

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Faher et al.
U.S. Patent No.: 12,254,103 Attorney Docket No.: 56407-0023IP1
Issue Date: March 18, 2025
Appl. Serial No.: 17/767,153
Filing Date: April 7, 2022
Title: SECURITY MECHANISM FOR NAMESPACES USED IN
ELECTRONIC IDENTIFICATION ON MOBILE
DEVICES

Mail Stop Patent Board

Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

**PETITION FOR *INTER PARTES* REVIEW OF UNITED STATES PATENT
NO. 12,254,103 PURSUANT TO 35 U.S.C. §§ 311–319, 37 C.F.R. § 42**

TABLE OF CONTENTS

I.	REQUIREMENTS	1
A.	Standing	1
B.	Challenge	1
C.	Claim Construction	2
D.	Level of Ordinary Skill in the Art.....	3
II.	THE '103 PATENT.....	3
A.	Specification	3
B.	Prosecution History.....	4
III.	UNPATENTABILITY	5
A.	[GROUND 1A]: Makhotin-Coulomb Renders Claims 1-4, 6-10 Obvious	5
1.	Makhotin (OKTA-1004)	5
2.	Coulomb (OKTA-1005).....	7
3.	Coulomb's Effective Filing Date and Prior Art Status	9
4.	The Makhotin-Coulomb Combination	10
5.	Application of Makhotin-Coulomb to Claims	15
B.	[GROUND 1B]: Makhotin-Coulomb-Ahn Renders Claim 5 Obvious ..	35
1.	Ahn (OKTA-1008).....	35
2.	The Makhotin-Coulomb-Ahn Combination.....	37
3.	Application of Makhotin-Coulomb-Ahn to Claims	38
C.	[GROUND 1C]: Makhotin-Coulomb-Sharma Renders Claim 16 Obvious	39

1.	Sharma (OKTA-1007).....	39
2.	The Makhotin-Coulomb-Sharma Combination	40
3.	Application of Makhotin-Coulomb-Sharma to Claims.....	42
D.	[GROUND 2A]: Jones-Coulomb Renders Claims 1-4, 6-10 Obvious ..	46
1.	Jones (OKTA-1010).....	46
2.	Jones-Coulomb Combination.....	48
3.	Application of Jones-Coulomb to Claims	51
E.	[GROUND 2B]: Jones-Coulomb-Takayama Renders Claims 11-15 Obvious	66
1.	Takayama (OKTA-1011)	66
2.	The Jones-Coulomb-Takayama Combination.....	68
3.	Application of Jones-Coulomb-Takayama to Claims	70
F.	[GROUND 2C]: Jones-Coulomb-Sharma Renders Claim 16 Obvious ..	81
1.	The Jones-Coulomb-Sharma Combination	81
2.	Application of Jones-Coulomb-Sharma to Claims	82
IV.	PAYMENT OF FEES – 37 C.F.R. § 42.103.....	86
V.	MANDATORY NOTICES	86
A.	Real Party-In-Interest Under 37 C.F.R. § 42.8(b)(1).....	86
B.	Related Matters Under 37 C.F.R. § 42.8(b)(2)	87
C.	Lead And Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3).....	87
D.	Service Information	87

EXHIBITS

OKTA-1001	U.S. Patent No. 12,254,103 to Faher et al. (“the ’103 Patent”)
OKTA-1002	Prosecution History of the ’103 patent (“the Prosecution History”)
OKTA-1003	Declaration and Curriculum Vitae of Dr. Michael I. Shamos
OKTA-1004	U.S. Patent Application Pub. No. 2015/0127529 to Makhotin et al. (“Makhotin”)
OKTA-1005	U.S. Patent Application Pub. No. 2022/0222330 to Jogand-Coulomb et al. (“Coulomb”)
OKTA-1006	U.S. Provisional Patent Application No. 62/827,626 (“Coulomb-provisional”)
OKTA-1007	U.S. Patent Application Pub. No. 2015/0327071 to Sharma et al. (“Sharma”)
OKTA-1008	U.S. Patent No. 8,402,526 to Ahn (“Ahn”)
OKTA-1009	Oasis Identity Metasystem Interoperability Version 1.0 Standard (“Oasis”)
OKTA-1010	U.S. Patent Application Pub. No. 2015/0186864 to Jones et al. (“Jones”)
OKTA-1011	European Patent Application Pub. No. EP1132839B1 (“Takayama”)
OKTA-1012	RFC 2246 TLS Protocol Version 1.0 (January 1999)
OKTA-1013	Stallings, “Computer Organization and Architecture,” 10 th Ed. 2016

- OKTA-1014 Pythonhosted.org, “Django v1.2 documentation,” July 5, 2010,
available at
[https://pythonhosted.org/django_simple_feedback/ref/unicode.h
tml](https://pythonhosted.org/django_simple_feedback/ref/unicode.html)
- OKTA-1015 U.S. Provisional Patent Application No. 62/828,694 (“Second
Coulomb-provisional”)
- OKTA-1016 Declaration of June Ann Munford

LISTING OF CHALLENGED CLAIMS

Claim 1	
[1.pre]	A method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device, comprising:
[1.1]	associating security policies with each of a plurality of supported namespaces on a mobile device; and
[1.2]	operating a reader executing a reader module to communicate with the mobile device and to select a namespace to access a data item stored on the mobile device based on the security policies associated with the plurality of supported namespaces on the mobile device.
Claim 2	
[2.pre]	The method of claim 1 for managing security policies for data items stored in the electronic identification (eID) wallet on the mobile device, comprising:
[2.1]	transmitting a list of supported namespaces to a verifier module executing on a verifier terminal; and
[2.2]	selecting, by the verifier module, at least one candidate namespace from the list of supported namespaces based on confidence the verifier terminal assigns to the namespace, whitelisting or blacklisting of namespaces, or overhead associated with satisfying a security policy of the namespace from the security policies associated with the plurality of supported namespaces on the mobile device.
Claim 3	
[3]	The method of claim 2 for managing security policies for data items stored in the electronic identification (eID) wallet on the mobile device further comprises operating the reader to select a namespace to access a data item from the plurality of supported namespaces on the mobile device based on confidence the verifier terminal associates with each namespace in the plurality of supported namespaces.

Claim 4	
[4.1]	The method of claim 2 for managing security policies for data items stored in an electronic identification (eID) wallet on the mobile device, wherein the data item stored on the mobile device is stored in a hardware memory and wherein the association of security policies and namespaces is stored in a hardware memory,
[4.2]	the method further comprising operating a processor of the mobile device to transmit a list of supported namespaces and associated security policies to the verifier terminal.
Claim 5	
[5.pre]	The method of claim 1 for managing security policies for data items stored in the electronic identification (eID) wallet on the mobile device, comprising:
[5.1]	transmitting a list of supported namespaces to a verifier module; and
[5.2]	selecting, by the verifier module, at least one candidate namespace by displaying a dialog window on a verifier terminal user interface allowing an operator to select a namespace.
Claim 6	
[6]	The method of claim 1 for managing security policies for data items stored in the electronic identification (eID) wallet on the mobile device further comprising: prior to transmitting a list of supported namespaces to a verifier terminal via the reader, filtering out any namespaces that the user selects to not transmit and only transmitting those namespaces that the user has acquiesced to having transmitted to the verifier terminal.

Claim 7	
[7]	The method of claim 1 for managing security policies for data items stored in the electronic identification (eID) wallet on the mobile device, comprising: transmitting the security policy of each of the plurality of supported namespaces from the mobile device to the reader.
Claim 8	
[8.pre]	The method of claim 1 for managing security policies for data items stored in the electronic identification (eID) wallet on the mobile device,
[8.1]	wherein a security policy is transmitted as a sequence of bytes having bits identifying required authentication protocol, bit values denoting required HASH type, bit values denoting required signature scheme, or bit values denoting secure messaging options,
[8.2]	wherein the security policy is one of the security policies associated with the plurality of supported namespaces on the mobile device.
Claim 9	
[9]	The method of claim 1 for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device, wherein a required authentication is selected from one or more of digital signature, reader authentication, certificate verification, secure messaging, role authentication, and user consent.
Claim 10	
[10]	The method of claim 1 for managing security policies for data items stored in an electronic identification (eID) wallet on the mobile device, further comprises operating the reader to select a namespace to access a data item from the plurality of supported namespaces on the mobile device based on a whitelist of namespaces by which the reader selects a namespace based on the namespace being in the whitelist of namespaces or a blacklist of namespaces by which the reader does not select a namespace based on the namespace being in the blacklist.

Claim 11	
[11.pre]	A mobile device comprising:
[11.1]	a processor; and
[11.2]	a memory for storing instructions executable by the processor and for storing electronic identity (eID) data, the memory including an eID wallet application having instructions to cause the processor to:
[11.3]	receive a list of selected namespaces from a reader;
[11.4]	in response to receiving the list of selected namespaces from the reader, transmitting security rules associated with each selected namespace according to a defined bytestring template.
Claim 12	
[12.pre]	The mobile device of claim 11, wherein the eID wallet application further comprises instruction to cause the processor to:
[12.1]	receive a request for supported namespaces from the reader;
[12.2]	transmit a list of supported name spaces to the reader.
Claim 13	
[13]	The mobile device according to claim 12, wherein the eID wallet application further comprises instruction to cause the processor to: prior transmitting a list of supported namespaces to the reader, filter out any namespaces that the user selects to not transmit and only transmitting those namespaces that the user has acquiesced to having transmitted to the reader.
Claim 14	
[14]	The mobile device according to claim 13, wherein the eID wallet application further comprises instruction to cause the processor to: transmit a security policy of each of the plurality of supported namespaces to the reader connected to a verifier.

Claim 15	
[15]	The mobile device according to claim 14, wherein the security policy is transmitted as a sequence of bytes having bits identifying required authentication protocol, bit values denoting required HASH type, bit values denoting required signature scheme, or bit values denoting secure messaging options.
Claim 16	
[16.pre]	A method for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device, comprising:
[16.1]	associating a security policy with each of a plurality of supported namespaces on a mobile device;
[16.2]	transmitting the security policy of each of the plurality of supported namespaces to a reader connected to a verifier;
[16.3]	selecting, by the reader, at least one of the namespaces as candidate namespaces, and transmitting from the reader to the mobile device, a list containing the candidate namespaces;
[16.4]	transmitting to the reader by the mobile device, the security policy associated with each of the selected candidate namespaces;
[16.5.1]	operating the reader to: determine for which of the candidate namespaces the reader can satisfy the security policy of the namespace; and
[16.5.2]	if the verifier can satisfy the security policy of at least one candidate namespace, selecting one of the candidate namespaces for which the verifier terminal can satisfy the security policy, to access a data item, and demonstrating satisfaction of the security policy to the mobile device;
[16.5.3]	if the verifier cannot satisfy the security policy of any of the candidate namespaces, rejecting access to the data item; and

[16.5.4]	upon successful demonstration by the reader to the mobile device of satisfaction of the security policy of the selected namespace, granting access to the data item by the mobile device to the reader.
----------	---

Okta, Inc. petitions for *Inter Partes* Review (“IPR”) of claims 1-16 (“Challenged Claims”) of U.S. Patent No. 12,254,103 (“’103 patent”).

I. REQUIREMENTS

A. Standing

Okta certifies that the ’103 patent is available for IPR, and Okta is not barred or estopped from requesting IPR.

B. Challenge

Okta requests IPR on grounds 1A-2C listed below.

Ground	Claims	Basis for Rejection
1A	1-4, 6-10	§103-Makhotin+Coulomb
1B	5	§103-Makhotin+Coulomb+Ahn
1C	16	§103-Makhotin+Coulomb+Sharma
2A	1-4, 6-10	§103-Jones+Coulomb
2B	11-15	§103-Jones+Coulomb+Takayama
2C	16	§103-Jones+Coulomb+Sharma

Each reference qualifies as prior art under the assumed Critical Date of 10/18/2019.

Reference	Effective Filing Date	Publication Date	Prior Art Basis
Makhotin	11/5/2014	5/7/2015	§§102(a)(1)–(2)
Coulomb	4/1/2019 ¹	7/14/2022	§102(a)(2)
Sharma	10/07/2015	11/12/2015	§§102(a)(1)–(2)

¹ The relied upon disclosures of Coulomb are supported by an earlier-filed provisional application to which Coulomb properly claims priority. *See* §II.A.3, *infra*.

Ahn	5/27/2009	3/19/2013	§§102(a)(1)–(2)
Jones	12/29/2014	7/2/2015	§§102(a)(1)–(2)
Takayama	9/18/2000	4/4/2012	§§102(a)(1)–(2)

C. Claim Construction

The Challenged Claims should be construed according to the *Phillips* standard, meaning the claim terms are generally given their “ordinary and customary meaning” in view of the ’103 patent’s specification. *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005); 37 C.F.R. §42.100.

Okta submits that the Board need not expressly construe any claim terms at this time because the prior art discloses or otherwise renders obvious every limitation of the Challenged Claims under any reasonable interpretation. *See Wellman, Inc. v. Eastman Chem. Co.*, 642 F.3d 1355, 1361 (Fed. Cir. 2011). However, if the Board finds it necessary to interpret the claim term “**namespace**” (claims 1-8, 10-14, 16), the ’103 patent states:

A namespace is a symbolic mechanism for organizing and identifying pieces of data. To access a piece of data a requestor specifies namespace identifier and a local name (unique within the namespace but not necessarily unique with respect to other namespaces).

OKTA-1001, 1:25-30. Accordingly, if a construction is required, the term “namespace” should be construed as “symbolic mechanism for organizing and identifying pieces of data.” OKTA-1003, ¶¶71-82, 39. The analysis below in Section

III proves the Challenged Claims are obvious under this construction (and any other reasonable interpretation).

D. Level of Ordinary Skill in the Art

A person of ordinary skill in the art (“POSITA”) relating to the subject matter of the ’103 patent would have had (1) a bachelor’s degree in computer engineering, electrical engineering, or a related field, and (2) two years of industry experience working with electronic identification wallets, including security protocols for such systems. OKTA-1003, ¶¶65-70. Additional graduate education could substitute for professional experience, and *vice versa*. *Id.*

II. THE ’103 PATENT

A. Specification

The ’103 patent describes “[a] technology for managing security policies for data items stored in an electronic identification (eID) wallet on a mobile device.” OKTA-1001, 1:58-66. The technology includes “operating a reader executing a reader module to communicate with the mobile device and to select a namespace to access a data item stored on the mobile device based on the security policies.” *Id.*; OKTA-1003, ¶¶38-64. Figure 3 (below) shows a mobile device 103 executing an eIDWallet app 309 containing multiple namespaces 313a-n, where “[e]ach namespace provides access to a number of data elements and defines its own names for those data elements.” OKTA-1001, 7:30-53.

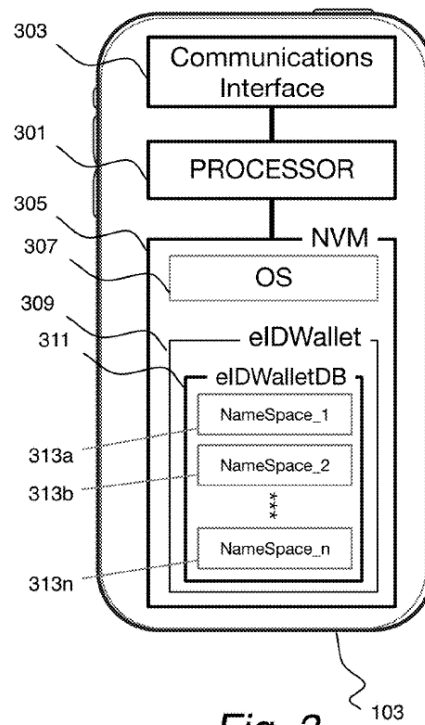


Fig. 3

OKTA-1001, FIG. 3.

The mobile device provides “security policy access rules associated with each of the requested namespaces” to a reader. *Id.*, 9:37-39. “The reader 109 determines if there is at least one namespace with acceptable access rules” and “selects a namespace with an acceptable security policy.” *Id.*, 10:14-34. In some embodiments, “the reader 109 is connected to an automated verifier 105,” while in other embodiments “the reader 109’ and the verifier 105’ may be one machine.” *Id.*, 7:8-16, 8:45-51.

B. Prosecution History

The ’103 patent issued from a national phase application of PCT/EP2020/076906 filed Sept. 25, 2020. OKTA-1001, Cover. Original claims 1,

4-5, 9, and 11 were allowed without any rejections from the examiner and the remaining claims faced rejections under 35 U.S.C. §112 for minor informalities. OKTA-1002, 265-270. The applicant amended the claims to address the 112 rejections, and the claims were subsequently allowed. OKTA-1002, 274-280, 299-306.

