

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: John J. Giobbi Attorney Docket No.: 42342-0137IP1
U.S. Patent No.: 8,886,954
Issue Date: November 11, 2014
Appl. Serial No.: 13/710,109
Filing Date: December 10, 2012
Title: BIOMETRIC PERSONAL DATA KEY (PDK) AUTHEN-
TICATION

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. 8,886,954 PURSUANT TO 35 U.S.C. §§ 311–319,
37 C.F.R. § 42

TABLE OF CONTENTS

I.	REQUIREMENTS FOR IPR	1
A.	Grounds for Standing.....	1
B.	Challenge and Relief Requested.....	1
C.	Claim Construction	2
II.	OVERVIEW OF THE '954 PATENT	3
III.	THE CHALLENGED CLAIMS ARE UNPATENTABLE.....	4
A.	[GROUND 1] – Burger Renders Obvious Claims 1, 2, 4, 5, 7-13, 15, 16, 18-24, 26-29	4
1.	Burger.....	4
2.	Application of Burger to the '954 Claims.....	22
B.	[GROUND 2] – Burger and Robinson Render Obvious Claims 3, 14, 17.	89
1.	Robinson.....	89
2.	Combination of Burger and Robinson	92
3.	Application of Burger and Robinson to the '954 Claims.....	95
C.	[GROUND 3] – Burger and Orsini Render Obvious Claims 6 and 25 ..	97
1.	Orsini	97
2.	Combination of Burger and Orsini.....	98
3.	Application of Burger and Orsini to the '954 Claims	102
IV.	PTAB DISCRETION SHOULD NOT PRECLUDE INSTITUTION.....	102
A.	35 U.S.C. §314(a) - <i>Fintiv</i>	102
B.	35 U.S.C. §325(d) – <i>Advanced Bionics</i>	105
V.	CONCLUSION AND FEES	107
VI.	MANDATORY NOTICES UNDER 37 C.F.R § 42.8(a)(1).....	107
A.	Real Party-In-Interest Under 37 C.F.R. § 42.8(b)(1).....	107
B.	Related Matters Under 37 C.F.R. § 42.8(b)(2)	107
C.	Lead And Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3).....	108
D.	Service Information	108

EXHIBITS

MSC-1001	U.S. Patent No. 8,886,954 to John J. Giobbi (“the ’954 Patent”)
MSC-1002	Excerpts from the Prosecution History of the ’954 Patent (“the ’954 Prosecution History”)
MSC-1003	Declaration and Curriculum Vitae of Dr. Patrick Traynor
MSC-1004	Complaint, <i>Proxense, LLC v Microsoft Corporation</i> , 6:23-cv-00319, W.D. Tex., filed April 28, 2023
MSC-1005	US Patent Application Publication No. 2005/0050367 (“Burger”)
MSC-1006	US Patent Application Publication No. 2003/0177102 (“Robinson”)
MSC-1007	Institution Decision, <i>Samsung Electronics America, Inc. v. Proxense, LLC</i> , IPR2021-01444, Paper 11 (PTAB Feb. 28, 2022)
MSC-1008	Definition of “transaction,” Merriam-Websters Collegiate Dictionary, 10 th Ed., 1999
MSC-1009	Google Pixel Serial Number Guide, HomeServe webpage, https://www.homeserve.com/en-us/customers/find-serial-number-device-type/google/
MSC-1010	US Patent No. 8,977,860 (“Barrus”)
MSC-1011	US Patent No. 7,681,050 (“Blom”)
MSC-1012	US Patent No. 10,755,300 (“Goodhart”)
MSC-1013	US Patent Application Publication No. 2009/0070219 (“D’Angelo”)
MSC-1014	US Patent No. 10,929,869 (“Rosenberg”)
MSC-1015	RESERVED

MSC-1016	Memorandum, Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation (USPTO June 21, 2022) (“Director’s Guidance”)
MSC-1017	Microsoft’s Opening Brief in support of its Motion to Dismiss for Failure to State a Claim, <i>Proxense, LLC v Microsoft Corporation</i> , 6:23-cv-00319, W.D. Tex., filed July 10, 2023
MSC-1018	Microsoft’s Reply in support of its Motion to Dismiss for Failure to State a Claim, <i>Proxense, LLC v Microsoft Corporation</i> , 6:23-cv-00319, W.D. Tex., filed August 10, 2023
MSC-1019	Order Canceling Markman Hearing, <i>Proxense, LLC v Microsoft Corporation</i> , 6:23-cv-00319, W.D. Tex., Jan. 9, 2024
MSC-1020	RESERVED
MSC-1021	US Patent Application Publication No. 2004/0049687 (“Orsini”)
MSC-1022	<i>Ex-Parte</i> Re-examination Request of ’905 patent; Re-examination application number 90/015,053
MSC-1023	Motion to Transfer, <i>Proxense, LLC v Microsoft Corporation</i> , 6:23-cv-00319, W.D. Tex., Aug. 21, 2023
MSC-1024	Motion to Stay pending resolution of the Motion to Transfer, <i>Proxense, LLC v Microsoft Corporation</i> , 6:23-cv-00319, W.D. Tex., Mar. 8, 2024
MSC-1025	Order Granting Motion to Stay pending resolution of the Motion to Transfer, <i>Proxense, LLC v Microsoft Corporation</i> , 6:23-cv-00319, W.D. Tex., Mar. 26, 2024
MSC-1026	“How to find the serial number on TP-Link devices,” https://www.tp-link.com/us/support/faq/503/ (last visited April 15, 2024)
MSC-1027	Order Denying Motion to Transfer, <i>Proxense, LLC v Microsoft Corporation</i> , 6:23-cv-00319, W.D. Tex., April 18, 2024

MSC-1028 US Patent Application Publication No. 2002/0147658
 (“Kwan”)

MSC-1029 US Patent Application Publication No. 2002/0143634 (“Ku-
 mar”)

LISTING OF CHALLENGED CLAIMS

Claim 1	
[1pre]	A method comprising:
[1.1]	persistently storing biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying an integrated device and a secret decryption value in a tamper proof format written to a storage element on the integrated device that is not capable of being subsequently altered;
[1.2]	responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan;
[1.3]	comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;

[1.4]	responsive to a determination that the scan data matches the biometric data, wirelessly sending one or more codes and other values from the plurality of codes and other data values for authentication to a third party that operates a trusted authority, wherein the one or more codes and other data values includes the device ID code; and
[1.5]	receiving, at an application, an access message from the trusted authority indicating that the trusted authority successfully authenticated the one or more codes and other data values sent to the third party and allowing the user access to the application.
Claim 2	
[2]	The method of claim 1, wherein the one or more codes and other data values are transmitted to the trusted authority over a network.

Claim 3	
[3]	The method of claim 1, further comprising: registering an age verification for the user in association with the device ID code.
Claim 4	
[4]	The method of claim 1, wherein the one or more codes and the other data values indicate that the biometric verification was successful.
Claim 5	
[5]	The method of claim 1, wherein the biometric data includes one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.
Claim 6	
[6]	The method of claim 1, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.

Claim 7	
[7]	The method of claim 1, wherein the application includes one or more of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file and a financial account.
Claim 8	
[8]	The method of claim 1, wherein the application includes a file including medical information.
Claim 9	
[9]	The method of claim 1, wherein the application includes a financial account.
Claim 10	
[10]	The method of claim 1, further comprising: establishing a secure communication channel prior to sending the one or more codes and other data values for authentication.

Claim 11	
[11.1]	The method of claim 1, further comprising: receiving a request for the one or more codes and other data values without a request for biometric verification; and
[11.2]	responsive to receiving the request for the one or more codes and other data values without a request for biometric verification, sending the one or more codes and other data values without requesting the scan data.
Claim 12	
[12.pre]	An integrated device comprising:
[12.1]	a persistent storage media that stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to the persistent storage media and not capable of being subsequently altered;

[12.2]	a validation module, coupled to communicate with the persistent storage media, that receives scan data from a biometric scan for comparison against the biometric data, and that sends one or more codes and other data values from the plurality of codes and other data values for authentication by a third party that operates a trusted authority, wherein the one or more codes and other data values includes the device ID code; and
[12.3]	a radio frequency communication module that receives an access message from the trusted authority indicating that the trusted authority successfully authenticated the one or more codes and other data values to the third party and allowing the user access to an application.
Claim 13	
[13]	The integrated device of claim 12, wherein the one or more codes and other data values are transmitted to the trusted authority over a network.

Claim 14	
[14]	The integrated device of claim 12, wherein an age verification is registered in association with the device ID code.
Claim 15	
[15]	The integrated device of claim 12 comprising: an LED to be activated for requesting the biometric scan.
Claim 16	
[16.pre] n 15	A method for authenticating a verified user using a computer processor configured to execute method steps, comprising:

[16.1]	wirelessly receiving one or more codes and other data values from a plurality of codes and other data values including a device ID code, wherein the plurality of codes and other data values comprises the device ID code uniquely identifying an integrated device associated with a biometrically verified user, the device ID code being registered with a trusted authority for authentication, the trusted authority operated by a third party;
[16.2]	requesting authentication of the integrated device using the one or more codes and other data values by the trusted authority;
[16.3]	receiving, at an application, an access message from the trusted authority indicating that the trusted authority successfully authenticated the one or more codes and other data values to the third party; and
[16.4]	in response to receiving the access message, allowing the biometrically verified user access to the application.

Claim 17	
[17]	The method of claim 16, further comprising: registering a date of birth or age with the trusted authority.
Claim 18	
[18.1]	The method of claim 16, further comprising: establishing a secure communications channel with the integrated device,
[18.2]	wherein the one or more codes and other data values associated with the biometrically verified user is received from the integrated device.
Claim 19	
[19]	The method of claim 16, wherein the application includes one or more of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file and a financial account.
Claim 20	
[20]	The method of claim 16, wherein the application includes a file including medical information.

Claim 21	
[21]	The method of claim 16, wherein the application includes a financial account.
Claim 22	
[22.pre]	A system, comprising:
[22.1]	an integrated hardware device that stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated hardware device and a secret decryption value in a tamper proof format written to a storage element in the integrated hardware device that is not capable of being subsequently altered, and that wirelessly sends one or more codes and other data values from the plurality of codes and other data values, wherein the one or more codes and other data values include the device ID code; and

[22.2]	an authentication circuit that receives the one or more codes and other data values and sends the one or more codes and other data values to a third party that operates a trusted authority for authentication, and that receives an access message from the trusted authority indicating that the trusted authority successfully authenticated the one or more codes and other data values to the third party and allows the user to access an application.
Claim 23	
[23]	The system of claim 22, wherein the integrated hardware device receives an authentication request from the authentication circuit, and in response, requests a biometric scan from the user to generate scan data.
Claim 24	
[24]	The system of claim 22, wherein when the integrated hardware device cannot verify scan data as being from the user, the integrated hardware device does not send the one or more codes and other data values.

Claim 25	
[25]	The system of claim 22, wherein the integrated hardware device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.
Claim 26	
[26]	The system of claim 22, wherein the biometric data includes one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.
Claim 27	
[27]	The system of claim 22, wherein the application includes one or more of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file and a financial account.

Claim 28	
[28]	The system of claim 22, wherein the application includes a file including medical information.
Claim 29	
[29]	The system of claim 22, wherein the application includes a financial account.

Microsoft Corporation (“**Petitioner**” or “**Microsoft**”) petitions for *Inter Partes* Review (“**IPR**”) of claims 1-29 (“**the Challenged Claims**”) of U.S. Patent No. 8,886,954 (“**the ‘954 Patent**”). This Petition presents compelling evidence demonstrating a reasonable likelihood that the Challenged Claims are invalid.

I. REQUIREMENTS FOR IPR

A. Grounds for Standing

Petitioner certifies that the ‘954 Patent is available for IPR. This petition is being filed within one year of service of a complaint against Microsoft. MSC-1004. Microsoft is not barred or estopped from requesting review of the Challenged Claims on the below-identified grounds.

B. Challenge and Relief Requested

Microsoft requests an IPR of the Challenged Claims on the grounds noted below. Dr. Patrick Traynor provides supporting testimony in his Declaration (MSC-1003, ¶¶[1]-[183]).

Ground	Claim(s)	35 U.S.C. § 103
1	1, 2, 4, 5, 7-13, 15, 16, 18-24, 26-29	Burger
2	3, 14, 17	Burger and Robinson
3	6, 25	Burger and Orsini

The earliest application that the ‘954 Patent claims priority from is US

provisional application No. 60/637,538, filed on December 20, 2004. MSC-1001, cover. While Petitioner does not concede that December 20, 2004 is the priority date that should be accorded to the '954 Patent, for the purposes of this proceeding, each of the references asserted in this Petition qualifies as prior art under 35 USC §§102(a), (b), or (e) (as shown in the table below) even if December 20, 2004 is used as the priority date of the '954 Patent.

Reference	Filing Date	Publication Date
US 2005/0050367 (Burger or MSC-1005)	Sept. 30, 2004	Mar. 3, 2005
US 2003/0177102 (Robinson or MSC-1006)	Feb. 19, 2003	Sept. 18, 2003
US 2004/0049687 (Orsini or MSC-1021)	Jun. 11, 2003	Mar. 11, 2004

C. Claim Construction

No formal claim constructions are necessary because “claim terms need only be construed to the extent necessary to resolve the controversy.” *Wellman, Inc. v. Eastman Chem. Co.*, 642 F.3d 1355, 1361 (Fed. Cir. 2011). For completeness, Petitioner notes the three phrases addressed by the Board during a prior IPR proceeding (IPR2021-01444) in this family of patents. In IPR2021-01444, the Board

noted that:

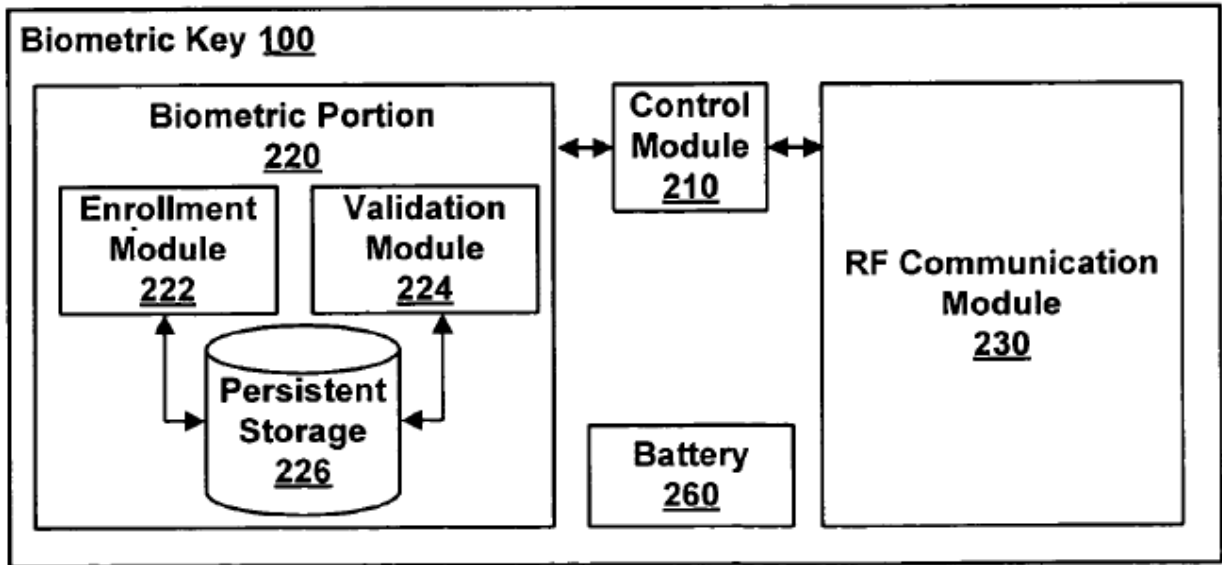
- 1) “interpretation of ‘tamper proof format’ is not necessary to determine whether to institute an *inter partes* review”;
- 2) “[t]he plain meaning of ‘third-party trusted authority’ suggests an entity or party separate from the principal parties to a transaction”; and
- 3) “no further interpretation of the ‘access message’ limitations is necessary.”

