easily be copied, forged, or altered and it is difficult to issue a "challenge" to a remote networked user to prove that they are the person named in the credential. An eavesdropper who obtains both the credential and the answer to the challenge can later pretend successfully to be the person named in the credential.

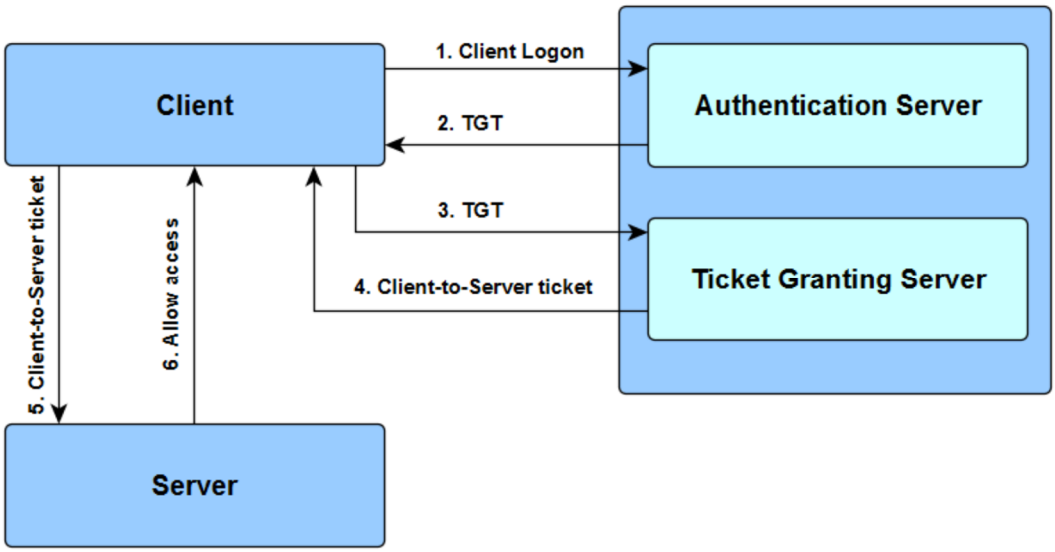
98. These problems were recognized and solved long before the Patent. A solution to (1) is to have the issuer include some encrypted material in the credential that only the true issuer is able to generate, e.g., a digital signature. Digital signatures have been known since 1976. Another solution to (1) is to have the issuer verify over a network in real-time that the credential is valid. This has commonly been done in everyday credit and debit card transactions since 1973. When a customer presents a credit card to a merchant, the merchant makes a request in real-time whether the card is valid and whether the card has sufficient credit to cover the transaction. The request is routed to the bank that issued the credit card, and a response is received within 5-15 seconds. Such requests were originally made over private dial-up networks maintained by credit card agencies, such as Visa, and were later made (at least partially) over the Internet. Note that solving (1) validates the credential, but does not prove that the presenter of the credential is the person named in the credential.

99. A solution to (2) is to require the presenter of the credential to furnish additional information to prove that they are the person named in the credential. This protects against credentials being copied or stolen. In the banking industry, this was done starting in 1967 by requiring the user to enter a PIN at an ATM machine. A thief who stole an ATM card would not be able to use it without knowing the PIN.

PINs are still used in the credit/debit card industry even though embedded chips and NFC communication have replaced magnetic stripes.

100. The problem of remote authentication of a user over a network was solved at MIT in the 1980s using a mechanism called "Kerberos." *See* EX1019. Fundamentally, users need access to various resources on a network such as documents and network services. It is impractical to require every server on a network to maintain a database containing encrypted passwords of every authorized user and to force users to enter a username and password each time they request a document or service. The Kerberos solution was to maintain a single server (the Authentication Server) storing usernames and passwords, analogous to the OVER engine of the Patent. The Client seeking network services would authenticate themselves once to the Authentication Server using the traditional username/password process. The Authentication Server then generates a ticket-granting ticket (TGT) and sends it back to the Client. When the Client wants to access a Server, it requests a ticket for that particular server from a Ticket Granting Server. To do so, the Client must send the TGT and the identity of the desired Server. The Ticket Granting Server then sends to the Client a Client-to-Server Ticket, which, when presented to the Server by that Client, will authenticate the Client to the Server and the Server will perform services for the Client. The process is shown in the

diagram below, which is not from EX1019, but accurately reflects the Kerberos process.



101. It can readily be seen that the Authentication Server and the Ticket Granting Server correspond to the OVER engine of the Patent. The Client-to-Server Ticket corresponds to the OVER File of the Patent. The Server corresponds to the third-party client verifying device of the Patent. Step [1.6] of the Patent, "receiving, from an OVER file third-party client verifying device, a verifying request to verify that the OVER file transmitted to the user authenticates the user based on a scan associated with the OVER file on the OVER file storage client device of the user," is not literally present in the diagram because the OVER file is sent from the Client to the Server along with the request for service and no "scan" is performed. Instead, the Over File itself is transmitted to the Server. Step [1.7] of the Patent is also not literally present in the diagram because (1) there is no "scan"; and (2) the claimed

"authentication message" is actually contained in the initial request to the Server. For these reasons, Kerberos does not anticipate any Challenged Claim. However, it will readily be recognized that the Client-to-Server Ticket of Kerberos is a "token" corresponding to the user's original credential (username/password) maintained on the Authentication Server.

102. Thus, by December 21, 2012, there was nothing inventive using a secure credential for authentication.

B. Tokens

103. The use of a surrogate or "token" in place of an actual credit card number or other credential was a well-known security practice long before the Patent. It was long known that fraud can occur if an unauthorized party obtains a user's credit card number. Unfortunately, in older credit card transactions, there was no way to prevent the merchant itself from obtaining the user's credit card number, as the merchant had to present that number to a credit card network in order to be paid.

104. In 2001, the idea of token was introduced by the company TrustCommerce, which replaced the credit card number (primary account number or "PAN") with a randomized number, called a token. *See* EX1020. When a merchant needed to process a payment, it could use the associated token and TrustCommerce would process the payment on their behalf, replacing it with the

true credit card number before introducing the transaction into the credit card network. In this manner, the merchant never learned the user's credit card number. In such systems, the credential itself was stored remotely from the token and would not be transmitted with the token. Thus a wrongdoer who somehow obtained the token would not gain any information about the credential itself.

105. On July 20, 2004, Singer at al. filed an application that became U.S. Patent 7,014,107 on March 21, 2006, entitled "Wireless Payment Processing System" ("Singer," EX1021). It discloses a tokenization process for making credit card payments, as shown in its Fig. 1., below:

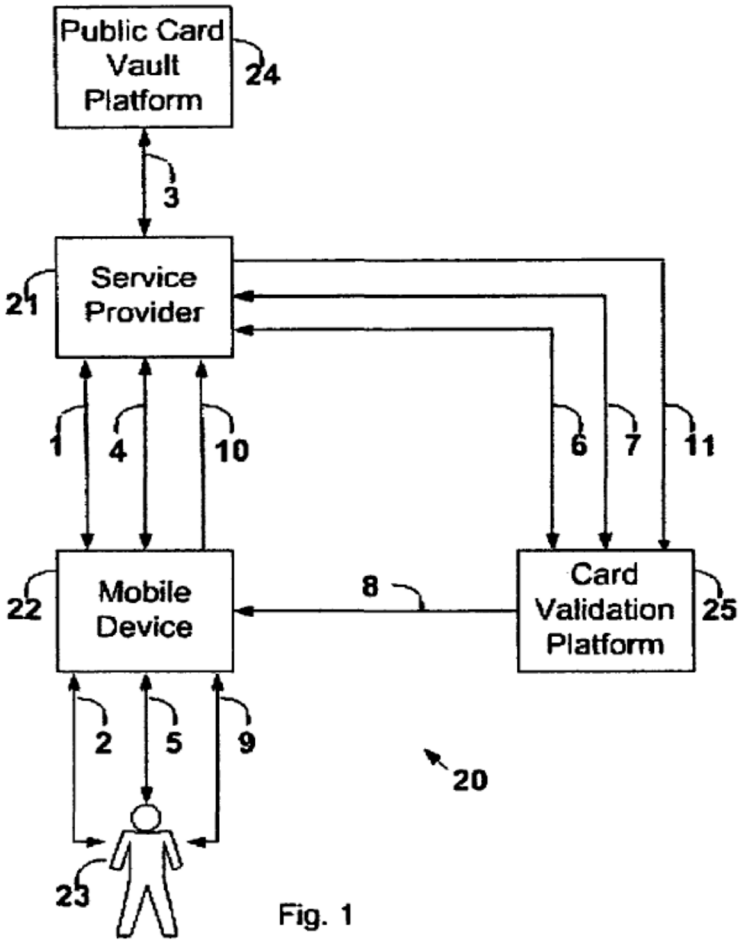


Fig. 1

106. The Card Owner 23 wishes to make a payment to Service Provider 21 from Mobile Device 22 but does not want the Service Provider to learn the credit card number. Singer discloses that the communications between Mobile Device 22 and Service Provider 21 are close-range, using Bluetooth. As described at 2:33-3:57, the process starts when 21 sends message 1 to 22 requesting a credential. The credential can be a password, PIN or biometric of the Card Owner. The device 22 sends to 21 the credential and an identifier of the Mobile Device.

107. Service Provider 21 then sends the credential and identifier to Public Card Vault Platform 24. This is a repository of names of credit card holders along with their identifiers and credentials and incomplete information about their credit cards (e.g., the last two digits of each card number and a card name). Platform 24 sends to 21 the available cards for the Card Owner, which 21 then sends to Mobile Device 22. The Card Owner then selects one of the cards for payment and the selection is passed to Service Provider 21. The Service Provider 21 then requests a preauthorization for the selected card by sending a message 6 to the Card Validation Platform 25 that includes the credential, identifier, and incomplete card data. The Card Validation Platform contacts the issuing bank (not shown in the drawing) to validate the selected card. If the card is validated, the Platform 25 generates a temporary card token and sends it back to the Service Provider 21. The purpose of the preauthorization is to confirm that the card is valid.

108. Service Provider 21 returns the temporary card token to Platform 25 along with a transaction amount. Platform 25 obtains an authorization from the issuing bank for that transaction amount and also receives an authorization token containing a public part and a private part. Platform 25 then sends 21 the public part of the authorization token and a check digit of the private part of the authentication token. Platform 25 sends a text message to Mobile Device 22 along with the card token and the private part of the authorization token.

109. The Card Owner 23 is then asked whether or not to authorize the payment. If so, Mobile Device 22 sends the Service Provider the card token and the private part of the authorization token. In order to receive payment, the Service Provider 21 sends the card token along with the (now complete) authorization token to the Card Validation Platform 25, which then processes the payment through a credit card network.

110. Singer discloses the use of a card token and proximity transmission between the Card Owner's Mobile Device and the Service Provider. The process of Singer was rather clumsy and was refined by the industry in the ensuing years.

111. Shift4 Corporation released a system to the public during an industry Security Summit in Las Vegas, Nevada in 2005. In a 2006 manual, Shift4 defined tokenization as a "term used to describe the replacement of the card number used in transactions processing with a Token. The Token is a unique identifier comprised of a 16-character, alphanumeric code that is used to reference sensitive cardholder data. In keeping with PCI, as well as the legal requirements of the FACT Act, the Token contains only the last four digits of the card number. The last four digits of the account number become the first four in the Token. Spaces 5-16 are random characters that are globally unique to that transaction." *See* EX1022. The abbreviation PCI in the preceding quote refers to the Payment Card Industry, which developed standard for handling credit card transaction data.

112. On March 1, 2007, Arnold published "Credit Card Information Surrogate: A Method and System for using surrogates to integrate PCI-level security for legacy information systems." *See* EX1023. It discloses "a method and system for assignment of a consumer credit card surrogate, based on card account number issuing methods." *Id.* at. 1. (A "surrogate" is another word for "token.") It continues, "For protection of credit card data, to help educate and expose some of the issues with card account surrogate (vendors sometimes refer to a tokenization) systems that are offered from payment gateway and software vendors.: *Id.* at 3. Further, "Surrogate Implementation. The Data Vault implements the generation and storage of surrogates at the time an initial authorization is run on a credit card. The surrogate is stored in the vault with the encrypted and salted-SHA1 of the card account number. If a card transaction comes into the payment application where the card account number begins in a 9, payment application knows to ask the Data Vault to exchange the surrogate for the actual account number. The payment application then proceeds to process the transaction as though any normal payment request." *Id.* at 10.

113. On October 30, 2008, Morin et al. U.S. Patent Application Publication 2008/0270166 was published, entitled, "Transcript, Course Catalog and Financial Aid Apparatus, Systems, and Methods" ("Morin," EX1017) It discloses secure storage and transmission of verified electronic versions of academic transcripts. See,

e.g., [0090] ("Once the application 18 receives a request from a user, or other authorized entity, it opens a communication channel with the first institution's information management system 14, requests the transcript data (Step 2) and performs any necessary verification/registration procedures. The information system 14 of the first institution typically includes a database with the relevant transcript data."). The electronic transcript of Morin is a credential, as well as corresponding to an "OVER file" of the Challenged Claims.

114. In 2008, Microsoft unveiled its "Geneva" Framework for authenticating credentials securely over networks. *See* EX1024. It discloses at pp. 6-7:

> ***Security Token.*** *The user delivers a set of claims to your application piggybacked along with her request. In a web service, these claims are carried in the security header of the SOAP envelope. In a browser-based web application, the claims arrive via an HTTP POST from the user's browser, and may later be cached in a cookie if a session is desired. Regardless of how they arrive, they must be serialized somehow, and this is where security* ***tokens*** *come in. A security* ***token*** *is a serialized set of claims that is digitally signed by the issuing authority. The signature is important – it gives you assurance that the user didn't just make up a bunch of claims and send them to you.*
>
> ***Issuing Authority.*** *There are lots of different types of issuing authorities, from domain controllers that issue Kerberos tickets,*

> *to certificate authorities that issue X.509 certificates, but the specific type of authority I'll be talking about in this paper issues security* ***tokens*** *that contain claims. The issuing authority I'm speaking of is a web application or web service that knows how to issue security* ***tokens****. It must have enough knowledge to be able to issue the proper claims for the target relying party given the user making the request, and may be responsible for interacting with user stores to look up claims and authenticate the users themselves.*
>
> ***Security Token Service (STS).*** *A security* ***token*** *service (STS) is the plumbing that builds, signs, and issues security* ***tokens*** *according to the interoperable protocols that I'll discuss in the upcoming section called Standards. There's a lot of work that goes into implementing these protocols, but Geneva Framework does all of this heavy lifting for you, making it feasible for someone who isn't an expert in the protocols to get an STS up and running with very little effort.*

Microsoft's Geneva was a very general system for remote authentication using tokens that was not limited to online payments.

115. Naturally, the PCI was interested in payment security, so it developed tokenization standards. In 2011, Thakar et al. published "PCI Compliance for Dummies" (EX1025) to help explain these standards. It discloses on p. 28: "The goal of protecting cardholder data is at the heart of PCI. Various technical methods of protecting cardholder data exist, such as encryption, tokenization, truncation,

masking and hashing. But you don't have to be a tech guru to understand their purpose: to make cardholder data *unreadable* to unauthorized people." (emphasis in original). Further on p. 37: "For all remote access to the network, you need to implement two-factor authentication. The standard suggests using a remote authentication and dial-in service, a terminal access controller access-control system with tokens, or a virtual private network (VPN) with individual certificates."

116. Later in 2009, the call for tokenization grew. In May 2009, the trade magazine *Digital Transactions* published an article by Ben Jackson entitled "Token Gestures" (EX1026), which discloses:

> *With no end in sight to the rash of data breaches, the concept of replacing card data with so-called **tokens** is catching on.*
>
> *Broadly, **tokens** work as follows: A merchant hires a company that takes the card number from its system and returns a **token** that the merchant uses for its records. The **token** acts as an index or reference number that the vendor could use to look up the actual information. The **token** vendor then sends the actual card number to the processor and authorizing bank.*
>
> *The **tokens** help large enterprises because once they replace credit card numbers with **tokens**, companies can share data across different business units without needing to create PCI protections in each unit. The **tokens** contain the last four digits of a credit card number so that companies can use them for analysis and customer relationship services.*

117. In September 2009, First Data, a large credit card processor, publishes a whitepaper entitled, "Data Encryption and Tokenization: An Innovative One-Two Punch to Increase Data Security and Reduce the Challenges of PCI DSS Compliance" (EX1027). "DSS" refers to the Data Security Standard. The whitepaper discloses on p. 12:

> *"**Tokenization** of sensitive data. An increasingly popular approach for the protection of sensitive data is the use of a token (or alias) as a substitute for a real credit card number. In the process of **tokenization**, a payment card is used in a transaction and, once authorized, the cardholder data is sent to a centralized and highly secure server called a "vault," where it is stored securely. Immediately after, a random unique number is generated and returned to the merchant's systems for use in place of the cardholder data. The end result is that the **token** can be used in various business applications as a reliable substitute for the real card data.*

118. On October 1, 2009, Mattsson U.S. Patent Application Publication 2009/0249082, was published, entitled "Method and Apparatus for Tokenization of Sensitive Sets of Characters" ("Mattsson," EX1028) It discloses at [0105]:

> ***Tokenization** is often based on two key facets in an enterprise: First-Centralization of sensitive information. All credit card numbers stored in disparate business applications and databases are removed from those systems and placed in a highly secure, centralized encryption management server that can be protected*

> *and monitored utilizing robust encryption technology.* ***Tokenization*** *is like network segmentation, as a way to move card data to another internal or external server. However, the access to the card data is still in your POS or other systems, so be careful of how a* ***tokenized*** *system can be attacked. Secondly,* ***tokenization*** *of information. Each credit card number that previously resided on an application or database is replaced With a* ***token*** *that references the credit card number. A* ***token*** *can be thought of as a claim check that an authorized user or system can use to obtain the associated credit card number.*

119. The Mattsson theme was followed on March 18, 2010, with Leach U.S. Patent Application Publication 2010/0070754, entitled "Payment Encryption Accelerator" ("Leach," EX1029). Its Abstract discloses:

> *Embodiments of the invention provide a system for encrypting web session data which may include a session management module adapted to receive data from a web application module and provide a* ***token*** *that represents the data in encrypted form to the web application, wherein the web application is adapted to use the* ***token*** *to represent the data. The system may also include a* ***tokenize****r module communicably coupled to the session management module, wherein the* ***tokenizer*** *module is adapted to receive the data and generate the* ***token****. Further, the system may include a database communicably coupled to the session management module, wherein the database is adapted to receive*

*the **token** and the data, associate the **token** with the data, and store the **token** and the data.*

120. On October 29, 2009, Stafford U.S. Patent Application Publication 2009/0271321 was published, entitled "Method and System for Verification of Personal Information" ("Stafford," EX1012). Its Abstract discloses:

In one form, there is disclosed a system (100) for storing, validating and disseminating credential information about an entity. The system (100) generates data representing at least part of the credential information and a data representation of at least part of a document supporting that information and stores the credential information and data representation in a database (120) in an encrypted form.