III. UNPATENTABILITY

A. [GROUND 1A]: Makhotin-Coulomb Renders Claims 1-4, 6-10 Obvious

1. Makhotin (OKTA-1004)

Makhotin describes a payment system in which “a portable communication device” stores “multiple payment applications with multiple application identifiers (AIDs) pointing to or otherwise associated with these payment applications.”² OKTA-1004, [0007]-[0008]. “The payment applications store payment information associated with one or more consumer accounts.” *Id.*, [0011]. “‘Payment information’ may include any data that may be used to identify an account and use the account for a payment transaction,” including “payment credentials,” “personal information associated with a user or a consumer (e.g., name, billing address,

² General descriptions provided for Makhotin and all other references and combinations thereof are incorporated into each subsection and mapping of the claims that includes citations to these references.

residential address, date of birth, etc.), account information,” and “cardholder verification information.” *Id.*, [0046].

Makhotin describes that “an access device (e.g., POS terminal) can select a particular application identifier and eventually a payment application to which it is linked when a contactless card or mobile NFC device is presented [to] the access device.” OKTA-1004, [0009].

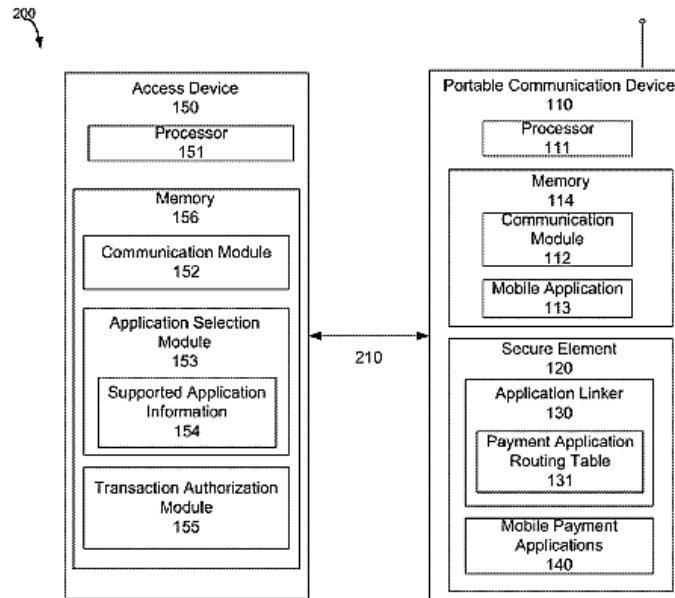


FIG. 2

OKTA-1004, FIG. 2.

A merchant associated with the access device “may desire to select a payment application that provides *the best fraud protection, most rigorous authentication processes for users, most reliable transaction processing, [and/or] most secure transaction environment.*” OKTA-1004, [0024]. For example, “if the authentication processing is more rigorous and/or the fraud risk is lower for a

particular payment application, the merchant may select the preferred payment application.” *Id.*, [0041]. “The access device may then send a communication to the [mobile device] using the selected application identifier” and the mobile device returns “the appropriate authentication and payment information to the access device for initiation of a transaction.” *Id.*, [0036].

2. Coulomb (OKTA-1005)

Similar to both Makhotin and the ’103 patent, Coulomb describes a mobile device executing “[a] wallet application” that is “loaded with several documents,” such as “a mobile driving license (mDL) 902, a first vehicle registration 910 for a first vehicle, a second vehicle registration 920 for a second vehicle, a first insurance policy,” etc. OKTA-1005, [0169].

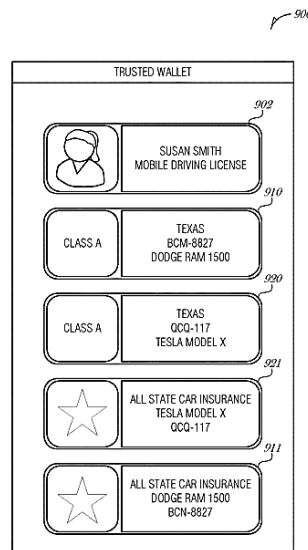


FIG. 9

OKTA-1005, FIG. 9; OKTA-1015, 9-10.

Specifically, Coulomb describes “an improved credential system that provides a portable, electronically verifiable, and aggregated credential. Identity credentials (e.g., documents, cards, mobile profiles, etc.) include information such as a first and last name, a date of birth, an address, etc.” OKTA-1005, [0024]. Such credentials can take the form of “a driving license, health coverage, flight ticket, etc.” *Id.*, [0073]. The stored credentials can also include “payment credentials, which allows a verifier to check a buyer’s identity or age information in the same transaction as payment, access control data so that biometrics of the person identity may be verified during access control, etc.” *Id.*

“Data elements from document types are defined in Namespaces ...Namespaces may include data elements for several kind of documents.” OKTA-1005, [0172]-[0174]. Coulomb’s namespaces “may be at the package level” or “may be at the data element level.” *Id.*, [0059]. Here, like the ’103 patent, “[a] namespace defines the meaning of the tag to make sure such meaning is the same for all issuers thus allowing the verifier to request something specific.” *Id.* “For instance, a namespace of ‘personal_info’ may be used for the tags ‘first_name’ and ‘last_name’ and be labeled as ‘personal_info:first_name’ and ‘personal_info:last_name.’” *Id.*

In Coulomb’s disclosure, the user’s mobile device interacts with “a Verifier”—“a device or an application that receives and verifies data from an issuer package”—to “obtain data from a Holder device, for example a point-of-sale, and

then contact one or more Issuers to validate the data.” OKTA-1005, [0043]-[0044]. “The verifier device 110 may be a point-of-sale terminal with a beacon,” which “may request certain information, such as a user’s name and credit card number, and the user device 112 may respond with the information.” *Id.*, [0057].

Coulomb discusses that some credentials are associated with “security mechanisms such as an electronic security certificate.” OKTA-1005, [0003]. For example, some credentials can require “some digital signature or equivalent (e.g., message authentication code (MAC), crypto checksum, etc.).” *Id.*, [0085], [0049], [0129]. Other examples of security requirements for various namespaces include “a personal identification number (PIN) or biometrics.” *Id.*, [0158].

3. Coulomb’s Effective Filing Date and Prior Art Status

Coulomb is prior art under AIA 35 U.S.C. § 102(a)(2) as of its effective filing date of Apr. 1, 2019 based on Provisional App. No. 62/827,626 (OKTA-1006, “’626 provisional”). Because the ’103 patent is subject to the AIA version of §102, “there is no need” for Okta to demonstrate that the ’626 provisional provides support for any claim of Coulomb. *Penumbra, Inc. v. RapidPulse, Inc.*, IPR2021-01466, Paper 34 at 32 (Mar. 10, 2023) (precedential) (quoting MPEP §2154.01(b)). Nevertheless, though unnecessary, Okta notes that Coulomb’s claim 99 is supported by the ’626 provisional. OKTA-1003, ¶¶105-107 (citing OKTA-1006, pp. 14-15, 17-23, 26, 31-37, 39-44, 47, 56, 62-65, 67-71, 104-107).

Consistent with the *Penumbra* precedent and §102(d), Okta submits that Coulomb meets the ministerial requirements for claiming priority to the '626 provisional because (i) Coulomb properly claims the benefit of the '626 provisional, (ii) the PCT application for which Coulomb is the national phase entry (PCT/EP2020/076906) was filed during the pendency of the '626 provisional, and (iii) the applications all share common inventors. OKTA-1005, codes (22), (60), (72); OKTA-1006, 1-7; OKTA-1015, codes (22), (30), (71)-(72). Moreover, the '626 provisional fully supports the Coulomb disclosures relied upon in this Petition. Accordingly, the discussion of Coulomb below includes parallel pin citations showing non-limiting examples of supporting subject matter descriptions in the '626 provisional. Because Coulomb incorporates the '626 provisional by reference, each of these parallel citations provides an independent basis to support the accompanying obviousness analysis.

4. The Makhotin-Coulomb Combination

A POSITA would have been prompted to apply in the context of Makhotin Coulomb's teachings to:

- include digital identification documents organized as part of an eID wallet along with the payment applications on Makhotin's portable communication device; and

- organize the digital identification documents of Coulomb and the payment application information of Makhotin as namespaces on the resulting device.

OKTA-1003, ¶¶116-126. Multiple reasons, taken individually or collectively, would have prompted a POSITA to apply Coulomb to Makhotin in such a manner.

First, such a modification would allow users “to have their documents accessible via their mobile communication device rather than carrying separate physical documents.” OKTA-1005, [0021]; OKTA-1006, 55. As Coulomb recognizes, “people often carry a mobile communication device and would prefer” to have such documents on their phone, including credentials issued by DMVs “universities, healthcare providers, financial institutions, utilities companies, airlines, etc.” OKTA-1005, [0020]-[0021]; OKTA-1006, 55. Such an application of Coulomb’s teachings to Makhotin would lead to the “user experience [being] improved” by carrying multiple types of digital cards on a single device. OKTA-1006, 55; *see also id.*, 9-10; OKTA-1005, [0022] (“convenience is improved by carrying a single device.”); OKTA-1003, ¶¶120, 104, 108-115.

Second, applying Coulomb’s teachings to Makhotin would expand the capabilities and utility of Makhotin’s system with minimal increases in overhead or complexity. OKTA-1003, ¶121. Makhotin already discloses storing, accessing, selecting, and otherwise utilizing multiple digital cards that include sensitive

identifying and payment information on a single mobile device, and integrating Coulomb's teachings would expand the capabilities of the resulting system by adding different types of cards, including identification cards, insurance cards, tickets, etc., to the payment cards already present in Makhotin. OKTA-1004, [0007]-[0011], [0046]; OKTA-1005, [0020]-[0024], [0073], [0124]; OKTA-1006, 18, 55, 58-59, 97-98.

Third, the Makhotin-Coulomb combination would have allowed payment cards of Makhotin and identification cards of Coulomb to be associated with "a confidence level." OKTA-1005, [0024]; *see also* OKTA-1006, 9-13, 32, 59-61, 100; OKTA-1003, ¶¶122-123. Doing so would permit the access/merchant device to select an electronic card with a higher confidence level to ensure data accuracy, while allowing the user device to "keep information up to date across many different issuers of information." OKTA-1005, [0024].

Fourth, the Makhotin-Coulomb combination would have allowed the identity and other credentials disclosed by Coulomb to be selected and utilized according to the security and selection protocols described in Makhotin, which would ensure that a given device reader (e.g., Makhotin's access device) is capable of processing the credential and that the required security protocols are implemented when accessing the credential. OKTA-1004, [0024], [0028]-[0029], [0041]-[0042]; OKTA-1003, ¶124. Digital identification documents, like payment cards, often have different

levels of security. OKTA-1003, ¶131. For example, security features for a student ID card may be less robust than for a passport or driver's license. As such, selection of identification cards according to a required security policy using Makhotin's approach is likewise applicable and beneficial to Coulomb's digital identification cards, which are analogous with respect to different security levels.

Fifth, Makhotin discloses storing electronic payment card information on a mobile device and Coulomb solves the rudimentary design problem of how to store such information by storing user information arranged as digital cards (e.g., Makhotin's payment applications) as namespaces. OKTA-1003, ¶¶125, 76-82. Such an implementation would simplify access to multiple credentials exhibiting identifier conflicts while allowing the designers to avoid developing a technique from scratch. OKTA-1003, ¶¶125, 77; OKTA-1005, [0058]-[0059]; OKTA-1006, 15; OKTA-1009, 7-9 (describing common use of namespaces to organize data items in eID wallets), 28, 55-57; OKTA-1016, ¶¶7-26. Furthermore, it provides a convenient, known framework for addressing and accessing each data item, using namespace data item tags to allow reader devices to unambiguously access the data items. OKTA-1003, ¶125, 118, 110-111.

Sixth, storing electronic cards using namespaces (as taught by Coulomb) would efficiently eliminate naming conflicts between data items of the different cards that share names (e.g., card holder name, address, birth date, etc.). OKTA-

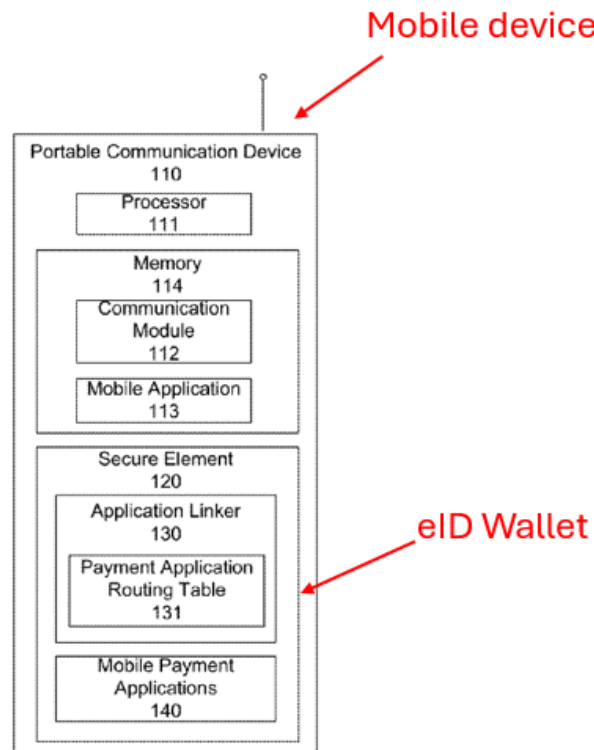
1003, ¶¶125, 77. This “allow[s] the verifier to request something specific” by making each field identifier “the same for all issuers,” ensuring consistency of information storage and retrieval across platforms. OKTA-1005, [0059]; OKTA-1006, 15-19; OKTA-1003, ¶119.

Seventh, a POSITA would have been prompted to combine Makhotin and Coulomb because doing so was the application of known techniques (Coulomb’s storage and access of identification credentials as namespaces in an eID wallet on a mobile device) to a known device (Makhotin’s portable communication device) ready for improvement to yield predictable results. *See KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007); OKTA-1003, ¶¶116-119. Both references disclose mobile devices containing digital representations of real-world cards containing sensitive personal information (including payment information) that allow for secure access of such information, and a POSITA would have had a reasonable expectation of success in making the proposed modifications without significantly altering or hindering the structure and function of Makhotin’s system. OKTA-1003, ¶¶125-126, 117. Indeed, Makhotin expressly contemplates that a POSITA would implement “[m]any variations of the invention” and Coulomb discloses such known and beneficial variations. OKTA-1004, [0154].

5. Application of Makhotin-Coulomb to Claims

Element [1.pre]

The Makhotin-Coulomb combination provides Element [1.pre] and renders obvious claim 1 as a whole. For example, Makhotin's system includes "a portable communication device 110" storing "multiple payment applications with multiple application identifiers (AIDs) pointing to or otherwise associated with these payment applications." OKTA-1004, [0058], [0007]-[0009] ("mobile NFC phones"); OKTA-1003, ¶¶96-103, 128-134.



OKTA-1004, FIG. 2 (partial).

"The payment applications *store payment information* associated with one or more consumer accounts." *Id.*, [0011]. Makhotin describes that "wallets and/or

other payment applications which are configured to collate and/or combine payment information may store multiple payment information.” *Id.*, [0104]. The “payment information” stored as part of each payment application includes ***identifying information*** for “a user or a consumer (e.g., name, billing address, residential address, date of birth, etc.)” in addition to payment credentials and account information. *Id.*, [0045]-[0046].

To a POSITA, the multiple payment applications of Makhotin that store identifying information (and other payment information) for the user, taken collectively, teach or suggest the ’103 patent’s claimed “electronic identification (eID) wallet.”³ OKTA-1003, ¶¶128-130; OKTA-1001, 1:11-20 (“electronic identification (eID), provides the ability to use mobile devices to store identification documents”); OKTA-1004, [0104] (“wallets”). The individual pieces of information stored by the payment applications teach or suggest the claimed “data items.” OKTA-1003, ¶130; OKTA-1004, [0011]-[0012], [0025], [0045].

In Makhotin’s disclosure, each payment application is also associated with one or more “security policies,” as claimed. OKTA-1003, ¶¶131, 103. For example, “each application identifier (AID) may have different authentication methods

³ As discussed at Element [1.1], *infra*, each individual payment application provides a namespace within the wallet.

associated with the processor.” OKTA-1004, [0041]. Such authentication methods can include “e.g., signature, online PIN, etc.” *Id.*, [0029]. “[A] particular application identifier may indicate that these payment applications require specific authentication methods (e.g., challenge response, password entry, etc.)” *Id.*, [0042]. Consistent with Makhotin, the ’103 patent expressly identifies different “required authentication protocol[s],” including required “digital signature[s],” as examples of the claimed “security policies.” OKTA-1001, 3:31-37, 1:43-49. Moreover, Makhotin’s “payment applications [can be] ***ranked by security*** and/or reliability of ***user authentication technique employed***.” OKTA-1004, [0028]. For example, the merchant access device can determine which payment application “provides the best fraud protection” or “most secure transaction environment.” *Id.*, [0024].