MSC-1007, 11-15. The references asserted in this Petition render the claims obvious even if these earlier positions adopted by the Board are used in this proceeding. MSC-1003, ¶¶[43]-[44].

Petitioner reserves the right to respond to any constructions offered by Patent Owner or the Board. Petitioner is not conceding that each challenged claim satisfies all statutory requirements. Petitioner is not waiving any arguments concerning other grounds that cannot be raised in IPR proceedings.

II. OVERVIEW OF THE '954 PATENT

The '954 patent discloses a biometric key 100, as shown in FIG. 2 below, that can be used to perform the biometric verification of a user using a trusted key authority. MSC-1001, 4:40-5:62, 6:56-62; MSC-1003, ¶¶[45]-[49].



MSC-1001, FIG. 2.

III. THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. [GROUND 1] – Burger Renders Obvious Claims 1, 2, 4, 5, 7-13, 15, 16, 18-24, 26-29

1. Burger

As shown in Burger's FIG. 1 below, Burger's system 100 includes a Pocket Vault 102, an associated token 102a, network server(s) 114, interface stations 104a-c coupled to the network server(s), commercial card reader(s) 106, commercial bar code reader(s) 107, and computers 108, 110, and 112 operated by one or more advertisers, non-financial media issuers, and financial media issuers, respectively. MSC-1005, ¶¶[51], [93], [96]-[97]; MSC-1003, ¶¶[50]-[51].

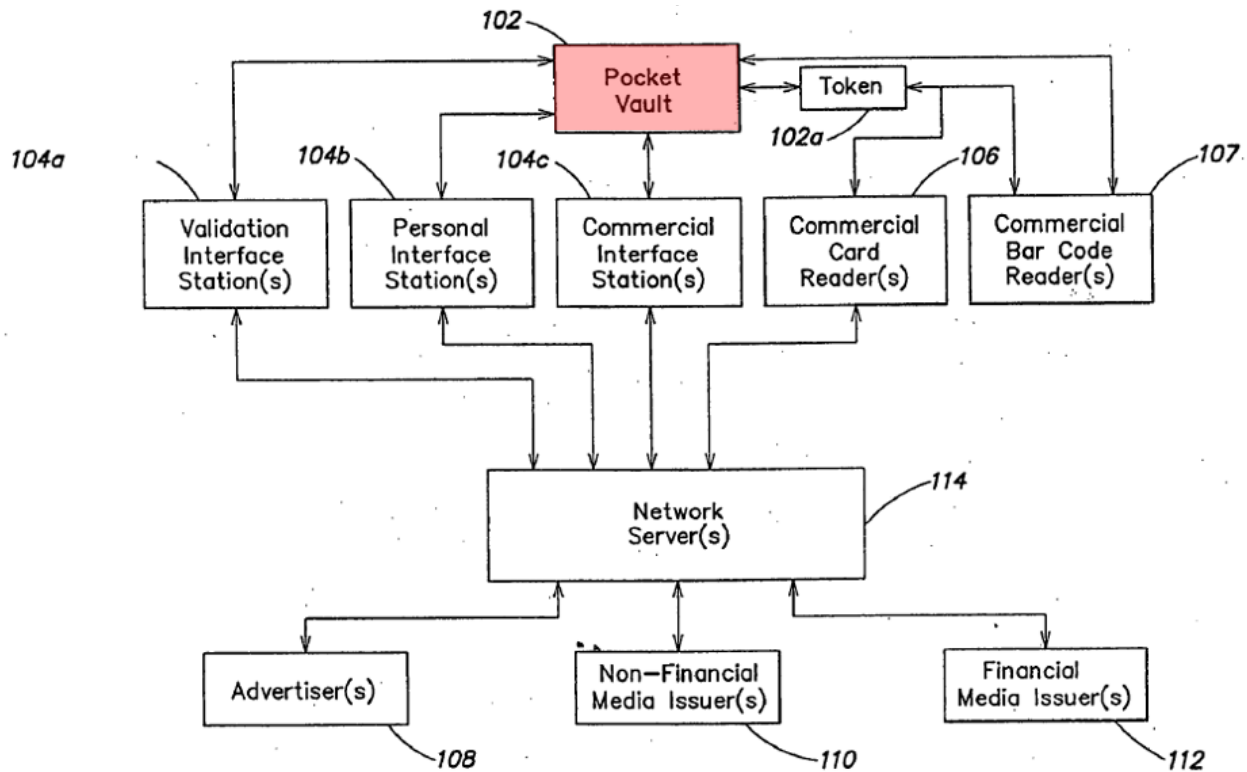


FIG. 1

MSC-1005, FIG. 1¹.

An example of the Pocket Vault is shown below in Burger's FIG. 2.

Burger's Pocket Vault includes "a controller 202, ... a transceiver 204, a user input device 206, a docking interface 208, a read/write memory 210, a write-once memory 212, a power manager 214, an indicator 215, a display 216, a token port 218, and a fingerprint scanner 220, all coupled to the controller 202." MSC-1005, ¶[118]. Burger "is not limited to any particular type of memory. The memory 210 may, for example, comprise a suitable non-volatile SRAM. Similarly, any suitable

¹ Annotations to figures in the petition are marked up in color.

memory device that permits a only [sic] single write operation to take place may be employed as the write-once memory 212.” MSC-1005, ¶[127]. The Pocket Vault may also include a hard-wired memory (not shown) to store device serial numbers and key operating system and encryption software components.” MSC-1005, ¶[118]; MSC-1003, ¶[52].

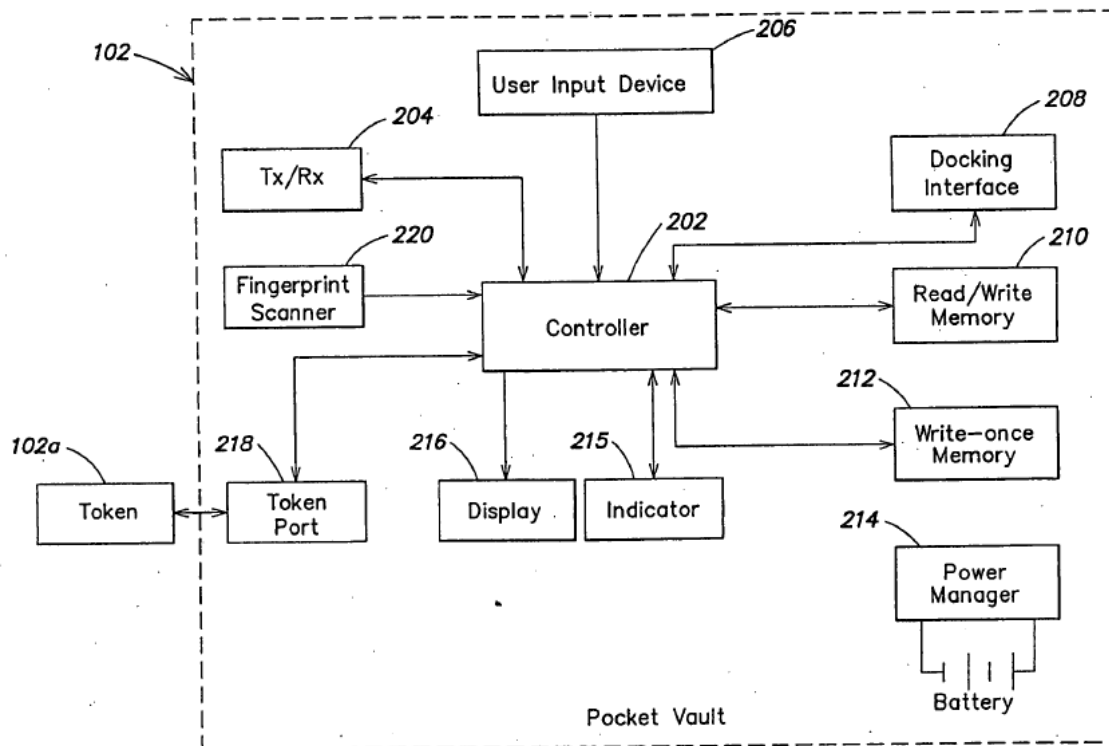


FIG. 2

MSC-1005, FIG. 2.

Memory 210 can include a high-security section used to “store value-based or value-linked media such as debit and credit cards and certain ID information such as driver's licenses, passports.” MSC-1005, ¶[129]; MSC-1003, ¶[53].

The controller 202 includes “a low-power multiprocessor or microcomputer

having an on-board SRAM and/or flash memory.” MSC-1005, ¶[122]. “The controller 202 may include a software-programmable and encryption-protected or hard-wired unique chip ID. In one embodiment, this chip ID [(Pocket Vault ID)] is released from the Pocket Vault only after the fingerprint scanner 220 ... has successfully authenticated the identity of the holder.” MSC-1005, ¶[122]; MSC-1003, ¶[54].

The Pocket Vault includes a display 216 (e.g., touch screen) to dynamically display branding and advertising messages or desired media (e.g., a credit card, driver's license, library card). MSC-1005, ¶¶[109], [110], [132], [133]; MSC-1003, ¶[55].

The Pocket Vault can also include a token 102a, which “may be used by the Pocket Vault holder to engage in a transaction.” MSC-1005, ¶[103]. Token 102a can be released from the Pocket Vault and can display information such as credit card information and used in transactions with retailers. MSC-1005, ¶¶[103]-[104], [155]-[158]; MSC-1003, ¶[56].

Burger's Pocket Vault also includes a scanning device such as a fingerprint scanner 220, iris or retina scanner, an optical sensor, and/or a voiceprint. MSC-1005, ¶[135]; MSC-1003, ¶[57].

When a user is interested in using the Pocket Vault, the user's biometric fea-

ture is used to authenticate the user. MSC-1005, ¶[112]. “In one illustrative embodiment, authentication information used to validate the holder's identity (e.g., the stored fingerprint ...) is stored within the to-be-accessed device,” that is the Pocket Vault, “and the validation is performed in its entirety on-board the same device, such that the user-specific authentication information never leaves the device in which it is stored. Thus, using this technique, the likelihood that such information will be intercepted by unauthorized third parties may be reduced significantly.” MSC-1005, ¶[112]. Moreover, “a trust relationship may be established between the network server 114 and the Pocket Vault 102.” MSC-1005, ¶[114]; MSC-1003, ¶[58].

In one example shown in FIG. 4 (reproduced below), Burger's network server may include a database 406 that stores “a real-time record of critical reference data along with transaction histories Examples of specific items that may be stored in the database 406 include: a list of current Pocket Vault holders ...; ... a list of currently authorized or registered Pocket Vaults 102, identified by chip ID and linked to the holder list; a list of currently authorized or registered tokens 102a, identified by chip ID and linked to the holder list; ... authorized media data received from media issuers that has not yet been downloaded to individual Pocket Vaults 102.” MSC-1005, ¶[146], FIG. 4; MSC-1003, ¶[59].

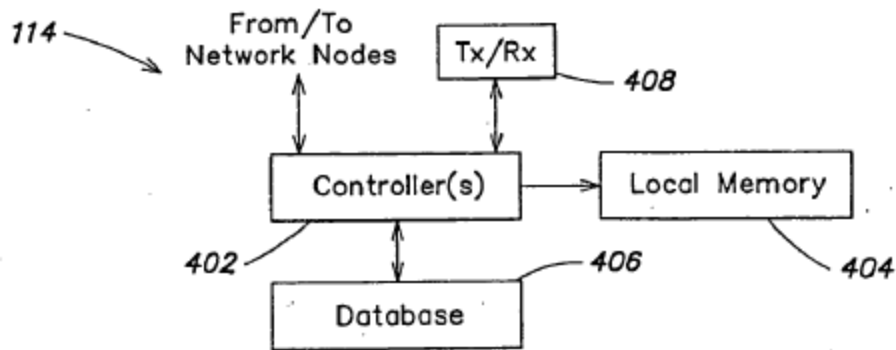


FIG. 4

MSC-1005, FIG. 4.

FIG. 27 (shown below) depicts another example implementation of a network server 114 that “include[s] one or more controllers 402 and a database 406, as described above in connection with FIG. 4. In addition, the network server may include a communication protocol layer 2716, which provides low-level communication functions to server communications software.” MSC-1005, ¶¶[0540], [0077], [0531], [0542]; MSC-1003, ¶[60].

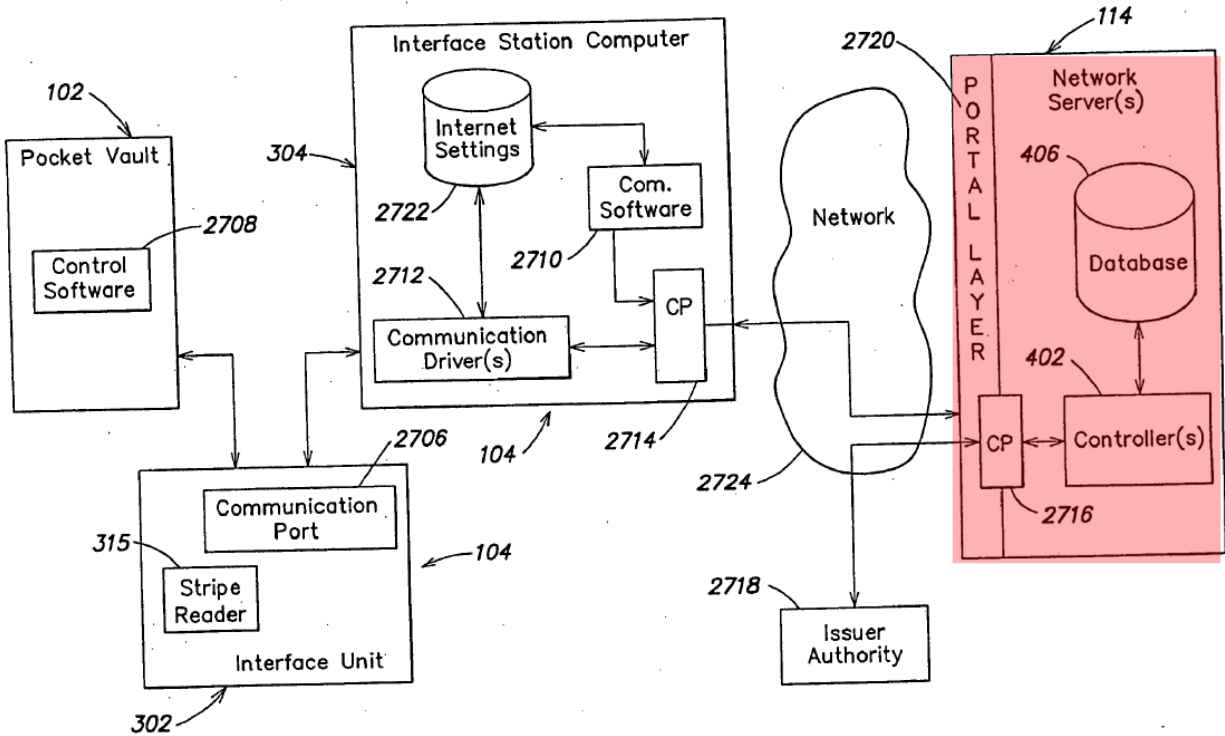
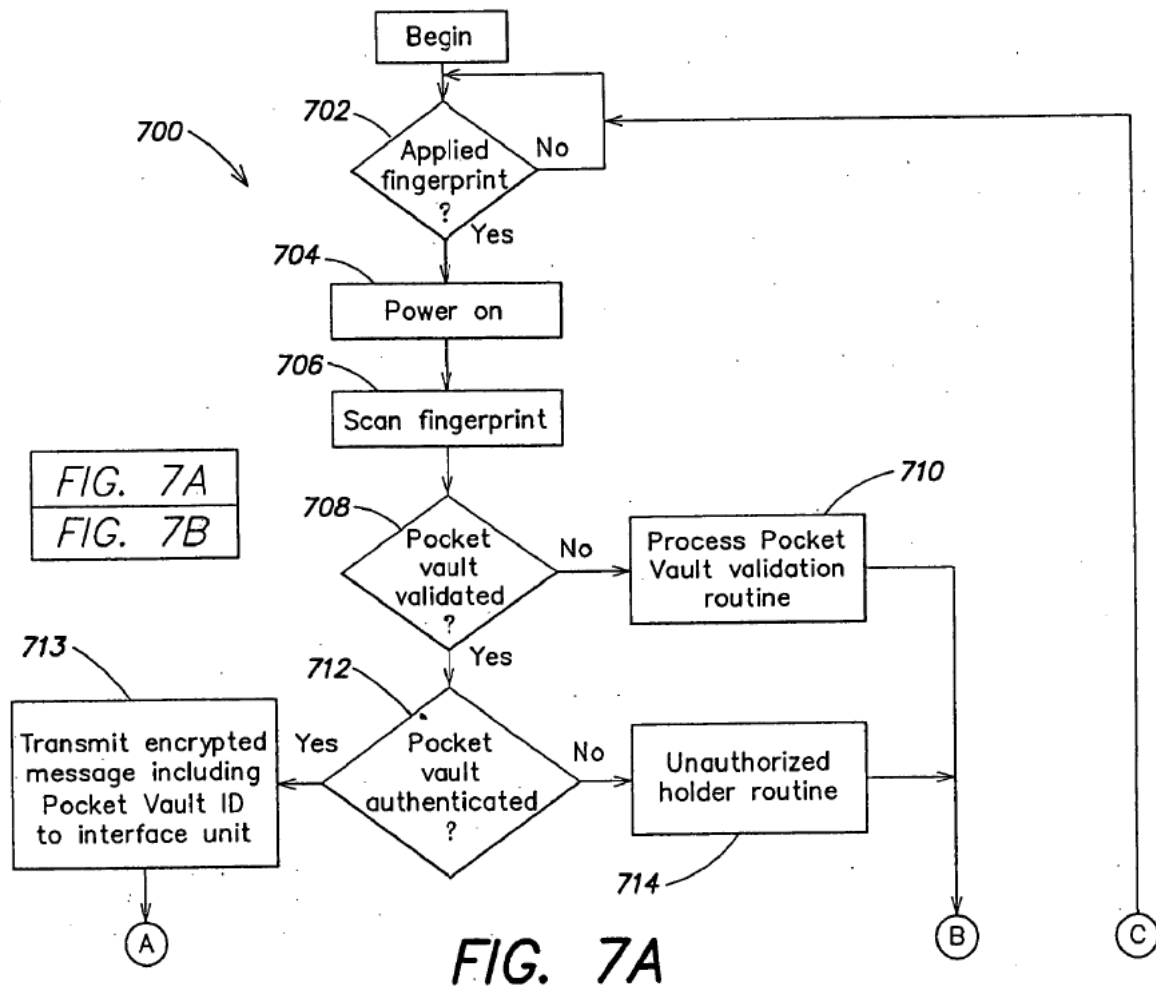