121. 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 at [0010] ("Receiving a document including credential information about an entity; Verifying at least part of the credential information included in the document; Generating data representing at least part of the credential information; Generating a data representation of at least part of the document; and Storing at least part of the credential information and data representation in a database in an encrypted form."), [0062] (scanning credential documents), [0073]-[0075] ("Preferably sensitive information can only be released…after confirmation by the entity as well as the generation (and purchase)

of key signatures."), [0093]-[0097] (providing key signatures), [0107]-[0125] (releasing credential information), Figs. 2-3.

122. Stafford also refers to a "token" for holding credential information, but the "token" of Stafford is a physical device that does not correspond to the "tokens" accused by Patent Owner to be virtual representations of credentials. Hence I make no further reference to the physical tokens of Stafford. The OVER files of the '859 Patent correspond instead to Stafford's encrypted credential information, which pertains to an "entity," which may be an individual.

123. Stafford's credential information is verified:

> *In a third aspect the present invention provides a system for providing credential information about an entity, the system including: a database storing, encrypted verified entity characteristic data relating to the entity, said verified entity data including, a representation of at least part of a document attesting to one or more characteristics of the entity, data representative of said one or more characteristics of the entity; and entity identification data associated with the* ***encrypted verified entity characteristic data****.*

Id. at [0024].

124. On May 10, 2010, ProPay issued a press release (EX1030) containing the following:

> *Lehi, Utah – May 10, 2010 – On the heels of winning the 2010 ETA ISO of the Year Award ProPay (www.propay.com), an industry leader in End-to-End Payment Security, credit card processing, and electronic payment services, announced today that is has added encryption and* ***tokenization*** *of Automated Clearing House (ACH) data (bank routing and account numbers) to its suite of ProtectPay services. The addition of this functionality illustrates ProPay's proactive approach to helping organizations protect sensitive data.*

125. By that time, the importance of tokenization had become apparent to the Federal Reserve Bank, which published a whitepaper by Sullivan entitled "The Changing Nature of U.S. Card Payment Fraud: Issues for Industry and Public Policy" on May 21, 2010 (EX1031). It discloses on p. 16:

> *Another initiative disguises a card account number by replacing it with a* ***token*** *number. This "****tokenization****" would occur after a card payment has been authorized so that a merchant can store the transaction information without having to store the card account number (Taylor). Merchants can retrieve the card account number for later processing, if needed. Both of these options could make merchant and processor computer networks less of a target because they would not store or transmit sensitive payment card information in forms that would be useful to hackers."*

126. Also in May 2010, CyberSource issued a manual on how to implement tokenization, entitled "CyberSource Electronic Check Services Implementation Guide" ("CyberSource," EX1032). It discloses on p. 62:

> *Payment **Tokenization**. If you are using Payment **Tokenization**, you can process a debit or credit by using information that is stored in a customer profile. CyberSource uses the subscription ID to reference the customer profile information in the CyberSource database. Instead of providing all the information that is normally required for a transaction, you only need to provide the following values:*
>
> *• Merchant ID*
>
> *• Merchant reference code*
>
> *• Amount of the payment or credit*
>
> *• Subscription ID*

127. On July 14, 2010, Petitioner Visa published "Visa Best Practices for Tokenization Version 1.0" (EX1033). It discloses on p. 1:

> *How **Tokenization** Works. **Tokenization** defines a process through which PAN data is replaced with a surrogate value known as a "**token**." The security of an individual **token** relies on properties of uniqueness and the infeasibility to determine the original PAN knowing only the surrogate value. As a reference or surrogate value for the original PAN, a **token** can be used freely by systems and applications within a merchant environment. Where properly implemented, **tokenization** allows*

> *merchants to limit the storage of cardholder data to within the* ***tokenization*** *system, potentially simplifying an entity's assessment against the PCI DSS. As a reference or surrogate value for the original PAN, a* ***token*** *can be used by systems and applications within a merchant environment without having to consider the security implications associated with the use of cardholder data.*

128. On March 3, 2011, Palgon et al. filed an application that matured into U.S. Patent 8,458,487, entitled "System and Method for Format Preserving Tokenization of Sensitive Information" (EX1034). Its Abstract discloses:

> *Systems and methods for secure access and utilization of sensitive data such as credit card numbers, Social Security Numbers, personal identifying information, etc. A tokenizing strategy component provides for creating, managing, and storing* ***tokenization*** *strategies on behalf of a plurality of users. A data* ***tokenizing*** *component is operative to (a) receive an input data string of sensitive data from a user, (b) apply a selected* ***tokenization*** *strategy to the input data string to generate a* ***tokenized*** *data string, and (c) provide the* ***tokenized*** *data string for storage in association with the input data string. A secure server including a secure database stores the* ***tokenized*** *data string and the input data string in a corresponding mapped relationship.*

129. Tokenization was adopted by the PCI, which established a Tokenization Taskforce. In August 2011, it published "PCI DSS Tokenization Guidelines" (EX1035) to supplement Version 2.0 of the PCI Data Security Standard. It explains different ways of generating tokens, stating:

> *One of the primary goals of a **tokenization** solution should be to replace sensitive PAN values with non-sensitive **token** values. For a **token** to be considered non-sensitive, and thus not require any security or protection, the **token** must have no value to an attacker. **Tokens** come in many sizes and formats. Examples of some common **token** formats are included in the following table.*

Table 1: Selected Examples of Token Formats*

PAN	Token	Comment
3124 005917 23387	7aF1Zx118523mw4cwl5x2	Token consists of alphabetic and numeric characters
4959 0059 0172 3389	729129118523184663129	Token consists of numeric characters only
5994 0059 0172 3383	599400x18523mw4cw3383	Token consists of truncated PAN (first 6, last 4 of PAN are retained) with alphabetic and numeric characters replacing middle digits.

** **Note:** This table provides a selection of examples only, and does not include all possible token formats.*

EX1035, p. 5

130. The Tokenization Guidelines go on to explain the difference between single-use and multi-use tokens:

> ***Tokens** can be generally identified as either single-use or multi-use. A single-use **token** is typically used to represent a specific,*

*single transaction. A multi-use **token** represents a specific PAN, and may be used to track an individual PAN across multiple transactions. A multi-use **token** always maps a particular PAN value to the same **token** value within the **tokenization** system. Determining whether single-use or multi-use **tokens**, or a combination of both, are appropriate for a particular merchant environment will depend on the merchant's specific business need for retaining tokens.*

EX1035, p. 5

131. Further at p. 9:

*1. The requesting application passes a **token**, along with necessary authentication information, to a **tokenization** system.*

*2. The **tokenization** system verifies the authentication information presented by the requesting application. If this check fails, the **de-tokenization** process fails, and information is logged for monitoring. Otherwise, the process continues to Step 3.*

*3. The **tokenization** system queries the card data vault for a record associated with the **token**, retrieves the PAN if found, and proceeds to Step 4. If no such **token** exists, the de-tokenization operation fails, and information is logged for monitoring.*

*4. The **tokenization** system returns the PAN value retrieved from the card data vault, if found, to the requesting application. If the PAN is not found, then an error message is returned.*

132. On October 20, 2011, Shader et al. U.S. Patent Application Publication 2011/0258122, entitled "Payment System to Facilitate Transactions," was published ("Shader," EX1036). Its Abstract reads:

> *Disclosed herein are systems and method for facilitating transactions between a merchant-partner and a customer. In general, the systems and methods include: (a) staging a transaction between the merchant-partner and the customer; (b)* ***tokenizing*** *the transaction by linking one or more transaction instructions to a* ***token*** *ID; (c) providing the customer with the* ***token*** *ID, wherein the customer can then present the* ***token*** *ID and a payment to a point-of-sale terminal; (d) receiving confirmation that the customer has presented, to a point-of-sale terminal, the* ***token*** *ID and a payment in accordance with the one or more transaction instructions; (e) notifying the merchant-partner that the customer provided the payment to the point-of-sale terminal; and (f) settling the transaction between the point-of-sale terminal and the merchant-partner.*

133. On December 29, 2011, Randazza et al. U.S. Patent Application Publication 2011/0320316, entitled "Payment System and Methods" was published ("Randazza," EX1037). It contains the following disclosures:

> *Examples of a payment* ***token*** *useable in the invention include, e.g., a driver's license card or other physical card, an electronic* ***token****, a* ***token stored in a mobile payment device, a cellular device, a smart phone****, a wireless device, a handheld electronic*

device; a personal digital assistant; etc. Preferably the payment ***token*** *is not a card with a magnetic stripe or bar code conventionally used to conduct a debit or credit card transaction by a financial institution or third party processor for financial settlement of funds due a retailer. Id.* at [0047]

In another preferred embodiment, the invention provides a method for a system having a plurality of persons; a plurality of payment ***tokens*** *issued under authority of an entity (such as, e.g., Apple; AT&T; etc.); a retail site configured with a first signal, the first signal being common to the plurality of payment* ***tokens****; a routing system for receiving a signal and generating a network address in response to the received signal, the routing system including a plurality of wide area communication links, the routing system being configured using the first signal, the system further including a second signal on a first payment token in the plurality of payment* ***tokens****; and a second system storing an association between the second signal and account information, the entity and an owner of the second system not being affiliated, the entity not being affiliated with a retailer, method comprising the steps, performed at the retail site, of: receiving the first and second signals from the first payment* ***token****; sending the first and second signals into the routing system, to cause the second system to perform the steps of determining whether the first payment* ***token*** *can effect payment; responsive to the determining step, conditionally sending a message to cause an institution to send an ACH entry to the Federal Reserve ACH system, to pass*

> *the entry to a bank, where an account is issued a debit, to cause a transfer of funds to the owner of the retail site, and making an entry in an accounting system, to effectively increment an amount owed by the owner of the retail site to the owner of the second system; wherein the method further includes the step, performed at the retail site, of: conditionally effecting a transaction with a holder of the first payment* ***token****, depending on a signal received from the second system. Id.* at [0022]

134. In 2011, First Data published "A Primer on Payment Security Technologies: Encryption and Tokenization" (EX1038). It discloses on p. 5:

> ***Tokenization****. An increasingly popular approach for the protection of sensitive data is the use of data substitution with a* ***token*** *(or alias) as a replacement for a real credit card number. In the process of* ***tokenization****, actual cardholder data is used in a payment transaction and, once the transaction is authorized, this very sensitive data is sent to a centralized and highly secure server called a "vault" where it is stored securely. At the same time, a random unique number is generated and returned to the merchant's systems for use in place of the cardholder data. The vault manager maintains a reference database that allows the* ***token*** *number to be exchanged for the real cardholder data if it is needed again for, say, a chargeback. Meanwhile the* ***token*** *number, which cannot be monetized, can be used in various auxiliary business applications as a reliable substitute for the real card data.*

135. By 2012, tokenization was becoming widespread. On January 19, 2012, Smith et al. U.S. Patent Application Publication 2012/0016731, entitled "Mobile System and Method for Payments and Non-Financial Transactions" ("Smith," EX1039) was published. It discloses at [0027]:

> *The e-wallet is consumer centric because it enables consumers to upload all types of card accounts to the e-wallet. The e-wallet is a service provided by the TPPN (third Party payment network or gateway provider for mobile payment services) and may be a customized e-wallet solution for the mobile payment system. The CMA has ability to select the* ***tokenized*** *payment method data used by the TAS for calling the TPPN's e-wallet according to he* [sic] *corresponding* ***token*** *and card account of the user.*

136. On February 13, 2012, Neafsey et al. filed provisional application 61/598,212 ("Neafsey Provisional," EX1016). Subsequently, an application claiming priority to the Neafsey Provisional was filed on February 13, 2013, which published on August 15, 2013, as U.S. Patent Application Publication 2013/0212248 ("Neafsey," EX1015) entitled "Credential Management System".

137. I understand that the disclosure in Neafsey is available as prior art as of the filing date of the Neafsey Provisional insofar as the same subject matter is disclosed in the Neafsey Provisional and the Neafsey Provisional provides written description support for at least one claim in Neafsey. As I discuss below, the Neafsey Provisional supports at least claim 1 of Neafsey. I illustrate that the same subject

matter is present in both Neafsey references by providing citations to the matching disclosure in both references throughout the remainder of my declaration.

138. Claim 1 of Neafsey recites the following:

[Preamble] A method, comprising:

[1.1] providing, with at least one server, a cloud credential management service including generating credentials of at least two different types;

[1.2] receiving, with the server, a credential request from a customer computer to assign a virtual credential to a mobile device; and

[1.3] transmitting, with the server, the virtual credential to the mobile device.

139. Below, I illustrate that the Neafsey Provisional discloses a method including each of these claim limitations.

140. **Preamble**: The Neafsey Provisional discloses embodiments including "apparatuses, systems, devices, hardware, methods, and combinations for credential management services." EX1016, 2; *see also id.*, claims 1-14, 18 (each reciting a method).

141. **Neafsey Step [1.1]**: The Neafsey provisional discloses "providing, with at least one server, a cloud credential management service including generating credentials of at least two different types." For example, the Neafsey provisional discloses that "[g]enerally, a provider makes the cloud credential management

service 102 available to one or more customers over the Internet." EX1016, 5; *see also id.*, Fig. 1. The cloud credential management service includes credentials of at least two different types. *See* EX1016, 11-12 ("[D]ifferent types of credentials may be generated and hosted in a cloud credential management service 504. There are credentials of different types…and each credential type has distinct algorithms…."); *see also id.*, 12 ("Virtual credentials 502 can be generated by the cloud credential management service 504 in multiple formats (e.g., prox, Mifare, EVI, optical, XceedID, eISA) depending on the requesting host."), Fig. 9.

142. **Neafsey Step [1.2]**: The Neafsey provisional discloses "receiving, with the server, a credential request from a customer computer to assign a virtual credential to a mobile device." For example, Neafsey discloses that "Virtual credentials 502 can be generated by the cloud credential management service 504 in multiple formats…depending on the requesting host." EX1016, 12. By "requesting host," the Neafsey Provisional is referring to a customer's computing device, such as a mobile device, that has requested to be assigned a virtual credential. *See* EX1016, 8 ("FIG. 4 illustrates a cloud credential management service 308 that transmits virtual credentials 302 to a credential host 310, such as a mobile device."), 4 ("The mobile device 104 may be a mobile phone, such as a cell phone or smartphone, a tablet computer, such as an iPad, a smartcard, or any other type of mobile computing device.").

143. **Neafsey Step [1.3]**: The Neafsey provisional discloses "transmitting, with the server, the virtual credential to the mobile device." For example, the Neafsey provisional teaches that the requested credentials are "hosted and delivered via a mobile device such as a smartphone." EX1016, 12; *see also id.*, 4 ("The cloud credential management service 102 may generate and deliver credentials 110 to the mobile devices 104, reader devices 106, and other devices such as computers 108."), Fig. 9 (showing transmission of different types of requested credentials to mobile devices). Accordingly, the Neafsey Provisional discloses Neafsey Limitation 1.3.

144. As I have shown above, the Neafsey Provisional provides a written description of each limitation of claim 1 of Neafsey. The following claim chart summarizes the locations of relevant support for each limitation of claim 1 of Neafsey:

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, 5, 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.

145. Fig. 4 of Neafsey shows a credential management system in which virtual credentials are issued to a mobile device 310 for presentation to a credential reader 304:

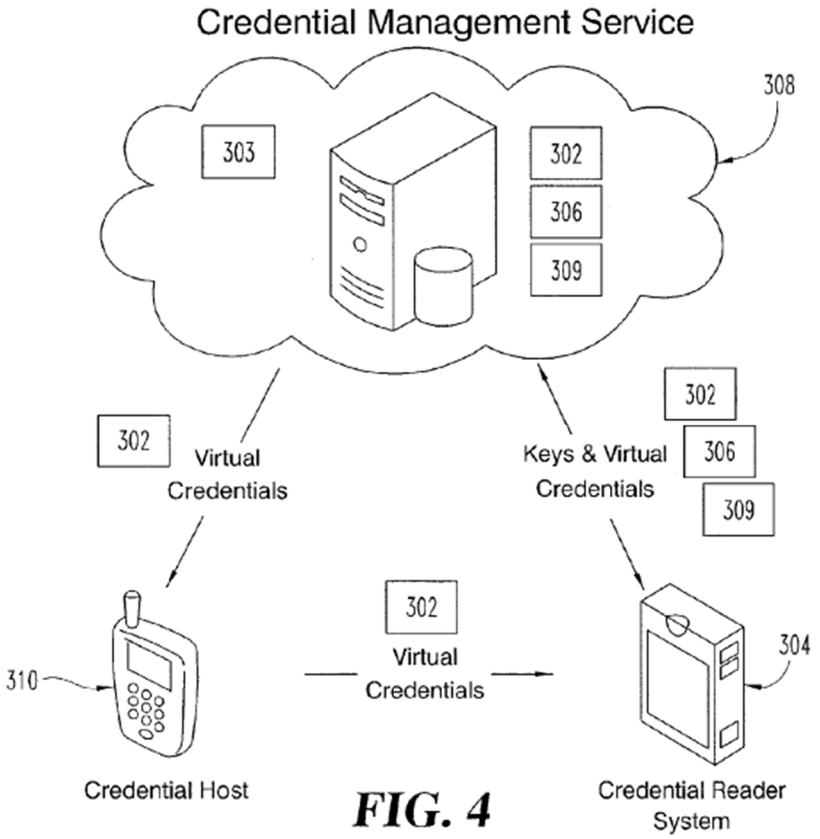


FIG. 4

EX1015, Fig. 4; EX1016, Fig. 4.