Coulomb’s teachings confirm that the Makhotin-Coulomb combination provides “data items stored in an electronic identification (eID) wallet on a mobile device,” as claimed.⁴ OKTA-1003, ¶¶132-134. Coulomb describes a mobile device executing “[a] wallet application” that is “loaded with several documents,” such as “a mobile driving license (mDL) 902, a first vehicle registration 910 for a first

⁴ Here, and elsewhere throughout the analysis of Ground 1A, Coulomb’s teachings provide an additional basis for addressing the ’103 patent’s claim elements, independent of the provided basis in Makhotin, which is also sufficient.

vehicle, a second vehicle registration 920 for a second vehicle, a first insurance policy,” etc. OKTA-1005, [0169], [0173], [0043]; OKTA-1006, 8-9, 18, 52, 96-100, 104.

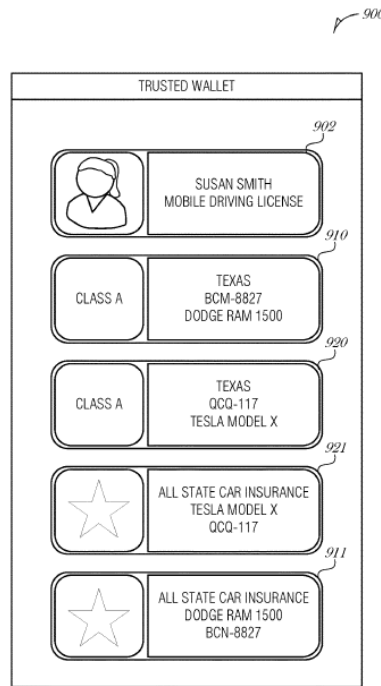


FIG. 9

OKTA-1005, FIG. 9; OKTA-1006, 52, 93; OKTA-1015, 9-10.

Coulomb’s wallet facilitates “an improved credential system that provides a portable, electronically verifiable, and aggregated credential. Identity credentials (e.g., documents, cards, mobile profiles, etc.) include information such as a first and last name, a date of birth, an address, etc.” OKTA-1005, [0024]; OKTA-1006, 9. As such, the Makhotin-Coulomb combination provides an eID wallet storing data items. OKTA-1003, ¶¶132-134.

In addition, a POSITA would have understood that the security management techniques for individual electronic cards stored on the mobile device of the Makhotin-Coulomb combination would have applied equally to the identity credentials disclosed by Coulomb and the payment applications disclosed in Makhotin. OKTA-1003, ¶¶134, 124. For example, both Makhotin and Coulomb disclose that their respective electronic cards are associated with security policies including authentication schemes, such as required digital signatures and PINs. OKTA-1004, [0024], [0028]-[0029], [0041]-[0042]; OKTA-1005, [0085], [0049], [0129], [0158]; OKTA-1006, 11, 15-17, 28, 99-100, 106.

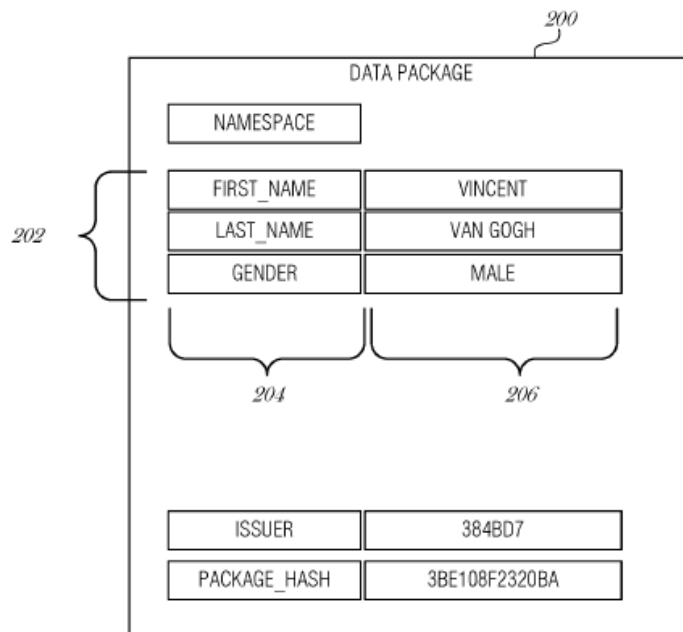
Element [1.1]

Each payment application on Makhotin's mobile device functions as the claimed "namespace." OKTA-1003, ¶¶135, 100, 116-118. While nominally referred to as "applications," Makhotin describes that "[t]he payment applications *store* payment information associated with one or more consumer accounts." OKTA-1004, [0010]-[0011] ("access device *supports* multiple application identifiers that are also *supported* by the portable communication device"), [0013]-[0014] ("...*supported* payment applications"). This "payment information" may include "payment credentials," "personal information associated with a user or a consumer (e.g., name, billing address, residential address, date of birth, etc.), account information," and "cardholder verification information." *Id.*, [0045]-[0046]. Each

application is associated with an “application identifier” for identifying the payment application and accessing the stored data of the payment application. *Id.*, [0007]-[0008], [0047], [0050], [0129]-[0134]. These payment applications therefore meet the ’103 patent’s “namespace” definition because each functions as “a symbolic mechanism for organizing and identifying pieces of data.” OKTA-1003, ¶¶135, 118; OKTA-1001, 1:25-30. Makhotin’s “application identifiers” are parallel to the ’103 patent’s “namespace identifier[s],” while Makhotin’s individual fields of information stored as part of each payment application (“e.g., name, billing address, residential address, date of birth, etc.”) are parallel to the ’103 patent’s namespace “local name[s].” OKTA-1003, ¶135; OKTA-1001, 1:25-30.

Coulomb confirms that the data items of the electronic cards (Makhotin’s payment applications and Coulomb’s credentials) are stored according to namespaces in the Makhotin-Coulomb combination. OKTA-1003, ¶¶136, 111-113, 119. Specifically, per Coulomb, “[d]ata elements from document types are ***defined in Namespaces***. Documents (credentials) correspond to database tables. Namespaces may include data elements for several kind of documents.” OKTA-1005, [0172], [0064] (“Tags stored in a package may refer to data elements from the same namespace”); OKTA-1006, 15-19, 88, 96-97. Coulomb is express that such credentials include “payment credentials” similar to the payment applications of Makhotin. OKTA-1005, [0073], [0057]. The namespaces “may be at the package

level” or “may be at the data element level.” OKTA-1005, [0059]; OKTA-1006, 15-19. “For instance, a namespace of ‘personal_info’ may be used for the tags ‘first_name’ and ‘last_name’ and be labeled as ‘personal_info:first_name’ and ‘personal_info:last_name.’” *Id.*



OKTA-1005, FIG. 2, *see also* FIGs. 3A-3D; OKTA-1006, 88; OKTA-1003, ¶136.

Makhotin also describes associating each payment application (namespace) with one or more “security policies,” as claimed. OKTA-1003, ¶¶137-138, 103. For example, “each application identifier (AID) may have different authentication methods associated with the processor.” OKTA-1004, [0041]. Such authentication methods can include “e.g., signature, online PIN, etc.” *Id.*, [0028]-[0029], [0024] (“...most secure transaction environment”). “[A] particular application identifier may indicate that these payment applications require specific authentication methods

(e.g., challenge response, password entry, etc.).” *Id.*, [0042]. The ’103 patent identifies different “required authentication protocol[s]” including required “digital signature[s]” as examples of the claimed “security policies.” OKTA-1001, 3:31-37, 1:43-49.

Returning to Makhotin, an “application linker” executing on the mobile device “may provide priorities or preferences associated with the list of application identifiers,” with the preferences based on “authentication techniques and reliability of particular payment applications (e.g., payment applications ranked by security and/or reliability of user authentication technique employed...).” OKTA-1004, [0028]. Makhotin’s security policies would have been equally applied to the identity credentials of Coulomb in the combination to keep sensitive identity information secure from intrusive parties and provide a basis for confidence. OKTA-1003, ¶¶138, 134, 124.

Element [1.2]

Makhotin’s “access device (e.g., POS terminal)” teaches or suggests the claimed “reader.” OKTA-1004, [0009]; OKTA-1003, ¶139. To start, Makhotin describes “*communication between an access device* and a plurality of payment applications on [the] *portable communication device*.” OKTA-1004, [0023], [0064] (“communication may occur between a contactless element of portable communication device 110 and an access device 150”). The access device includes

an “application selection module 153”—a reader module, as claimed—that “*determine[s] supported applications* from the list of available payment applications.” *Id.*, [0077].

For example, the access device (reader executing a reader module) can “select an application identifier and/or payment application using the associated application identifier, and use the selected application identifier to obtain payment information from the highest priority payment application that the access device supports.” OKTA-1004, [0026], [0024] (“selection of a supported payment application during a transaction according to the preferences and/or configuration details of an access device”). “The access device may then send a communication to the application linker [of the portable communication device] using the selected application identifier which may forward the request to a particular payment application associated with the selected application identifier.” *Id.*, [0036], [0050] (“selection message”). Makhotin also describes that the selection of the payment application (namespace) is for purposes of accessing a data item stored on the portable communication device—e.g., “[t]he selected application may then be selected for payment... and may provide the appropriate authentication and payment information to the access device for initiation of a transaction.” *Id.*; OKTA-1003, ¶139.

Makhotin is also clear that the selection of a payment application by the application selection module 153 of the access device is based on the security

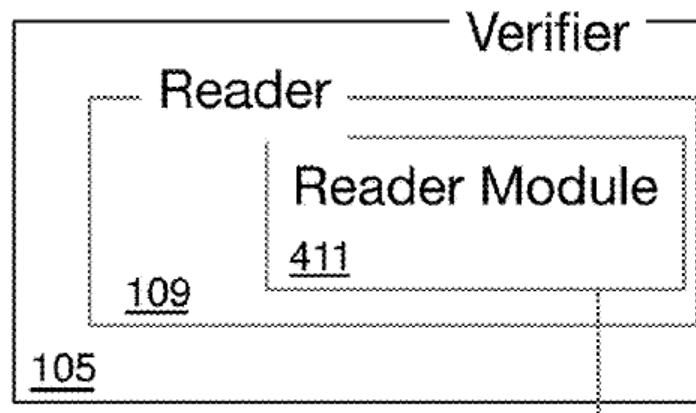
policies associated with the payment applications (namespaces). OKTA-1003, ¶¶140-142; OKTA-1004, [0041], [0028]-[0029] (“...ranked by security”), [0024] (“...provides the best fraud protection.”). For example, “the access device 150 may use *priority information* and/or preferences stored in the supported application information 153A to determine *a preferred application* for use in the transaction,” including based on “*authentication* and configuration options of the payment applications (*type of authentication and/or level of authentication* performed).” OKTA-1004, [0078]. Notably, “the application selection module 153 of the access device 150 may *use authentication processes*, configuration details of the payment applications, and any other relevant information to *identify a preferred payment application*.” *Id.*, [0127]; *see supra*, Elements [1.pre]-[1.1] (mapping Makhotin’s authentication schemes to the claimed “security policies”). Makhotin describes that the “priorities or preferences associated with the list of application identifiers” that are used by the access device to select a payment application “may be based on...*authentication techniques* and reliability of particular payment applications (e.g., payment applications ranked by *security and/or reliability of user authentication technique* employed[.]” OKTA-1004, [0028].

In another example, the access device rejects a payment application from the list of available applications that “may implement an authentication technique that is not supported by the access device (e.g., signature, online PIN, etc.).” OKTA-

1004, [0029], *see also*, [0024] (selection based on “best fraud protection, most rigorous authentication,” or “most secure transaction environment.”), [0032] (“...most robust consumer authentication.”), [0041]-[0042] (selection of payment application when “authentication processing is more rigorous and/or the fraud risk is lower.”). As would have been clear to a POSITA, such a security-policy-based selection would have been equally applied to Coulomb’s identity credentials in the combination to maintain security of sensitive information. OKTA-1003, ¶¶141, 138.

Elements [2.pre]-[2.1]

The ’103 patent states that “the reader 109’ and the verifier 105’ may be one machine.” OKTA-1001, 7:8-16, 8:45-51 (“...merged into one unit.”), 10:45-51. Figure 6a shows the reader integrated into the verifier:



OKTA-1001, FIG.6a (partial). Consistent with the ’103 patent, Makhotin’s access device (POS terminal) provides both the claimed reader and the claimed verifier terminal. OKTA-1003, ¶¶145-146. For example, Makhotin’s access device verifies that it supports a given payment application. OKTA-1004, [0029].

Makhotin's communication device transmits "a list of available application identifiers...to an access device so that the access device may select a supported payment application." OKTA-1004, [0034]-[0035], [0043], [0050], [0066]-[0067]. In this way, like the '103 patent, the application selection module 153 of Makhotin's access device provides the claimed verifier module (as well as the claimed reader module, per Element [1.2]). OKTA-1003, ¶147. The application selection module (verifier) receives the "list of the available payment applications from the portable communication device 110" via a communication module 152 of the access device. OKTA-1004, [0075]-[0077].

Element [2.2]

After receiving the list of payment applications, "[t]he application selection module 153 may determine supported applications from the list of available payment applications through any suitable manner," including by "compar[ing] application identifiers from the list of available payment applications to supported application information 153A present on the access device 150" which provides the claimed whitelisting. OKTA-1004, [0077], [0034], [0123]; OKTA-1003, ¶148. Additionally, Coulomb discloses that each namespace is "associated with a ***confidence level***" and the merchant device may specify "a minimum confidence level" for identity documents during selection. OKTA-1005, [0024], [0028], [0037], [0041]; OKTA-1006, 9-13, 32-33, 59-61, 105-107; OKTA-1003, ¶149.

Claim_[3]

Makhotin describes that in some scenarios, the access device “select[s] a payment application that provides the...most reliable transaction processing.” OKTA-1004, [0024], [0028] (“reliability of particular payment applications”). In another example, the access device (POS terminal) selects a payment application for which “the authentication processing is more rigorous and/or the fraud risk is lower for a particular payment application.” *Id.*, [0040]-[0041]. A POSITA would have recognized that each of these examples demonstrates selection of a namespace (payment application, per Element [1.1]) based on associated confidence. OKTA-1003, ¶¶151-153.

As an additional basis for finding obviousness, Coulomb discloses that each namespace is “associated with a confidence level, which informs about the relevance of the issuer for the issued data elements.” OKTA-1005, [0024], [0037], [0041]; OKTA-1006, 32-33; OKTA-1003, ¶154. “For example, a minimum confidence level may be specified for data elements from identity documents.” OKTA-1005, [0028]; OKTA-1006, 32-33, 105-107. When requesting a data element of a particular payment application (namespace, per Element [1.1]) the requesting device (e.g., Makhotin’s access device) “may also specify a minimum level of assurance required for the requested data elements” to ensure that the received information “match[es] the target confidence level.” OKTA-1005, [0047], [0149], [0150]-

[0152], [0178]-[0182], Cls. 5-11; OKTA-1006, 11-13, 24, 32-33, 60, 105-107. In the Makhotin-Coulomb combination, a POSITA would have applied Coulomb's teachings by configuring Makhotin's access device to use confidence levels in namespace selection, thereby increasing the accuracy/reliability of the received information. OKTA-1003, ¶154.

Element [4.1]

The information items stored as part of the multiple payment applications of Makhotin teach or suggest the claimed "data items." *Supra*, Elements [1.pre], [1.2]; OKTA-1003, ¶¶130, 134, 159; OKTA-1004, [0045]-[0046]. "[T]he payment applications, and the corresponding payment information [are] provisioned or otherwise stored on a secure element or other secure storage trusted execution environment of a portable communication device." OKTA-1004, [0025], [0037], [0045], [0066]-[0068], [0086]. Furthermore, "[t]he secure element 120 may include a secure memory" and be "hardware, software, or a combination of hardware and software." *Id.*, [0065], [0081], [0146]-[0147]; *see also* OKTA-1005, [0172], [0063]-[0066] (describing storing data items organized by namespace), [0058]-[0059], [0220]; OKTA-1006, 15-19, 39-41, 88, 96-97; OKTA-1003, ¶¶158-159.

Makhotin describes that "preferences and/or priority information [is] stored at the application linker" and this information includes "authentication techniques and reliability of particular payment applications," such as "security" of the

authentication technique for each payment application. OKTA-1004, [0030], [0066]-[0067] (“application linker” stored as part of “secure element 120”).