FIG. 27

MSC-1005, FIG. 27.

An example method of using Burger's Pocket Vault to perform user and device authentication is shown in Burger's FIG. 7A below. As shown, when a user's fingerprint is applied to the fingerprint scanner 220, the power manager 214 powers on the Pocket Vault. MSC-1005, ¶¶[178]-[181]. "[T]he fingerprint scanner 220 [then] scans the applied fingerprint of the Pocket Vault holder" and determines whether the Pocket Vault has been validated (step 708). MSC-1005, ¶¶[181]-[182]. "In one embodiment, the Pocket Vault 102 is not validated until: (1) a user's fingerprints have been stored in the fingerprint memory (e.g., the write-once

memory 212 of FIG. 2), and (2) the Pocket Vault 102 has received and stored encrypted validation information (e.g., a PKI certificate) from the network server 114.” MSC-1005, ¶[182]; MSC-1003, ¶[61].



MSC-1005, FIG. 7A.

“When, at the step 708, it is determined that the Pocket Vault 102 has already been validated,” at step 712 “it is determined whether Pocket Vault 102 has been authenticated, e.g., whether the fingerprint scanned at the step 706 matches

one of the fingerprints stored in the fingerprint memory 212.” MSC-1005,

¶¶[183]-[184], [209]-[210]. After “it is determined that the Pocket Vault 102 has been properly authenticated,” “an encrypted message including the unique Pocket Vault chip ID is transmitted to the pocket vault interface unit 302” or network server at step 713. MSC-1005, ¶¶[185]-[186], [101], [114]-[116]. Subsequently, a Pocket Vault holder can be granted access to the contents of his or her Pocket Vault. MSC-1005, ¶[187]; MSC-1003, ¶¶[62]-[63].

In some embodiments, after the unique Pocket Vault chip ID is transmitted and a Chameleon Card (token) is determined to be on-board the Pocket Vault, an “AUTHORIZED HOLDER” routine (step 722) is performed, as shown in FIGS. 7B, 10A, (reproduced below) and 11. MSC-1005, ¶¶[189]-[195]. In the “AUTHORIZED HOLDER” routine, advertisements sent from an advertiser 108 to the network server 104 are provided to the Pocket Vault for display. MSC-1005, ¶¶[236]-[238], FIG. 10A. In addition, a user can make selections to enter a wireless transaction. MSC-1005, ¶¶[257]-[262], FIGS. 10A, 11; MSC-1003, ¶[64].

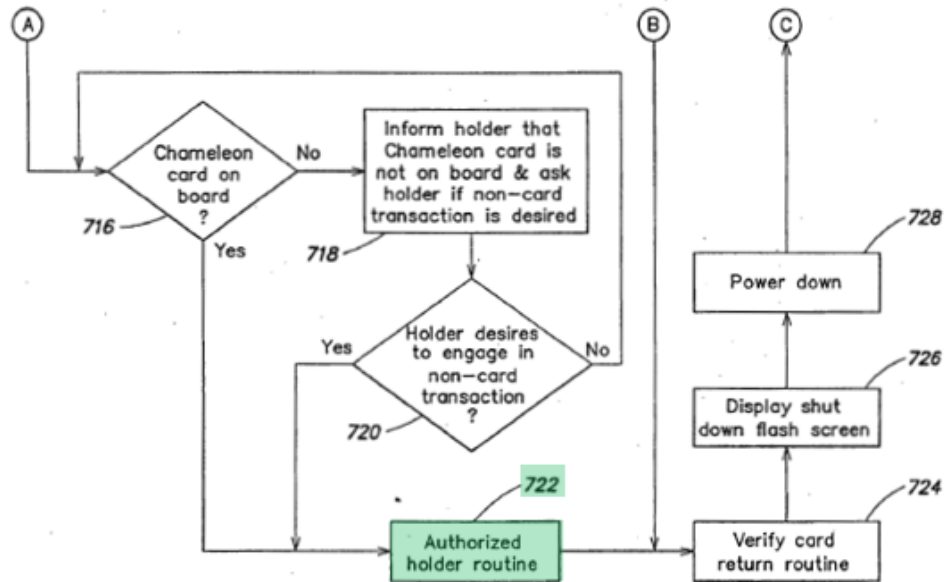


FIG. 7B

MSC-1005, FIG. 7B

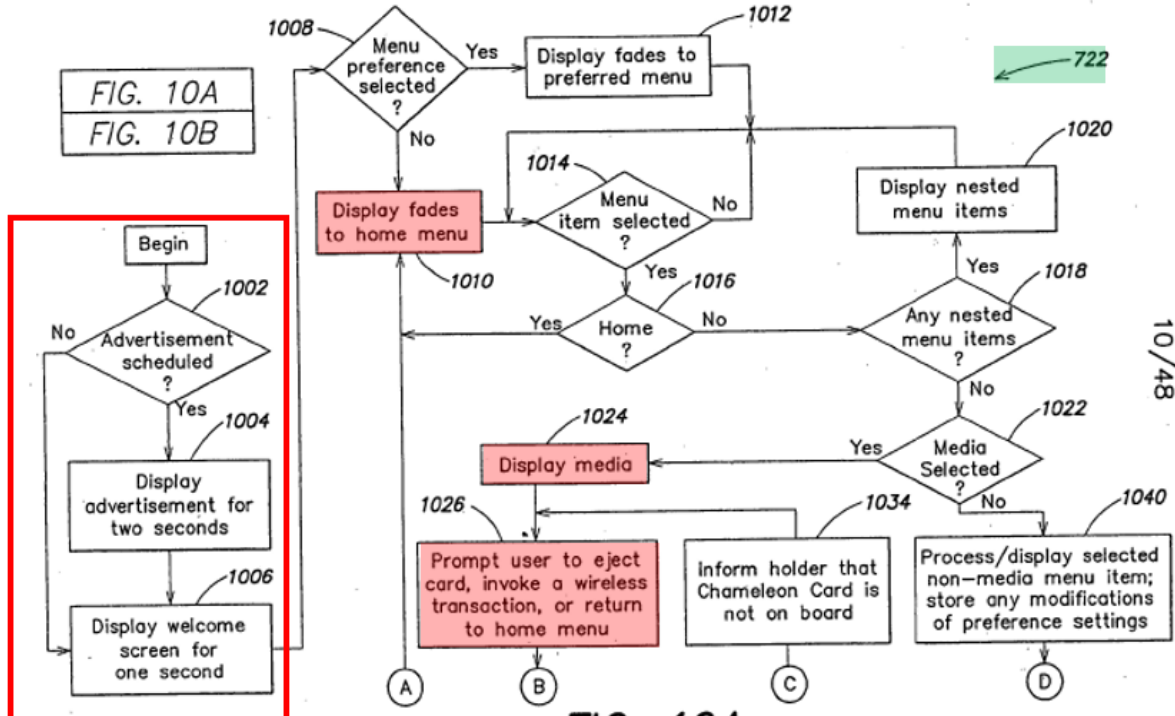


FIG. 10A

MSC-1005, FIG. 10A.

Burger's Pocket Vault can be used as a "wallet replacement" to execute a transaction. MSC-1005, FIGS. 19, 24, 25, ¶[93]. When a request to authorize a transaction has been made, Burger's network server implements the operations depicted in FIGS. 24 and 25 (reproduced below). MSC-1005, FIG. 19, ¶[0474]; MSC-1003, ¶[65].

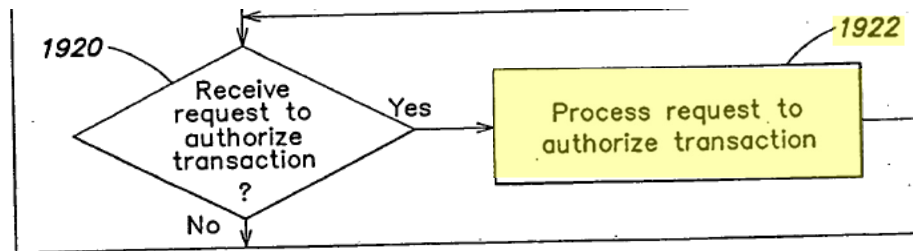


FIG. 19

MSC-1005, FIG. 19.

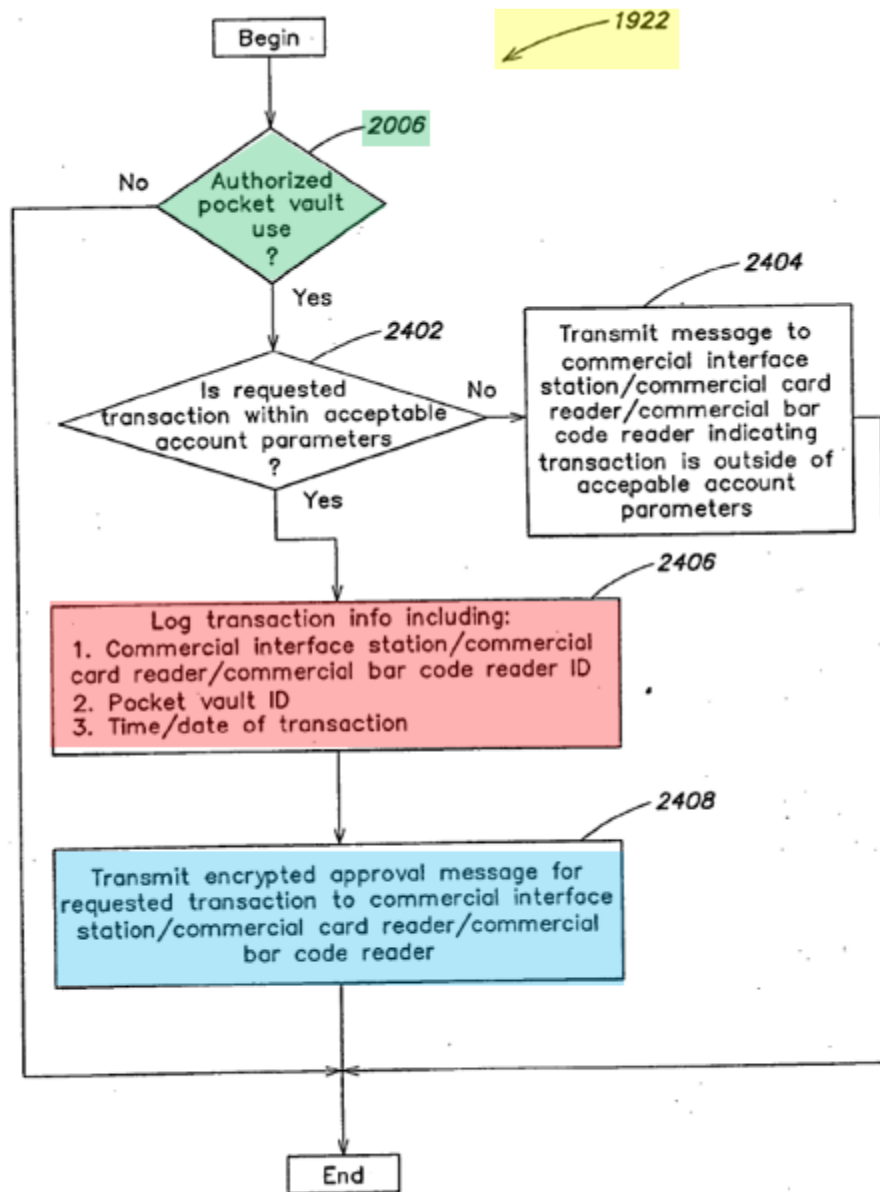
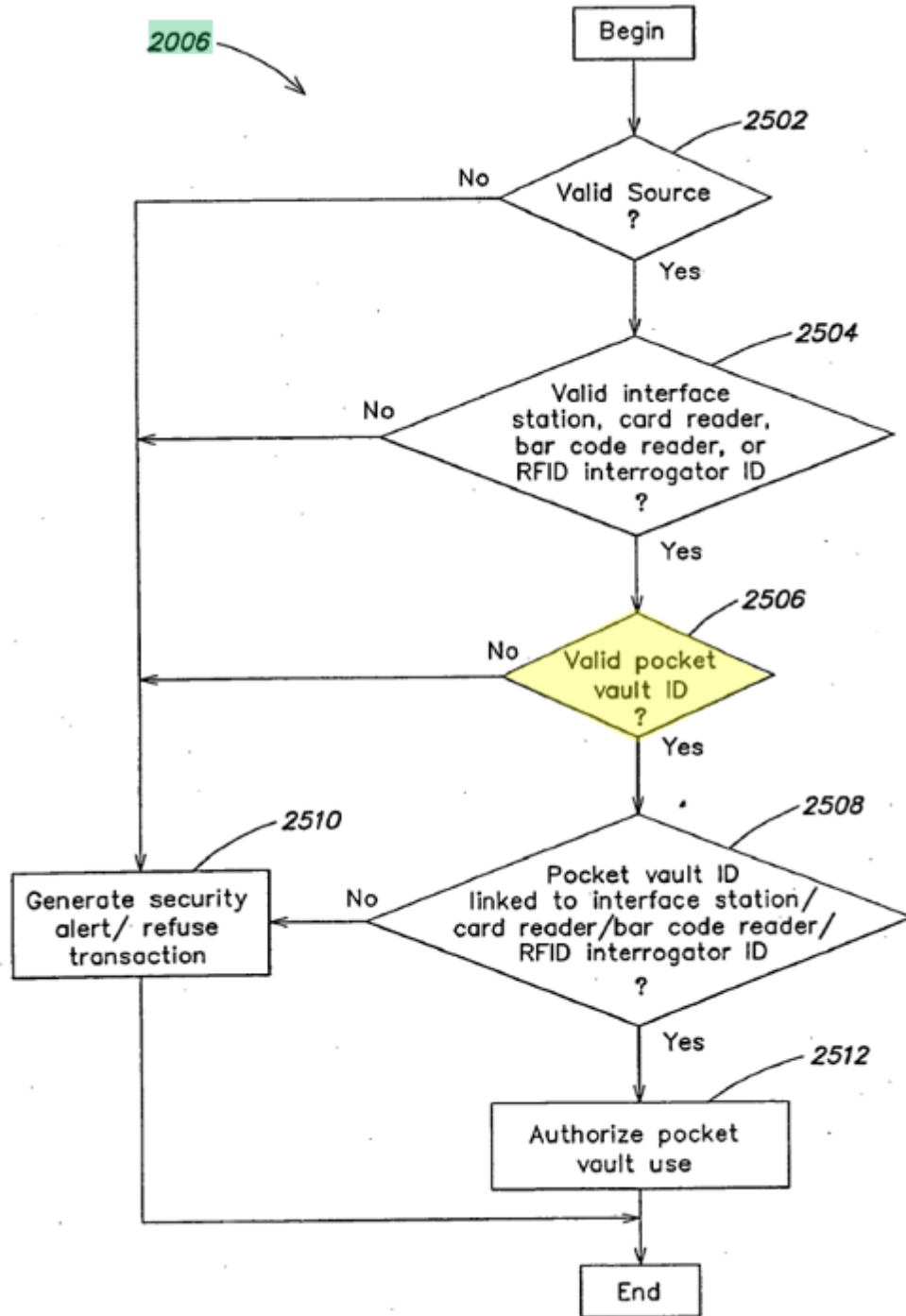


FIG. 24

MSC-1005, FIG. 24.