146. Neafsey also discloses that the credential may include a "unique device identifier" along with a token:

> *Once authenticated, at operation 326, the credential host 310 then requests to be enrolled with the credential management service 308 by sending a request along with a specifier such as a* ***unique device ID****.*

EX1015, [0048]; EX1016, 10.

> *At operation 412, the device 402 then sends a* ***unique device identifier*** *to the credential management service 406 along with the token.*

EX1015, [0056]; EX1016, 11.

147. Neafsey discloses a credential in the form of a QR code:

> *Virtual credentials 502 can be generated by the cloud credential management service 504 in multiple formats (e.g., prox, MIFARE Classic, MIFARE DESFire EVl* [sic, EV1]*, optical, Xceed1D* [sic, XceedID]*, elSA, bar code,* ***QR code****) depending on the requesting host.*

EX1015, [0061]; EX1016, 12 (describing optical codes, which a POSITA would understand to include bar codes and QR codes); *see* EX1012, [0032], [0106] (QR and bar codes captured with camera), Fig. 12D (showing QR code); EX1013, [0095] (QR codes and barcodes are "visual element[s] suitable for scanning.").

148. The foregoing passage also discloses sending credentials to different devices is device-specific formats.

149. Neafsey also discloses the "status indicator" of the '859 Patent as an "authentication status," for example:

> *Process 311 then proceeds from operation 312 to operation 314. At operation 314, the cloud credential management service 308 transmits an* ***authentication status****, which may include a* ***token****, to the reader system 304.*

EX1015, [0042]; EX1016, 10.

150. Neafsey is an obviousness reference discussed in more detail beginning at ¶¶368.

151. On June 14, 2012, Langley et al. U.S. Patent Application Publication 2012/0150669, entitled "System and Method for Point of Service Payment Acceptance Via Wireless Communication" (EX1040) was published.

152. Fig. 1 of Langley shows a recipient client device 102B bearing a machine readable token 804 interacting with a merchant client device 102C:

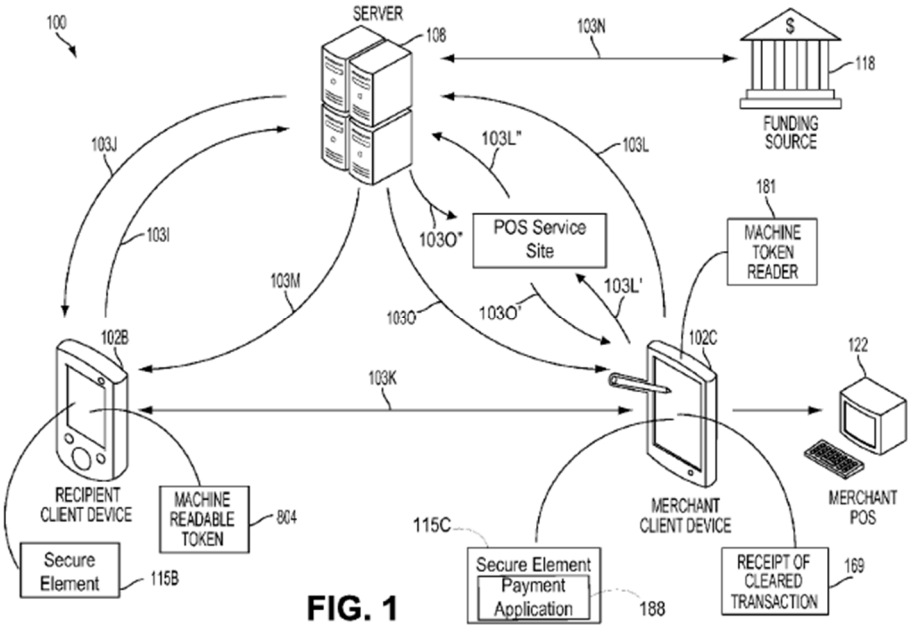


FIG. 1

153. Langley explains as follows:

> [0089] *As described above, the CPCD 102B may be associated with any number of account types including, but not limited to, a stored value account, a credit account, a debit account, etc.*

*The virtual machine-readable **token** 804 that is representative of an associated account similar to traditional physical tokens.*

[0090] *As the requesting CPCD 102B may be identified via methods known by one of ordinary skill in the art of telecommunications, the server 108 may identify an associated account and encrypt the requested account data by virtue of generating a virtual machine-readable **token** 804 at step 310. Once the virtual machine-readable **token** 804 is generated, it may be transmitted at step 315 to the requesting CPCD 102B.*

[0091] *The CPCD 102B receives the virtual machine-readable **token** 804 at step 320. In step 325, the CPCD 102B renders and presents the virtual machine-readable **token** 804 to a MPCD 102C for payment as illustrated in FIG.1. In some embodiments, one or more of the previously-described steps of 305-315 may take place at the time when the CPCD 102B is being used to offer payment to obtain the virtual machine readable **token** 804.*

154. On June 7, 2012, an application was filed that was published on December 13, 2012, as Oborne U.S. Patent Application Publication 2012/0316992 ("Oborne," EX1011), entitled "Payment Privacy Tokenization Apparatuses, Methods and Systems." These apparatuses, methods and systems are referred to in Oborne as "PPT."

155. The Abstract of Oborne states:

> *In one embodiment, the PPT obtains a **token** arbitration request including unique source-neutral universally-resolvable payment **token** information from a merchant for processing a purchase order from a user. The PPT queries a **token** database for issuer information on an issuer using the payment **token** information, and obtains the issuer information. The PPT also determines that the user should be queried for payment options based on the issuer information, and provides a payment options request to a user mobile device. Upon obtaining a response from the mobile device, the PPT generates a purchase authorization request based on the payment options and pre-defined settings for issuers to be contacted for processing the purchase order, and provides the generated purchase authorization request to the issuer.*

156. Oborne discloses tokenization and communication of an OVER file using NFC, which Patent Owner considers a "scan," and by QR code, which surely is a "scan."

157. Fig. 6A from Oborne is reproduced below. It depicts an in-store tokenized purchase by a User 6.01, who interacts with a merchant's point-of-sale terminal 6.02.

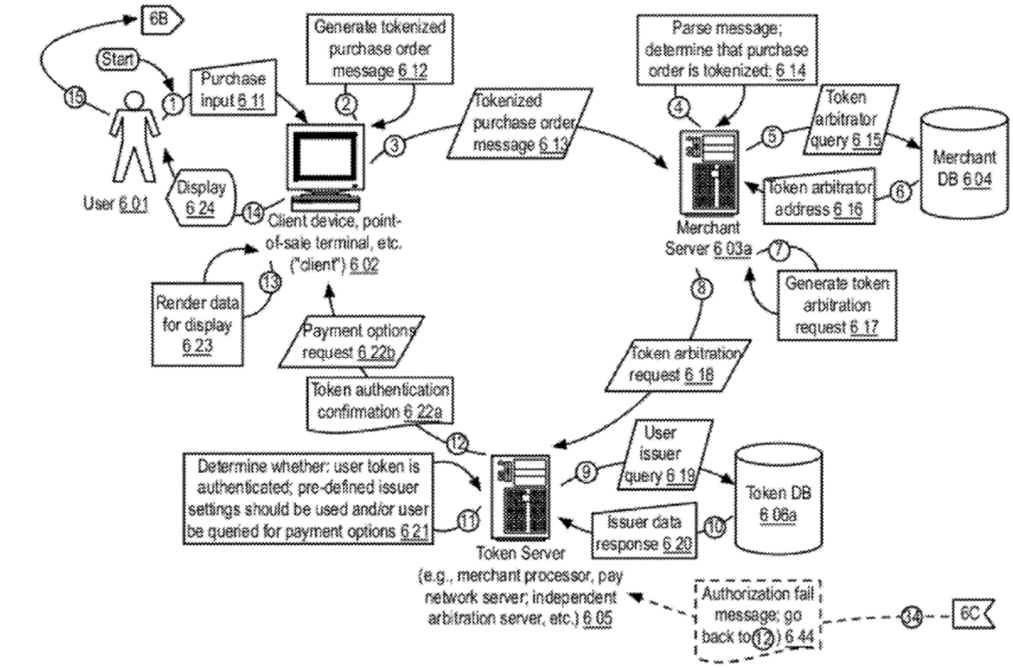


FIGURE 6A

Example: Token-Based Purchase Transaction

158. As described at [0048]:

> *The user may communicate with a merchant server, e.g., 603a, 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 (e.g., 602). For example, the user may provide user input, e.g., purchase input 611, into the client indicating the user's desire to purchase the product. In various implementations, the user input may include, but not be limited to: keyboard entry, card swipe, activating a RFID/* ***NFC*** *enabled hardware device (e.g., electronic card having multiple accounts, smartphone, tablet, etc.), mouse clicks, depressing buttons on a joystick/game console, voice commands, single/multi-touch gestures on a touch-sensitive interface, touching user interface elements on a touch-sensitive display, and/or the like.*

159. Payment by QR code is described by Oborne in several paragraphs:

> *The price and total payable information may also be displayed, along with a QR code 915k that captures the information necessary to effect a snap mobile purchase transaction. Id.* at [0078]
>
> *In another example, money may be transferred to Brian S. via QR code as indicated by the QR code icon 917d. Id., [0080]*
>
> *With reference to FIG. 10D, in one embodiment, the mode tab 1040 may facilitate selection of a payment mode accepted by the payee. A number of payment modes may be available for selection. Example modes include, blue tooth 1041, wireless 1042, snap mobile by user-obtained QR code 1043, secure chip 1044, TWITTER 1045, 13 near-field communication (NFC) 1046, cellular 1047, snap mobile by user-provided QR code 1048, USB 1049 and FACEBOOK 1050, among others. Id.* at [0093]

160. In one implementation, a pay card such as a credit card, debit card, pre-paid card, smart card and other pay accounts may have an associated code such as a bar code or QR code. Such a code may have encoded therein pay card information including, but not limited to, name, address, pay card type, pay card account details, balance amount, spending limit, rewards balance, and/or the like, *Id.* at [0108]. The techniques used by Oborne were well-known in the field.

Oborne is an obviousness reference discussed in more detail beginning at ¶206, below.

161. On September 21, 2012, an application was filed that was published on February 28, 2013, as Purves et al. U.S. Patent Application Publication 2013/0054454 ("Purves," EX1013), entitled "Wallet Service Enrollment Platform Apparatuses, Methods and Systems."

162. Purves discloses a system for enrolling payment account in a consumer's virtual wallet. EX1013, Abstract. The issuer of a credit card, for example, can share payment information with a virtual wallet provider. Purves teaches that a user may select a payment credential from their wallet my choosing among visual representations (e.g., images) of the credentials stored in the wallet. EX1013, Fig. 20b. This is also described at [0104]:

> *In some implementations, the user may be presented to a card management screen (e.g., from an issuer, merchant, and/or like source) that allows the user to select 2012 bank credit cards 2013a and/or debit cards 2013b to be used in the user's virtual wallet. In some implementations, information 2014 related to each card may be displayed with the card selection, including the card number, the card balance, images of the card, and/or like identifying information.*

163. Purves also teaches the use of tokens as replacements for actual credentials, and that tokens may be encrypted:

> *In one implementation, the merchant server may use the user sign as a trigger to request current user information from the wallet server. The merchant server may generate and send a user information request message 926 to the wallet server. The user information request message 926 may include, without limitation, the customer ID that is unique to the customer and the merchant relationship, a token, an API key, a digital certificate, and/or the like. In one implementation, the token may be generated using one or more parameters such as the merchant's API key, customer ID, merchant ID, merchant name, customer name, and/or the like. In a further implementation, the token may be encrypted. In one implementation, the token may be a string that is created by the MD5 Message Digest algorithm hash of one or more of the parameters listed above. Id.,* [0073]

164. Purves further discloses at [0095] that payment credentials can be communicated by QR code:

> *As another example, using a quick response (QR) code scan, a near-field communication (NFC) tap or other mobile trigger in lieu of a WSEP button may also trigger a wallet connection or login. As yet another example, using a voice password, repeatable gestures or action, biometrics, and/or the like may trigger a wallet connection or login*

165. Harris et al. U.S. Patent Application Publication 2012/0310838 ("Harris," EX1014), entitled "Local Usage of Electronic Tokens in a Transaction Processing System," was published on December 6, 2012.

166. Its Abstract discloses:

> *A method for the use of electronic transactional tokens includes: generating a plurality of transactional **tokens** including a first token; associating each of the transactional **tokens** with a plurality of users, the first **token** associated with a first user; monitoring usage of the transactional tokens in a plurality of transactions in a local region or network; and in response to receiving transactional data for the first transaction, updating the first **token** from a first state to a second state (e.g., to provide a benefit when the token is applied in the local region or network). The **tokens** may be generated and monitored using a **token** processing system, which uses transaction data received by a transaction handler that is handling transaction processing for the transactions.*

167. I note that the "state" of the tokens in Harris corresponds to the "status indicator" of the '859 Patent.

168. In view of the foregoing, by December 21, 2012, there was nothing inventive about generating from a credential a tokenized representation of the credential.

C. QR Codes

169. QR codes have been available since 1994 and have found multiple uses in transactions and authentication.

170. In 2009, Starnberger et al. published "QR-TAN: Secure Mobile Transaction Authentication" ("Starnberger," EX1041) Its Abstract discloses:

> *QR-TANs are a transaction authentication technique based on two-dimensional barcodes. Compared to other established techniques, QR-TANs show three advantages: First, QR-TANs allow the user to directly validate the content of a transaction within a trusted device. Second, validation is secure even if an attacker manages to gain full control over a user's computer.*

171. Further,

> *QR-TANs use a method based on transaction-signing that has been adapted to fit the capabilities of commonly used Web-based applications. QR-TANs are based on two-dimensional QR barcodes. Similar to other approaches [2]–[6], QR-TANs authenticate transactions by using a trusted device. This device can be a mobile phone with a display and a camera with a modest resolution. QR-TANs use QR codes for the transmission of information. Id.* at 578

172. As discussed above, Neafsey, Purves, and Oborne disclose displaying virtual credentials as QR codes. As discussed below at ¶176, Langley also discloses such use of QR codes.

173. Laracey U.S. Patent Application Publication 2011/0251892 ("Laracey," EX1042), entitled "Mobile Phone Payment Processing Methods and Systems," was published on October 13, 2011, more than one year before the Priority Date. It discloses a method of making a purchase from a mobile phone by scanning a token displayed on the phone in the form of a QR code or by transmitting it using NFC:

> *Referring first to FIG. 8A, a mobile device 802 is shown which has a display 836 showing an image of a check out* ***token*** *(represented as a dynamic two dimensional* ***bar code image*** *or "****QR code*** *837) which has been captured or imaged by a camera associated with the mobile device 802. The checkout* ***token*** *or code has been captured by a customer operating the mobile device 802 during the course of a payment transaction using embodiments of the present invention (e.g., the display shown in FIG. 8A may have been captured during the transaction processing described at Step 430 of FIG. 4B, or step "13 of FIG. 6, etc.).*

Id. at [0163].

> *The mobile device 700 can also include one or more wireless communication Subsystems 724. Such as an 802. 11b/g communication device, RFID,* ***NFC****, and/or a Bluetooth(R) communication device.*

Id. at [0156].

> *A number of terms are used herein for convenience and ease of exposition. For example, the term "capture" will be used to refer to the act of scanning, reading or other capturing of a "checkout* ***token****" (an identifier used to facilitate transactions pursuant to some embodiments). The term "capturing (or "captured) is not intended to be limiting, and is intended to encompass embodiments where a mobile device is operated to receive a checkout* ***token*** *(or data associated with a checkout* ***token****) via key entry, via* ***image capture****, via RFID reading, and using other* ***Scanning****, reading, or other techniques described herein.*

Id. at [0019].

174. On August 16, 2012, Hammond et al. U.S. Patent Application Publication 2012/0209749, entitled "Snap Mobile Payment Apparatuses, Methods and Systems" (EX1043) was published. Its Abstract discloses:

> *The SNAP MOBILE PAYMENT APPARATUSES, METHODS AND SYSTEMS ("SNAP) transform real-time-generated merchant-product* ***Quick Response codes*** *via SNAP components into virtual wallet card-based transaction purchase notifications. In one embodiment, the SNAP obtains a snapshot of a* ***QR code*** *presented on a display screen of a point-of-sale device from a mobile device. The SNAP decodes the* ***QR code*** *to obtain product information included in a checkout request of the user, and merchant information for processing a user purchase transaction with a merchant providing the* ***QR code****. The SNAP accesses a user virtual wallet to obtain user account information*

to process the user purchase transaction with the merchant. Using the product information, merchant information and user account information, the SNAP generates a card authorization request, and which the SNAP provides to a payment network for transaction processing. Also, the SNAP obtains a purchase receipt confirming processing of the user purchase transaction.

175. The information communicated by QR code may include a token:

*In some implementations, a first user 121b may desire to pay a second user 121a an amount of money (or a value equivalent, e.g., virtual currency, alternate real currency, rewards, miles, points, etc.), e.g., P2P Snap mobile payment 120. The second user 121a may generate a limited time-validity **QR code**, e.g., 122, including information on the amount of money to be transferred, as well as a privacy **token**/alias linked to a financial account of the second user. The second user may display the **QR code** generated to the first user (e.g., by holding the second user's mobile phone displaying the **QR code** to the first user; sending the **QR code** by email, Social network message, tweet, etc.). The first user may take a snapshot of the **QR code** using the first user's mobile phone, e.g., 123, and utilize the amount of money, the second user's privacy **token**/alias linking to a financial account, and the first user's virtual wallet linked to the first user's mobile phone, to generate a purchase transaction request for processing by the payment network.*

Id. at [0026].