The “application identifiers” are also stored on the portable communication device. OKTA-1004, [0035], [0094] (“on a secure element”), [0095]-[0110], Figure 3. “[A] particular application identifier may indicate that these payment applications require specific authentication methods (e.g., challenge response, password entry, etc.),” thereby teaching that the association of security policies and namespaces (Makhotin’s payment applications, per Element [1.1]) is stored in hardware memory of the portable communication device. *Id.*, [0042]; OKTA-1003, ¶¶160-161. Makhotin’s “application identifier[s] may also include additional information including...any other relevant information” for a payment application. OKTA-1004, [0038], [0047], [0067], [0075], [0122]. As discussed at claim 1, *supra*, the relevant information for selecting a supported payment application includes the associated security policies for the payment applications. OKTA-1004, [0041]-[0041], [0028]-[0029], [0024]; OKTA-1003, ¶¶161, 137-138.

Element [4.2]

Makhotin’s “portable communication device compris[es] a processor and a computer-readable medium coupled to the processor.” OKTA-1004, [0012], [0147], [0153]. Makhotin also describes how “an application linker [on the portable communication device] may provide a list of available application identifiers

provisioned on the portable communication device to an access device so that the access device may select a supported payment application.” OKTA-1004, [0034]-[0035], [0050], [0066]-[0067]. The “application linker” is stored as part of “secure element 120” on the portable communication device. *Id.* [0066]-[0067]. Makhotin’s access device provides the claimed verifier terminal. *Supra*, Elements [2.pre]-[2.1]; OKTA-1003, ¶¶162, 145-146.

Furthermore, the information provided to the access device by the portable communication device includes both the supported namespaces and the associated security policies. OKTA-1003, ¶¶163-164. For example, the “application identifier[s] may indicate that these payment applications require specific authentication methods.” OKTA-1004, [0042]. “The application identifier may also include additional information including...any other relevant information” for a payment application. OKTA-1004, [0038], [0047], [0067], [0075]. “[T]he application linker 130 generates and sends a list of available payment applications to the access device 150. The list of available payment applications may include application identifiers associated with the available payment applications as well as any other relevant information to an access device 150 for determining supported payment applications and selecting a supported payment application.” *Id.*, [0122]. As discussed at claim 1, *supra*, the relevant information for selecting a supported payment application includes the associated security policies for the payment

applications. OKTA-1004, [0041]-[0041], [0028]-[0029], [0024]; OKTA-1003, ¶¶163, 137-138.

Claim [6]

Makhotin's application linker "generates and sends a list of available payment applications to the access device 150" including "application identifiers" and "any other relevant information." OKTA-1004, [0122]. When generating this list, "the application linker module 130 may ***filter*** and/or qualify those application identifiers provided to in the list of available payment applications to ***only include application identifiers associated with those payment applications that may be used in a transaction.***" *Id.*, [0088]. This filtering is based on user selection. OKTA-1003, ¶¶165-168. More specifically, "a consumer may select the default or active mobile payment application for use in transactions." OKTA-1004, [0089]. "For example, a consumer may activate a single payment application before approaching an access device 150 and the available application identifiers [plural] may be those application identifiers associated with the active payment application" and "the application linker module 130 may determine application identifiers associated with an active payment application on the portable communication device 110 and may not report unavailable payment applications to the access device 150." *Id.*, [0090]. In another example, the "consumer sets a limit of the top 3 payment applications [to] be presented to the access device 150." *Id.*, [0092].

Claim_[7]

See Element [4.2]. OKTA-1003, ¶¶169-173, 162-163. Makhotin's access device provides both the claimed reader and the claimed verifier terminal (*supra*, Elements [2.pre]-[2.1]).

Elements_[8.pre]-[8.1]

Makhotin discloses that messages are exchanged using SSL protocol, which includes messages transmitted as a sequence of bytes having bits. OKTA-1004, [0112], [0122], OKTA-1003, ¶¶178-180 (citing Internet RFC 2246 (OKTA-1012)), 43-46, 61. For example, Makhotin describes that messages are sent between the devices "using a secure encryption method (e.g., 128-bit SSL or equivalent)." OKTA-1004, [0122]. The SSL protocol specifies that "[t]he basic data block size is one byte (i.e. 8 bits)" and that hash and encryption information is communicated in byte streams. OKTA-1012, 6, 10-15; OKTA-1003, ¶¶45, 176-178; OKTA-1016, ¶¶27-29. This includes required HASH type and encryption type. *Id.*

Furthermore, a POSITA would have understood that communications between digital computing devices such as those described in Makhotin are transmitted as a sequence of bytes having bits. OKTA-1003, ¶¶85-95, 177; OKTA-1012, 6; OKTA-1013, 146, 448; OKTA-1014. Additionally, Makhotin describes that each application identifier is a character string. OKTA-1004, [0047] (describing a "standardized" application identifier with an example of "A000000031010"). A

POSITA would have recognized that a character string is a sequence of bytes having bits that convey information. OKTA-1003, ¶¶182, 90-91; OKTA-1014; OKTA-1013, 446-447. Additionally, the “‘application identifier’ may include ...information about an application on the device” including information on “specific authentication methods (e.g., challenge response, password entry, etc.)” for the application. OKTA-1004, [0047], [0042]. A POSITA would have recognized that bits included in the application identifiers identifying the challenge response denote secure messaging options. OKTA-1003, ¶¶181-182. Makhotin also discloses that the required authentication/security policies can include an indication of required signature authentication, which are bit values denoting a required signature scheme. OKTA-1004, [0029], [0041], [0046]; OKTA-1003, ¶181.

Element [8.2]

As addressed with respect to claim 1, *supra*, the “challenge response” and “signature” requirement security policies discussed with respect to element [8.1] are examples of the security policies associated with the plurality of supported namespaces (payment applications) on Makhotin’s portable communication device. OKTA-1003, ¶¶183-184; OKTA-1004, [0029], [0041]-[0042], [0046]. For example, “each application identifier (AID) may have different authentication methods associated with the processor” including “challenge response” security requirements. OKTA-1004, [0041]-[0042], [0028]-[0029] (“signature, online PIN”).

Claim [9]

Makhotin discloses that the payment applications (namespaces, per Element [1.1]) require different “authentication techniques” and gives examples of “signature, online PIN, etc.” OKTA-1004, [0028]-[0029], [0041] (“some payment processing networks may use *signature authentication*... [or] *PIN for account holder verification*.”), [0046] (“authentication process for transaction processing (e.g., online PIN, signature, etc.)”). A POSITA would have recognized that these disclosures of “signature authentication” are a “digital signature” authentication requirement while requiring a “PIN” provides the claimed “user consent.” OKTA-1003, ¶187. As another example, “a particular application identifier may indicate that these payment applications require specific authentication methods (e.g., challenge response, password entry, etc.)” OKTA-1004, [0042]. Furthermore, “[a]n authorization request message may be protected using a secure encryption method (e.g., 128-bit SSL or equivalent) in order to prevent data from being compromised,” which again indicates secure messaging. OKTA-1004, [0112]. These are both examples of secure messaging. OKTA-1003, ¶187.

As an additional basis for finding obviousness, Coulomb discloses that the information packages can have an associated “digital signature or equivalent (e.g., message authentication code (MAC), crypto checksum, etc.)” OKTA-1005, [0085], [0129], [0205]; OKTA-1006, 22, 29, 32, 36-37, 47. Application of this teaching to

Makhotin would have resulted in increased security for the information exchanged in the resulting system, such as by “ensur[ing] the application will not connect to a malicious site or address.” OKTA-1005, [0205] OKTA-1003, ¶188.

Claim_[10]

As discussed at Element [2.2], Makhotin demonstrates that the access device (reader) “selects a namespace to access a data item from the plurality of supported namespaces on the mobile device based on a whitelist of namespaces...,” as claimed. OKTA-1003, ¶¶192, 148; OKTA-1004, [0077], [0034], [0123].

B. [GROUND 1B]: Makhotin-Coulomb-Ahn Renders Claim 5 Obvious

1. Ahn (OKTA-1008)

Ahn describes a “user device 12” having “information card storage 24” in which “user identities are digitally represented in the form of information cards.” OKTA-1008, 6:57-7:25; OKTA-1003, ¶¶194-198.

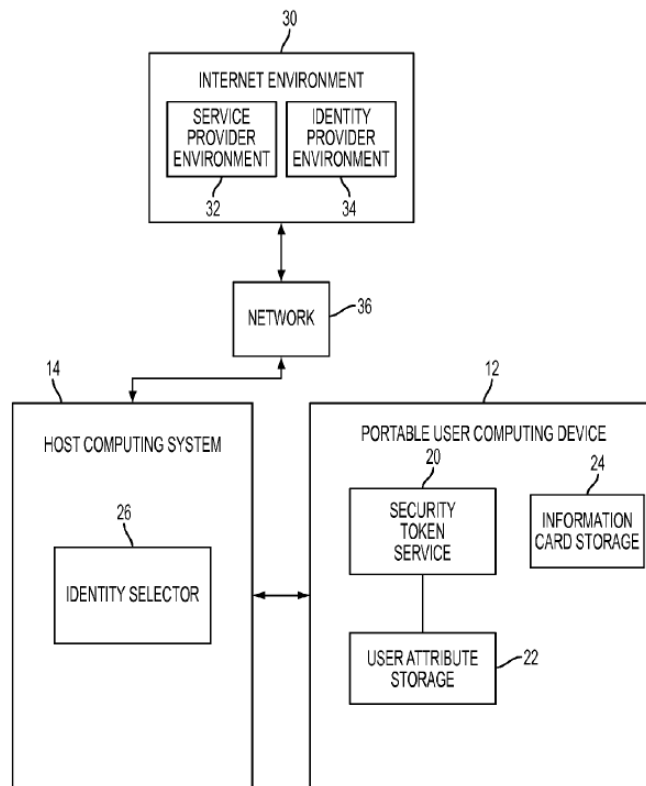


FIG. 1

OKTA-1008, FIG. 1.

“Each information card represents the user’s identity in different contexts and contains references to different subsets of user attributes.” *Id.*, 7:34-41. A “security policy governs the authentication process and specifies the identity requirements required by the relying party to first authenticate the user's identity and then to authorize access.” *Id.*, 10:51-61. Subsequently the identity selector of the host system “determines which information cards within its domain of operation satisfy the identity requirements of the security policy.” *Id.*, 10:62-11:8. “The identity selector then displays the information cards that are determined to satisfy the security

policy.” *Id.*, 11:39-48. “The user then selects one of the information cards that are presented.” *Id.* The identity selector then sends a token request to the user device which returns a security token containing the desired user attribute information. *Id.*, 11:49-65.

2. The Makhotin-Coulomb-Ahn Combination

A POSITA would have predictably applied the teachings of Ahn to Makhotin-Coulomb such that, in scenarios where the access device supports more than one payment application (e.g., can satisfy the security requirements), the access device “displays the [payment applications] that are determined to satisfy the security policy” to allow user selection of a supported payment application. OKTA-1008, 11:39-65; OKTA-1003, ¶¶199-204.

Multiple reasons would have prompted a POSITA to apply Ahn to Makhotin-Coulomb in such a manner. First, displaying the supported payment applications (and/or identification cards of Coulomb) would allow the user to select a preferred card. OKTA-1003, ¶200. For example, the user could select a payment card with the best interest rate, preferred rewards, the lowest current balance, or the most accurate information. *Id.*

Second, such a modification would allow users to select a different card for different scenarios without having to change settings prior to each interaction. OKTA-1003, ¶201. By presenting the eligible cards at the time of the transaction,

users would be able to select a preferred card without having to enter a settings menu to change the “default settings associated with the payment applications.” OKTA-1004, [0028]-[0029]; OKTA-1003, ¶201.

Third, such a modification would allow an employee of the merchant to select a preferred card, such as a card that has the lowest transaction fee/overhead for the merchant, a card provided by or otherwise affiliated with the merchant, or an identification card believed to be most accurate. OKTA-1003, ¶202.

Fourth, such a modification was the application of known techniques (Ahn’s displaying of electronic cards on a merchant device for selection) to a known system ready for improvement to yield predictable results. OKTA-1003, ¶¶199, 203. A POSITA would have had a reasonable expectation of success in making the proposed modifications without significantly altering or hindering the structure and function of Makhotin’s system. OKTA-1003, ¶¶203-204; OKTA-1004, [0154].

3. Application of Makhotin-Coulomb-Ahn to Claims

Elements_[5.pre]-[5.1]

See Ground 1A, Elements [2.pre]-[2.1]. OKTA-1003, ¶¶206-207.

Element_[5.2]

Makhotin’s access device provides the claimed verifier terminal. *See* Ground 1A, Element [2.1]. Ahn demonstrates that in the Makhotin-Coulomb-Ahn combination, after determining which “information cards...satisfy the security

policy,” the “identity selector then *displays the information cards that are determined to satisfy the security policy*” and “[t]he user then selects one of the information cards that are presented.” OKTA-1008, 11:39-48, 7:19-25, 7:34-41, 9:41-52, 10:24-32 (“...displays a set of Information Card icons from which the user selects”), FIG. 7; OKTA-1004, [0114] (describing display functionality of Makhotin’s access device), [0091]; OKTA-1005, [0227]; OKTA-1003, ¶¶208-213.

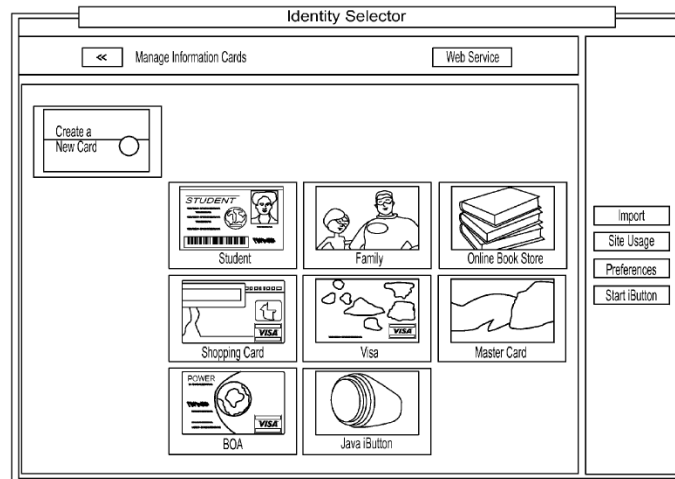


FIG. 5

OKTA-1008, FIG. 5.

C. [GROUND 1C]: Makhotin-Coulomb-Sharma Renders Claim 16 Obvious

1. Sharma (OKTA-1007)

Sharma discloses a system “to provide payment capabilities using contactless communication” between “a merchant access device (e.g., POS terminal)” and a mobile device having one or more digital wallets. OKTA-1007, [0002], [0027], [0034]-[0036]. Sharma discloses various techniques “to limit the use of the

untrusted account credentials.” *Id.*, [0028]. The merchant access device (POS terminal) can select payment applications according to priority, such as based on “transaction security.” *Id.*, [0053]; OKTA-1003, ¶¶215-119.

Sharma further discloses that the access device provides information to the mobile device storing the payment applications to “allow the mobile device 110 to determine whether the access device 120 is configured to process the type of transaction that is associated with the selected account.” OKTA-1007, [0082]. This information allows “the mobile application [to] validate[] that the access device 120 is authorized to access the account credentials associated with the selected UAIDs” and “supports the TPO of the UAID that is selected.” *Id.*, [0129]-[0131]. In Sharma, “UAID” stands for “untrusted applet identifier” and TPO stands for “terminal processing options.” *Id.*, [0031], [0080].

2. The Makhotin-Coulomb-Sharma Combination

Makhotin discloses that the access device determines if it is “capable of processing” payment information for a given payment application, including determining if the payment application requires “an authentication technique that is not supported by the access device (e.g., signature, online PIN, etc.).” OKTA-1004, [0028]-[0029], [0078], [0127]. A POSITA would have predictably applied the teachings of Sharma to Makhotin such that upon selecting a payment application for which the access device can support the required security policy, the access device

provides information to the mobile device to demonstrate that the access device can satisfy the associated security policy. OKTA-1007, [0082], [0129]-[0131]; OKTA-1003, ¶¶219-225.

Multiple reasons would have prompted a POSITA to apply Sharma to Makhotin-Coulomb in such a manner. First, such a modification would allow the mobile device to have confidence that the access device can satisfy the security requirements for the provided information (e.g., that the access device can be trusted), thereby increasing overall security for the system. OKTA-1003, ¶222.

Second, providing information that allows “the mobile application [to] validate[] that the access device [] is authorized to access the account credentials associated with the selected UIDs” and “supports the TPO of the UID that is selected” would have resulted in a system that saves time and communication bandwidth by avoiding the initiation of payment processes or other information access processes for which the access device is unequipped. OKTA-1007, [0129]-[0131]; OKTA-1003, ¶223.