MSC-1005, FIG. 25.

As shown above, in response to the request to authorize a transaction, the network server determines whether the Pocket Vault is authorized. MSC-1005,

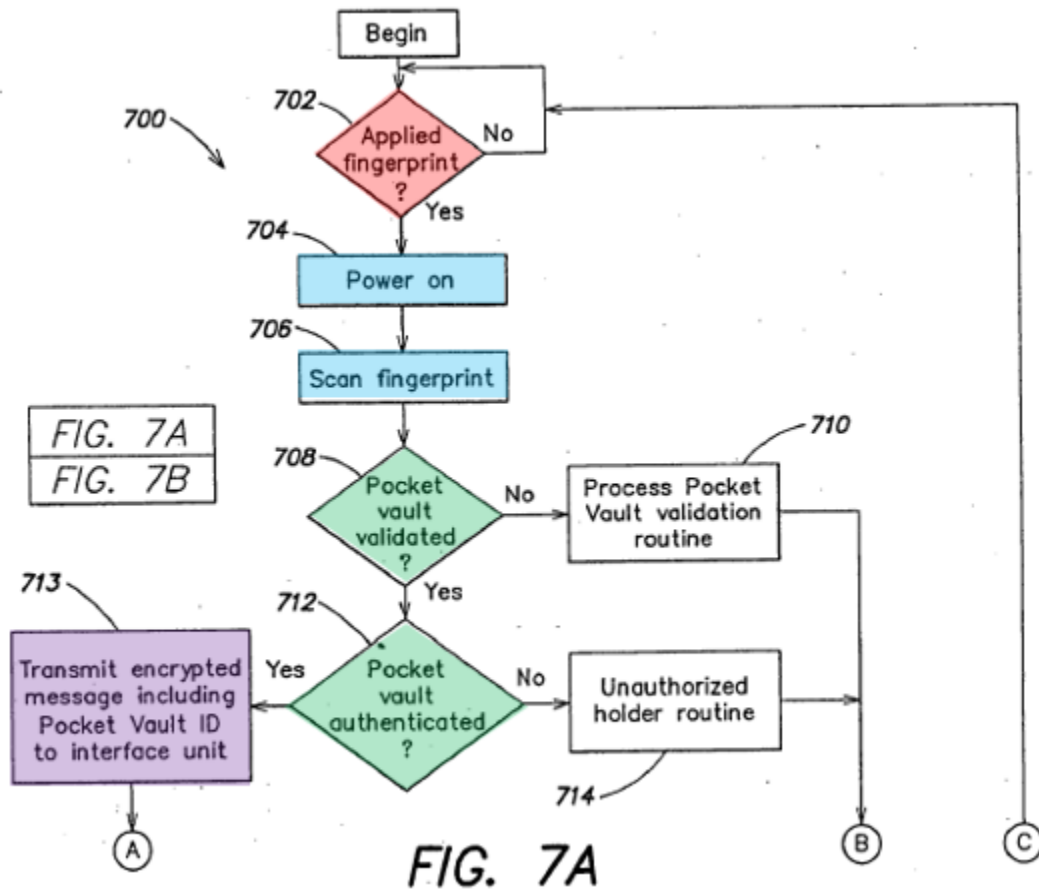
FIGS. 24, 25; ¶¶[0511]-[513]. To determine whether the Pocket Vault is authorized, it is determined (1) whether the point of sale terminal or other entity with which a transaction is being attempted is connected to a valid source, and (2) whether the ID of the interface station, card reader, barcode reader or RFID interrogator is valid, and is properly linked to the source to which is connected. MSC-1005, FIG. 25; ¶¶[0520]-[523]. If the network server determines that there is a valid source and the ID is valid, the network server proceeds to determine whether the Pocket Vault ID is valid, and upon, doing so, determines that the Pocket Vault is authorized. MSC-1005, FIG. 25; ¶¶[0524]-[529], [182]; MSC-1003, ¶[66].

After the Pocket Vault use is authorized, “an encrypted approval message is transmitted to the entity with which the transaction is being attempted (e.g., a commercial interface station 104C, a card reader 106, or a barcode reader 107).” MSC-1005, FIG. 24; ¶¶[0511]-[513], [0518]; MSC-1003, ¶[67].

Dr. Traynor’s Provided Example Use Case

When a user is interested in using the Pocket Vault for a transaction e.g., at a grocery store or retail store, the user places a finger on the Pocket Vault scanner (*see* red annotated diamond in FIG. 7A below). MSC-1005, FIG. 7A, ¶¶[320], [158], [95]. The Pocket Vault activates and then obtains a biometric scan (e.g., fingerprint or retina scan) (*see* blue annotated rectangles in FIG. 7A below) of the user and checks to see if a matching record is stored in the Pocket Vault memory

(see green annotated diamonds in FIG. 7A below). In response to determining that the scanned biometric data matches the stored biometric data, the Pocket Vault transmits its Pocket Vault ID to the network server (see purple annotated rectangle in FIG. 7A below). MSC-1003, ¶¶[68]-[69].



MSC-1005, FIG. 7A.

Next, the Pocket Vault holder is granted access to contents of the Pocket Vault, and if the Pocket Vault includes a token (also referred to as Chameleon Card), an Authorized Holder Routine (step 722) is performed (see yellow annotations in FIG. 7B below) in which a welcome screen and ads are displayed and a

user can select, through a displayed menu, a desire for executing a transaction using the Pocket Vault (*see* red annotations in FIG. 10A below). *See e.g.*, MSC-1005, step 722 in FIG. 7B, step 1026 in FIG. 10A; steps 1920, 1922 in FIG. 19; ¶¶[320], [189], [158], [95], [96], [125], [236]-[238], [155]-[158]; MSC-1003, ¶[70].

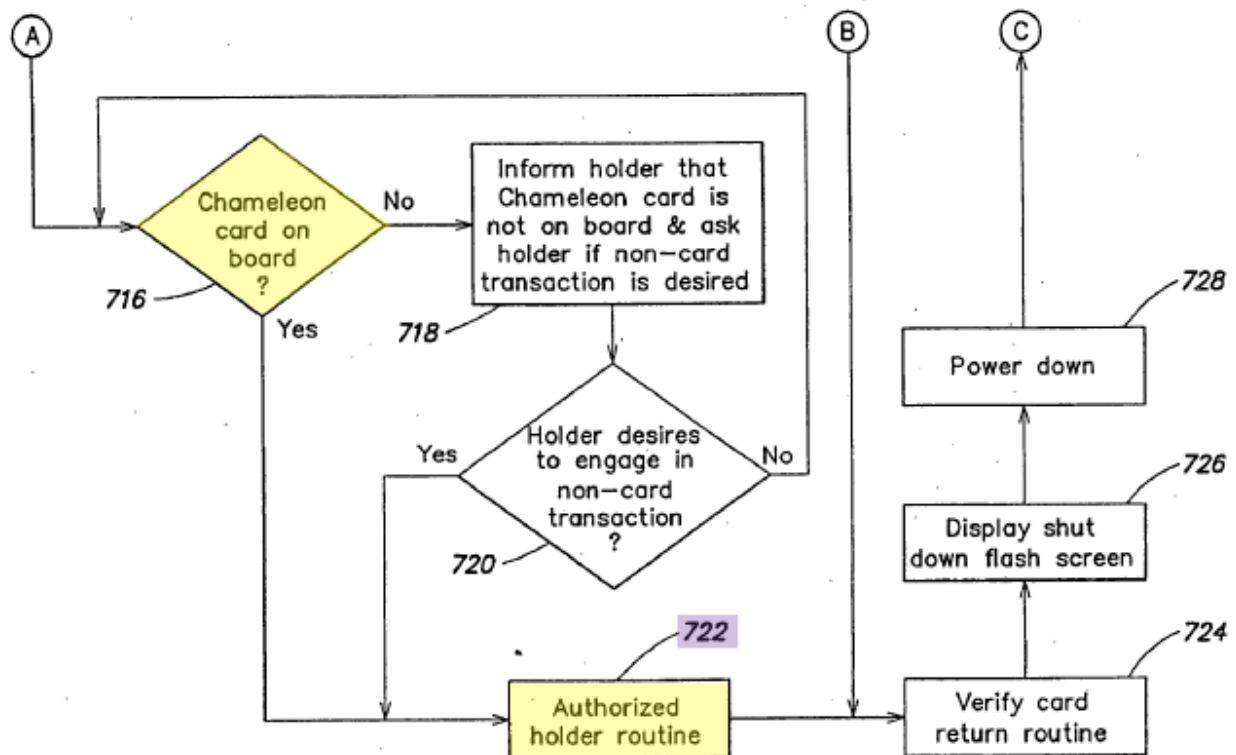
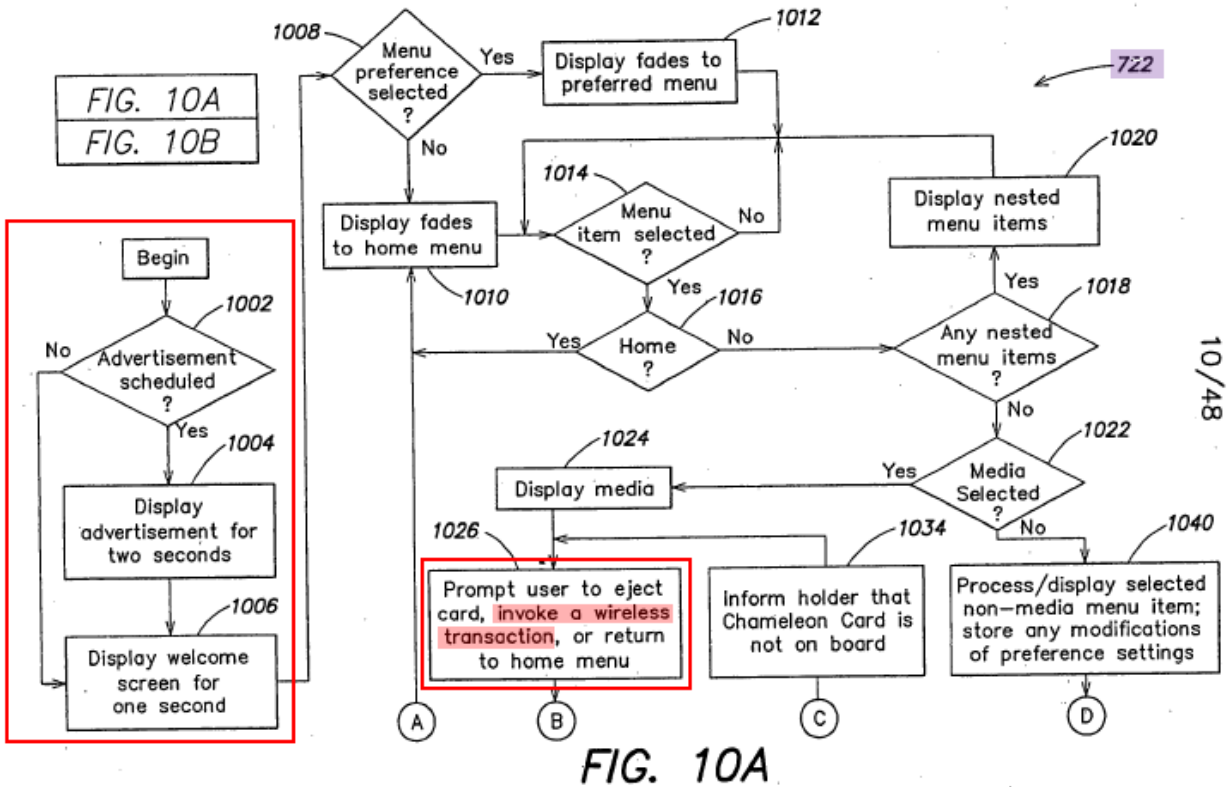


FIG. 7B

MSC-1005, FIG. 7B.



MSC-1005, FIG. 10A (displaying the steps performed in the Authorized Holder Routine 722 of FIG. 7B).

The network server then determines whether the Pocket Vault is authorized to be used, e.g., by checking whether the transmitted Pocket Vault ID matches a stored ID in the network server, and then transmits an approval message for the transaction. MSC-1005, FIGS. 19 (steps 1920, 1922), 24 (steps 2006, 2406, 2408), 25 (Steps 2506), ¶¶[0511]-[529], [182]; MSC-1003, ¶¶[71]-[73].

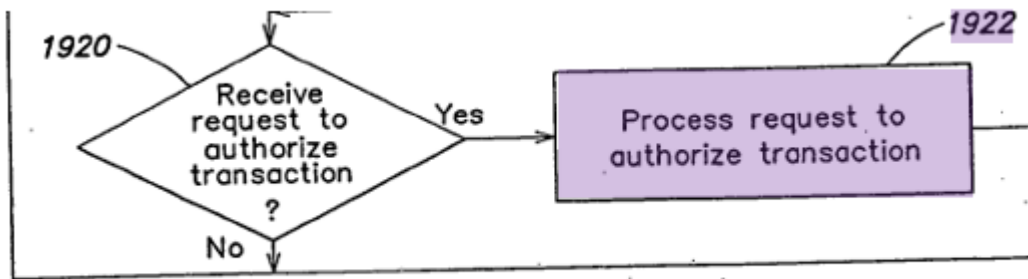


FIG. 19

MSC-1005, FIG. 19 (bottom portion of FIG. 19).

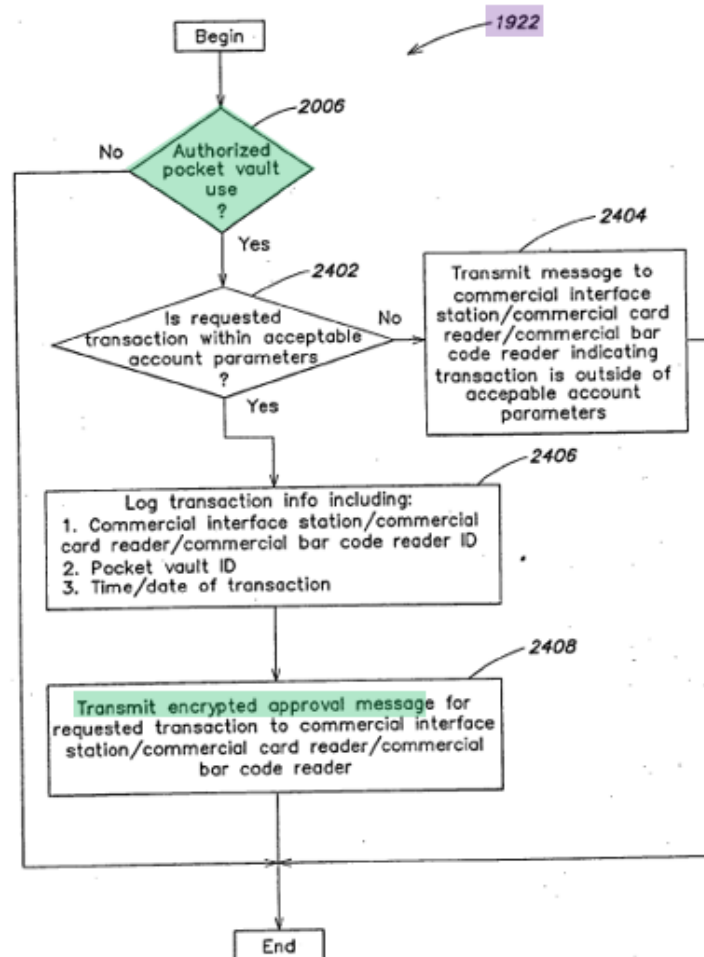


FIG. 24

MSC-1005, FIG. 24 (displaying) the steps performed in the step(s) of processing a request to authorize a transaction of FIG. 19.