176. Langley (EX1040) also discloses at [0171] the display of a credential using a QR code:

> *This diagram is similar to FIG. 10B, however, instead of a one-dimensional bar code being displayed, a two-dimensional barcode 804B is displayed for a merchant using the MPCD 102C to Scan Such a barcode 804B. The 2-D bar code may include, but is not limited to, the following symbologies: Aztec Code, 3-DI, ArrayTag, Small Aztec Code, Chromatic Alphabet, Chromocode, Codablock, Code 1, Code 16K, Code 49, ColorCode, Compact Matrix Code, CP Code, CyberCode, d-touch, DataGlyphs, Datamatrix, Datastrip Code, Dot Code A, EZcode, Grid Matrix Code, High Capacity Color Bar code, HueCode, INTACTA.CODE, InterCode, MaxiCode, mCode, MiniCode, Micro PDF417, MMCC, Nintendo e-ReaderiDot code, Optar, PaperDisk, PDF417, PDMark,* ***QR Code****, QuickMark Code, Semacode, Smart Code, Snowflake Code, ShotCode, SuperCode, Trillcode, UltraCode, UnisCode, VeriCode, VSCode, WaterCode, for example.*

177. Thus, by December 21, 2012, it was not inventive to use a QR code to communicate an authentication token.

D. Near-Field Communication

178. Near-Field Communication (NFC) permits two-way wireless digital communication between two devices that are in proximity to one another. NFC became a standard for close-range communication on December 8, 2003, when

ISO/IEC standard 21481 was published and adopted by the European Computer Manufacturers Association (ECMA) as Standard ETSI TS 102 312. NFC was available on Nokia smartphones and the Samsung Nexus Android phone in 2010.

179. As discussed above, Neafsey (EX1015-EX1016) and Oborne (EX1011) disclose transmitting virtual credentials using NFC.

180. The Abstract of Langley discloses the use of NFC to communicate a payment token:

> *A system and method for remitting payment from a consumer's credit or stored value account by digital presentations of account information are described. A merchant may create one or more merchant account at a point-of-sale service site ("POS service site") and associate one or more merchant portable computing devices ("MPCDs") with one or more of the merchant accounts. Each MPCD may be configured to receive customer data from a customer via one of a visual capture and a wireless communication, such as a near field communication (**NFC**) or a machine-readable **optical code**. The customer data may be received from an **NFC**-capable physical **token** such as an EMV card, or a virtual **token** presented by a customer portable computing device ("CPCD") using a **NFC** or a machine-readable optical code. Each MPCD may contain a point-of-sale payment application supplied by the POS service site that may capture data representative of a consumer account from the received customer data.*

181. Digital Transactions at 20 discloses:

> ***NFC****-enabled handsets contain a special chip that can communicate over a very short range--typically about 4 centimeters--to establish a link with another* ***NFC*** *device, such as a point-of-sale reader. The chip interacts with the phone's operating system and with an electronic wallet in the phone containing card-account details.*

182. Harris at [0437] discloses:

> *In another embodiment, the reader (163) includes a contactless reader, such as a radio frequency identification (RFID) reader, a near field communications (****NFC****) device configured to read data via magnetic field coupling (in accordance with ISO standard 14443/****NFC****), a Bluetooth transceiver, a WiFi transceiver, an infrared transceiver, a laser scanner, etc.*

183. Laracey at [0156] discloses:

> *The mobile device 700 can also include one or more wireless communication subsystems 724. Such as an 802. 11b/g communication device, RFID,* ***NFC****, and/or a Blue tooth R communication device.*

184. Hammad at [0026] discloses:

> *In alternate implementations, the two users may share the data encoded in the QR code via methods alternate to the QR code, including but not limited to: near-field communications (****NFC****),*

> *Wi-Fi™, Bluetooth™, cellular network, SMS, email, text messages and/or the other communication protocols.*

185. Thus, by December 21, 2012, it was not inventive to use NFC for communication in an authentication transaction.

E. Credential Identifiers

186. It is almost universal for authentication credentials to carry identifiers. A driver's license has a license number. A passport has a passport number. A credit card has a credit card number. This is essential because the name of the holder of the credential may not be unique (e.g., John Smith), while the credential identifier can be unique. This idea is not new – it stands to reason that in order to determine if a credential is valid, there has to be some way to look it up in a database of credentials.

187. Oborne, for example, discloses a credential identifier in the form of a "token identifier" at [0047]:

> *For example, the token server may generate a unique and resolvable **token identifier** irrespective of the token requesting channel (e.g., merchant, issuer, acquirer, payment network, user, etc.). In some implementations, the token server keeps track of all generated tokens via **token identifiers**, and as each is created, subsequent requests for creation of a token with the same **token identifier** will be denied.*

188. Langley discloses at [0114]:

> *Specifically, the stored value account issuer server 108B is responsible for creating and managing the client unique identifiers 155,* ***virtual card identification numbers*** *167, primary account numbers ("PANs") 165, and merchant identifiers 170 of FIG. 7AB discussed in greater detail below.*

189. Harris discloses at [0023]:

> *In one embodiment, the token processing system maintains data for the tokens of each user (e.g., a* ***unique identifier for each token*** *that is associated with that user). The token processing system may, for example, maintain data regarding various attributes for each token and also transaction histories associated with each token.*

190. Thus, by December 21, 2012, it was not inventive to identify a credential using a credential identifier.

F. Device Identifiers

191. It was well-known to use device identifiers to tie electronic representations to particular devices. As discussed above at ¶146, Neafsey discloses using a device identifier as part of a credential.

192. Further, Oborne expressly includes a device "MAC address" in its token. EX1011, table in [0047], excerpted here:

> *<token>*
>
> *. . .*
>
> *<!-- In some embodiments, client_details are optional and the token may be*

tied to a specific client-->

<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_fingerprint>font list, ***MAC address****, memory size, hardware chip, screen resolution</client_fingerprint>*

</client_details>

193. Harris discloses at [0075]:

> *For example, the above coupon may be entered into a user network that is associated with an iPhone or iPad mobile device. The coupon is associated with this network and is also associated with an* ***ID for this mobile device****. The* ***mobile device ID*** *may be referenced to a specific user or group of users of the mobile device (e.g., this reference may be stored in user device information 422).*

194. Laracey discloses at [0066]:

> *In some embodiments, where the customer registers from a browser on their mobile device, or by first downloading a payment application having a registration module onto their mobile device, the system may capture unique identifying information associated with the mobile device (e.g., such as a hardware serial number, an ASIN, a UUID or other device identifiers).*

195. That is, in Laracey, the registration of the payment application ties the use of that application to the device identifier.

196. Thus, by December 21, 2012, it was not inventive to tie a credential to a particular device using a device identifier.

G. Status Indicators

197. As discussed above at ¶148, Neafsey discloses a credential status indicator. As discussed above at ¶167, Harris also discloses a token status indicator referred to as "state."

198. On April 30, 2009, Adams et al. U.S. Patent Application Publication 2009/0113543, entitled "Authentication Certificate Management for Access to a Wireless Communication Device" ("Adams," "EX1044) was published. It contains extensive disclosures of status indicators associated with token. For example, at [0046] is describes:

> *In various embodiments, the **status** represented in the status indicator 45 may be indicated as being "valid", "revoked", or "on hold." A **status** such as "on hold" may be a subcategory of "revoked"; if subcategories of "revoked" **status** are provided, then the **status indicator** may also comprise a reason code as well, which provides a further explanation why the certificate was revoked. The "on hold" **status** may mean that an administrator may have reason to believe that the private key 55 corresponding to the certificate 35 has been compromised for some reason. For example, the user may have reported that he*

> *or she had misplaced the security token 108, which may prompt an administrator to change the* ***status*** *of the certificate to "revoked" and/ or "on hold". If the user had reported the security token 108 stolen, then the* ***status*** *indicator 45 would indicate "revoked" and the reason code may indicate "stolen", or may be blank. This* ***status*** *information may first be updated at the source CRL or other certificate status source, and would be updated at the user device 100 as described below. Other revocation reasons will be apparent to those skilled in the art. It will also be apparent that the certificate* ***status*** *need not literally comprise indicators such as "revoked" or "on hold"; the* ***status*** *indicator 45 may be encoded in any appropriate format. For example, the status indicator 45 may comprises numeric codes which may be interpreted by a human with reference to an established information technology policy for that user device 100.*

199. Thus, by December 21, 2012, it was not inventive to provide a token status indicator.

H. Reason for Invalid Credential

200. When a transaction fails because a user credential, such as a token, is found to be invalid, it is natural and expected for the user to be informed of the reason for invalidity, e.g., "Your credit card has expired." Many references disclose this.

201. For example, Langley discloses at [0097]:

> *A transaction declined notice or message may be sent to the MPCD 102C and the method 300 may end. The message may include a* ***code*** *or identifier indicating the* ***reason for declining the transaction****.*

202. CyberSource discloses "reason codes" at p. 88:

> *ecAuthenticateReply_reasonCode. Numeric value corresponding to the result of the overall request. See "****Reason Codes*** *for the Simple Order API" on page 125 for a list of possible values.*

203. The referenced page 125 lists 18 different "reason codes," some relating to authentication or verification, including the following:

> *101 The request is missing one or more required fields.*
>
> *102 One or more fields in the request contains invalid data.*
>
> *200 The request was declined by CyberSource because it did not pass the eFunds ID Verification check.*
>
> *388 Error: The routing number did not pass verification as described in "ACH Verification" on page 13.*

204. The passage from Adams cited in ¶198 also discloses reason codes.

205. Thus, by December 21, 2012, it was not inventive to provide a reason that a credential was found invalid.

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

206. Oborne discloses or suggests each limitation of claim 1, as well as the imitations of claims 2, 4-10, 13-14, and 16-21, arranged as in each claim. Specifically, Oborne teaches using tokens representing credentials such as credit cards to perform payment transactions. Here I apply the construction of "OVER file" as advanced by Patent Owner in the Complaint, EX1018 (i.e., as encompassing a token).

207. As I discuss below, limitation 1.3 requires that the OVER file's "virtual representation" (which Patent Owner maps to a token) must be verified as an official representation of a credential by an issuer. Oborne teaches or at least suggests that its token server may be operated by the issuer of a user's credentials. In such a system, it would at minimum have been obvious that the OVER file comprising a virtual representation of the credential has been verified by the issuer as an official representation, since the issuer is the entity issuing the token as well as the credential. As I explained above beginning at ¶103, the use of tokens was well-established and familiar to issuers. *See, e.g.*, EX1033 (Visa publication providing best practices for tokenization). An arrangement where a credential issuer also issued tokens, as taught by Oborne, and thus verified their status as representations of their own credentials, would have been a routine and predictable

application of known technology. It was therefore guaranteed that the virtual representation (token) had been verified by the issuer.

A. Claim 1

208. Oborne teaches or suggests each limitation of claim 1.

1. Preamble

1. A computer-implemented method comprising:

209. Whether or not the preamble is limiting, Oborne clearly teaches a computer-implemented method. See, e.g., EX1011 Figs. 1A, 4, 6A-6E, and 15, and [0114]-[0122], which show and describe computer system architectures.

2. Limitation 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;

210. Oborne's "payment privacy tokenization apparatus" or "PPT" apparatus to "transform payment token-based purchase orders, via PPT components, into multi-issuer purchase payment funds transfers" is the claimed "(OVER) generation and verification engine." EX1011, [0022], [0166]. The system includes a "token server," also referred to as a "token arbitrator," that may be any entity involved in the PPT, such as "part of the payment network (e.g., a

pay network server).” EX1011, [0053]. Oborne states that the “the source of the token” may be the “issuer” (e.g., a funding source for the user’s account). EX1011, [0047]-[0048] (noting in XML comments that the token administrator may be the funding source, or that “alternatively token administrator may be different from funding source”), [0029] (user may obtain token from funding source). Oborne depicts an arrangement of customers, parties, and the pay network server (which can include the PPT apparatus) in Fig. 4, reproduced below:

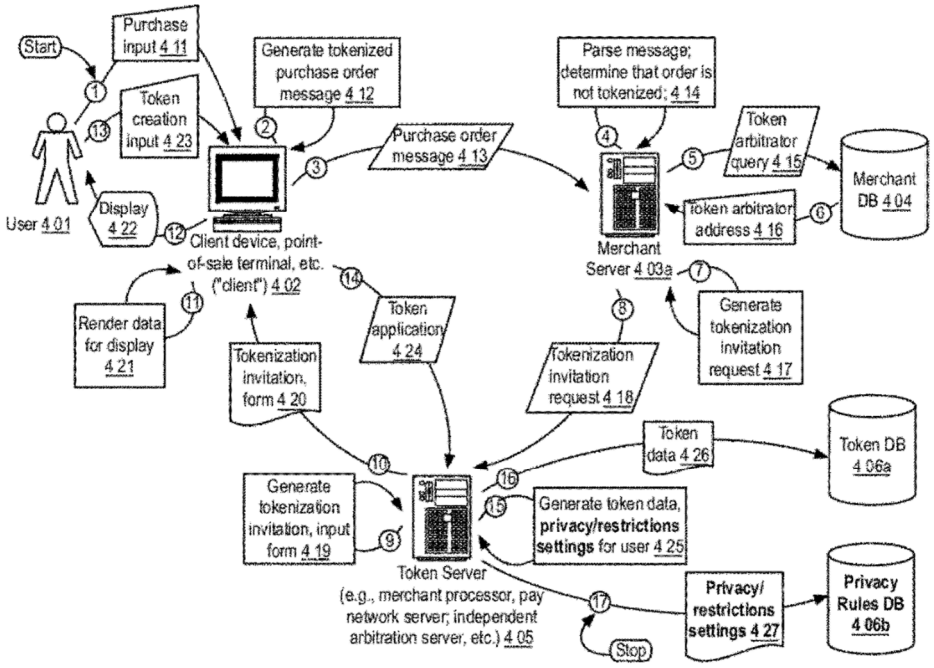
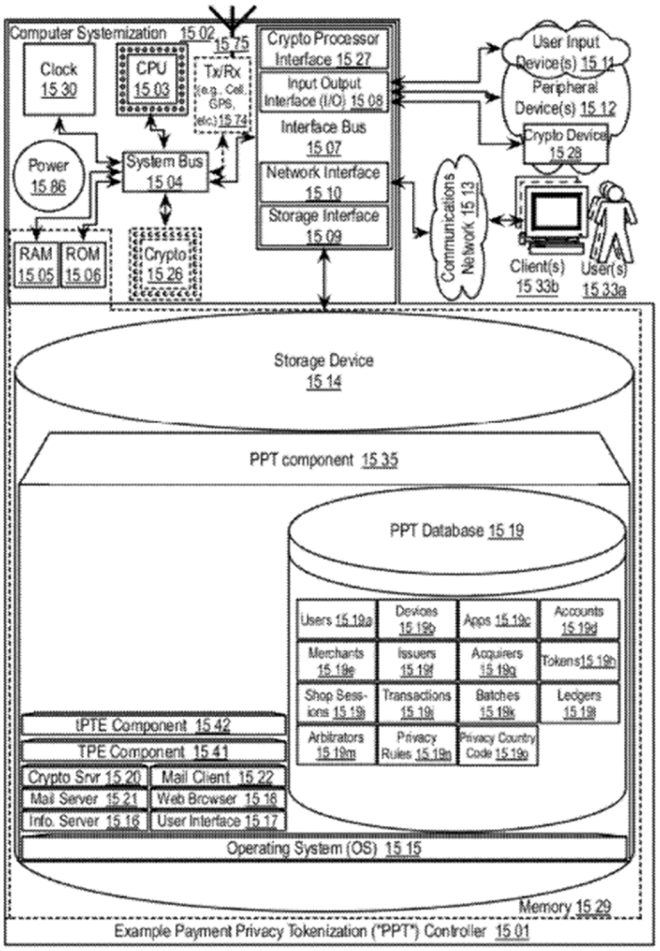


FIGURE 4 Example: Token-Based Purchase Enrollment

211. As I explain below in connection with limitations 1.3 and 1.6, the disclosed apparatus generates and verifies OVER files. Oborne thus discloses the recited OVER engine.

212. Further, the apparatus of Oborne performs the recited "storing" step because it stores information associated with a credential of a user for proving the user's identity or qualifications. Oborne's PPT apparatus includes a storage device storing account information in a database, as shown (storage device 1514) in Fig. 15:



EX1011, Fig. 15; see *id*., [0114], [0146]-[0151]. The database's "Accounts table 1519d," includes fields with information associated with a credential (e.g., information about the user's credit cards) and useful for proving the identity or qualifications of a user, such as "account_number," "issuer_name,"

"account_address," "routing_number," etc. EX1011, [0147]. Oborne teaches that a user "desir[ing] to utilize a card" may use "tokens in lieu of payment information," using the token to prove identity to a merchant as a stand-in for credit card or account information (thus, for proving the user's identity or qualifications, wherein said information is used to prove the user's identity or qualifications). EX1011, [0025].

3. Limitation 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;

213. Oborne teaches using tokens as a substitute for payment information. EX1011, [0025]. To generate token information, the user communicates, e.g., via "a personal computer, mobile device, television, point-of-sale terminal, kiosk, ATM, and/or the like," and provides input "indicating the user's desire to purchase the product." EX1011, [0035]. 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 Near Field Communication (NFC) enabled device) EX1011, [0035], [0049], [0093]. If the

user wants to use tokenization, the client "may generate a competed [sic, completed] application form, and provide, e.g., 424, the token application to the token server (either directly or via the merchant server)." EX1011, [0040]. *See also* [0041]-[0047], which describes the process of generating and using a token, and [0054], describing token authentication. Sending the token application form is the claimed OVER file generation request, as claimed.

214. Oborne provides a sample encoding in XML of a tokenization application form:

```
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_adress> 123 Green St., City, ST 12345
        </shipping_address>
        <ship_type> Express </ship_type>
        <ship_carrier> FedEx </ship_carrier>
        <ship_account> 0908765432 </ship_account>
        <tracking_flag> ON </tracking_flag>
        <sign_flag> ON </sign_flag>
    </shipping_info>
</token_application_form>
```

EX1011, [0040]. This form includes the recited "information associated with the credential," such as account number, type, billing address, etc., as can be seen in the encoding shown above, and which are stored by Oborne's PPT apparatus. The token server uses values from the form to generate a token record. EX1011, [0041]. The request is thus "based on the information associated with the credential."

215. POSTing the form to Oborne's server constitutes the claimed "OVER file generation request."

4. Limitation 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;

216. Oborne teaches that the token server "parse[s] the form to extract data fields and values from the form" to generate a data record and data structure for a token (corresponding to the claimed "OVER file"), as well as a "token identifier" representing the token, which is then provided to the user. EX1011, [0047]-[0048]. The process is illustrated in Oborne Fig. 5.