Third, the proposed modification was the application of known techniques (Sharma’s demonstration of satisfaction of security policies for accessing data items) to a known system ready for improvement to yield predictable results. OKTA-1003, ¶224. A POSITA would have had a reasonable expectation of success in making the

proposed modifications without significantly altering or hindering the structure and function of Makhotin's system. OKTA-1003, ¶224; OKTA-1004, [0154].

3. Application of Makhotin-Coulomb-Sharma to Claims

Element [16.pre]

See Ground 1A, Element [1.pre].

Element [16.1]

See Ground 1A, Element [1.1].

Element [16.2]

See Ground 1A, Elements [4.2], [6.1], [7]. Furthermore, Makhotin's access device 150 communicates with a merchant computer 160 and functionality ascribed to either can be performed by the other. OKTA-1004, [0062], [0111]-[0114], [0143]-[0155]. Makhotin therefore provides a reader connected to a verifier, and it would have been obvious for any functionality ascribed to the access device 150 to be performed by the merchant computer 160. OKTA-1003, ¶¶229-231.

Element [16.3]

See Ground 1A, Element [1.2]. For example, Makhotin's "access device may analyze the list of payment application priorities and may determine if the access device supports each application identifier" and then "select the application identifier associated with" the highest priority for which the access device supports the application identifier. OKTA-1004, [0029]. The access device then "send[s] a

selection command to the application linker of the portable communication device requesting payment information from the payment application associated the application identifier.” *Id.*, [0030], [0036]; OKTA-1003, ¶¶232-234.

Element [16.4]

See Ground 1A, Elements [4.2], [7]. Additionally, Makhotin discloses that at least some of the information for a security policy associated with a candidate namespace (payment application/ID card, per Element [1.1]) is payment information provided upon selection of a given payment application identifier. OKTA-1003, ¶¶235-236. “For example, payment information may include...***card verification value (CVV)***, etc.),...***authentication process for transaction processing (e.g., online PIN, signature, etc.)***.” OKTA-1004, [0046], [0056]. Makhotin’s mobile device returns “the appropriate authentication and payment information to the access device for initiation of a transaction” in response to receiving the selection communication from the access device. *Id.*, [0036], [0059], [0079]-[0080].

Element [16.5.1]

Makhotin’s access devices determines if it “is not capable of processing” payment information for a given payment application, such as by determining if the payment information requires “an authentication technique that is not supported by the access device (e.g., signature, online PIN, etc.).” OKTA-1004, [0029], [0078]; OKTA-1003, ¶237.

Sharma similarly discloses that “depending on the type of credentials selected, different security levels for the transaction may exist.” OKTA-1007, [0082]. The access device/terminal has associated “Transaction Processing Options (TPO)” that “may include a TPO indicator that indicates which transaction data types the access device 120 supports.” *Id.*, [0081]; OKTA-1003, ¶238.

Element [16.5.2]

Makhotin’s access device selects the highest priority application that “the access device 150 supports” such as based on security policy (required authentication). OKTA-1004, [0078]. For example, if a payment application “implement[s] an authentication technique that is not supported by the access device,” the access device selects the highest priority application that is supported. *Id.*, [0029], [0078]; OKTA-1003, ¶¶239-240. This selection is to access a data item stored on the mobile device (*supra*, Element [1.2]). OKTA-1003, ¶¶240, 139.

The Makhotin-Coulomb-Sharma combination further provides demonstrating satisfaction of the security policy to the mobile device. OKTA-1003, ¶241. Sharma discloses “the mobile application may also request access device configuration information (also referred to as “transaction processing options” (*TPO*)) ***from the merchant access device 120 to determine what processing options the merchant access device supports.***” OKTA-1007, [0125]. The access device “send[s] a “GPO Request” with the MID and the TPO that are supported back to the

mobile application 112. The TPO may include a bitmask of access device 120 supported contactless payment options.” *Id.*, [0126]. Sharma discloses that “the TPO (also referred to as access device configuration options) allow the mobile device 110 to determine whether the access device 120 is configured to process the type of transaction that is associated with the selected account applet.” *Id.*, [0082], *see also*, [0129]-[0131]. A POSITA would have recognized that such supported processing options for the payment applications would have included the required security protocols in the resulting combination. OKTA-1003, ¶241.

Element_[16.5.3]

Sharma discloses that “if the TPO indicates that... the UAID transaction data is not supported by the merchant access device” the response “sent to the merchant access device 120 includ[es] an error code” rather than providing access to the payment information (data items). OKTA-1007, [0131]. As another example, if “the access device 120 is not configured to process those types of transactions, an error would occur and the transaction would be terminated.” *Id.*, [0130]-[0132]; OKTA-1003, ¶¶242-243.

Furthermore, Makhotin discloses that if the access device determines that a payment application (namespace) requires “an authentication technique that is not supported by the access device (e.g., signature, online PIN, etc.),” that payment

application (namespace) is not selected (i.e., rejects access to the data item). OKTA-1004, [0029]; OKTA-1003, ¶244.

Element [16.5.4]

Sharma discloses that “the mobile application 112 checks both that the MID is valid and that the TPO from the merchant access device 120 support the type of transaction data associated with the applet of the UAID.” OKTA-1007, [0131]. If the TPO indicates that it can satisfy the required security policy scheme, “the merchant access device 120 receives an appropriate ‘GPO Response’ from the mobile application and the transaction is processed.” *Id.*, [0133], [0127]; *see also* OKTA-1004, [0036], [0050]; OKTA-1003, ¶¶245-247.

D. [GROUND 2A]: Jones-Coulomb Renders Claims 1-4, 6-10 Obvious

1. Jones (OKTA-1010)

Jones describes “a mobile phone...hav[ing] various card data (e.g., debit card, credit card, etc.) provisioned into multiple payment applications which may be identified by application identifiers (AIDs).” OKTA-1010, [0026]. Each “payment application...store[s] and provide[s] payment information for a transaction.” *Id.*, [0035]. “‘Payment information’ may include any data that may be used to identify an account and use the account for a payment transaction” including “personal information associated with a user or a consumer (e.g., name, billing address, residential address, date of birth, etc.), account information.” *Id.*, [0046]. The

payment credentials are arranged as a “mobile wallet.” *Id.*, [0028]; OKTA-1003, ¶¶248-252.

The mobile phone provides “a list of AIDs...to a POS terminal to allow for the POS terminal to...select a payment application that the POS terminal supports and is configured to process transactions with based on the received AIDs.” OKTA-1010, [0026]. In some cases, “[w]here multiple AIDs are supported, the POS terminal may select multiple AIDs such that multiple transaction payloads can be prepared.” *Id.*

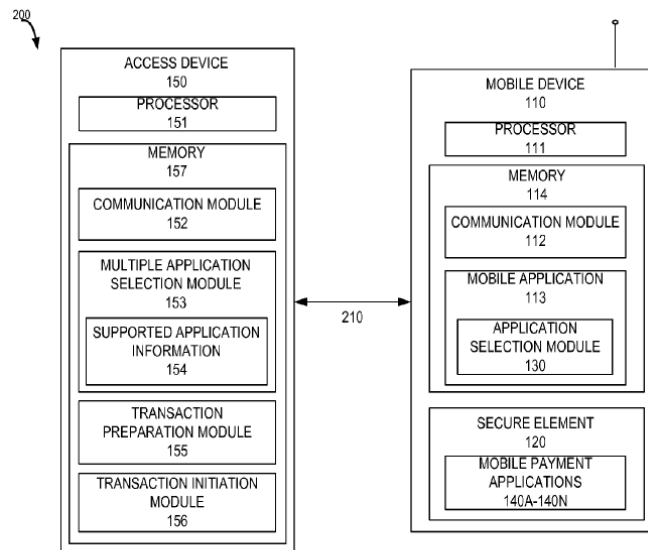


FIG. 2

OKTA-1010, FIG. 2.

Jones discloses that “the POS may determine a preferred application for processing the transaction based on a priority order of the supported AIDs.” *Id.*, [0028]. The priority can be determined based on “transaction security.” *Id.*, [0040].

2. Jones-Coulomb Combination

A POSITA would have been prompted to apply in the context of Jones Coulomb's teachings to:

- include digital identification documents organized as part of an eID wallet along with the payment applications on Jones's mobile device; and
- organize the digital identification documents of Coulomb and the payment application information of Jones as namespaces on the resulting device.

OKTA-1003, ¶¶254-264. Multiple reasons, taken individually or collectively, would have prompted a POSITA to apply Coulomb to Jones in such a manner.

First, such a modification would allow users "to have their documents accessible via their mobile communication device rather than carrying separate physical documents." OKTA-1005, [0021]; OKTA-1006, 55. "[P]eople often carry a mobile communication device and would prefer" to have such documents, including official credentials, on their phone. OKTA-1005, [0020]-[0021]; OKTA-1006, 55. Applying Coulomb's teachings to Jones would achieve this desirable result and thus lead to the "user experience [being] improved." OKTA-1006, 55; *see also id.*, 9-10; OKTA-1005, [0022] ("convenience is improved by carrying a single device."); OKTA-1003, ¶¶258, 108-115.

Second, such a modification would expand the capabilities of Jones's system with minimal increases in overhead or complexity. OKTA-1003, ¶259. Jones already discloses storing, accessing, selecting, and otherwise utilizing multiple digital cards that include sensitive identifying and payment information on a single mobile device. OKTA-1010, [0025]-[0030], [0036]. Applying Coulomb's teachings to Jones would expand the capabilities of the resulting system by adding additional types of cards, including identification cards, thereby increasing overall utility. OKTA-1005, [0020]-[0024], [0073], [0124]; OKTA-1006, 18, 55, 58-59, 97-98; OKTA-1003, ¶259.

Third, the Jones-Coulomb combination would have allowed payment cards of Jones and identification cards of Coulomb to associate "a confidence level, which informs about the relevance of the issuer for the issued data elements" with each card while "keep[ing] information up to date across many different issuers of information." OKTA-1005, [0024]; OKTA-1006, 9-13, 32, 59-61, 100; OKTA-1003, ¶¶260-261.

Fourth, the Jones-Coulomb combination would have allowed the identity and other credentials disclosed by Coulomb to be selected and utilized according to the security and selection protocols described in Jones, which would ensure that a given device reader (Jones's access device) is capable of processing the credential and that the required security protocols are implemented when accessing the credential.

OKTA-1010, [0040], [0104]-[0105]; OKTA-1003, ¶¶262. Implementation of Jones's security protocol-based selection to Coulomb's identity credentials would ensure that sensitive information of the identity credentials remains secure.

Fifth, organization of the digital cards as namespaces "allow[s] the verifier to request something specific" by making each field identifier "the same for all issuers" thus ensuring consistency of information storage and retrieval across platforms. OKTA-1005, [0059]; OKTA-1006, 15-19; OKTA-1003, ¶¶256-257, 110, 77.

Sixth, Jones discloses storing electronic payment card information on a mobile device and Coulomb solves the rudimentary design problem of how to store such information by storing user information arranged as digital cards (e.g., Jones's payment applications) as namespaces. OKTA-1003, ¶¶263, 76-82; OKTA-1005, [0058]-[0059]; OKTA-1006, 15. Such an implementation would have saved both time and money. *Id.* Furthermore, it provides a convenient, known framework for addressing and accessing each data item via namespace data item tags. *Id.*

Seventh, such a modification is simply application of known techniques (Coulomb's storage and access of identification credentials as namespaces in an eID wallet on a mobile device) to a known device (Jones's mobile device) ready for improvement to yield predictable results. *KSR*, 550 U.S., 417; OKTA-1003, ¶¶254-256, 264. Both references disclose mobile devices containing digital representations of real-world cards containing sensitive personal information (including payment

information) that allow for secure access of such information and a POSITA would have had a reasonable expectation of success in making the proposed modifications without significantly altering or hindering the structure and function of Jones's system. OKTA-1003, ¶¶255, 264; OKTA-1010, [0187] (“[m]any variations”).

3. Application of Jones-Coulomb to Claims

Element [1.pre]

The Jones-Coulomb combination provides Element [1.pre] and renders obvious claim 1 as a whole. For example, Jones's system includes “a mobile phone...hav[ing] various card data (e.g., debit card, credit card, etc.) provisioned into multiple payment applications which may be identified by application identifiers (AIDs).” OKTA-1010, [0026]; OKTA-1003, ¶¶266-271.

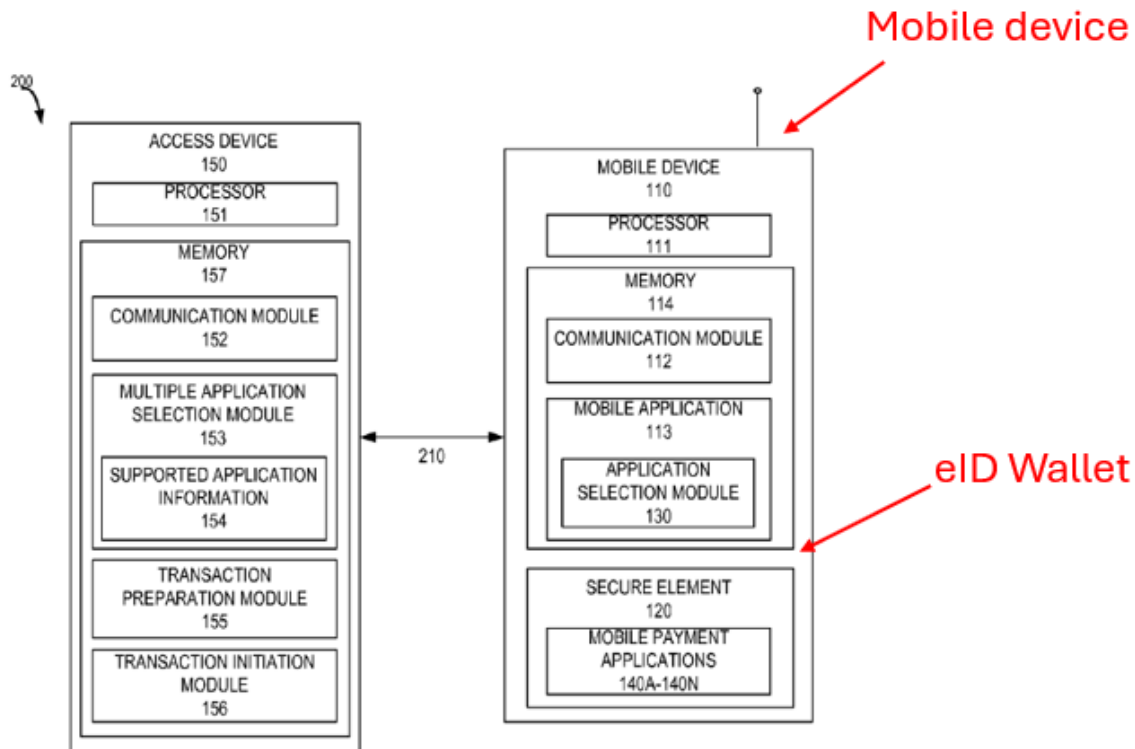


FIG. 2

OKTA-1010, FIG. 2.

The payment applications store “payment information,” which includes payment credentials and “personal information associated with a user or a consumer (e.g., name, billing address, residential address, date of birth, etc.).” *Id.*, [0035], [0046]. The payment credentials are arranged as a “mobile wallet.” *Id.*, [0028].

A POSITA would have recognized that the “mobile wallet” storing “various card data” including personal identification information for the user teaches or suggests the ’103 patent’s claimed “electronic identification (eID) wallet.” OKTA-1003, ¶¶267-268; OKTA-1001, 1:11-20. The individual fields of information stored

by each payment application on the mobile device teach or suggest the claimed “data items.” OKTA-1003, ¶268; OKTA-1010, [0035], [0046].

Each payment application is also associated with one or more “security policies,” as claimed. OKTA-1003, ¶269. For example, Jones’s access device determines “transaction security” for each payment application, including “applications that require a high level of authentication” and payment applications associated with “payment networks [having] a better security track-record.” OKTA-1010, [0040], [0047] (“signature”), [0105] “an online PIN” requirement provides “a higher level of security.”), [0104] (“CVMs associated with the AID.”). Like Jones, the ’103 patent identifies different “required authentication protocol[s]” including required “digital signature[s]” as examples of “security policies.” OKTA-1001, 3:31-37, 1:43-49.