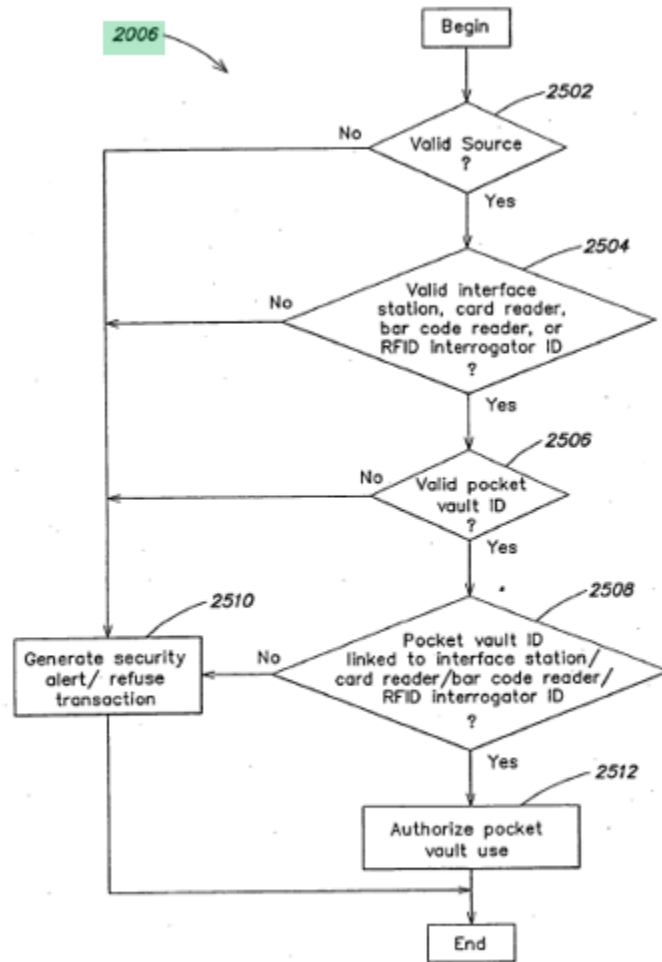


FIG. 25

MSC-1005, FIG. 25 (displaying the steps performed in the operation 2006 of authorizing use of a Pocket Vault in FIG. 24).

2. Application of Burger to the '954 Claims

[1.pre]

As explained below in [1.1]-[1.5], Burger teaches systems and methods (“*A method*”) for verifying a Pocket Vault holder during authentication of a Pocket Vault used in transactions involving financial and/or non-financial media. MSC-

1005, ¶¶[0002], [0010], [0127]-[0128]; MSC-1003, ¶[89].

[1.1]

Burger's Pocket Vault 102, shown below in FIG. 2, is “*an integrated device*” at least because it integrates a plurality of components including a fingerprint scanner 220, display 216, memories 210, 212, and token 102a/token port 218.

MSC-1005, ¶¶[0118], [0134]. The Pocket Vault is self-contained with a set of authentication security features to ensure privacy. MSC-1005, ¶¶[0094], [0095]; MSC-1003, ¶[90].

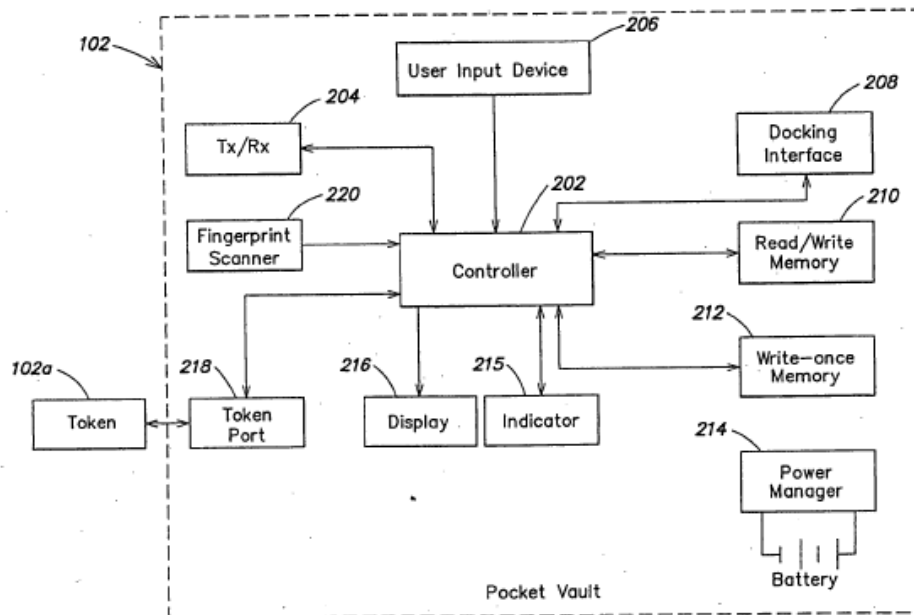


FIG. 2

MSC-1005, FIG. 2.

Like the '954 patent, Burger recognizes the importance of storing biometric data on the same device that authenticates a user's biometric scan. MSC-1005, ¶[112] (“the validation is performed in its entirety on-board the same device, such that the user-specific authentication information never leaves the device in which it is stored”), ¶[114]. Burger's Pocket Vault includes a write-once memory 212 or any suitable memory device that permits only a single write operation to take place (*“a storage element on the integrated device that is not capable of being subsequently altered”*). MSC-1005, ¶¶[127], [182], FIG. 2 (reproduced below); MSC-1003, ¶[91].

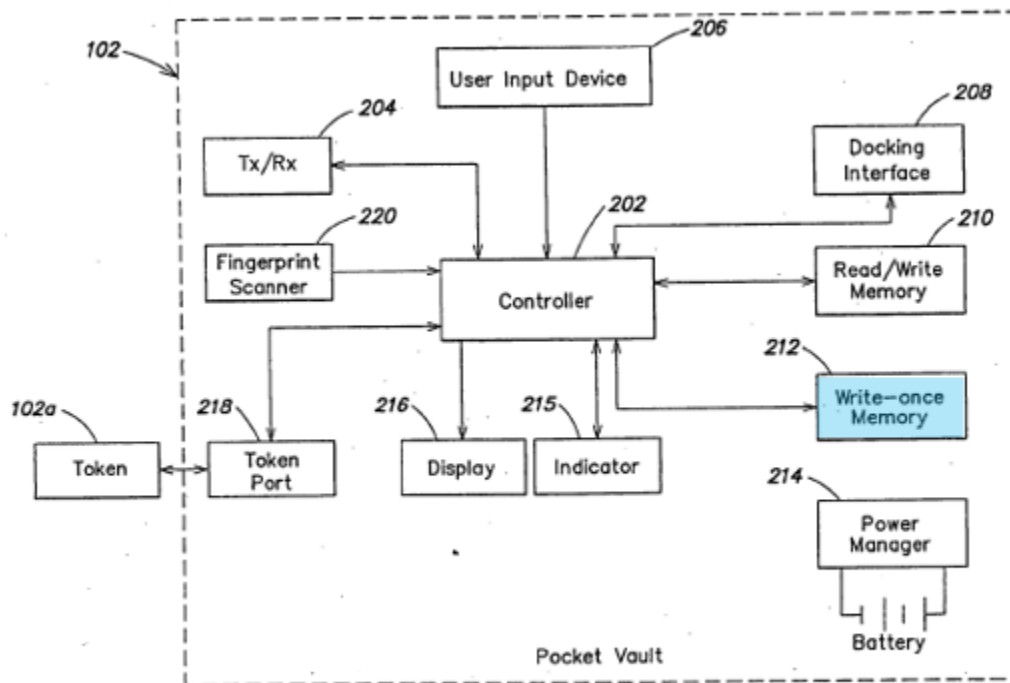


FIG. 2

MSC-1005, FIG. 2.

The Pocket Vault stores authentication information, such as user fingerprints (“*biometric data of a user*”), device serial numbers such as a Pocket Vault ID, and encryption/decryption information (“*a plurality of codes and other data values comprising a device ID code uniquely identifying an integrated device and a secret decryption value*”). MSC-1005, ¶¶[0112], [114], [118], [122], [127], [129]. Indeed, Burger teaches that the network server provides the PKI certificate to the Pocket Vault and grants the Pocket Vault authority to permanently store authentication information (“*persistently storing biometric data and a plurality of codes and other data values ...*”). MSC-1005, ¶¶[114], [182]; MSC-1003, ¶[92].

In particular, a person of ordinary skill in the art at the Critical Date (POSITA) would have understood that a device serial number is typically unique to the device and would have, therefore, been often used as a device ID to advantageously distinguish that particular device from other such devices. MSC-1003, ¶¶[22]-[23], [93]. Thus, a POSITA would have understood that Burger’s Pocket Vault ID number renders obvious “*a plurality of codes and other data values comprising a device ID code uniquely identifying an integrated device.*” MSC-1003, ¶[93]. The ’954 patent suggests that a device ID code can be both the “plurality of codes” and “other data values.” MSC-1001, 8:18-25. Consistent with the description in the ’954 patent, Burger’s Pocket Vault ID thus satisfies “*a plurality of*

codes and other data values comprising a device ID code uniquely identifying the integrated device.” MSC-1003, ¶¶[93]-[94].

Alternatively, it was also known and would have been obvious to a POSITA that a device ID code includes different parts such that one part of the device ID code, which includes two or more alphanumeric code data, corresponds to the “plurality of codes” and another portion of the device ID code, which may also include two or more alphanumeric code data, corresponds to the “other data values.” MSC-1003, ¶[95]. Neither the claims nor the specification impose any restriction as to the individual contents of the “*plurality of codes*” or the “*other data values.*”

Burger also discloses that encryption and decryption may be employed when transferring information and that encryption software resides in the hard-wired memory. MSC-1005, ¶¶[118], [551]-[552], [154]. Encryption techniques including “asymmetric-key encryption types, such as public key encryption or private key encryption, may be used.” MSC-1005, ¶[552]. Thus, it would have been obvious to a POSITA that Burger also discloses “*persistently storing ...a secret decryption value.*” MSC-1003, ¶[96]. For example, asymmetric encryption, also known as public-key encryption, is a process that uses a pair of related keys (one public key and one private key) to encrypt and decrypt a message and protect it from unauthorized access or use. A public key, such as PKI certificate, is a cryptographic key that can be used by any person to encrypt a message so that it can only

be decrypted by the intended recipient with their private key. A private key, also known as a secret key, is only maintained by the key's initiator and can be used to decrypt a message. Thus, it would have been obvious to a POSITA that to use “asymmetric-key encryption types, such as public key encryption or private key encryption,” Burger’s system would have included a private key (“*secret decryption value*”). MSC-1003, ¶[96]. Moreover, because such a private key should not be accessible to anyone other than the holder of the private key or modified without the holder’s consent, keeping the private key secure is important to prevent unauthorized parties from improperly using or modifying the private key. Accordingly, it would have been obvious to a POSITA that the private key would be stored in a secure location where it cannot be tampered with (“*a secret decryption value in a tamper proof format*”). MSC-1003, ¶[96].

It would have been obvious to a POSITA that a “write-once memory” 212 or a memory device that permits only a single write operation to take place stores data in “*a tamper proof format*,” because the stored data in the memory is tamper resistant. MSC-1010, 10:56-63 (“physical tamper proof device is a write once memory”), 6:25-29; MSC-1011, 1:12-28; MSC-1003, ¶[97].

While Burger explicitly discloses storing a user’s biometric data in the write-once memory 212, and storing other data such as the Pocket Vault holder’s private key (encryption/decryption information) and device serial numbers in a hard-wired

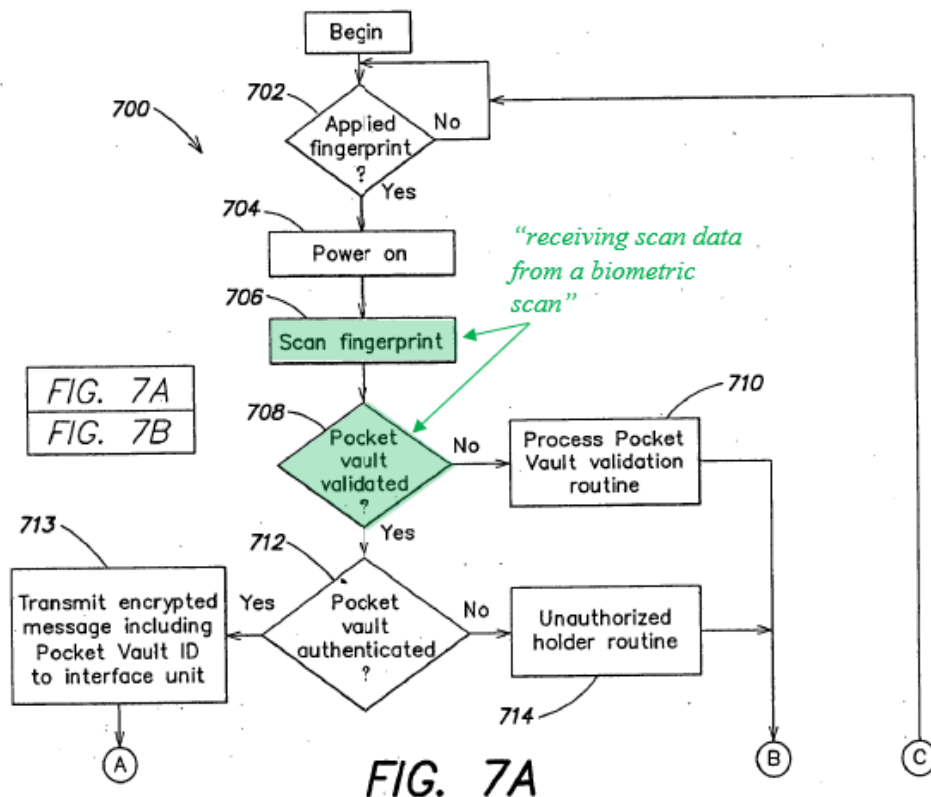
memory that is not shown, it would have been obvious for all this information to be persistently stored “*in a tamper proof format written to a storage element on the integrated device that is not capable of being subsequently altered.*” MSC-1003, ¶[98]. For instance, it would have been obvious that the hard-wired memory is also implemented as a protected, write-once memory so that sensitive information such as a device ID code and encryption/decryption information is not tampered with and is kept secure. *Id.* Moreover, a POSITA would have understood that information, such as the user’s biometric data, device ID, and private key, is unique and is typically not subject to change. *Id.* For instance, a user’s fingerprint does not change, and a unique device ID code would not typically be modified to another serial number. Because biometric data or unique device ID code is sensitive data that is not subject to change and is not typically modified after storage, it would have been obvious to a POSITA to persistently store such data in the tamper proof memory of the Burger system. *Id.*

[1.2]

As depicted below in Burger’s FIGS. 7A and 2, a user can activate the Pocket Vault by applying a finger on the fingerprint scanner 220 or perform “a physical action, e.g., the activation of a hardware switch.” MSC-1005, ¶¶[0178]-

[0180]. In response to this activation, the Pocket Vault is powered up and “the fingerprint scanner 220 scan[s] the applied fingerprint of the Pocket Vault holder.”