217. Oborne Fig. 1B shows that the token is a virtual representation of a credential, such as a credit card:

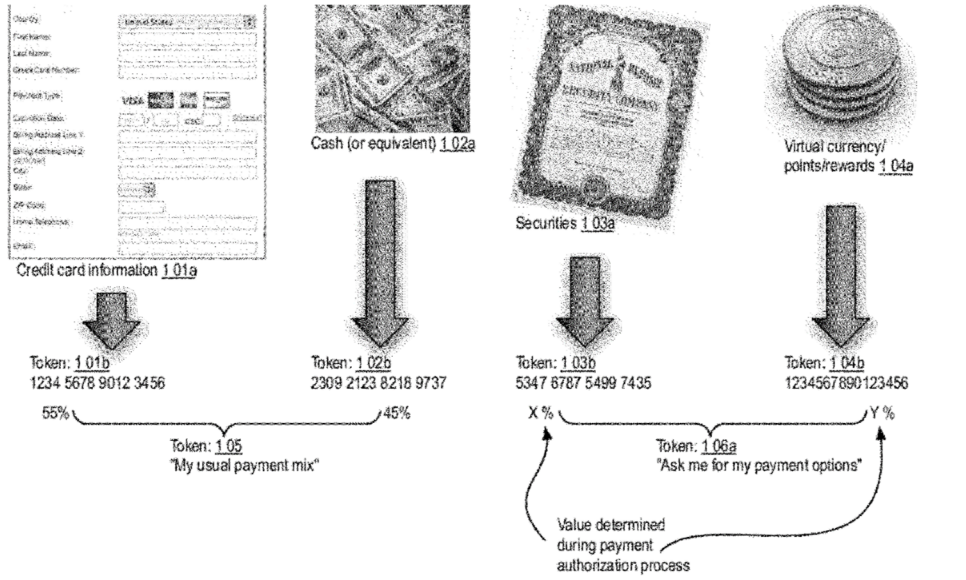


FIGURE 1B

Example: Payment Tokenization

EX1011, Fig. 1B. Oborne teaches that the token is "linked to credit card information," noting that the tokens are used "in lieu of payment information" such as "card information." EX1011, [0025]. Therefore, the token is a virtual representation of the credential and the token is generated based on the information associated with the credential, as claimed.

218. Oborne teaches or suggests that the token is verified by the issuing agency as an official representation. As discussed above in connection with limitation 1.1, Oborne teaches that any entity can operate as the token server, and it specifically states that the token may be provided by the credential's "funding source," e.g., by the bank that issued the credit card (credential). EX1011, [0029], [0047]-[0048], [0053]:

> For example, the user's payment token may be linked to one or more issuer financial institutions ("issuers"), such as banking institutions, which issued the account(s) for the user linked to the payment token. For example, such accounts may include, but not be limited to: credit card, debit card, prepaid card, checking, savings, money market, certificates of deposit, stored (cash) value accounts and/or the like. Issuer server(s), e.g., 609a-n, of the issuer(s) may maintain details of the user's account linked to the payment token.

Id., [0058]. 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.

See also id., ¶58 ("Issuer server(s), e.g., 609 a-n, of the issuer(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 verifies it to be an official representation of the credential.

219. Moreover, a POSITA 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. The issuer of a token representing a payment credential would logically ensure that the token accurately represented the credential. The existence of unofficial, forged or altered tokens in the marketplace

would create problems for both issuers and users. It would be a routine step to verify that the token was an official representation of the credential based on the credential data received and doing so would increase confidence that the token legitimately represented the credential.

220. Should Patent Owner argue that the claim requires that the credential, rather than the token, be verified by the issuer, a POSITA would have found it obvious that a credential is automatically verified simply because it was issued by an official issuer. Because the purpose of a credential is to be an official representation from the issuer, the very issuance of the credential means that the issuer has verified it.

5. Limitation 1.4

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

221. Oborne teaches that a "token may be provided as a data structure via HTTP(S) POST, as a file, as an attachment (e.g. via email), and/or provided to the client device for later use." EX1011, [0048]. The transmission to the client device is performed after receiving the token application as shown in Fig. 5, with step 517 occurring after a token generation request is received from the user (steps 508 and 515). *See* EX1011, [0040]-[0041], [0046]-[0047], and Fig. 5 (below). Oborne

sends a token ("OVER file") to the user's device ("OVER file storage client device of the user") in response to the OVER file generation request.

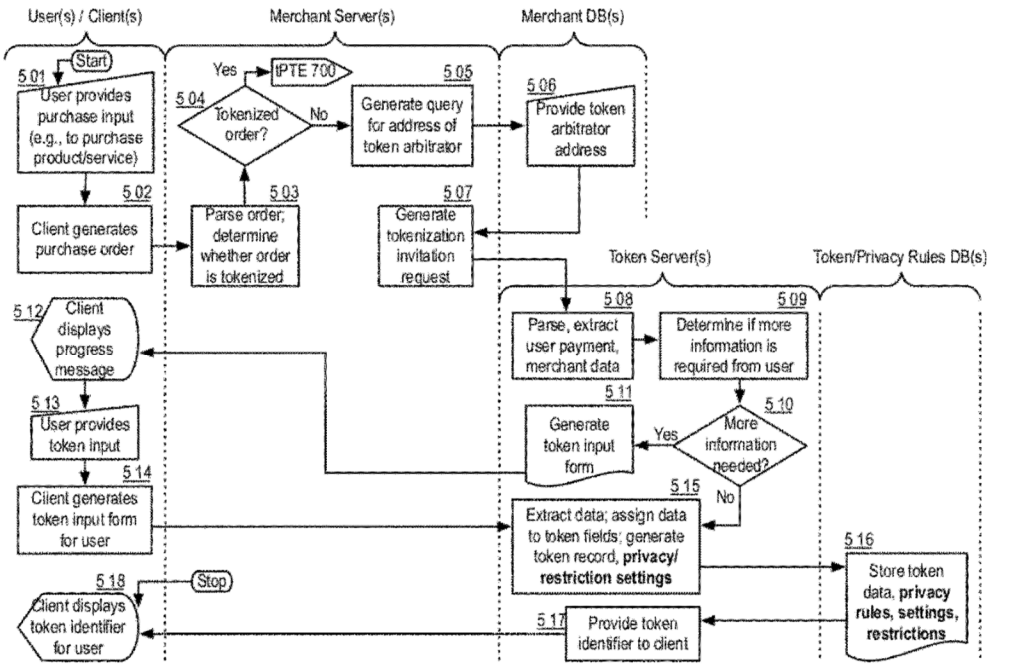


FIGURE 5 Example: Token-Based Purchase Enrollment ("TPE") component 500

6. Limitation 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;

222. Oborne teaches this limitation because a merchant's token arbitration request ("verifying request") is triggered by a purchase order request from a user ("based on a Near Field Communication (NFC) protocol-based communication"). Regarding the MFC communication, 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, [0049], [0049], [0093]. 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, [0050] (the client provides a "tokenized purchase order message to the merchant server"). Because Oborne's NFC activation triggers the purchase to be performed with the token between the user's client and the merchant's server, the NFC activation would be 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."

223. To process the purchase order request, the merchant server sends a "token arbitration request … to a token server." EX1011, [0051]-[0052]. This is the "verifying request" of limitation 1.5. An example of an XML encoding of a