Coulomb’s teachings confirm that the data items stored on the mobile device of the resulting Jones-Coulomb combination are stored in an eID wallet.⁵ OKTA-1003, ¶¶270-271, 132-133. Coulomb describes a mobile device executing “[a] wallet application” that is “loaded with several documents” such as “a mobile

⁵ Here, and elsewhere throughout the analysis of Ground 2A, Coulomb’s teachings provide an additional basis for addressing the ’103 patent’s claim elements, independent of the provided basis in Jones, which is also sufficient.

driving license (mDL) 902,” etc. OKTA-1005, [0169]; OKTA-1006, 8-9, 18, 52, 96-100.

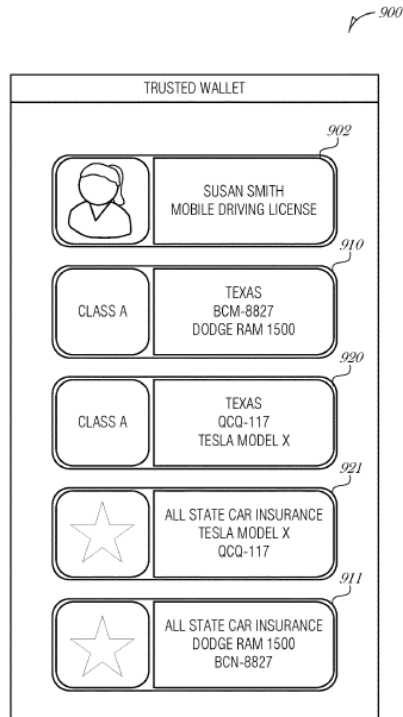


FIG. 9

OKTA-1005, FIG. 9; OKTA-1006, 52, 93; OKTA-1015, 9-10. This wallet provides “an improved credential system that provides a portable, electronically verifiable, and aggregated credential. Identity credentials (e.g., documents, cards, mobile profiles, etc.) include information such as a first and last name, a date of birth, an address, etc.” *Id.*, [0024]; OKTA-1006, 9. In addition, a POSITA would have understood that the security management techniques of Jones for individual electronic cards would have applied equally to Coulomb’s identity credentials to

ensure security of that sensitive information. OKTA-1003, ¶271; OKTA-1005, [0085], [0049], [0129], [0158] (Coulomb’s identification cards associated with security policies); OKTA-1006, 11, 15-17, 28, 99-100, 106.

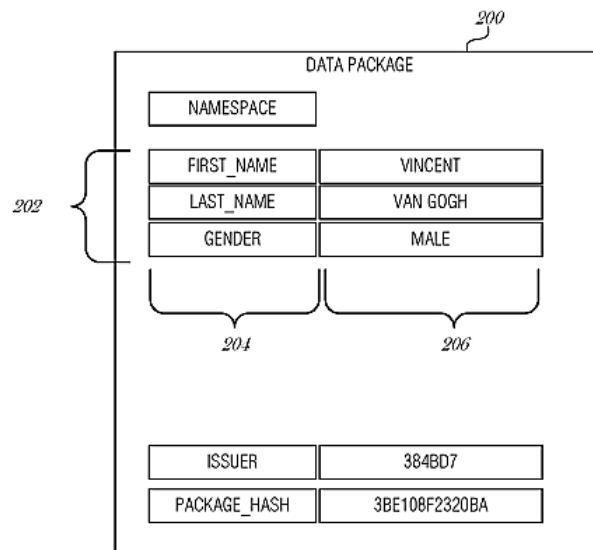
Element [1.1]

The payment applications stored on Jones’s mobile device function as the claimed “namespaces.” OKTA-1003, ¶272. The payment applications store “payment information” which includes payment credentials and “personal information associated with a user or a consumer (e.g., name, billing address, residential address, date of birth, etc.).” *Id.*, [0035], [0046], [0028]-[0030] (“...***supported*** payment applications”), [0072]. The payment applications therefore meet the ’103 patent’s “namespace” definition because each payment application functions as “a symbolic mechanism for organizing and identifying pieces of data.” OKTA-1003, ¶272; OKTA-1001, 1:25-30. Jones’s “application identifiers (AIDs)” are parallel to the ’103 patent’s “namespace identifier[s],” while Jones’s individual fields of information within each payment application are parallel to the ’103 patent’s namespace “local name[s].” OKTA-1003, ¶272; OKTA-1001, 1:25-30.

Additionally, Coulomb confirms that the data items of the electronic cards (Jones’s payment applications and Coulomb’s credentials) are stored according to namespaces. OKTA-1003, ¶¶273, 111-113. Coulomb describes that each of the “[i]dentity credentials (e.g., documents, cards, mobile profiles, etc.) include

information such as a first and last name, a date of birth, an address, etc.” OKTA-1005, [0024]; OKTA-1006, 9, 32.

In the Jones-Coulomb combination, “[d]ata elements from document types are *defined in Namespaces*. Documents (credentials) correspond to database tables. Namespaces may include data elements for several kind[s] of documents.” OKTA-1005, [0172], [0064]; OKTA-1006, 15-19, 88, 96-97; OKTA-1003, ¶274. Coulomb is express that such credentials include “payment credentials” similar to the payment applications of Jones. OKTA-1005, [0073], [0057]; OKTA-1006, 18, 98. The namespaces include identification information and “may be at the package level” or “may be at the data element level.” OKTA-1005, [0059]; OKTA-1006, 15-19.



OKTA-1005, FIG. 2; *see also* FIGs. 3A-3D; OKTA-1006, 88

Moreover, in the Jones-Coulomb combination, the “namespaces” are associated with “security policies,” as claimed. OKTA-1003, ¶¶275, 251. Jones’s

access device determines “transaction security” for each payment application (namespace), including “applications that require a high level of authentication” and payment applications associated with “payment networks [having] a better security track-record.” OKTA-1010, [0040], [0105], [0104] (“CVMs associated with the AID.”), [0100] (different verification levels), [0116], [0152]. For example, Jones describes associating PIN and CVM requirements with a payment application on the mobile device. *Id.*, [0105]. A POSITA would have recognized that applying such security policies to the identity credentials of Coulomb would have kept sensitive identity information secure from intrusive parties. OKTA-1003, ¶¶275, 262.

Element [1.2]

Jones’s access device teaches or suggests the claimed “reader,” and Jones’s multiple application selection module 153 teaches or suggests the claimed “reader module.” OKTA-1010, [0010]-[0011], [0054]-[0057], [0063]; OKTA-1003, ¶¶276-277. Jones describes “a mobile device communicating with an access device...[to] receiv[e] a plurality of application identifiers [(AIDs)] from the mobile device.” OKTA-1010, [0011], [0055] (RF communication).

Jones’s multiple application selection module (“reader module”) on the access device (“reader”) selects an electronic card—one or more of Jones’s payment applications or Coulomb’s identity credential cards stored at the mobile device as “namespaces” in the Jones-Coulomb combination—based on associated security

policies. OKTA-1003, ¶277. For example, “the access device 150 determines the first and second highest priority AID based on the processing capabilities, configuration options, and processing capabilities associated with each AID.” OKTA-1010, [0099], [0028]. Each “application identifier (AID) identifies a payment application installed on the mobile phone” and therefore selection of an AID is selection of a payment application (namespace). OKTA-1003, ¶277. Jones explains that “the multiple application selection module 153 of the access device 150 may use priority information and/or preferences...to determine the priority of the supported applications.” *Id.*, [0103]-[0107].

Jones discloses that this selection of AIDs associated with payment applications (and identity credential cards in the Jones-Coulomb combination) based on priority can use associated security policies as part of the selection process. OKTA-1003, ¶278. For example, “priority of AIDs may be based on...transaction security (e.g., applications that require a high level of authentication in order to process a transaction are given higher priority than other applications, payment networks with a better security track-record are provided priority).” OKTA-1010, [0040], [0104]-[0105], [0152] (selection based on “highest transaction security” or authentication requirements), [0104], [0099]-[0100]; Element [1.pre], *supra*.

This selection of a namespace is for the purpose of accessing a data item stored on the mobile phone. OKTA-1003, ¶279. The access device 150 “send[s] an

‘application selection’ command 306 with the selected AID to the application selection module 130 of the mobile device 110” and subsequently “the application selection module 130 may send a set of transaction processing information 312 including the payment credentials and any other relevant transaction processing information to the access device 150.” OKTA-1010, [0080], [0083]-[0085], [0108](“...the multiple application selection module 153 may obtain payment credentials associated with the primary AID and the secondary AID stored on the mobile device 110.”), [0134], [0035]-[0036] (payment application stores the payment credential information), FIGs. 3-4.

Elements_[2.pre]-[2.1]

The ’103 patent states “the reader 109’ and the verifier 105’ may be one machine.” OKTA-1001, 7:8-16, 8:45-51, 10:45-51, FIG. 6a. As such, Jones’s access device provides both the claimed reader and verifier terminal while the application selection module provides both the claimed reader module and verifier module. OKTA-1010, [0010]-[0011], [0054]-[0057], [0063], [0068], FIG. 2; OKTA-1003, ¶¶283, 145.

Jones’s access device receives “a list of available AIDs” from the mobile device. OKTA-1010, [0078], [0094], [0124], [0148]-[0150], [0026]. As discussed above, the AIDs identify namespaces in the combination (Jones’s payment applications and Coulomb’s identity credential cards). OKTA-1010, [0026]; OKTA-

1006, [0024], [0059], [0172]; OKTA-1006, 9, 15-19, 88, 96-97. The list of available AIDs is transmitted to the multiple application selection module 153 which “obtain[s] the list of available payment applications from the communication module.” OKTA-1010, [0072], [0099]-[0103], [0151]; OKTA-1003, ¶284.

Element [2.2]

Jones discloses “[t]he POS determines which AIDs it supports by comparing the list of AIDs to a list of supported AIDs stored in the POS.” OKTA-1010, [0028], [0102] (“...compare the received available AIDs to a list of supported AIDs.”). A POSITA would have recognized this comparison as whitelisting of namespaces (Jones’s payment applications). OKTA-1003, ¶285.

Coulomb discloses that each package (e.g., namespace) is “associated with a confidence level, which informs about the relevance of the issuer for the issued data elements.” OKTA-1005, [0024], [0037], [0041]; OKTA-1006, 32-33. Selection of a card can be based on “a minimum level of assurance required for the requested data elements.” OKTA-1005, [0028], [0047], [0149], [0150]-[0152], [0178]-[0182], Cls. 5-11; OKTA-1006, 32-33, 60, 105-107. A POSITA would have applied Coulomb’s teachings to Jones to include confidence level as a factor used by the access device to select a namespace (e.g., determine AID priority) to increase the probability of accuracy/reliability of the received information. OKTA-1003, ¶286.

Claim_[3]

See Element [2.2]. For example, namespace requests “may also specify a minimum level of assurance required for the requested data elements” to ensure that the received information “match[es] the target confidence level.” OKTA-1005, [0047], [0024], [0028], [0037], [0041], [0149], [0150]-[0152], [0178]-[0182], Cls. 5-11; OKTA-1006, 32-33, 60, 105-107; OKTA-1003, ¶¶286-292.

Element_[4.1]

Jones describes a “plurality of application identifiers being associated with two or more payment credentials stored on the mobile device.” OKTA-1010, [0013], [0035] (payment information stored “on a secure memory”), [0068]-[0069], [0083], [0090]-[0091]; OKTA-1005, [0172], [0063]-[0066] (storing data items organized by namespace), [0058]-[0059], [0220]; OKTA-1006, 15-19, 39-40, 88, 96-97.

Jones describes that the “Payment information” includes security policies such as “cardholder verification information (e.g., passcode, password, personal identification number (PIN), etc.), an *indication of an authentication process* for transaction processing (e.g., *online PIN, signature*, etc.)...and/or *any other suitable or relevant information* for performing a transaction.” OKTA-1010, [0036], [0069], [0088]-[0089]. Similarly, “an AID may indicate...any other information about a payment application or underlying account data associated with the payment application.” *Id.*, [0038]-[0039], [0097], [0101]. Jones goes on to describe that this

information stored in association with the AIDs for the payment applications includes associated security policies, such as “different cardholder verification methods (CVMs) that provide a higher or lower level of verification of a consumer's identity (e.g., PIN validation vs. Signature).” *Id.*, [0100], [0149]; OKTA-1003, ¶¶294-298. In another example, AID priority information includes “any suitable information including authentication...(e.g., type of authentication and/or level of authentication performed by the application)” to select one or more AIDs. OKTA-1010, [0104]-[0105] (“PIN”). Jones gives numerous other examples of security policies associated with payment applications and used for prioritizing/selecting AIDs and a POSITA would have recognized that it would have been useful and beneficial to store these security policies in association with the AIDs as part of the “any other relevant information” so that this information could be used for the AID selection described in Jones. OKTA-1010, [0038]-[0040], [0149], [0104]-[0105], [0116], [0152]; OKTA-1003, ¶298.

Element [4.2]

Jones describes that the mobile device 110 provides an available applications response 304 to the access device 150 that includes “a directory entry for each available AID on the mobile device” including AIDs, priority information “and/or *additional information relating to the particular AID.*” OKTA-1010, [0078]-[0079], [0094], [0097], [0124], [0148]-[0150]. A POSITA would have recognized

that this “additional information relating to the particular AID” would have predictably and beneficially include the security policy information associated with the AID so that such security policy information could be used by the access device to prioritize/select AIDs based on security policies (*supra*, Element [1.2]). OKTA-1003, ¶¶299-300; OKTA-1010, [0038]-[0040], [0149], [0104]-[0105] (selection based on an AID having “a higher level of security.”), [0116]. Jones’s mobile device includes a processor. OKTA-1010, [0063], [0052].

Claim [6]

Jones describes that “[i]n some embodiments, the application selection module 130 [of the mobile device] may provide AIDs for only those applications that are available for performing a transaction.” OKTA-1010, [0095]. For example, “a mobile payment application may not be active.” *Id.*, [0095]-[0096], [0148]. As another example, Jones states that “a consumer chooses their top three supported payment applications” and the access device further selects a payment application from this culled list. OKTA-1010, [0040], [0099]-[0107]; *see also* OKTA-1005, [0057] (“The user may selectively share data elements from one or more packages to the verifier device 110...”); OKTA-1006, 15; OKTA-1003, ¶¶301-304.

Claim_[7]

See analysis of Element [4.2]. OKTA-1003, ¶¶305-309, 299. Jones’s access device provides both the claimed reader and the claimed verifier terminal (Elements [2.pre]-[2.1], *supra*).

Elements_[8.pre]-[8.1]

Jones discloses that messages are exchanged using SSL protocol secure encryption, which includes messages transmitted as a sequence of bytes having bits. OKTA-1010, [0058], OKTA-1003, ¶¶314-315 (citing Internet RFC 2246 (OKTA-1012)), 43-46, 61. The SSL protocol specifies that “[t]he basic data block size is one byte (i.e. 8 bits)” and that hash and encryption information is communicated in byte streams. OKTA-1012, 6, 10-15; OKTA-1003, ¶¶45, 317. This includes required HASH type and encryption type. *Id.* Furthermore, a POSITA would have understood that communications between digital computing devices such as those described in Jones are transmitted as a sequence of bytes having bits. OKTA-1003, ¶¶85-95, 313; OKTA-1012, 6; OKTA-1013, 146, 448; OKTA-1014. Additionally, Jones expressly describes that each AID is a character string. OKTA-1010, [0039] (“the AID may have a standardized format” for example “A000000031010”) A POSITA would have recognized that a character string is a sequence of bytes having bits that convey information. OKTA-1003, ¶¶317, 90-91; OKTA-1014; OKTA-1013, 446-447. Additionally, “an AID may indicate...any other information about

a payment application or underlying account data associated with the payment application” including “cardholder verification methods (CVMs)” or verification protocols such as PIN validation or Signature. OKTA-1010, [0036]-[0039], [0047], [0074], [0085], [0097], [0100]-[0101], [0105], [0149]. The bits included in the application identifiers identifying the Signature satisfies the claimed “required signature scheme” and the PIN requirement are bit values denoting secure messaging options. OKTA-1003, ¶¶316-317.

Element [8.2]

As addressed with respect to claim 1, *supra*, the “online PIN” and “signature” requirement security policies discussed with respect to element [8.1] are examples of the security policies associated with the plurality of supported namespaces (payment applications) on Jones’s portable communication device. OKTA-1003, ¶¶318-319; OKTA-1010, [0036], [0047], [0074], [0085], [0097], [0100]-[0101], [0105], [0149]. For example, such authentication methods can include requirements for an “online PIN or a signature.” OKTA-1010, [0085], [0105].