MSC-1005, ¶[0181]. The application of the finger or physical action corresponds to “*a request for a biometric verification of the user*” because it is performed “with each attempted use of any of these devices” and because a biometric scan, such as a fingerprint scan or retina scan, is a known part of the process enabling such use. The controller 202 in the Pocket Vault receives biometric scan data (“*receiving scan data from a biometric scan*”), e.g., from the fingerprint scanner 220 or retina scanner. MSC-1005, ¶¶[135], [0182], [0112]; MSC-1003, ¶[99].



MSC-1005, FIG. 7A.

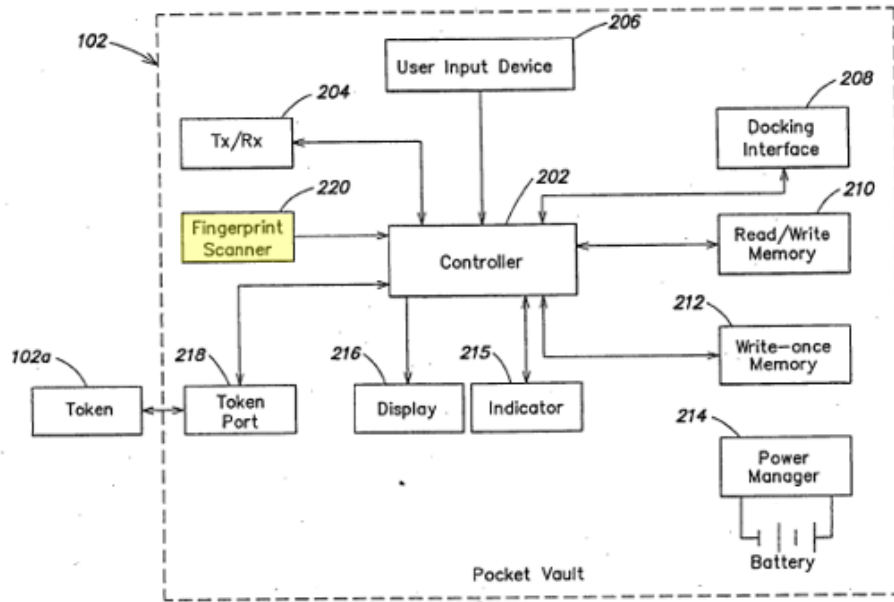


FIG. 2

MSC-1005, FIG. 2.

Although the example of Burger's mapping to the 954 claims is of fingerprint scanning, Burger discloses that various suitable authentication techniques could be used in place of fingerprint scanning, such as, e.g., retina scanning, voice recognition, hand geometry. MSC-1005, ¶¶[0112], [0135]; MSC-1003, ¶[100].

[1.3]

After receiving the scan data from the biometric scan, the user's scanned data are compared to biometric data stored in the write-once memory 212 to determine if the scanned data matches the user's stored biometric data (*"comparing the scan data to the biometric data to determine whether the scan data matches the biometric data"*). MSC-1005, ¶¶[0182]-[0184], FIGS. 7A, 2; MSC-1003, ¶[101].

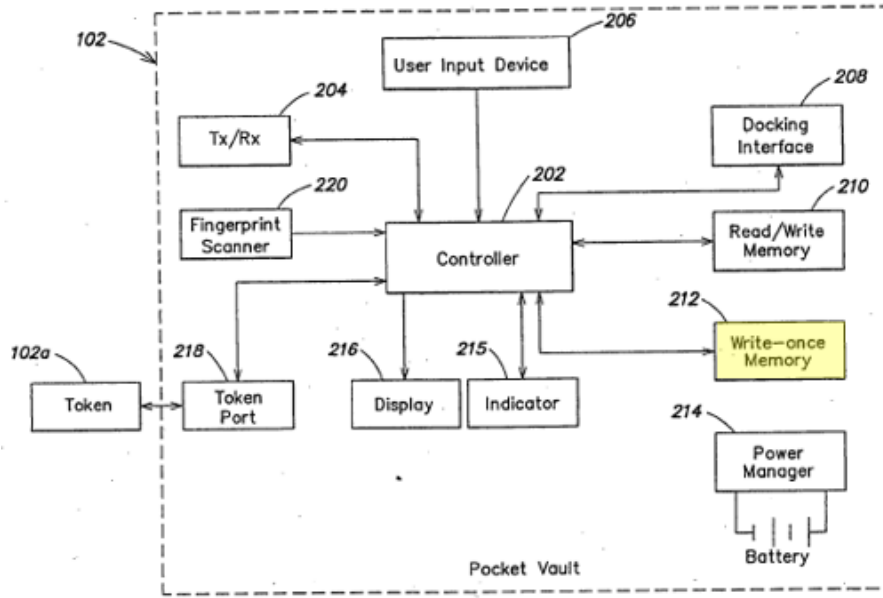


FIG. 2

MSC-1005, FIG. 2.

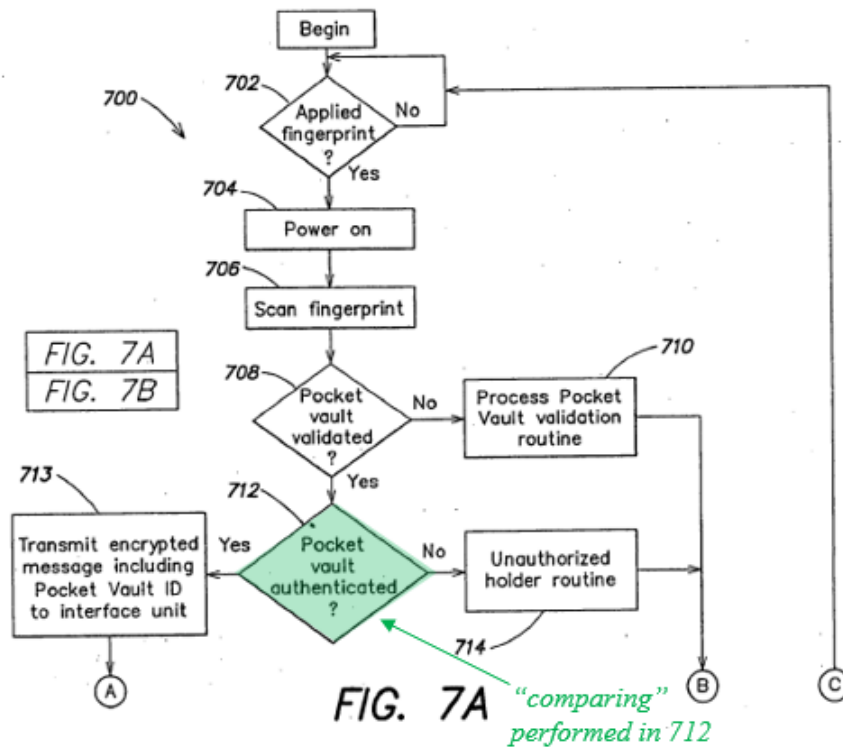
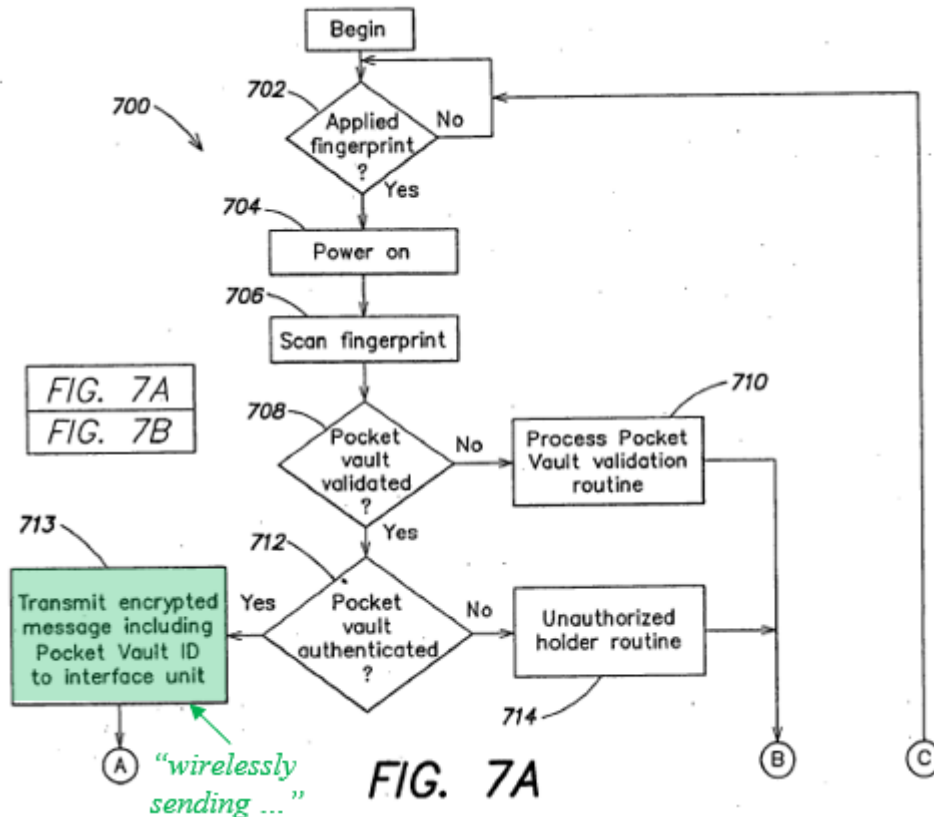


FIG. 7A "comparing"
performed in 712

MSC-1005, FIG. 7A.

[1.4]

As shown in FIG. 7A, at step 712 “it is determined whether Pocket Vault has been authenticated, e.g., whether the fingerprint scanned at the step 706 matches one of the fingerprints stored in the fingerprint memory 212.” MSC-1005, ¶¶[183]-[184], [209]-[210]. And “*responsive to a determination that the scan data matches the biometric data*” (step 712), the Pocket Vault wirelessly sends (step 713) an encrypted message including the unique Pocket Vault chip ID (“*wirelessly sending one or more codes and other values from the plurality of codes and the other data values ... wherein the one or more codes and other data values includes the device ID code*”). MSC-1005, ¶¶[0186], [114], [122], [146], FIG. 7A; MSC-1003, ¶[102].



MSC-1005, FIG. 7A.

In related disclosure, Burger teaches that authentication information, such as the encrypted message including the unique Pocket Vault ID, are transmitted to the network server. MSC-1005, ¶¶[0113]-[0114]. A POSITA would have understood that the encrypted message would have also included other codes and data values such as header information, destination information, or encrypted data or information that are typically included in encrypted messages. MSC-1003, ¶[103].

Communication between the various network elements, e.g., between the Pocket Vault, interface stations 104a-c, and network server can be wireless, and the Pocket Vault can communicate directly with the network server. MSC-1005,

¶¶[0099]-[0101], [0097], [0123], FIG. 1 (reproduced below); MSC-1003, ¶[104].

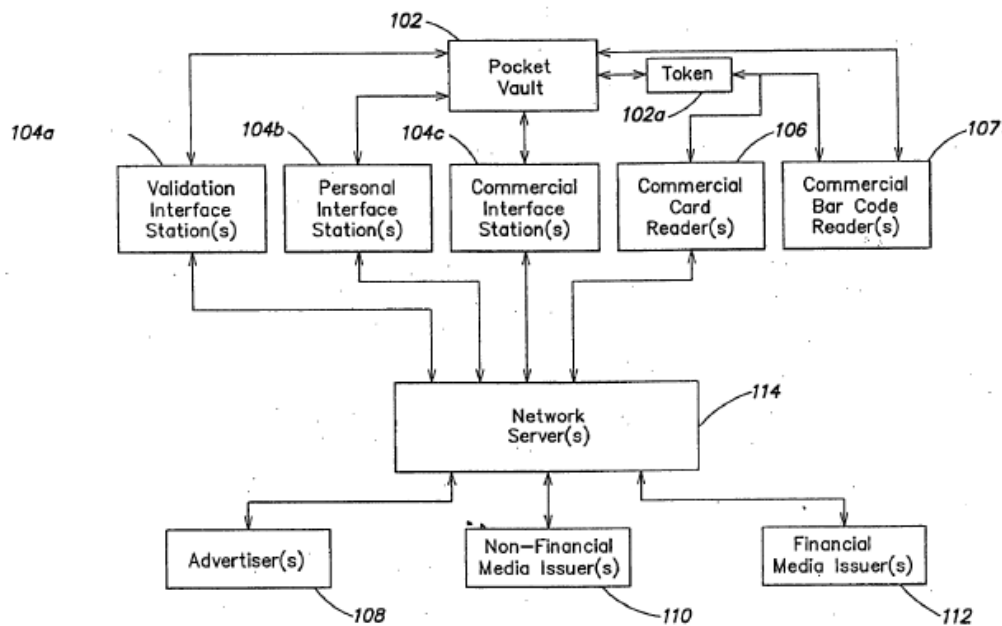


FIG. 1

MSC-1005, FIG. 1.

The table below lists the parties engaged in a transaction in Burger’s system, as described above consistent with the Use Case noted above in §III.A.1. MSC-1003, ¶[105].

First party	Second Party	Third party that operates a trusted authority	Trusted authority
Pocket Vault holder (user)	Retailer	Party operating the network server	The network server 114, as a whole, or, in some

			cases, a portion (a controller 402 and database 406) of the network server.
--	--	--	---

It would also have been obvious to a POSITA that Burger contemplates several possible transactions between different parties, as noted in the table below. MSC-1003, ¶[106]. In each example noted below, the first party is the Pocket Vault holder.

Transaction	Second Party	Third party	Trusted authority
Obtaining payment information or authorization for charging a credit card or bank account	Financial media issuer 112 (e.g., bank or credit card company)	Party operating the network server	The network server 114, as a whole, or, in some cases, a portion (a controller 402 and database 406) of the network server
Obtaining authorization to	Non-financial media		

enter a secure building or facility	issuer 110 (e.g., hotel card key issuer, library, building management for company)		
Obtaining advertisement content or related information	Advertiser(s) 108		

MSC-1005, ¶¶[94], [98], [103]-[104], [110]-[111], [117], [128]-[129], [155]-[158], [237]-[240], [255], [324]-[328], [0511]-[513], [679]; MSC-1003, ¶[107].

“A Third Party that Operates a Trusted Authority”

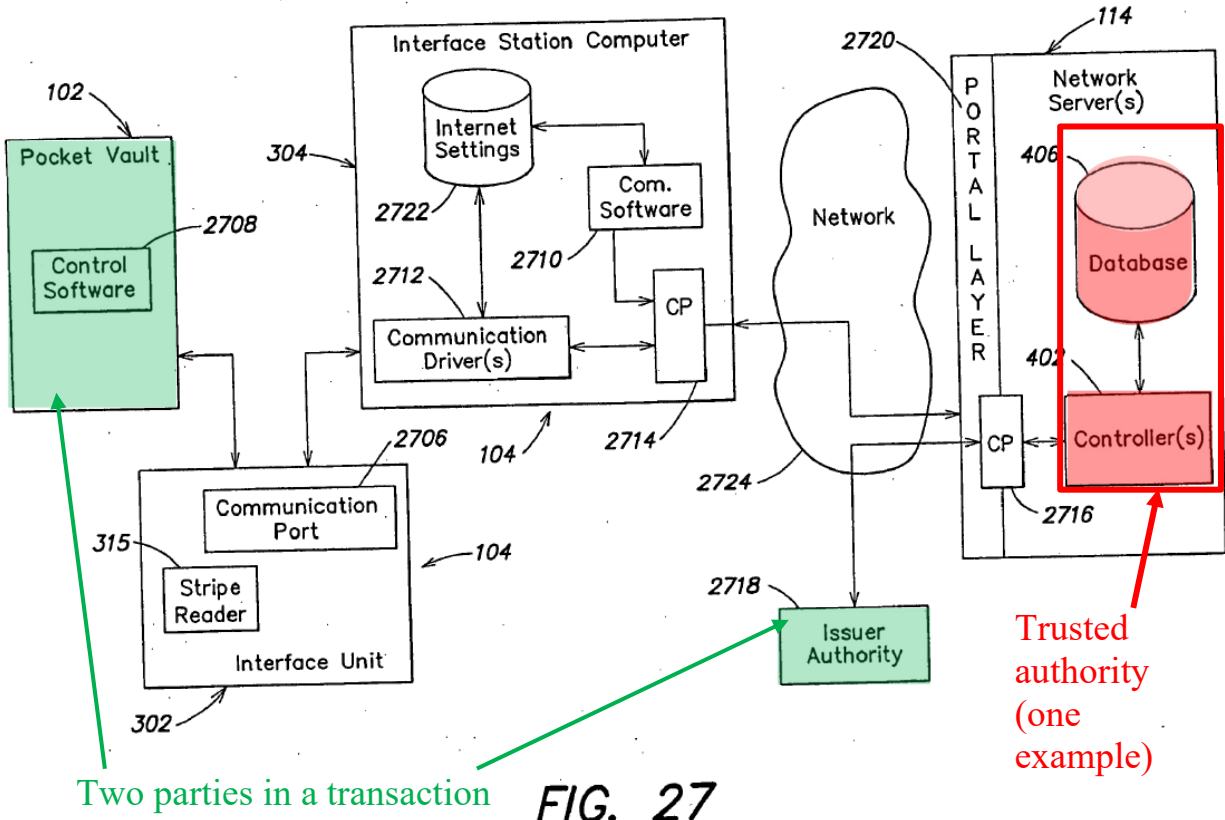
In an earlier IPR proceeding, the Board construed “‘third-party trusted authority’ as a trusted authority that is an entity separate from the parties to a transaction.” IPR2021-01444, Paper 11 at 15. Consistent with this description, the network server is “*a trusted authority*.” Alternatively, the controller 402 and database 406 collectively within the network server are “*a trusted authority*.” MSC-

1005, ¶¶[146], [0531]-[0543], FIG. 27. In both cases, the party that runs the network server is the “*third party that operates a trusted authority*.” MSC-1005, ¶¶[146], [237], [0531]-[0543], FIG. 27. The network server (or the company running it) is a separate entity from the user/Pocket Vault and the financial media issuers 112/non-financial media issuers 110/advertisers 108, and thus would have been understood by a POSITA to be a “third party.” MSC-1005, FIG. 1; MSC-1003, ¶[108].