verifying request is shown below. It includes a token_id field representing a token, is reproduced below, with the token_id highlighted:

```
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 I address below in limitation 1.6, Oborne teaches that the "token server may parse the token arbitration request message" and "determine whether the user token is authenticated." EX1011, [0053]-[0055]; *see also id.*, [0025] ("[A] user may desire to purchase a product … For example, the user may be able to pass a token … to a merchant … . For example, upon receiving a payment token from the user,

the merchant may pass the token to a transaction arbitrator."). Oborne thus teaches that the OVER engine (token server) receives the recited verifying request from a third-party device based on the recited NFC protocol-based communication.

7. Limitation 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

224. Oborne teaches that the token server processes the token arbitration request triggered by the NFC protocol-based communication (as discussed above in limitation 1.5) by extracting the token from the request and looking up the associated account number in a token database. In particular, the token server "extract[s] the payment token from the message," then issues a "query to a database, e.g., token database 606, using the payment token as a search term in the query." EX1011, [0053]. In response, the database provides information about how to proceed with processing, producing "instructions for the token server on how to proceed with payment processing." *Id.* This includes credential information such as user account numbers, as shown in the XML example (shown with highlighting) 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. Oborne also teaches that the "token server may determine whether the user token is authenticated." For example, if "no XML data is available associated with the payment token," this indicates that the "user has not signed up for payment tokenization services." EX1011, [0054]; *see also id.*, [0069] ("the token server may determine whether the user token is authenticated"). That is, 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.

225. Oborne teaches that more verification may optionally be performed. For example, the token server may further verify using biometric identification or may request a "user name and password to enable the token for payment processing." EX1011, [0054]. Further verification options can include using an authentication chip communicating in proximity with the user's card via RFID or similar technology. EX1011, [0026]. Thus, Oborne teaches that the correspondence of an NFC protocol-based communication with the user's credential information may be verified using various complementary techniques.

8. Limitation 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.

226. As discussed above in limitation 1.6, Oborne's token server determines whether the user token is authenticated (e.g., EX1011, [0054], [0069]), which corresponds to determining whether the recited NFC protocol-based communication corresponds to the recited "stored information."

227. Oborne teaches sending an authenticating message comprising an indicator of the authentication 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, [0069]. As shown in Fig. 7A, steps 712a-b, this message is sent to the merchant server ("third-party client verifying device"), which may then initiate enrollment or error-handling with the user device:

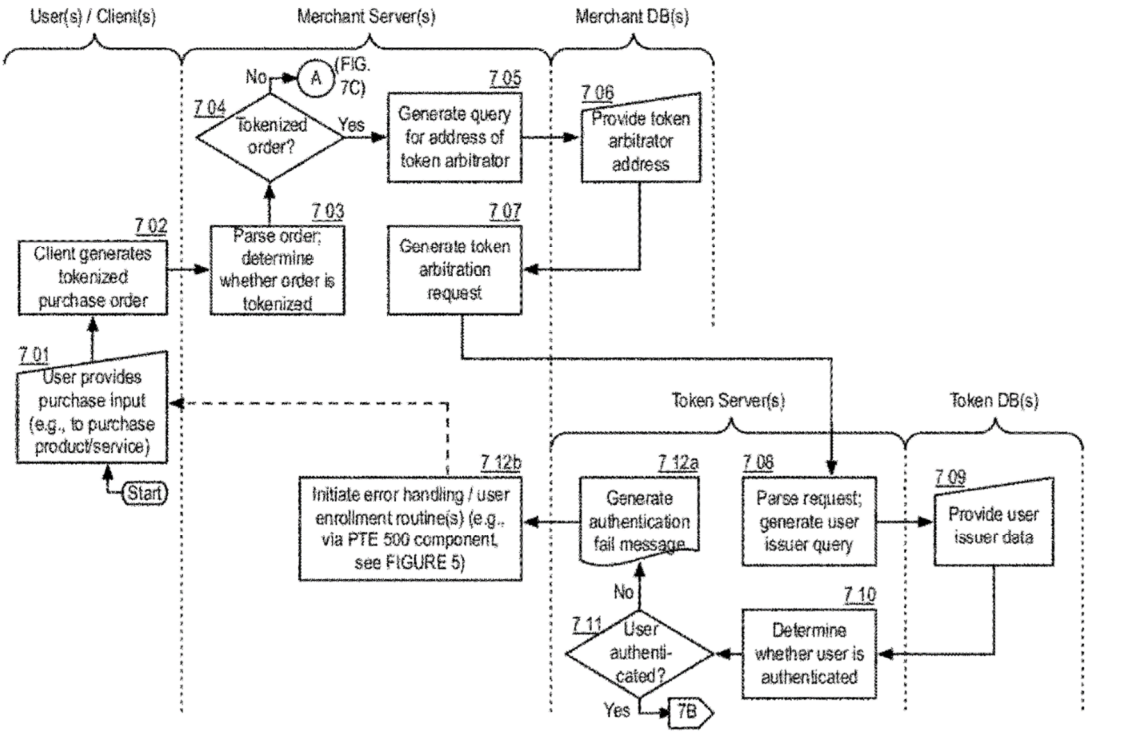


FIGURE 7A

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

EX1011, [0069], Fig. 7A. This indicates that the NFC protocol-based communication is not associated with the stored user data.

228. If the user token is authenticated, then the "token server may continue processing." EX1011, [0069]. The stored user account information is then used to procure payment authorization, and a message is sent to the merchant server indicating authorization, non-authorization, and/or "authorization in progress." EX1011, [0063] ("token server…may in turn forward the authorization success message, e.g., 647, to the merchant server"), [0061] (sending "an 'authorization fail' message to the merchant server, token server and/or client"), [0070] ("authorization in progress" message), Figs. 7B-C (showing process). Any of these messages is an indication that the token was authenticated, and thus that the NFC protocol-based communication corresponded properly to the stored user credential information.

229. Therefore, claim 1 was obvious over Oborne alone.

B. Claim 2

230. Claim 2 is essentially claim 1, but in which the user has more than one device, and an OVER file is sent to each device. Claim 2 depends from claim 1 and 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 goes on to recite three limitations identical to limitations 1.2-1.4, except that (1) the word "second" is used instead of "first"; (2) the generation copied from limitation 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." Oborne teaches these limitations.

231. (1)-(2) are satisfied by a user having two devices and receiving OVER files on each device. This would have been obvious in view of Oborne. A POSITA would find it unnatural to be restricted to using only a single device. Indeed, Oborne teaches that the token server may keep a device table with various identifiers for a user's devices, such as "device_ID," "device_name," "device_MAC," (referring to a MAC address) etc. EX1011, [0148].

232. (3) (that the second OVER file (i.e., the one destined for the second device) is invalid for use in the first device) would also have been obvious to the POSITA based on Oborne's disclosure of storing device ID's. Oborne teaches that "device fingerprinting may be utilized" to provide "additional security" for use of Oborne's tokens. EX1011, [0026]. There would be no purpose to device fingerprinting if a token could be used on any device. Similarly, Oborne provides an example of a token data structure that includes a "client_fingerprint" field with device-identifying information such as the client's MAC address. EX1011, [0047]. Device MAC addresses are 48 bits long and are globally unique. To obtain the additional security taught by Oborne, a POSITA would have been motivated to employ Oborne's device fingerprinting to tie a given token to a particular device,

such that the token for a second device would be invalid if used in a first device (since the device's fingerprint would not match).

233. Therefore, claim 2 was obvious over Oborne.

C. 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.

234. Regarding requesting authentication and receiving a status indicator and credential information, Oborne teaches these limitations in at least two ways. First, when adding a user's card to a wallet for Oborne's system, Oborne teaches that verification of the pay card's information 1252 (such as name, account number, etc.) may be performed, and that "verification may include contacting the issuer of the pay card for confirmation of the decoded information 1252 and any other relevant information." EX1011, [0108]. In light of this teaching, a POSITA would have found it obvious for the OVER engine to request a credential authentication from the issuing agency and receive a status indicator from the

issuing agency indicating whether the credential was valid. This was indeed common and performed in every credit card transaction.

235. Oborne also teaches that, when a tokenized transaction is performed, the token server contacts a pay network server that contacts "issuer server(s) corresponding to the payment token." EX1011, [0057]-[0058]. The issuer server parses the authorization request and "determine[s] whether the user can pay for the transaction using funds available in the account." EX1011, [0060]-[0061]. The issuer then provides a response, either an "authorization fail" message or a "notification of successful authorization," which is forwarded to the token server. EX1011, [0061]-[0063]. Such authorization success or fail messages would also be status indicators and credential information associated with the credential, received based on a validation request (a request to validate the credential's use in a transaction based on provided credential information). For example, a success message would indicate that the credential was valid as (a *status indicator*) well as providing confirmation that the credential corresponded to an account with sufficient funds for the transaction ("credential information associated with the credential"). A POSITA 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 are standard procedures used for transaction processing in a payment network (especially credit card networks, which require

validation of each transaction), allowing Oborne's system to be integrated into a system for traditional payment processing in a straightforward and predictable manner.

236. Storing the status indicator would have been obvious in view of Oborne. First, it was routine to maintain a log of events related to a payment credential, e.g., for fraud monitoring. Further, Oborne teaches generating "a transaction data record" for the pay network server to "store the details of the transaction and authorization." EX1011, [0062]. Oborne also teaches that "the token server may be … a pay network server." EX1011, [0039]. A POSITA would understand this as suggesting that the token server would store a received status indicator. Further, 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), would need to be stored to so that use of the credential could be monitored.

237. Therefore, claim 4 was obvious over Oborne.

D. 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.

238. As discussed above in claim 2, Oborne teaches using "device fingerprinting" to provide "additional security." EX1011, [0026]. A "device fingerprint" is a "device identifier" in the same sense that a human fingerprint identifies a person. Oborne's "token data structure" includes a "client_fingerprint" field with device information such as a MAC address. EX1011, [0047]-[0048], [0148] (identifying devices using device_ID, device_MAC, and similar fields). As explained above in claim 2, applying the device fingerprinting taught by Oborne would limit the token (and thus the credential) to the device having that given fingerprint.

239. Claim 5 was therefore obvious over Oborne.

E. 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.

240. This limitation was obvious, at least because it was common for tokens to be generated on a different server from the one on which the original credential were stored, at least for reasons of security.

241. Further, Oborne teaches that its systems may store data objects locally or in "remote storage facilities through a communications network." EX1011,

[0133]. As discussed above in limitation 1.1, Oborne teaches storing information associated with a credential in a database, including various references to the credential. *See* EX1011, [0148] (listing fields such as "account_number," "routing_number," etc. which would reference a credential); see also *id*., [0047] (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.

242. Therefore, claim 6 was obvious over Oborne.

F. 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.

243. As discussed above in claim 4, Oborne teaches receiving and storing various status indicators, each of which may result in different processing steps. A POSITA would have found it obvious to accomplish these different processings in response to different statuses (e.g., success, failed, insufficient funds, etc.) by checking the received status indicator. After all, that is the very purpose of the status indicator.

244. 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, via a database operation when creating a token. See EX1011, [0040], [0047] (identifying by account numbers of user's credentials associated with token); *see also id*., [0025], Fig. 1B (token may indicate mix of one or more specified credentials via token indicators). This operation stores the recited credential identifier.

245. Accordingly, claim 7 was obvious over Oborne.

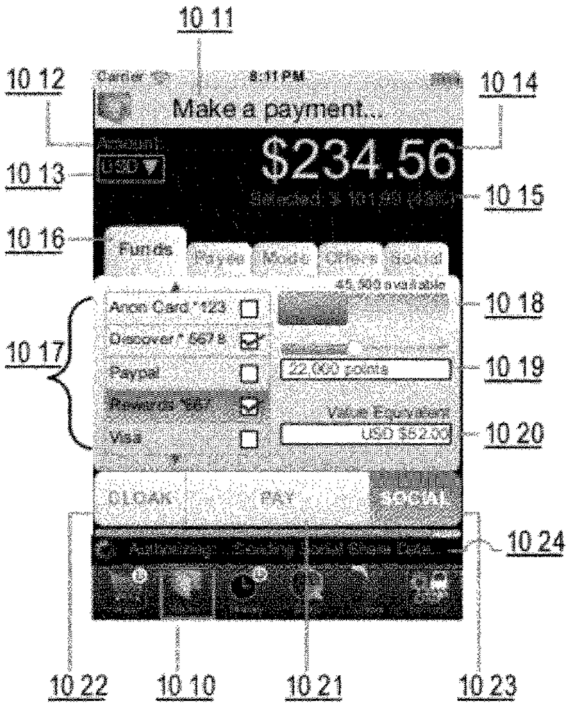
G. Claim 8

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

246. This limitation was obvious, at least because a virtual representation of a credential would be expected to contain a portion of the credential itself, e.g., the name of the holder.

247. Further, Oborne teaches that various payment account details (portion of the stored credential) are stored in a token data structure, and thus are included in the token. See EX1011, [0054] (including details such as account numbers). Oborne further teaches that the user device interface may display a portion of a

credential, such as part of an account number. EX1011, [0085]; *see id*., Fig. 10A (excerpted below).



In view of this disclosure, a POSITA 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 allow disclosed display of portions of credentials.

248. Therefore, Oborne renders claim 8 obvious.

H. <u>Claim 9</u>

249. Claim 9 is an apparatus form of claim 1. Limitations 9.1 and 9.2 recite components of the apparatus and are dealt with below. Limitations 9.3-9.8 correspond, respectively, to limitations 1.2-1.7 and use essentially identical

recitations, except for changing verb forms, e.g., changing "receiving" to "receive."

1. Preamble

1. An apparatus comprising:

250. Whether or not the preamble is limiting, Oborne clearly teaches an apparatus. *See, e.g.*, EX1011, Abstract (describing "PAYMENT PRIVACY TOKENIZATION **APPARATUSES**"), [0114]-[0122] (describing computerized apparatus used to perform Oborne's methods).

2. Limitations 9.1 and 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:

251. Oborne's "payment privacy tokenization apparatus" or "PPT" apparatus contains a processor:

> Typically, users, which may be people and/or other systems, may engage information technology systems (e.g., computers) to facilitate information

processing. In turn, computers employ **processors** to process information; such **processors** 1503 may be referred to as central processing units (CPU). EX1011, [0115].

252. The processors of Oborne include a memory unit storing instructions:

> CPUs use communicative circuits to pass binary encoded signals acting as **instructions** to enable various operations. These **instructions** may be operational and/ or data instructions containing and/or referencing other instructions and data in various processor accessible and operable areas of **memory** 1529 (e.g., registers, cache **memory**, random access **memory**, etc.).

253. *Id.* These instructions cause performance of the limitations recited in 9.3-9.8, corresponding, respectively to steps 1.2-1.7. Oborne's memory unit also stores information associated with a credential of a user, as explained above for limitation 1.1. *See supra* ¶¶210-228.

3. Limitations 9.3-9.7

254. These limitations effectively recite instructions for carrying out the steps, respectively of limitations 1.2-1.6, and are rendered obvious for the same reasons as those limitation. *See supra* ¶¶213-228.

i. Limitation 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.

255. As discussed above with respect to limitation 1.7, Oborne's token server determines whether the user token is authenticated (e.g., EX1011, [0054], [0069]), which involves determining whether the OVER file corresponds to the user's credential.

256. Oborne also 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, [0069]. As shown in Fig. 7A, steps 712a-b, this message is sent to the merchant server (third-party client verifying device), which may then initiate enrollment or error-handling with the user device.

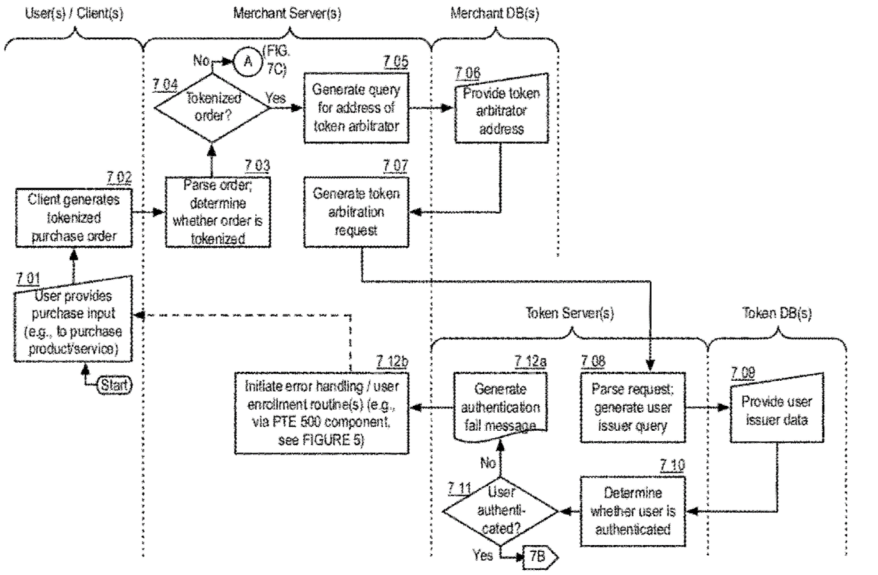


FIGURE 7A

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

EX1011, [0069], Fig. 7A. This is a status indicator indicating that the OVER file is does not correspond to the user's credential.

257. In the alternative, if the user token is authenticated, then the "token server may continue processing." EX1011, [0069]. The stored user account information is then used to procure payment authorization for the account associated with the token, and a message is sent to the merchant server indicating authorization, non-authorization, and/or "authorization in progress." EX1011, [0063] ("token server … may in turn forward the authorization success message, e.g., 647, to the merchant server"), 61 (sending "an 'authorization fail' message to the merchant server, token server and/or client"), 70 ("authorization in progress" message), Figs. 7B-C (showing process). Any of these messages is a "status

indicator" indicating that the token was authenticated, *i.e.*, that the OVER file corresponds to the user's credential.

258. Therefore, claim 9 was obvious over Oborne.

I. Claim 10

259. Claim 10 is an apparatus form of claim 2 and was therefore obvious over Oborne for the same reasons as for claim 2. *See supra*, ¶¶231-232, and the cross-references cited therein.

260. Therefore, claim 10 was obvious over Oborne.

J. Claim 13

261. Claim 13 is an apparatus form of claim 5 and was therefore obvious over Oborne for the same reasons as for claim 5. *See supra*, ¶, and the cross-references cited therein.

262. Therefore, claim 14 was obvious over Oborne.

K. Claim 14

263. Claim 14 is an apparatus form of claim 6 and was therefore obvious over Oborne for the same reasons as for claim 6. *See supra*, ¶¶240-241, and the cross-references cited therein.

264. Therefore, claim 14 was obvious over Oborne.

L. Claim 16

265. Claim 16 is an apparatus form of claim 7 and was therefore obvious over Oborne for the same reasons as for claim 7. *See supra*, ¶¶243-244, and the cross-references cited therein.

266. Therefore, claim 16 was obvious over Oborne.

M. 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.

267. As described in ¶224, Oborne teaches a credential identifier (account_num field). When the credential identifier matches the stored credential (credit card number) associated with the token, the authentication message itself comprises the status indicator—that is, it indicates that the user's credential is authorized by the issuer. See EX1011, [0061]-[0063].

268. Therefore, claim 17 was obvious over Oborne.

N. Claim 18

269. Claim 18 is similar to claim 1, with (under a logical understanding) "NFC" replaced with "Bluetooth," as described above at ¶72. The preamble and limitations 18.1-18.4 are identical, respectively, to the claim 1 preamble and limitations 1.1-1.4. Therefore, limitations 18.1-18.4 are disclosed by Oborne for the same reasons as limitations 1.1-1.4.

270. Under a proper understanding, limitations 18.5-18.7 correspond, respectively, to limitations 1.5-1.7 with "NFC" replaced by "Bluetooth." However, Oborne discloses Bluetooth for the same functions performed by NFC. *See, e.g.*, Ex1011, [0028] (Bluetooth as equivalent to RFID), [0080] (Bluetooth equivalent to near field communication), [0093] (Bluetooth equivalent to NFC). Therefore, for the reasons given above for limitations 1.5.-1.7, Oborne discloses limitations 18.5.18.7, and thus claim 18 was obvious over Oborne.

O. Claim 19

271. Claim 19 is identical to claim 2 except that it depends from claim 18 instead of claim 1. Therefore, claim 19 was obvious over Oborne for the same reasons as for claim 2. *See supra*, ¶¶230-232, and the cross-references cited therein.

P. Claim 20

272. Claim 20 is an apparatus form of claim 9. The preamble and limitations 20.1-20.5 are identical, respectively, to the preamble of claim 9 and limitations 9.1-9.5, *q.v.*

1. Limitations 20.6-20.7

273. Limitations 20.6-20.7, under a proper understanding, correspond, respectively, to limitations 18.5-18.6, *q.v.*

2. Limitation 20.8

274. Limitation 20.8 is identical to limitation 9.8, q.v.

275. Therefore, claim 20 was obvious over Oborne.

Q. Claim 21