Claim [9]

Jones discloses that the payment applications (namespaces) require different “authentication process[es]” and gives examples of “online ***PIN, signature***, etc.” OKTA-1010, [0036], [0047], [0085], [0105]; OKTA-1005, [0085], [0129], [0205]. This “PIN” provides the claimed “user consent.” OKTA-1003, ¶¶322-323. As

another example, authentication methods “include challenge response tests, passcode validation, and/or any other suitable processes for authenticating a consumer” which are forms of secure messaging OKTA-1010, [0047]; OKTA-1003, ¶322. Furthermore, “[a]n authorization request message may be protected using a secure encryption method (e.g., 128-bit SSL or equivalent) in order to prevent data from being compromised,” which again indicates secure messaging. OKTA-1010, [0058]. OKTA-1003, ¶322.

Claim [10]

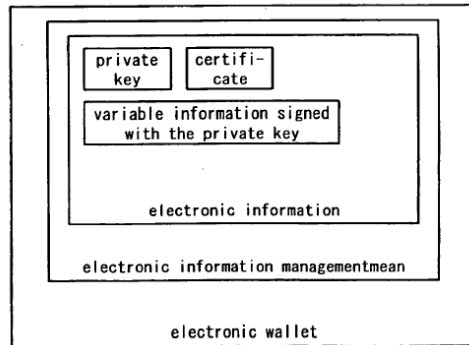
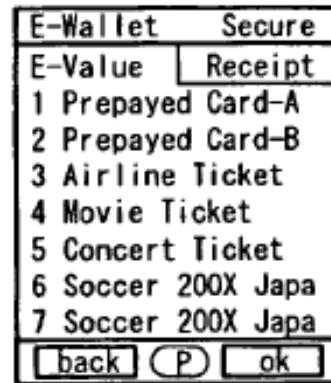
See Supra, Element [2.2], *supra*. OKTA-1003, ¶¶325-328, 285; OKTA-1010, [0028], [0102].

E. [GROUND 2B]: Jones-Coulomb-Takayama Renders Claims 11-15 Obvious

1. Takayama (OKTA-1011)

Takayama describes an “electronic wallet...for storing and managing information including valuable information.” OKTA-1011, [0013]. The electronic information includes security information, including use of a private key. *Id.*

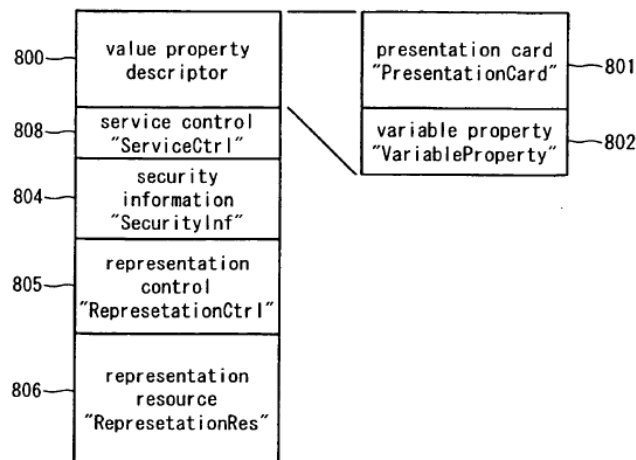
Fig. 3



OKTA-1011, FIGs 3, 10.

The “electronic tickets and prepaid cards that are dealt with in the present system will be referred to as ‘electronic value.’” *Id.*, [0035]-[0036]. As shown in FIG. 13, the data structure for the electronic value includes “security information 804...defining the security information such as encryption key of the electronic value and the like.” *Id.*, [0081]-[0082], [0097]-[0099].

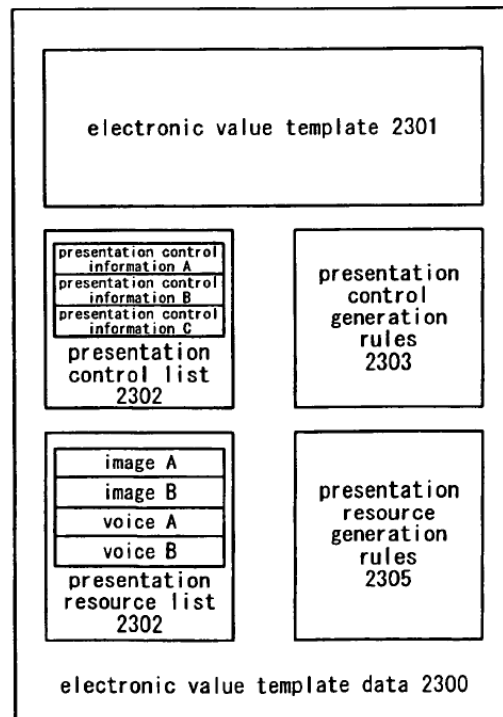
Fig. 13



OKTA-1011, FIG. 13; [0135]-[0138]; OKTA-1003, ¶¶329-333.

Electronic values are created using electronic value templates. OKTA-1011, [0123]-[0126]. The system includes an “electronic value template database 2202 [that] manage[s] the electronic value templates for each electronic value code (evCode), which indicates the type of electronic value.” *Id.*

Fig. 28



OKTA-1011, FIG. 28.

2. The Jones-Coulomb-Takayama Combination

Multiple reasons would have prompted a POSITA to apply Takayama to Jones-Coulomb to use templates to convey the security information (and other information) associated with each electronic card. OKTA-1003, ¶¶332-339. First, use of electronic value templates stored in an electronic template database, as

suggested by Takayama, would have saved resources as the mobile device would not need to recreate the entire data structure each time it transmitted a message containing payment/security/identifying information to the access device. OKTA-1011, [0123]-[0126], [0135]-[0137]; OKTA-1003, ¶335. This would have saved computing resources in the resulting system.

Second, use of templates for conveying payment/security/identifying information would have increased the utility of the system by allowing the resulting system to be compatible with a wide variety of devices by allowing for selection of an appropriate template “compatible and according to the type of mobile user terminal.” OKTA-1011, [0126]; OKTA-1003, ¶336.

Third, use of templates, as suggested by Takayama, to convey payment/security/identifying information would have ensured that the information is conveyed to the access device in a format that is readily understood and can be easily processed by the access device. OKTA-1003, ¶337. For example, Jones discloses that in some scenarios, the access device may need to “re-format the received payment credentials to conform to a predetermined communication protocol (e.g., ISO message format) for delivery to a payment processing network.” OKTA-1010, [0113], [0161]. Use of different templates having different information formats would prevent at least some of this need for re-formatting. OKTA-1003, ¶337.

Fourth, such a modification is the application of known techniques (Takayama's templates) to a known system ready for improvement to yield predictable results. OKTA-1003, ¶338. A POSITA would have had a reasonable expectation of success in making the proposed modifications without significantly altering or hindering the structure and function of Jones's system. OKTA-1003, ¶338; OKTA-1010, [0187].

3. Application of Jones-Coulomb-Takayama to Claims

Element_[11.pre]

Jones discloses "a mobile device." OKTA-1010, [0010]-[0013]; OKTA-1003, ¶¶341-343.

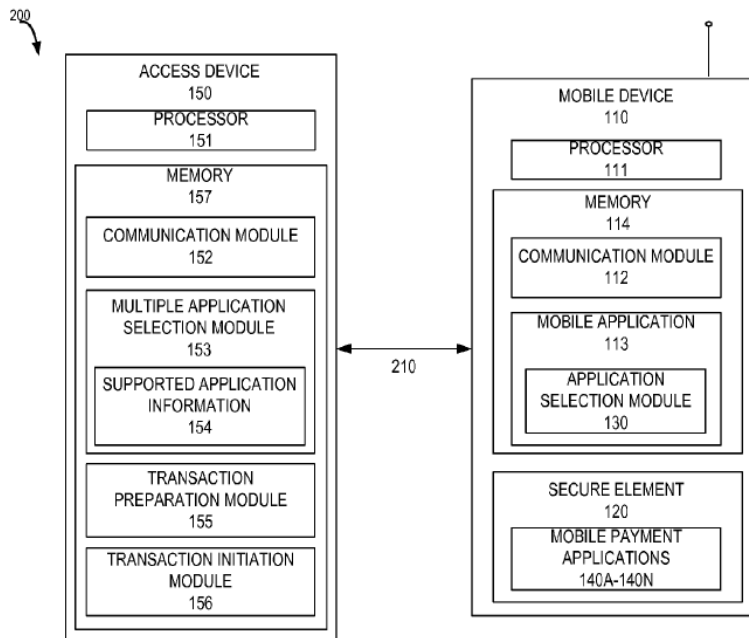


FIG. 2

OKTA-1010, FIG. 2.

Element [11.1]

Jones's mobile device includes a processor. OKTA-1010, [0063], [0052]; OKTA-1003, ¶¶344-345.

Element [11.2]

The memory of Jones's mobile device "stores code executable by the processor." OKTA-1010, [0052], [0066]-[0068], [0186]; OKTA-1003, ¶¶346-347. The mobile device stores "various card data" including identifying data such as "name, billing address, residential address, date of birth" arranged as a "mobile wallet" and is therefore an eID wallet OKTA-1010, [0026]-[0028], [0035], [0046]; OKTA-1003, ¶¶347, 267-268. Coulomb confirms the eID wallet storing eID data, describing "[a] wallet application" that is "loaded with several documents" such as "a mobile driving license (mDL) 902," etc. OKTA-1005, [0169], [0024]; OKTA-1006, 8-9, 18, 52, 96-100; OKTA-1003, ¶¶271, 347.

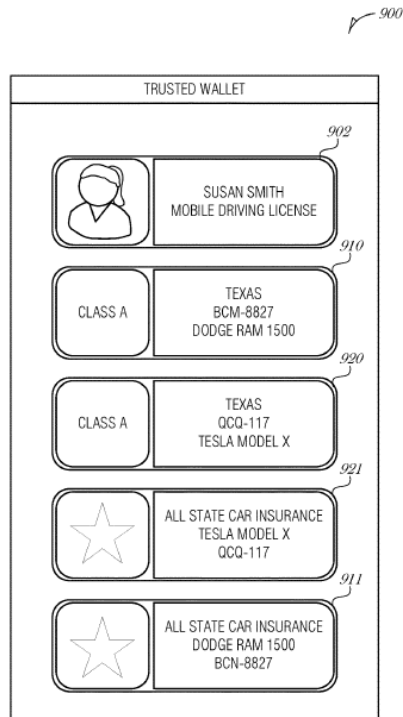


FIG. 9

OKTA-1005, FIG. 9; OKTA-1006, 52, 93; OKTA-1015, 9-10.

All software components “may be implemented as software code to be executed by a processor.” OKTA-1010, [0186]. Jones’s mobile application 113 and/or any of its subcomponents (such as application selection module 130) or a combination of the mobile application 113 and other applications is the claimed eID wallet application. *Id.*, [0063], [0066]-[0068]; OKTA-1003, ¶349.

Element [11.3]

Jones’s access device provides the claimed reader. *Supra*, Ground 2A, Element [1.2]; OKTA-1010, [0010]-[0011], [0054]-[0057], [0063], [0068]; OKTA-

1003, ¶¶350, 276. Jones further discloses the “multiple application selection module 153” of the access device “sending one *or more* of the selected AIDs to the mobile device 110 and receiving the payment credentials and transaction processing information.” OKTA-1010, [0107]-[0108], [0072] (describing accessing payment credentials for multiple “selected AIDs”), [0153]-[0154], [0134], [0108]; OKTA-1003, ¶350.

The payment applications/identification cards of the Jones-Coulomb-Takayama system are arranged as namespaces of data elements. *Supra*, Ground 2A, Element [1.1]; OKTA-1005, [0172], [0064], [0073], [0057], [0059]; OKTA-1006, 15-19, 88, 96-97; OKTA-1003, ¶¶272-274, 351.

Element [11.4]

Jones discloses that in response to receiving the “selection message...that includes all of the determined AIDs,” the mobile device transmits “any of the transaction processing information 312 described above in reference to FIG. 3.” OKTA-1010, [0108]-[0111]. This includes “*any other relevant transaction processing information* to the access device 150” such as security rules. OKTA-1010, [0083]; OKTA-1003, ¶¶352-360. For example, “the transaction processing information may include a transaction cryptogram,” “cryptogram information data (CID),” “a derived key indicator (DKI) that can be used to identify a master key (e.g. a master key associated with the issuer), [and] card verification results (CVR).”

OKTA-1010, [0084]-[0086]. This information can further include CVM, such as “a passcode, biometric (e.g., fingerprint), pattern lock (e.g., for a screen lock), signature, or online PIN.” *Id.* The authentication and verification information sent with the transaction information are security rules associated with the selected namespaces. OKTA-1003, ¶354.

Furthermore, these security rules are sent according to a defined bytestring template, in the Jones-Coulomb-Takayama combination. For example, Coulomb describe “registration templates” that are “embed[ed] information” included in the information packages exchanged between the user and merchant devices. OKTA-1005, [0208]-[0209]; OKTA-1006, 37-38; OKTA-1003, ¶¶355, 352-353. For example, “[t]he template information may specify the tag of the data elements to reference...the kind of document, the issuer, the name of the package, or other information.” *Id.* A POSITA would have recognized that the “other information” included as part of the template described in Coulomb would have included the security rules discussed above. OKTA-1003, ¶355. Coulomb’s FIGs. 3A-3D show that the information packages are transmitted according to a template including security information (signature):

300A

STANDALONE PACKAGE A	
URI	IDENTIFIER AND UPDATE LOCATION
NAMESPACE	
1ST TAG	1ST ELEMENT
...	
I_TH TAG	I_TH DATA ELEMENT
...	
N_TH TAG	LAST DATA ELEMENT
OPTIONAL INFORMATION	LBS DATA ACCESS CONTROL DATA ISSUER SIGNATURE

(A) ←

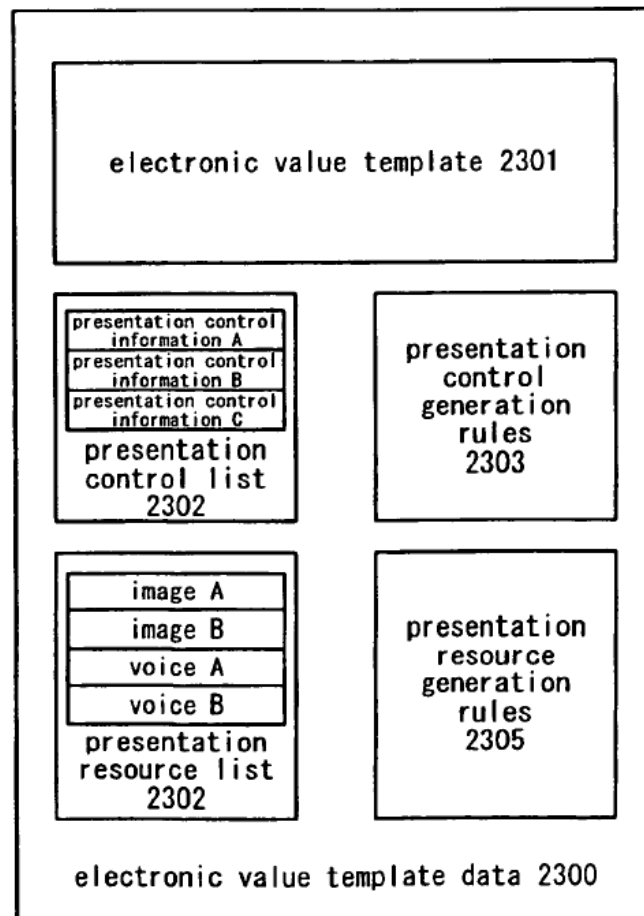
FIG. 3A

OKTA-1005, FIG. 3A; OKTA-1006, 97, 89; OKTA-1003, ¶355.

Takayama confirms that security information is transmitted according to a template. OKTA-1011, [0123]-[0126]; OKTA-1003, ¶356. This allows the mobile device to “issue an electronic value compatible and according to the type of mobile user terminal.” *Id.* Takayama discloses that the template is populated with information regarding a selected electronic value (such as electronic tickets and prepaid cards but also including Jones’s payment cards and Coulomb’s identity information cards in the combination), including security information. OKTA-1003, ¶356. For example, the mobile device selects an electronic value template and “will

generate an electronic value ID (evID), an electronic value private key (evPrivateKey) unique to the electronic value, and an electronic value certificate (evCertificate) for the key to generate the security information 804 of the electronic value in combination with the electronic value template 2301 of the electronic value template data 2300 selected (*generating the security information 2602*).” OKTA-1011, [0135]-[0138].