The network server or components within it are “*trusted*.” In particular, the database 406 stores a list of current Pocket Vault holders, a list of currently authorized or registered Pocket Vaults, identified by chip ID and linked to the holder list; a list of currently authorized or registered tokens, identified by chip ID and linked to the holder list. MSC-1005, ¶[146], FIG. 4 (reproduced below). Burger explains that “*a trust relationship* may be established between the network server 114 and the Pocket Vault 102. This relationship may involve, for example, the registration of a unique encrypted chip ID of the Pocket Vault 102 with the network server 114 through a secure Internet connection, the distribution of a digital certificate (e.g., a PKI certificate) to the Pocket Vault 102, and the grant of authority to the Pocket Vault 102 to permanently store the Pocket Vault holder's authentication information.” MSC-1005, ¶[114]. “Because of the creation of the above-described

trust relationships, each Pocket Vault 102 and each interface station 104 may *communicate securely with the network server 114*, as well as with any other networked devices or sites that *require a high level of trust*.” MSC-1005, ¶[116]. Indeed, the network server 114 or controller 402 and database 406 within the network server 114 are “***a trusted authority***” at least because they are trusted to store the device ID and authenticate the Pocket Vault. *See also* [1.5]; MSC-1003, ¶[109].

Accordingly, it would have been obvious to a POSITA that the party running the network server is “a third-party that operates a trusted authority” under several different example implementations. MSC-1003, ¶[110]. For example, the party running the network server may operate as “***a third-party that operates a trusted authority***” in a transaction between the Pocket Vault holder and a retailer, as noted above in the Use Case. MSC-1005, FIG. 19, ¶[0474]; FIGS. 24, 25, 27 (reproduced below); ¶¶[0511]-[513], [320], [158], [95].



MSC-1005, FIG. 27.

In another example, the controller 402 and database 406 of the network server or the network server (by itself) may be “*a third-party that operates a trusted authority*” when there is a transaction between a Pocket Vault holder and an issuer authority such as the advertiser 108, non-financial media issuer 110, or financial media issuer 112. MSC-1005, ¶[0541]; MSC-1003, ¶[111]. For instance, an advertiser may send information to the network server, which is then forwarded onto a Pocket Vault for display upon successful authentication of the user and Pocket Vault ID. MSC-1005, ¶[0117], [0146], [237] (“The advertiser 108 ... may ... have made arrangements with the company operating the network server 114 to

have certain advertising information uploaded to Pocket Vaults 102 when particular Pocket Vault holders interface their Pocket Vaults 102 with their personal interface stations 104b”), [541], FIG. 1 (reproduced below).

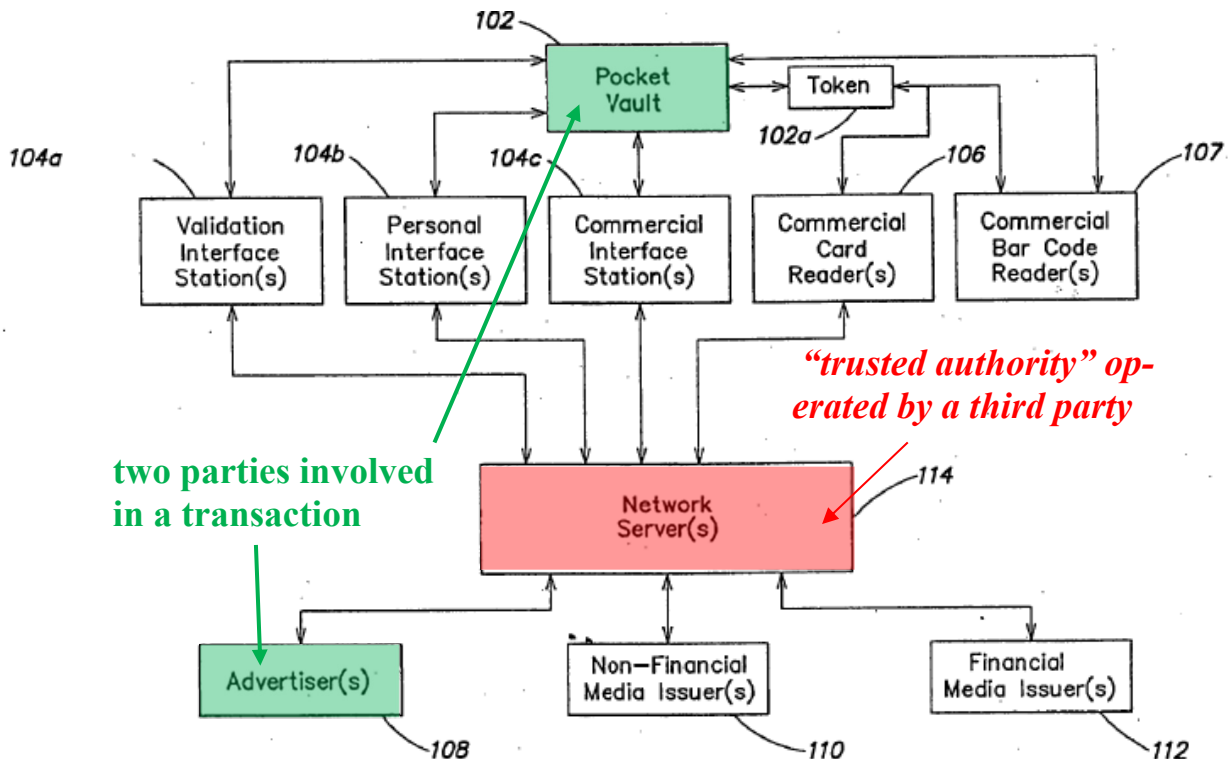
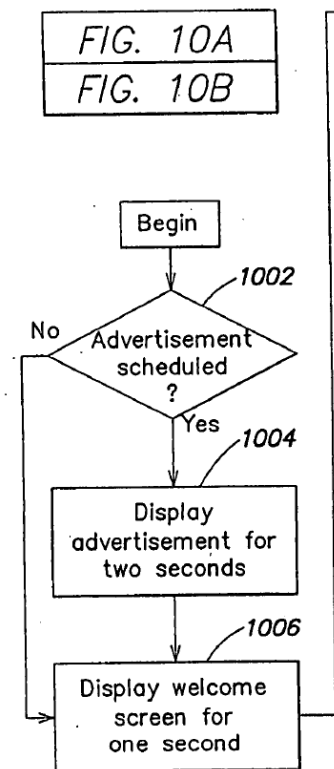


FIG. 1

MSC-1005, FIG. 1.

In some embodiments, after the unique Pocket Vault chip ID is transmitted and a Chameleon Card or token is determined to be on-board the Pocket Vault, an “AUTHORIZED HOLDER” routine is performed, as shown in FIGS. 10 and 11. MSC-1005, ¶¶[189]-[195]. As part of the “AUTHORIZED HOLDER” routine, advertisements sent from an advertiser 108 to the network server 104 are provided to the Pocket Vault for display. MSC-1005, ¶¶[236]-[238], FIG. 10 (reproduced

below); MSC-1003, ¶[112].



MSC-1005, FIG. 10 (portion of).

According to the Merriam-Websters Dictionary, a “transaction” is “a communicative action or activity involving two parties or things that reciprocally affect or influence each other” or “an act, process, or instance of transacting.” MSC-1008, 1252. In the use case example and consistent with Burger’s disclosure, the party that operates the network server or the controller 402 and database 406 of the network server is “*a third-party that operates a trusted authority*” because there is a transaction involving the display of advertisement content and potential subsequent selection of the advertisement by a user, which is a communicative action or activity involving two parties or things that reciprocally affect or influence each

other. MSC-1003, ¶[113]. For instance, the display of advertisement information impacts the user by conveying information to the user regarding the advertisement. The advertiser 108 also gets publicity, market exposure, and, if the user selects an advertisement, the advertiser can collect information on how useful or impactful the advertisement is. MSC-1012, 2:7-60, FIGS. 4, 8; MSC-1013, Abstract; MSC-1014, 1:19-3:21. In this transaction between the user/Pocket Vault holder of the Pocket Vault and the advertiser 108, the network server or the controller 402 and database 406 of the network server are “*a trusted authority*” as they have a secure and trusted connection with at least the Pocket Vault and operate as an intermediary device that facilitates information exchange between the advertiser 108 and the Pocket Vault. MSC-1003, ¶[113].

[1.5]

As described in the example use case above in §III.A.1, after the controller 402 and database 406 of the network server authenticate the Pocket Vault ID, the user is granted access to the Pocket Vault and can then select a transaction from a displayed menu. MSC-1005, step 722 in FIG. 7B (reproduced below); step 1026 in FIG. 10A (reproduced below); steps 1920, 1922 in FIG. 19 (reproduced below); ¶¶[320], [189], [95]-[96], [125], [236]-[238], [155]-[158]. Ultimately, the Pocket Vault or token coupled to the Pocket Vault displays credit card information to be used by a retailer. MSC-1005, ¶¶[0320], [0158], [0095]. Burger teaches that the

token coupled to Pocket Vault “may be used by the Pocket Vault holder to engage in a transaction.” MSC-1005, ¶[103]. A display in the token can “be configured to display information that is typically embossed or printed on such cards.” MSC-1005, ¶¶[0155]-[0158]; MSC-1003, ¶[114].

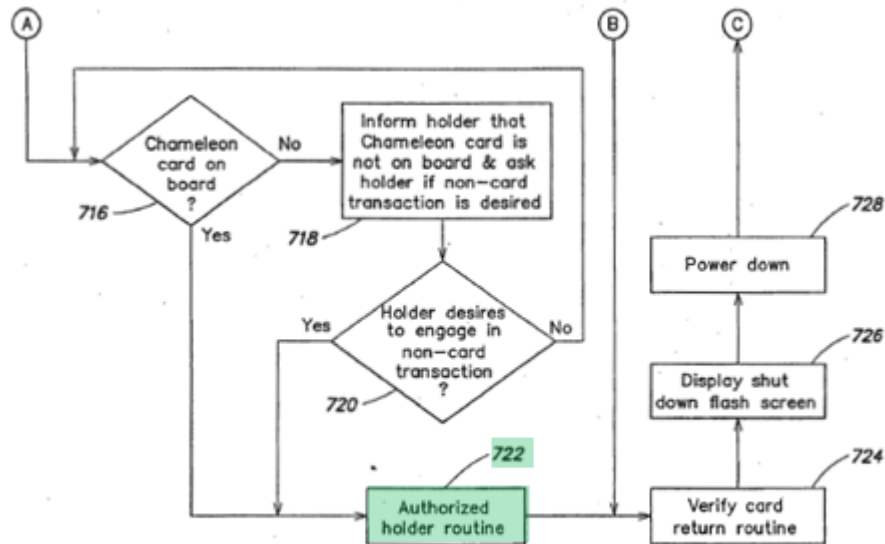


FIG. 7B

MSC-1005, FIG. 7B.

It would have been obvious that an application in the Pocket Vault would have received an access message from the controller 402 of the network server (*“receiving, at an application, an access message from the trusted authority”*) to allow users access to the application after the controller 402 and database 406 of the network server authenticated the Pocket Vault ID that was sent to the network server so that the Pocket Vault grants access to a user and displays sensitive information (e.g., credit or debit card info) for conducting a transaction. MSC-1003, ¶[115].

As an alternative mapping, the controller 402 of the network server also transmits an encrypted approval message in operation 2408 after the Pocket Vault is authorized by confirming that the Pocket Vault ID is valid (step 2006 in FIG. 24 (reproduced below); step 2506 in FIG. 25 (reproduced below)). MSC-1005, ¶¶[517]-[527], [182]-[186]. Because this encrypted approval message (*“access message”*) would have been received and processed by software related to the transaction (*“application”*) at the Pocket Vault in response to the Pocket Vault ID being successfully authenticated by the network server, Burger also discloses *“receiving, at an application, an access message from the trusted authority indicating that the trusted authority successfully authenticated the one or more codes and other data values sent to the third party and allowing the user access to the application”* in this additional way. MSC-1003, ¶[116]. Although operation 2408

indicates that the encrypted approval message is transmitted to an interface station (e.g., 104c, 106, 107), Burger also discloses that, in some cases, the communications may be directly between the Pocket Vault and the network server, and thus, it would have been obvious that the encrypted approval message could be sent to the Pocket Vault in addition to or instead of being sent to the interface stations. MSC-1005, ¶[101]; MSC-1003, ¶[116]. This may particularly be the case when a credit or debit card just needs to be displayed by the Pocket Vault or token coupled to the Pocket Vault. MSC-1003, ¶[116].