276. Claim 21 is identical to claim 2, except that it depends from claim 20 rather than claim 1. Hence claim 21 was obvious over Oborne for the same reasons as claim 2, *q.v.*

277. Accordingly, claims 1-2, 4-10, 13-14, and 16-21 were obvious over Oborne.

X. GROUND 2: CLAIMS 3, 11-12, AND 15 WERE OBVIOUS OVER OBORNE IN VIEW OF PURVES

A. Overview and Reasons to Combine

278. Claim 3 depends from claim 1 and claim 11 depends from claim 9. Both further recite generating a credential after the processor determines that no credential is stored. Claim 12 depends from claim 9 and recites a step to "request the credential from the issuing agency" and further that the issuing agency stores credentials issued by the issuing agency. Oborne teaches providing "user interface elements to generate new tokens" for accounts by providing a funding source and relevant information. EX1011, [0029]. Oborne's PPT also "keeps track of all generated tokens via token identifiers," ensuring that each such token is "unique." EX1011, [0047].

279. To the extent Oborne does not expressly disclose that this process includes generating and storing *the credential*, doing so would have been obvious

in view of Purves. Purves teaches generating and storing new credentials, such as new gift cards and reloadable prepaid cards. *See* EX1013, [0083]. This process results in generation and storage of new credentials when a credential is not already stored.

280. A POSITA would have been motivated to combine Oborne and Purves with a reasonable expectation of success to arrive at the claimed invention because both references are directed to similar applications, including the use of virtual wallets and credentials, and because the teachings of Purves would be recognized as useful for adding new credentials to the digital wallet of Oborne's PPT apparatus (for example, if a user had not yet added any credentials, or if adding further credentials were desired). 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).

B. Claims 3 and 11

281. Claims 3 and 11 depend from claims 1 and 9, respectively, and further recite "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." Oborne in view of Purves teaches this limitation.

282. Oborne teaches providing "user interface elements to generate new tokens" for accounts by providing a funding source and relevant information. EX1011, [0029]. Oborne's PPT also "keeps track of all generated tokens via token identifiers," ensuring that each such token is "unique." EX1011, [0047].

283. To the extent Oborne does not expressly disclose that this process includes generating the "credential", doing so would have been obvious in view of Purves, which 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, [0083] (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 Oborne's tokens is to represent a credential, and by generating the new credential, the user is able to benefit from Oborne's tokenization system.

284. Therefore, claims 3 and 11 were obvious over Oborne in view of Purves.

C. Claim 12

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.

285. As discussed in connection with claim 11, Purves teaches generation of new credentials, such as a gift card or prepaid card. EX1013, [0083]. Purves further teaches that the system may, with user consent, retrieve the user's "payment account information from the payment account issuer." EX1013, [0107]. The issuer responds by providing the user's account information ("credential 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, [0108]. Purves also provides an XML form with further examples of credential information provided by the issuer, including fields such as the user's name, address, ZIP code, account number, expiration date, etc. Thus, Purves teaches requesting the credential from the issuing agency and receiving the credential information transmitted by the issuing agency.

286. Further, as discussed above for claim 9, Oborne 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, [0060]-[0061]. 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, [0061]-[0063].

287. 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. This would be a normal process to maintain an audit trail of transactions.

288. It was obvious that the issuer would store credentials it issued, as this storage of credentials would allow the issuer to provide the appropriate credential information upon request, as taught by Purves. See EX1013, [0107]-[0108]. If new credentials were generated upon user request, such as the gift and prepaid cards taught by Purves (EX1013, [0083]), it would have been natural for the issuer to store such new credentials, at least until they were sent to the recipient, and, for normal business purposes, as long as they remained valid, so that the issuer's systems could confirm their existence. Consistent with this practice, Oborne teaches that the "user profile database" of the issuer can store "data associated with an account linked to the user's payment token." EX1011, [0060]; *see also id.*, [0044]-[0045] (storing credentials in token data record and token data structure). This would naturally include storing a credential, such as the new credential taught by Purves.

289. It would also have been obvious in view of Oborne and Purves to store the status indicator and credential in the PPT apparatus. When a credential was received, such as the new gift or prepaid card taught by Purves, it would have been natural that Oborne's system would store it for use with a token in a manner similar to how other credentials, such as regular credit cards, were stored in Oborne. See EX1011, [0045]-[0048] (storing credentials in token data record and token data structure).

290. Likewise, Oborne teaches or suggests storing status indicators. For example, Oborne teaches generating "a transaction data record" for the pay network server to "store the details of the transaction and authorization." EX1011, [0062]. Oborne also teaches that "the token server may be…a pay network server." EX1011, [0039]. A POSITA would have understood these teachings as suggesting that the token server can store a received status indicator. To 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 POSITA would have routinely stored the status indicator during normal token server operations.

291. Accordingly, claim 12 was obvious over Oborne in view of Purves.

D. <u>Claim 15</u>

292. Claim 15 depends from claim 9, and adds the limitation that "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." Oborne in view of Purves teaches this limitation.

293. Oborne teaches receiving and storing various status indicators, each of which leads to different processing steps. A POSITA 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, such as the stored credential discussed above for claim 12, for similar reasons as discussed for claim 16.

294. Further, Oborne 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, [0047]; *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 for each issuer, merchant, acquirer and/or payment network."). This operation results in storing the recited credential identifier. Thus, the status indicator comprises the stored status indicator, as recited in claim 15.

295. Accordingly, claim 15 was obvious over Oborne in view of Purves.

296. Therefore, claims 3, 11-12, and 15 were obvious over Oborne in view of Purves.

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

A. Overview and Rationale to Combine

297. Stafford teaches a system for "validating and disseminating credential information" that discloses almost all limitations of the independent claims as well as many dependent claim limitations. EX1012, Abstract. Stafford's system does not use tokens, but rather 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, [0107]-[0121].

298. Stafford discloses methods for providing credentials to third parties that parallel those described and claimed in the '859 patent. Stafford's system stores credential information for a user ("entity") in a credential database, provides users with key signatures representing those credentials, and allows a third party ("IdBus1"), with which the user has shared the key signatures, to receive verification of a credential from the system. See EX1012, [0010], [0097]-[0102], [0108], [0115], [0118]-[0126], Figs. 2-3.

299. Stafford teaches that the key signatures and other information may be provided to a third party "online or in person," and that the "delivery process may vary" based on the information provided and the recipient. EX1012, [0106]-[0113].

Stafford thus expressly suggests including other information with its key signatures and employing various known delivery processes as using an optical scan in the and including an image as a virtual representation of a credential in an OVER file, both of which are taught by Purves. In particular, Purves teaches providing issuer-verified representations of credentials (such as credit card images), as well as triggering transactions using near-field communications (NFC). EX1013, [0064]. As discussed in detail below for the independent claims, it would have been obvious to use these features as part of Stafford's credential distribution system (1) to provide user devices with convenient images of the credentials and (2) to use the well-known NFC communication-based protocol to transfer Stafford's key signatures to the third party.

300. A POSITA 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). Further, incorporating features such as credential images and NFC protocol-based communications into a credential management system such as Stafford's would have been straightforward, as the use of these features would have been familiar to the POSITA and their application would have been predictable.

301. A POSITA 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.

302. Similarly, a POSITA would have viewed Purves's NFC protocol-based 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 protocol-based communication, a POSITA would reasonably have expected to achieve these benefits for users.

303. The discussion of claims 1, 3-4, 6-9, 11-12, and 14-17 below provides further detail the POSITA's rationale to combine Stafford and Purves to arrive at the claimed invention with a reasonable expectation of success.

B. Claim 1

304. Stafford in view of Purves teaches each limitation of claim 1, as discussed below.

1. Preamble

1. A computer-implemented method comprising:

305. Whether or not the preamble is limiting, Stafford and Purves both teach a computer-implemented method. See, e.g., EX1012, [0054], Fig. 1; EX1013, [0130]-[0146].

2. Limitation 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;

306. Stafford teaches limitation 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, [0054] ("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).

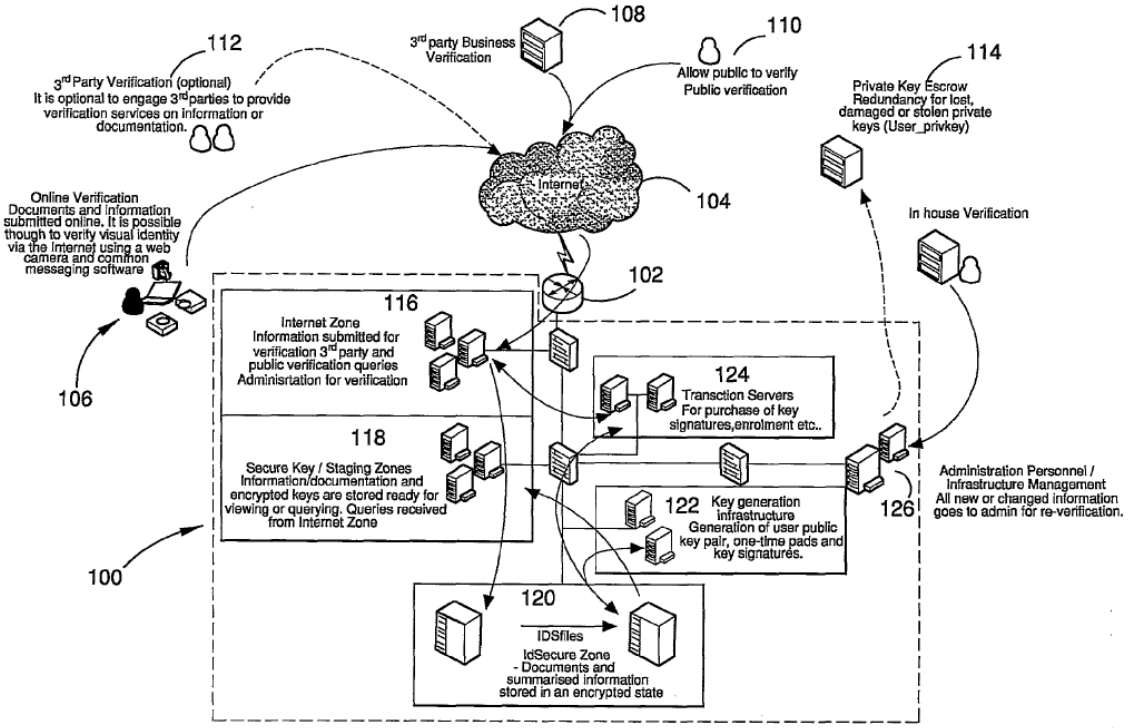


FIGURE 1

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, [0053]-[0054]. This includes memory (a "data store") hosting a "database of encrypted credential information." EX1012, [0057]. Credential information is encrypted using the user's public key, and further encryption (e.g., using a one-time-pad) is also employed to securely store the user's credential information. EX1012, [0058], [0071], [0089]. Stafford teaches that any of a variety of credentials may be used, such as driver's licenses, professional memberships, a degree (such as Ph.D.), etc. EX1012, [0004], [0065], [0131], [0139]. Stafford thus teaches limitation 1.1. *See also* the generation and verification functions in limitations 1.3 and 1.6, below.

3. Limitation 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;

307. 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 provides and sets the sensitivity of credential information. EX1012, [0054], [0081]. Sensitive credential information requires use of "highly secure symmetric or similar encryption process e.g. a one time pad" when being released. EX1012, [0088]; *see id.*, [0073]-[0074], Fig. 2 (showing credential release process). As discussed below for limitation 1.3, Stafford's process for using such highly secure encryption involves generation of an OVER file.

308. Stafford teaches that users can request release of sensitive credentials, and this request satisfies limitation 1.2. See EX1012, [0074] ("To release data, in a first example the entity (IdMember) logs on to the website and elects to 'release' information using the appropriate interface."). The request/release process is shown in Fig. 2, reproduced below.

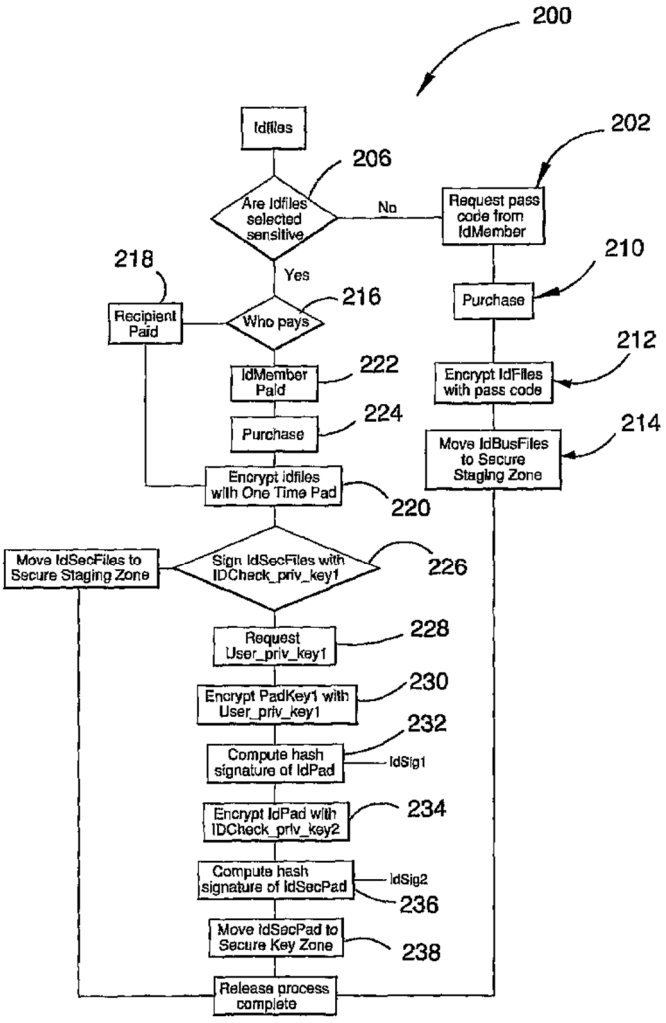


FIGURE 2

EX1012, Fig. 2. As shown in Fig. 2, 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, [0075]-[0079]; *see id.*, [0038], [0088], [0093]-[0095]. As discussed below for limitation 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.

309. Purves teaches that 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, [0035], [0049], [0093]; As is described in greater detail below in limitation 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.

310. Therefore, Stafford in view of Purves teaches limitation 1.2.

4. <u>Limitation 1.3</u>

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;

311. Stafford's system generates key signatures to release sensitive files, as discussed in connection with limitation 1.2. These signatures can comprise hash values (IdSig1 and IdSig2), which can either be displayed to the user or transmitted

electronically to the user's device (e.g., by email). EX1012, [0097]-[0099]. The credential to be released is stored in an encrypted format using one-time pads (referred to as IdSecPad and IdPad), and the hash values are of the credential's one-time pads, thereby identifying the encrypted credential. EX1012, [0116]-[0022]. The release of the credential is authorized by comparing the hash values to the IdSecPad and IdPad corresponding to the credential, with a match indicating that release is authorized. A hash value acts as a virtual representation of the stored credential, and is derived based on the information associated with the credential, so generating the hash values or similar key signature corresponds to the step of generating the OVER file.

312. 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, [0062], [0065], [0067]. However, to the extent that Stafford does not expressly teach that the files sent to the user (e.g., containing hash values) include a virtual representation verified by the issuing agency, this portion of the limitation is disclosed by Purves.

313. Purves teaches that a user device (e.g., a device implementing a digital wallet) may be sent an image of a credential (e.g., an image of a credit card provided by an issuer) to conveniently represent a real credential. EX1013, [0102], [0108]-[0109]. The image of a card may expressly be "from an issuer." EX1013,

[0085]. The server may also generate an on-the-fly image of the credential to be used to represent the credential on the user's device, optionally with "confidential information … obscured." EX1013, [0122]; *see also id.*, [0111]-[0112] ("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" as an official representation, as would an image produced from an actual credential, since an actual credential naturally represents itself.

314. In view of Purves's teaching to provide user devices with images representing a credential (such as a credit card), it would have been obvious to use similar credential 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 provided by the issuer 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, [0085], [0122]. Such an image would be a virtual representation verified by the issuer as being an official representation of the credential.

315. Should Patent Owner argue that the claim requires that the credential itself be verified by the issuer (as opposed to verifying the virtual representation),

this would also have been obvious, as Stafford expressly teaches contacting an issuer to verify a credential. See EX1012, [0065].

316. Therefore Stafford in view of Purves teaches limitation 1.3.

5. Limitation 1.4

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

317. Stafford in view of Purves teaches limitation 1.4. Stafford teaches that the key signatures generated by its online credential-database system can be sent to the user electronically (e.g., by email or by sending to a user's display to be copied). EX1012, [0097]-[0099]. As discussed for limitation 1.3, it would have been obvious to send an OVER file comprising a virtual representation (e.g., an issuer-verified credential image) and the key signatures encoded as a scannable QR code. Thus, Stafford in view of Purves teaches the recited transmitting step of limitation 1.4. Further, this transmission is performed in response to the request discussed for limitation 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). EX1012, [0093]-[0105], Fig. 2.

318. Therefore, Stafford in view of Purves teaches limitation 1.4.

6. Limitation 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;

319. Stafford in view of Purves teaches limitation 1.5. As illustrated in Fig. 3, Stafford teaches that a third-party client verifying device (referred to as IdBus1 at EX1012, [0108]) sends a request for release of information to the credential-database system. EX1012, [0115]; Fig. 3 (marked-up below)

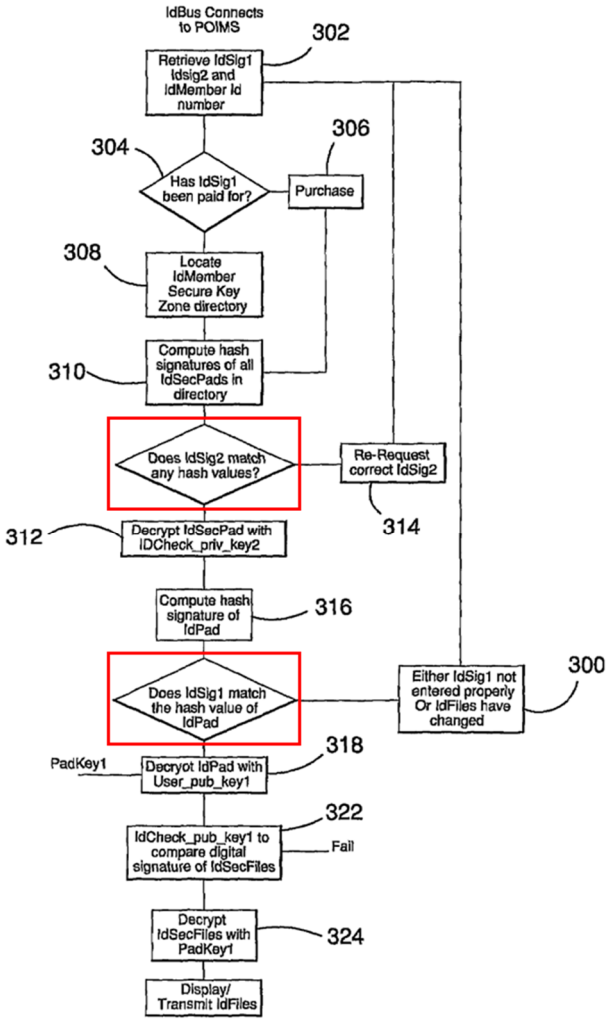


FIGURE 3

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, [0119]-[0122].

320. Purves teaches that an NFC interaction may be used to "trigger a wallet connection or login," in place of a card swipe or NFC interaction. EX1013, [0064]. *See also* ¶164, above. 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 protocol-based communication associated with an OVER file could be used to verify the OVER file transmitted to the user authenticates the user. EX1015, [0061]; EX1016, 12.

321. In light of Purves's teaching to use an NFC interaction in place of other credential interactions such as a card swipe, it would have been obvious to use an NFC protocol-based communication to transmit Stafford's key signature, as doing so would have allowed the user to more easily transmit the key signature to a third party. This NFC protocol-based communication would be used to transmit the key signatures to the third-party verification device in step 302 of Stafford's Fig. 3. 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 in view of Purves thus teaches limitation 1.5.

7. <u>Limitation 1.6</u>

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;

322. Stafford in view of Purves teaches this limitation. As discussed in limitation 1.5, the combination teaches sending a verifying request based on the

recited NFC protocol-based communication. Stafford's system responds to this request (and thus the associated NFC protocol-based communication of Stafford and Purves) by comparing the encoded hash values IdSig1 and IdSig2 of the key signature. EX1012, [0115]-[0021], Fig. 3 (marked up below).

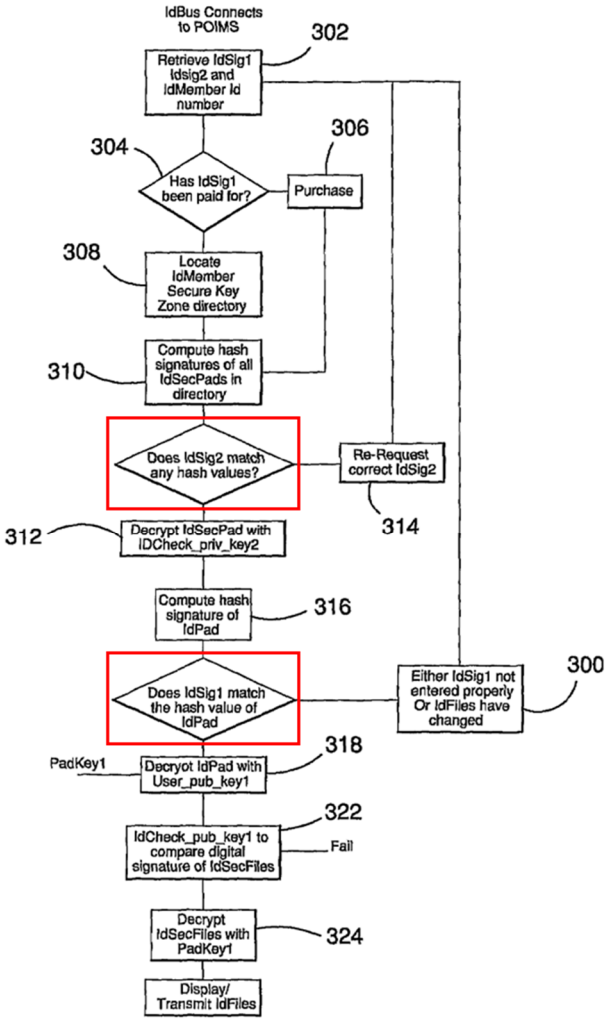


FIGURE 3

323. Checking the key signatures verifies that the NFC protocol-based communication (which provides the key signatures) corresponds with the information associated with the credential (since it matches the encrypted

credential's hash values). *See* EX1012, [0093] (IdFiles (credentials) encrypted with one-time pad) [0115]-[0122] (hash values match credential's one-time pad)

324. Therefore, Stafford in view of Purves teaches limitation 1.6,

8. Limitation 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.

325. Stafford teaches sending an authenticating message to the third-party device indicating whether the NFC protocol-based communication corresponds to the information associated with the credential of the user. For example, if either key signature fails to match, an appropriate message is sent to request the non-matching hash value again. EX1012, [0120]-[0122]. 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, [0120]-[0126]. These alternatives, indicated in Fig. 3 (marked-up below) both correspond to the recited authenticating message, since a repeated request message indicates a lack of correspondence and the sending of the IdFiles indicates a successful correspondence between the