Fig. 28

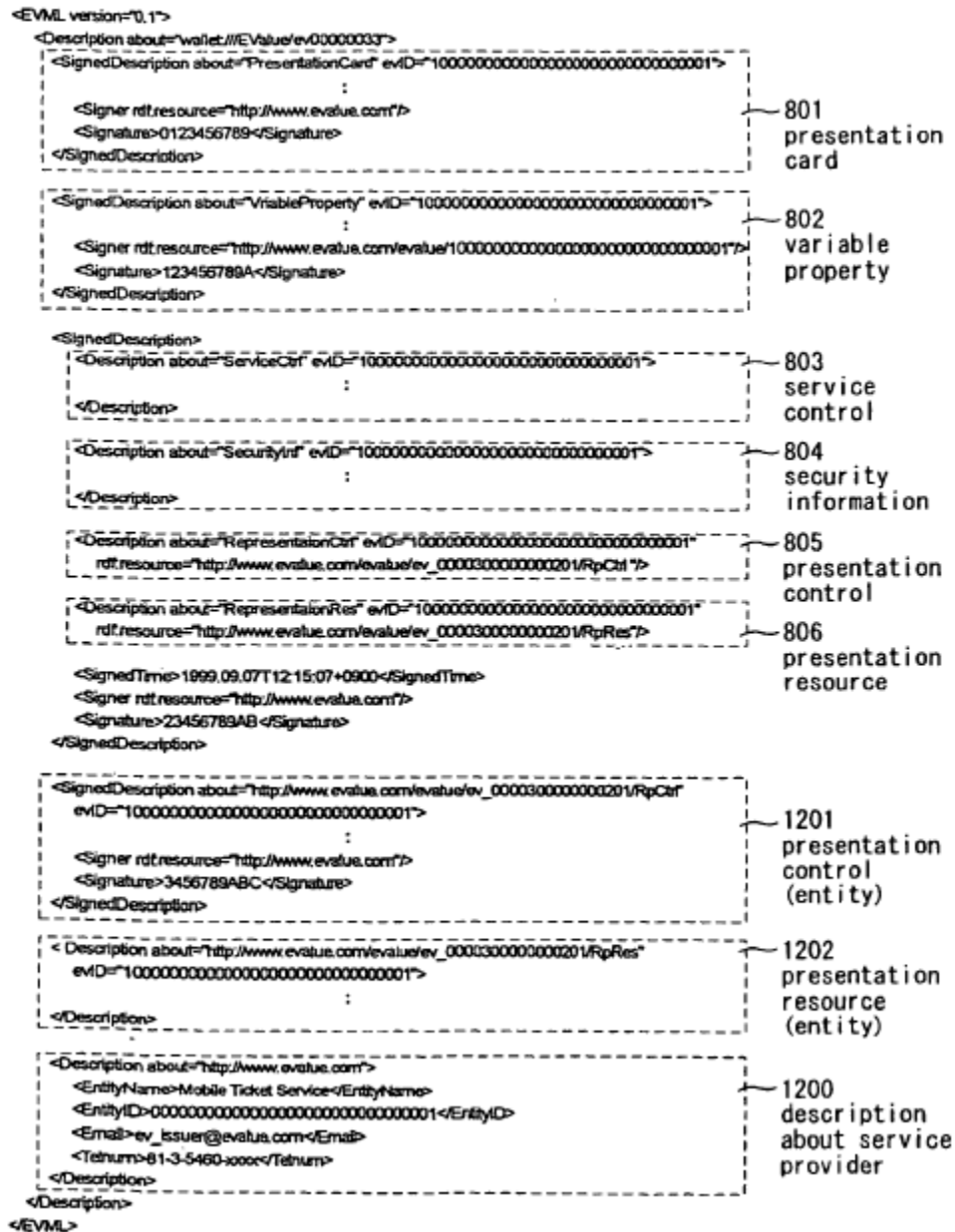


OKTA-1011, FIG. 28. These electronic values are sent to the merchant computing device. OKTA-1011, [0103]-[0106].

The Jones-Coulomb-Takayama combination provides, or at least renders obvious, that the template is a defined bytestring template. OKTA-1003, ¶357. The templates are defined because they are drawn from a template database. OKTA-1011, [0123]-[0126], [0135]-[0138]; OKTA-1003, ¶357. The templates (containing security rules and other information) would have been provided as bytestrings because strings of bytes of information are how digital devices communicate with each other. OKTA-1003, ¶¶357-358, 353, 85-95; OKTA-1013, 146, 448; OKTA-1014. For example, Jones describes the SSL protocol. OKTA-1010, [0058]. The SSL protocol specifies “[t]he basic data block size is one byte (i.e. 8 bits)” and that security information (rules) is communicated in byte streams. OKTA-1012, 6, 10-15; OKTA-1003, ¶¶314-317, 45.

Takayama shows that at least some of the information, such as the electronic value ID, are communicated as strings of bytes:

Fig. 17



OKTA-1011, FIG. 17.

Fig. 19

```
<Description about="ServiceCtrl" evID="10000000000000000000000000000001">
  <SC-module type="ticket" ID=1 number=$NUMBER start=$START_VALID end=$END_VALID
    used_flag=$USED validity_flag=$VALIDITY serial=$USE_SERIAL/>
  <SC-module type="verify_prop" ID=2 prop=$SEAT_NUM/>
  <SC-module type="set_message" ID=3 msg=$MESSAGE_2/>
</Description>

<Description about="SecurityInf" evID="10000000000000000000000000000001">
  <evOwner>
    <Description about="http://www.evalue.com/user/11000000000000000000000000000001"
      EntityName="Taro Suzuki"
      EntityID="11000000000000000000000000000001"/>
    </evOwner>
    <evResource>http://www.evalue.com/evalue/10000000000000000000000000000001</evResource>
    <evCertificate>
      0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF
    </evCertificate>
    <evPrivateKey>0123456789</evPrivateKey>
    <evAuthKey>0123456789ABCDEF</evAuthKey>
    <evhandlerAuthKey>ABCDEF0123456789</evhandlerAuthKey>
  </Description>
```

OKTA-1011, FIG. 19; *see also* OKTA-1010, [0039] (AID information conveyed as bytestrings).

A POSITA would have found it obvious and beneficial to apply these disclosures of Takayama and Jones to the resulting combination to convey the templates as bytestrings as this was the universally used communication scheme for facilitating communication between digital devices. OKTA-1003, ¶¶358-359.

Elements_[12.pre]-[12.1]

“The list of available AIDs may be requested by the access device 150” from the mobile device 110. OKTA-1010, [0094]. For example, “the access device 150

may initiate a transaction by sending an available applications request 302 to the mobile device 110 to request information on which payment applications (e.g., a list of AIDs) may be available on the mobile device 110.” OKTA-1010, [0077]-[0078], [0147]; OKTA-1003, ¶¶362-364.

The Jones-Coulomb-Takayama includes identity information cards in addition to payment cards and the electronic cards are arranged as namespaces of data elements. *Supra*, Ground 2A, Elements [1.pre]-[1.1]; OKTA-1005, [0172], [0169], [0024], [0064], [0073], [0057], [0059]; OKTA-1006, 8-9, 15-19, 52, 88, 96-100; OKTA-1003, ¶¶364, 268, 271-274.

Element_[12.2]

See Ground 2A, Elements [2.1], [4.2].

Claim_[13]

See Ground 2A, Claim [6].

Claim_[14]

See Ground 2A, Elements [4.2], [7].

Claim_[15]

See Ground 2A, Element [8.1].

F. [GROUND 2C]: Jones-Coulomb-Sharma Renders Claim 16 Obvious

1. The Jones-Coulomb-Sharma Combination

Multiple reasons would have prompted a POSITA to apply Sharma to Jones-Coulomb such that upon selecting a payment application for which the access device can support the required security policy, the access device provides information to the mobile device to demonstrate that the access device can satisfy the associated security policy. OKTA-1007, [0082], [0129]-[0131]; OKTA-1003, ¶¶378-382, 215-224.

First, such a modification would allow the mobile device to have confidence that the access device can satisfy the security requirements for the provided information (e.g., that the access device can be trusted), thereby increasing overall security for the system. OKTA-1003, ¶¶379-380.

Second, providing information that allows the “the mobile application [to] validate[] that the access device 120 is authorized to access the account credentials associated with the selected UAIDs” and “supports the TPO of the UAID that is selected” would have resulted in a system that saves time and communication bandwidth by avoiding initiation of payment processes or other information access processes for which the access device is unequipped. OKTA-1007, [0129]-[0131]; OKTA-1003, ¶381.

Third, this modification is application of known techniques (Sharma's demonstration of satisfaction of security policies for accessing data items) to a known system ready for improvement to yield predictable results. OKTA-1003, ¶382. A POSITA would have had a reasonable expectation of success in making the proposed modifications without significantly altering or hindering the structure and function of the Jones-Coulomb system. OKTA-1003, ¶382; OKTA-1010, [0187].

2. Application of Jones-Coulomb-Sharma to Claims

Element_[16.pre]

See Ground 2A, Element [1.pre].

Element_[16.1]

See Ground 2A, Element [1.1].

Element_[16.2]

See Ground 2A, Elements [4.2], [7]. Furthermore, Jones discloses that the access device 150 “may be incorporated into merchant computer 160” or otherwise communicate with the merchant computer 160 and that functionality ascribed to either the access device 150 or merchant computer 160 can be performed by the other. OKTA-1010, [0056]-[0060], [0177]-[0188]. Jones therefore provides a reader connected to a verifier and it would have been obvious for any functionality ascribed to the access device 150 to be performed by the merchant computer 160. OKTA-1003, ¶¶386-387, 299, 276.

Element [16.3]

See Ground 2A, Element [1.2]; Ground 2B, Element [11.3]. For example, “the multiple application selection module 153 [of the access device] may select and/or determine two or more AIDs for processing the transaction” and “each of the selected AIDs may be provided to the mobile device 110 in a single application selection message.” OKTA-1010, [0153]-[0157], [0107]-[0108], [0072], [0134], [0163]-[0164]; OKTA-1003, ¶¶277-278, 350.

Element [16.4]

See Ground 2A, Elements [4.2], [7]; Ground 2B, Element [11.4]. For example, Jones discloses that at least some of the information for a security policy associated with a candidate namespace (payment application) is payment information provided upon selection of a given payment application identifier. OKTA-1003, ¶¶391-392, 299. For example, “the application selection module 130 may send a set of transaction processing information 312 including the payment credentials and ***any other relevant transaction processing information*** to the access device 150.” OKTA-1010, [0083]. This information includes security rules. OKTA-1003, ¶393. For example, “the transaction processing information may include a transaction cryptogram,...cryptogram information data (CID),...cryptogram version number (CVN),...a master key (e.g. a master key associated with the issuer), card

verification results (CVR),” or CVM info such as a passcode or fingerprint. OKTA-1010, [0084]-[0086].

Element [16.5.1]

Jones discloses that the access device “determine[es] which of the AIDs from the list of AIDs are supported by the access device,” and that this determination is made using “application configuration information or any other information that may be provided with the list of AIDs.” OKTA-1010, [0101]. This information includes security requirements such as “verification methods (CVMs) that provide a higher or lower level of verification of a consumer's identity (e.g., PIN validation vs. Signature).” *Id.*, [0100], [0104], [0149]; OKTA-1003, ¶¶394-395.

Sharma similarly discloses that “depending on the type of credentials selected, different security levels for the transaction may exist.” OKTA-1007, [0082]. The access device/terminal has associated “Transaction Processing Options (TPO)” that “indicates which transaction data types the access device 120 supports.” *Id.*, [0081]; OKTA-1003, ¶396.

Element [16.5.2]

Jones discloses that the access device selects the highest priority application that “that the access device 150 is configured to process” and that this priority can be based on security policy, such as required authentication. OKTA-1010, [0099]-[0107], [0040], [0152]; *supra* Ground 2A, Element [1.2]. This selection is to access

a data item stored on the mobile device (*supra*, Element [1.2]). OKTA-1003, ¶¶397-398, 279; OKTA-1010, [0080], [0083]-[0085].

The Jones-Coulomb-Sharma combination further provides demonstrating satisfaction of the security policy to the mobile device. OKTA-1003, ¶399. Sharma discloses “the mobile application may also request access device configuration information (also referred to as “transaction processing options” (*TPO*)) ***from the merchant access device 120 to determine what processing options the merchant access device supports.***” OKTA-1007, [0125]. The access device “send[s] a “GPO Request” with the MID and the TPO that are supported back to the mobile application 112.” *Id.*, [0126]. “[T]he TPO (also referred to as access device configuration options) allow the mobile device 110 to determine whether the access device 120 is configured to process the type of transaction that is associated with the selected account applet.” *Id.*, [0082], *see also* [0129]-[0131]. Such supported processing options for the payment applications would have included the required security protocols in the resulting combination. OKTA-1003, ¶¶399, 395.

Element [16.5.3]

Sharma discloses that “if the TPO indicates that... the UAID transaction data is not supported by the merchant access device” the response “sent to the merchant access device 120 includ[es] an error code” rather than providing access to the payment information (data items). OKTA-1007, [0131]. As another example, if “the

access device 120 is not configured to process those types of transactions, an error would occur.” *Id.*, [0130]. When an error occurs “the transaction is terminated” (i.e., access to the data item is rejected). *Id.*, [0132]; OKTA-1003, ¶¶400-401.

Furthermore, Jones discloses that if the access device determines that “an alternate AID is not supported” that payment application (namespace) is not selected (i.e., rejects access). OKTA-1010, [0130]; OKTA-1003, ¶402.

Element [16.5.4]

Sharma discloses that “the mobile application 112 checks....that the TPO from the merchant access device 120 support the type of transaction data” for the UAID OKTA-1007, [0131]. If the security policy scheme can be satisfied, “the merchant access device 120 receives an appropriate ‘GPO Response’ from the mobile application and the transaction is processed.” *Id.*, [0133], [0127]; *see also* OKTA-1010, [0080]-[0085] (describing granting access to payment credential information for the selected payment application), [0108]; OKTA-1003, ¶¶403-405.

IV. PAYMENT OF FEES – 37 C.F.R. § 42.103

Petitioner authorizes the Patent and Trademark Office to charge Deposit Account No. 06-1050.

V. MANDATORY NOTICES

A. Real Party-In-Interest Under 37 C.F.R. § 42.8(b)(1)

Petitioner, Okta, Inc., and Okta GmbH are the real parties-in-interest.

B. Related Matters Under 37 C.F.R. § 42.8(b)(2)

Petitioner is not aware of any disclaimers, reexamination certificates or petitions for *inter partes* review for the '103 patent. Petitioner is not aware of any civil actions concerning the '103 patent.

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

Petitioner provides the following designation of counsel.

Lead Counsel	Backup counsel
Kenneth Darby, Reg. No. 65,068 Fish & Richardson P.C. 60 South Sixth Street Suite 3200 Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 Email: IPR56407-0023IP1@fr.com	Patrick J. Bisenius, Reg. No. 63,893 Nicholas Stephens, Reg. No. 74,320 Ryan Chowdhury, Reg. No. 74,466 Fish & Richardson P.C. 60 South Sixth Street Suite 3200 Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 PTABInbound@fr.com

D. Service Information

Please address all correspondence and service to the address listed above.

Petitioner consents to electronic service by email at IPR56407-0023IP1@fr.com.

Respectfully submitted,

Dated April 6, 2026

/Patrick J. Bisenius/
Patrick J. Bisenius, Reg. No. 63,893
Kenneth Darby, Reg. No. 65,068
Nicholas Stephens, Reg. No. 74,320
Ryan Chowdhury, Reg. No. 74,466
Fish & Richardson P.C.
3200 RBC Plaza, 60 South Sixth Street
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

(Control No. IPR2026-00327)

Attorneys for Petitioner

CERTIFICATION UNDER 37 CFR § 42.24

Under the provisions of 37 CFR § 42.24(d), the undersigned hereby certifies that the word count for the foregoing Petition for *Inter partes* Review totals 13,992 words, which is less than the 14,000 allowed under 37 CFR § 42.24.

Dated April 6, 2026

/Patrick J. Bisenius/

Patrick J. Bisenius, Reg. No. 63,893
Kenneth Darby, Reg. No. 65,068
Nicholas Stephens, Reg. No. 74,320
Ryan Chowdhury, Reg. No. 74,466
Fish & Richardson P.C.
3200 RBC Plaza, 60 South Sixth Street
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

Attorneys for Petitioner

CERTIFICATE OF SERVICE

Pursuant to 37 CFR §§ 42.6(e)(4)(i) *et seq.* and 42.105(b), the undersigned certifies that on April 6, 2026, a complete and entire copy of this Petition for *Inter partes* Review, Power of Attorney, and all supporting exhibits were provided via Federal Express, to the Patent Owner by serving the correspondence address of record as follows:

Thales Dis Cpl USA Inc.
Intellectual Property
900 South Pine Island Road, Suite 710
Plantation, Florida 33324

/Esther Goldschlager /

Esther Goldschlager
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
goldschlager@fr.com