credential information and the recited NFC protocol-based communication of limitation 1.5. EX1012, Fig. 3.

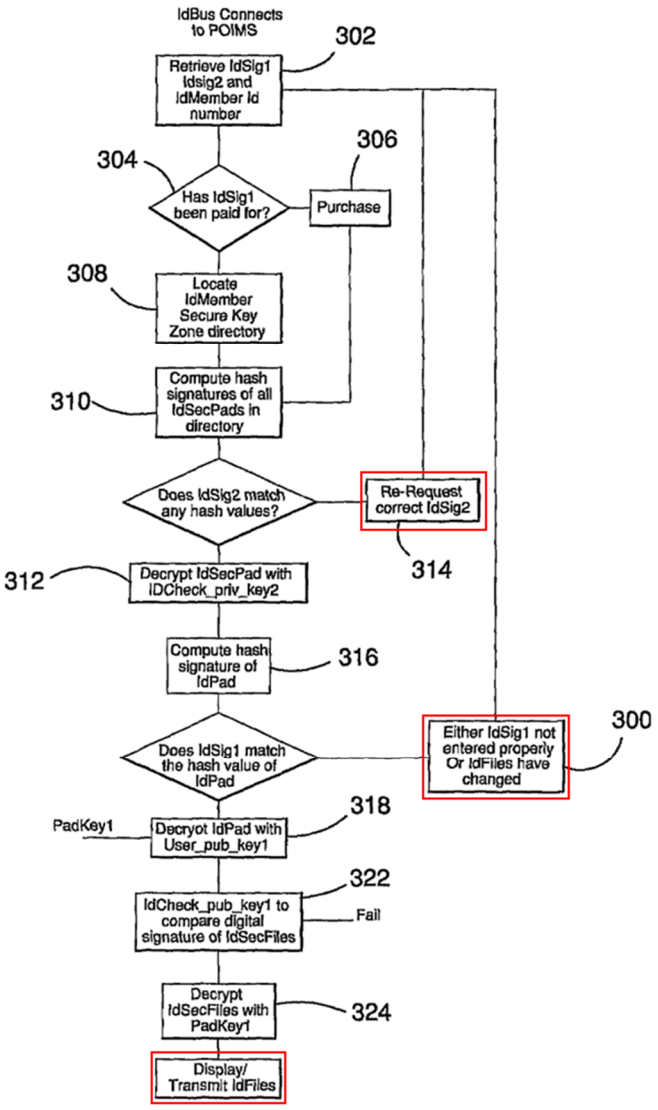


FIGURE 3

326. Therefore, Stafford in view of Purves thus teaches limitation 1.7.

327. Accordingly, claim 1 was obvious over Stafford in view of Purves.

C. Claim 3

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.

328. Stafford teaches that, in compiling a database, a document with credential information is received and a representation of the document is created. EX1012, [0010]. Stafford teaches that an administrative sub-system is used to "scan or upload hard copy documents into the system." EX1012, [0062]; *see id.*, [0067] ("The original documents are also electronically scanned and digitally signed and then encrypted…."). These are documents "attesting to one or more characteristics of the entity," *i.e.*, they are credentials. EX1012, [0024]. Stafford thus teaches generating, by the processor, the credential in the form of an electronic credential, such as a scanned original credential document.

329. Further, it would have been common sense for the processor to determine that no credential is stored after a document is first scanned and uploaded. *See* ¶55, above. 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 in that case for the processor to make a determination that no credential was stored, so that the document could be scanned and added to the

database, as otherwise, the newly-scanned credential would needlessly overwrite the previously stored credential. *Id*.

330. Accordingly, claim 3 was obvious over Stafford in view of Purves.

D. Claim 4

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.

331. Stafford teaches "automated verification" of its credentials, including "verification of document or data authenticity with a document's issuing body etc." EX1012, [0065]. For example, Stafford describes an authenticating request to a university, which "may verify that IdMember has a PhD." *Id*. Thus, Stafford expressly discloses the "requesting" and "receiving" steps of claim 4.

332. Stafford's system can also assign a confidence rating to a credential based on the issuer's reliability. EX1012, [0065]. The recipient can use these ratings to determine a credential's validity. *Id*. A POSITA would find it natural to store the indicators received from the issuing agency so that these confidence

ratings could be applied when deciding what the reliability of the credential information.

333. Accordingly, claim 4 was obvious over Stafford in view of Purves.

E. Claim 6

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..

334. Stafford teaches storing credentials in a remote system. *See* EX1012, [0062], Fig. 1 (showing various remote computers, including those 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, [0054]. Applying these teachings to remotely store credentials, a POSITA 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.), as otherwise, the remotely stored data would not be locatable. See above at ¶59. Indeed, Stafford expressly teaches generating references to its stored credentials, such as the key signatures IdSig1 and IdSig2, which locate a remotely-stored credential by matching hashes of its associated one-time pads stored in Stafford's system. See EX1012, [0033], [0119]-[0022], Fig. 3. Thus, it would have been

obvious to include a reference to the remotely stored credential as information associated with the credential.

335. Accordingly, claim 6 was obvious over Stafford in view of Purves.

F. Claim 7

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.

336. 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. 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, [0065] (The "user may choose not to release information to a recipient unless their confidence level is over a certain threshold."). A POSITA would implement such a process by checking the credential's status indicator to determine whether the credential had been validated and what the confidence level was based on the validator.

337. Stafford also teaches that a user may specify which credentials from a list of the user's stored credentials are to be released. EX1012, [0022] ("The authorisation for the provision of said credential data to a third party can includes an indication which credential data is to be provided"); *see id.*, [0075]-[0079] (authorization provided by "entity"). As discussed for claim 1, Stafford and Purves teach using an OVER file to release credentials. A POSITA would have found it obvious to use a credential identifier when the user specifies the credential to release (and thus be represented by the OVER file), so that the user's selection can be mapped by the system to the credential to released.

338. Thus, claim 7 was obvious over Stafford in view of Purves.

G. Claim 8

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

339. This limitation was purely conventional, as discussed above at ¶61. As discussed for claim 1, it would have been obvious in view of Purves to include a portion of a stored credential in an OVER file. EX1013, [0122] (credential image with confidential information obscured).

340. Therefore, claim 8 was obvious over Stafford in view of Purves.

H. Claim 9

1. Preamble

341. Whether or not the preamble is limiting, Stafford and Purves both teach an apparatus. See, e.g., EX1012, [0054], Fig. 1 (computerized system 100 and accompanying components); EX1013, Abstract, [0130]-[0146].

2. Limitations 9.1 and 9.2

342. 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 limitations 9.1 and 9.2.

343. 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, [0054]; *see id.*, Fig. 1 (depicting system 100 as a system comprising computers). Thus, Stafford discloses a computer apparatus that stores credential information. A POSITA would have understood that such a system would include a processor coupled to a memory unit storing instructions and the user's credential information.

344. Purves confirms that such a computer system would include a processor and memory. For example, Purves teaches that "computers employ processors to process information," which "may be referred to as central processing units (CPU)," and which operate on "instructions and data in various processor accessible and operable areas of memory." EX1013, [0127]; *see also id.*, [0132] (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, [0131]-[0149].

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

346. Fig. 1 (below), which depicts a system that stores credential information. EX1012, [0054] ("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).

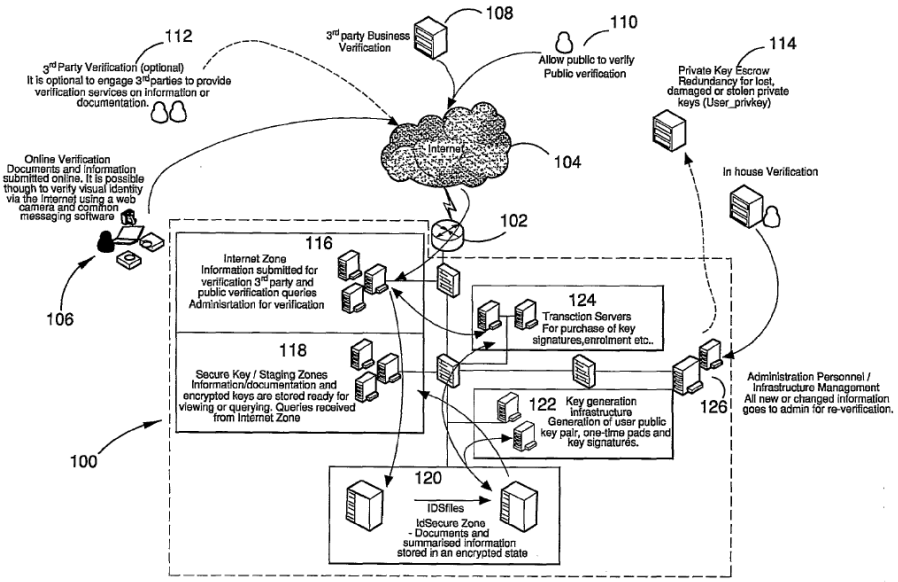


FIGURE 1

As discussed above in ¶¶120-123, Stafford uses the terms "entity" (as well as the term "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, [0053]-[0054]. This includes memory (a "data store") hosting a "database of encrypted credential information." EX1012, [0057]. Credential information is encrypted using the user's public key, and further encryption (e.g., using a one-time-pad) is also employed to securely store the user's credential information. EX1012, [0058], [0071], [0088]. Stafford teaches that any of a variety of credentials may be used, giving examples including driver's licenses, professional memberships, a degree (such as Ph.D.), etc. EX1012, [0004], [0065], [0131], [0139]. Stafford thus stores information associated with a user's credential.

347. Thus, Stafford and Purves teach limitations 9.1 and 9.2.

3. Limitations 9.3-9.7

348. Stafford in view of Purves teaches limitations 9.3-9.7 for similar reasons to limitations 1.2-1.6. *See supra* ¶¶307-324.

4. Limitation 9.8

349. Stafford teaches sending an authentication message to the third-party device indicating whether the scan corresponds to the OVER file. For example, where either key signature fails to match, an appropriate message is sent to re-

request the non-matching hash value. EX1012, [0120]-[0122]. 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, [0120]-[0126]. 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 indicates a lack of correspondence and the sending of the IdFiles indicates a successful correspondence between the credential information and the recited scan. EX1012, Fig. 3.

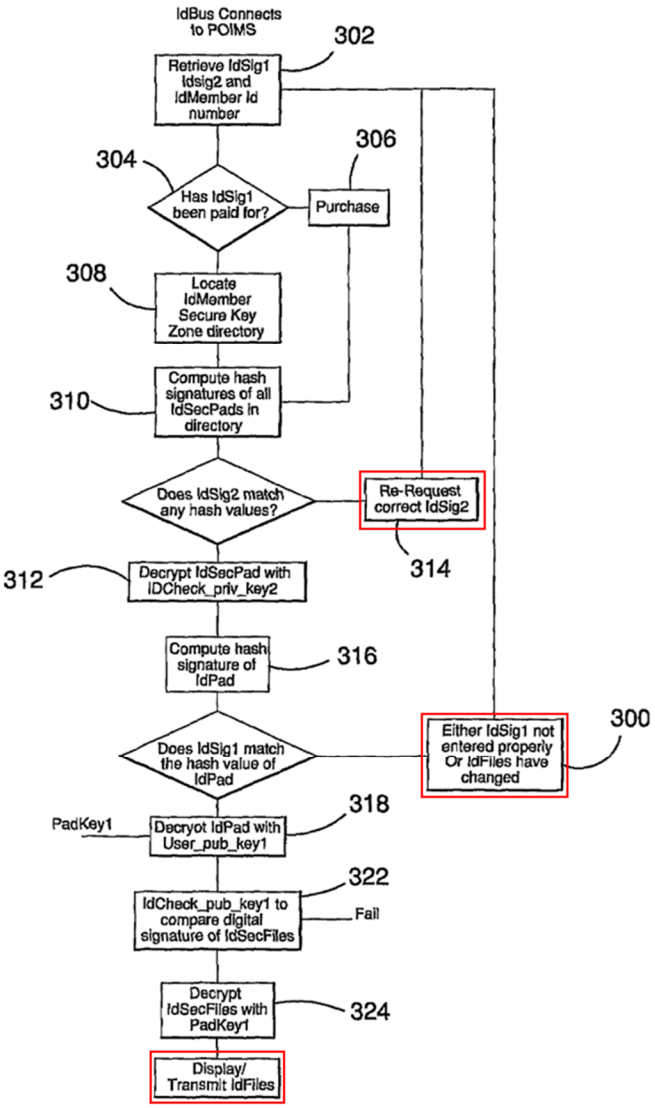


FIGURE 3

350. Stafford further teaches that its system can assign a confidence rating to a credential based on the issuer's reliability. EX1012, [0065]. 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 this rating when sending credentials to a recipient would be a further example of a "status

indicator indicating whether the OVER file corresponds to the credential of the user." For example, a credential verified by a trusted issuer would indicate that the OVER file corresponds to an actual credential of the user.

351. Therefore, Stafford in view of Purves teaches limitation 9.8.

352. Accordingly, claim 9 was obvious over Stafford in view of Purves.

I. Claim 11

353. Stafford in view of Purves teaches claim 11 for similar reasons to claim 3. *See supra* ¶¶328-330.

354. Therefore, claim 11 was obvious over Stafford in view of Purves.

J. Claim 12

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.

355. As discussed for claim 4, Stafford teaches "automated verification" of its credentials, including "verification of document or data authenticity with a document's issuing body etc." EX1012, [0065]. For example, Stafford describes an

authenticating request to a university, which "may verify that IdMember has a PhD." *Id*. Thus, Stafford expressly discloses the "requesting" and "receiving" steps of claim 12..

356. Stafford's 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, [0065]. When This verification from an issuer to which Stafford's system applies a reliability assessment is a received 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, [0067]. This verification would include verifying more than just a status of valid or invalid, but also particular details (such as the name for the credential, and information such as associated numbers). *See* EX1012, [0004] (information for driver's license includes "number on the drivers license used for identification" and "name on the license"), [0062] (documentation information can include scans of an entire credential document). Stafford stores the credential (EX1012, [0067]), and a POSITA 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.

357. A POSITA would have expected that an issuer would store the issued credentials as a matter of course. For example, as discussed above in Ground 2, Purves teaches generation of new credentials by issuers, (e.g., gift and prepaid cards, see EX1013, [0083]), and 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. This is consistent with Stafford's teaching that an issuer can be contacted to verify a credential (see EX1012, [0065]), as storing the credential would allow the issuer to verify its authenticity. For example, Stafford describes a scenario involving verification of an academic degree (EX1012, [0065]), and a POSITA 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, [0089]-[0090] ("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).").

358. Therefore, claim 12 was obvious over Stafford in view of Purves.

K. Claim 14

359. Stafford and Purves teach claim 14 for similar reasons to claim 6. *See supra* ¶334.

360. Therefore, Stafford in view of Purves renders claim 14 obvious.

L. Claim 15

361. Claim 15 requires checking the stored status indicator. Stafford teaches storing a status indicator, as discussed for claim 12. *Supra*, 355-358. 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, [0065] (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 POSITA would have found it obvious to implement such a process by checking the credential's status indicator (such as an indication that a given issuer had verified the credential) along with the issuer's confidence rating to determine whether the credential was validated and what the confidence level was based on the validating issuer.

362. Thus, claim 15 was obvious over Stafford in view of Purves.

M. Claim 16

363. Stafford and Purves teach claim 16 for similar reasons to claim 7. *See supra* ¶¶334.

364. Therefore, claim 16 was obvious over Stafford in view of Purves.

N. Claim 17

365. 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 the reliability of the issuer. See supra ¶332; EX1012, [0065] (confidence rating sent with credential), 120-26, Fig. 3 (credential sent upon matching key signatures).

366. Accordingly, claim 17 was obvious over Stafford in view of Purves.

367. Therefore, claims 1, 3-4, 6-9, 11-12, and 14-17 were obvious over Stafford in view of Purves.

XII. GROUND 4: CLAIMS 2, 5, 10, 13, AND 18-21 WERE OBVIOUS OVER STAFFORD IN VIEW OF PURVES FURTHER IN VIEW OF NEAFSEY

A. Overview and Rationale to Combine

368. 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.

369. A POSITA 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.

370. As described above in Ground 3, Stafford in view of Purves renders obvious the computer-implemented method of claims 1 and 9. *See supra* §XX;. Claims 18 and 20 differ from claims 9 and 1, respectively, only in that, under a proper understanding, the former claims require the use of Bluetooth in place of NFC protocol-based communications. Purves teaches using Bluetooth transceivers as part of its virtual wallet computer system. EX1013, [0131], [0139]. However, should Patent Owner argues that Purves does not explicitly teach using Bluetooth in the same manner as NFC described above, Neafsey teaches using both Bluetooth and NFC protocol-based communication. EX1015, [0031]; EX1016, 6. Should Patent Owner argues 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.

371. A POSITA would have been motivated to incorporate the Bluetooth communication module of Neafsey into the device of Oborne and Purves to be used to trigger the use of tokens to purchase goods because the Bluetooth

communication would serve a virtually identical role. The combination would thus be a simple substitution of known elements to achieve predictable results.

372. The introduction of Bluetooth would provide greater flexibility to users, increasing convenience and allowing a greater range of mobile devices to be employed (e.g., devices with Bluetooth could be used even if a device were not NFC-enabled). A POSITA would reasonably expect to achieve the benefits of adapting the credential management system of Stafford and Purves to transmit key signatures using a Bluetooth protocol-based communication at least because Bluetooth was a well-known technology and would require only a one-to-one substitution with NFC.

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

B. Claim 18

374. Whether or not the preamble is limiting, Stafford and Purves both teach an apparatus. See, e.g., EX1012, [0054], Fig. 1 (computerized system 100 and accompanying components); EX1013, Abstract, [0130]-[0146].

1. Limitations 18.1-18.4

375. Stafford in view of Purves teaches limitations 18.1-18.4 for reasons to those for limitations 1.1-1.4. *See supra* ¶¶306-318.

2. Limitations 18.5-18.7

376. Recalling that limitations 18.5-18.7 are effectively limitations 1.5-1.7, respectively, with "Bluetooth" substituted for "NFC," Stafford in view of Purves teaches limitations 18.5-18.7 for reasons to those for limitations 1.5-1.7. *See supra* ¶¶319-327.

377. Limitations 18.5-18.7, properly understood, require using both a Bluetooth protocol-based communication instead of a NFC protocol. Neafsey teaches utilizing Bluetooth in the same manner and in conjunction with the NFC protocol described above.

378. Should Patent Owner argue that claim 18 should be interpreted as written, then Neafsey also discloses that a single device may have both Bluetooth and NFC capability. EX1015, [0031]; EX1016, 6 (input/output system using Bluetooth or NFC, optionally using "more than one system."). Therefore, all arguments made regarding the use of NFC in limitations 1.5-1.7 similarly hold for the addition of Bluetooth.

C. Claim 20

379. Claim 20 is an apparatus form of claim 18. The preamble and limitations 20.1-20.5 are identical, respectively, to the preamble of claim 9 and limitations 9.1-9.5, *q.v.*

1. Limitations 20.6-20.7

380. Limitations 20.6-20.7, under a proper understanding, correspond, respectively, to limitations 18.5-18.6, *q.v.*

2. Limitation 20.8

381. Limitation 20.8 is identical to limitation 9.8, q.v.

382. Therefore, claim 20 was obvious over the combination of Stafford, Purves, and Neafsey.

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

383. Claims 5 and 13 add limitations to their parent claims to a device identifier limiting the credential to the client device. Claims 2, 10, 19, and 21 add limitations to their parent claims to generating and transmitting a requested second OVER file to a second client device that is invalid for use on a first client device. These additional limitations, arranged as in their specific claims, are taught by the combination of Stafford, Purves, and Neafsey.

384. Neafsey teaches that clients may have different devices, and that credentials may be provided in different formats appropriate to such different devices. EX1015, [0061]; EX1016, 12. Neafsey further teaches that different credential representations may be generated based on a "unique device ID" of the recipient device. EX1015, [0049]; EX1016, 10. A POSITA 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. A POSITA would have understood different client devices would sometimes require using different formats appropriate to each device, as certain formats could not be used on certain devices. see EX1015, [0061] (device may be smartphone or smartcard); EX1016, 11.

385. Claims 5 and 13 recite that the OVER file contains a device identifier limiting the validity of the OVER file to the device having that device identifier. 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, [0049], [0061]; EX1016, 10-12. In combination, a POSITA 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. A POSITA would also have recognized that tying a credential to a specific device prevents the use of that credential if it is stolen or copied and thus provides a security benefit.

386. Each of claims 2, 10, 19, and 21, repeats limitations 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. Thus, the combination of Stafford, Purves, and Neafsey teaches the limitations of claims 2, 10, 19, and 21 for reasons similar to those for claims 5 and 13.

387. A POSITA would have reasonably expected success in combining Stafford, Purves, and Neafsey as described above. The references involve well-understood and related technologies for electronic credentials and transactions, each of which would function predictably in combination. It was well-known to provide a file to a device in a format that the device could recognize and process.

388. Therefore, claims 2, 5, 10, 13, and 18-21 were obvious over the combination of Stafford, Purves, and Neafsey.

XIII. CONCLUDING STATEMENT

389. Relying on my education, experience, skill, and training in the relevant field of art, and after reviewing the materials identified above, it is my opinion that each of the Challenged Claims is invalid.

XIV. JURAT

390. In signing this declaration, I recognize that the declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I also recognize that I may be subject to cross-examination in the case and that cross-examination will take place within the

United States. If cross-examination is required of me, I will appear for cross-examination remotely within the United States during the time allotted for such cross-examination at a time and place agreed by counsel.

391. I declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Executed January 26, 2024 at Pittsburgh, PA

By: 
Michael Ian Shamos