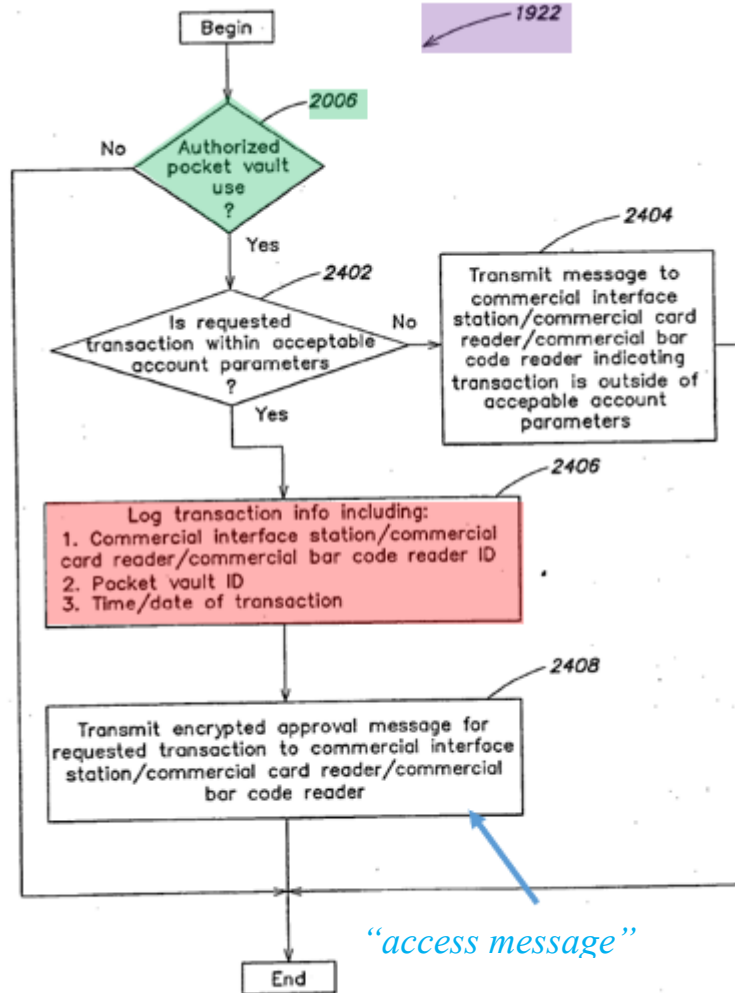
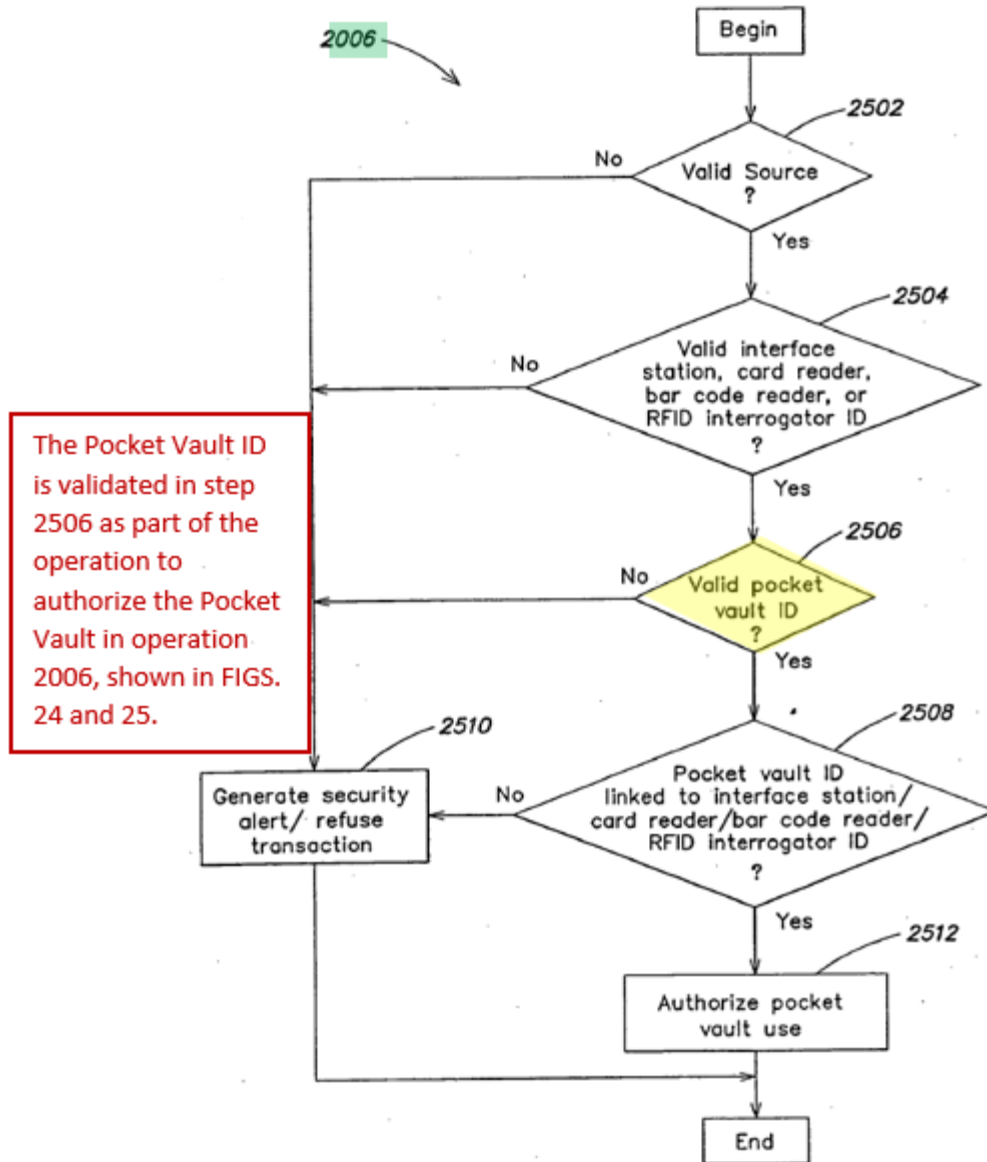


FIG. 24

MSC-1005, FIG. 24.



MSC-1005, FIG. 25.

Under another example implementation of the authorized holder routine 722 in Burger, an advertising message based on an advertisement received from the network server and a welcome screen are displayed in response to authentication of the Pocket Vault. MSC-1005, ¶¶[0194], [0236]-[237], FIG. 7B, 10A (reproduced below). The user can then access *an application*, such as an advertisement file or

software. MSC-1005, ¶[0242], FIGS. 26H-26K, 14. Again, it would have been obvious that for the Pocket Vault to be allowed to display the advertisements and home menu, the controller of the Pocket Vault would have received an access message from the network server (“*receiving, at an application, an access message from the trusted authority*”) to “*allow[] the user access to an application*” after and conditioned on the network server successfully authenticating the Pocket Vault ID that was sent to the network server (“*the trusted authority successfully authenticated the one or more codes and other data values sent to the third party*”).

MSC-1003, ¶[117].

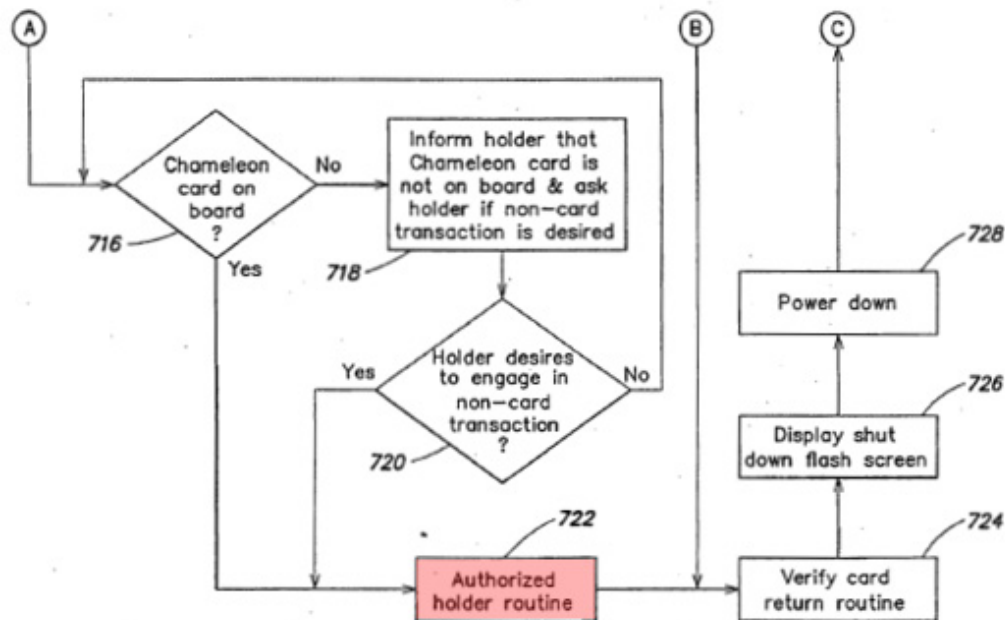


FIG. 7B

MSC-1005, FIG. 7B.

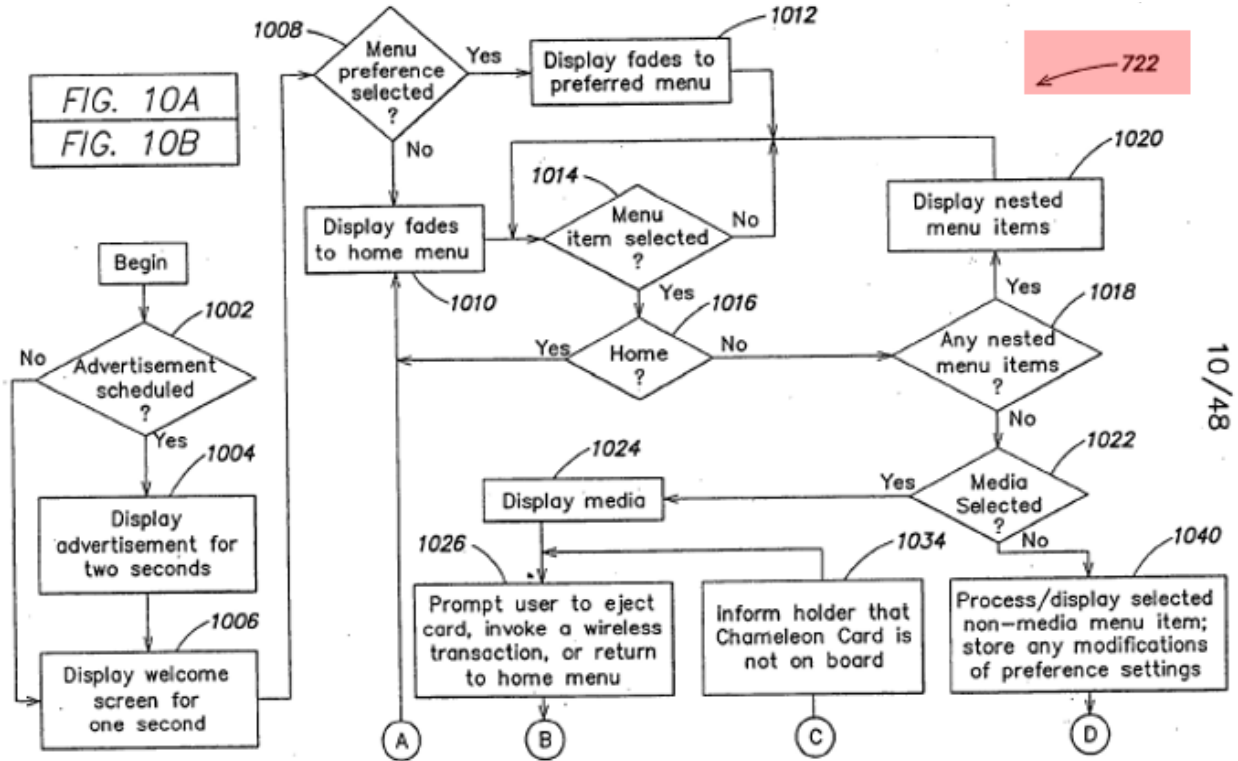
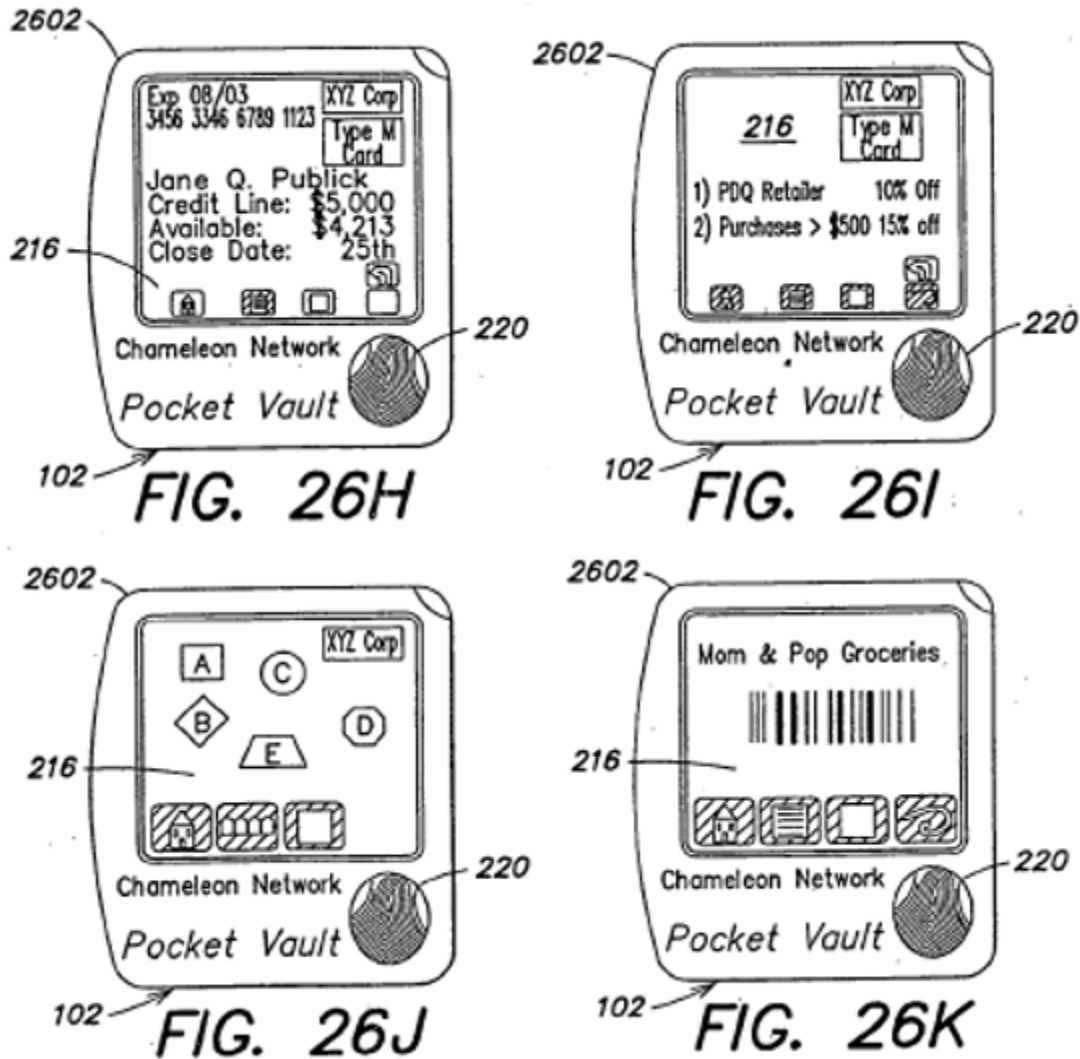


FIG. 10A

MSC-1005, FIG. 10A.



MSC-1005, FIGS. 26H-26K.

Note that the '954 patent explains that an application may be a computer software, file, financial account, or lock. MSC-1001, 6:18-24. Consistent with this description and in view of the above-noted examples, it would have been obvious to a POSITA that Burger renders obvious an “*application*” in the various ways noted in the table below. MSC-1003, ¶[118].

“application”	Implementation in Burger (after the Pocket Vault has been authenticated by the network server)
File or computer software (when a user is involved in a financial transaction with a retailer or credit card company)	A file or computer software that stores credit card information is accessed and data therein is displayed. A specific software (e.g., credit card specific user interface) is accessed to display credit card information.
File, computer software, or web site (in a non-financial transaction)	A file or computer software containing advertising data is accessed and data therein is displayed. A particular website is accessed and displayed to display advertisement data.
Keyless lock	A room key (showing the hotel logo) is downloaded and displayed, and the Pocket Vault can be used to unlock the guest’s hotel room.

MSC-1005, step 722 in FIG. 7B, step 1026 in FIG. 10A; steps 1920, 1922 in FIG. 19, FIGS. 26H-26K, 14; ¶¶[320], [189], [94]-[96], [110], [125]-[129], [236]-[238], [155]-[158], [517]-[527], [182]-[186], [101]-[102], [0242], [250], [679]-[680]; *see also infra* [7]. A POSITA would have understood that a user would only be allowed access to the computer software or file (“**application**”) for displaying the above-noted content after the network server sends a message back to the Pocket Vault indicating that the Pocket Vault has been authenticated by the network server. MSC-1003, ¶[119].

[2]

As noted above in [1.5], Burger discloses that an encrypted message including the Pocket Vault ID (“***the one or more codes and other data values***”) is wirelessly transmitted to the controller 402 and/or database 406 of the network server (“***trusted authority***”). MSC-1005, ¶¶[0186], [114], [122], [146], FIG. 7A. The transmission can be made over any one of various suitable networks, such as network 2724 in FIG. 27, the Internet, a packet-switched communication system, hardwired (including fiber optic connections) systems, or wireless (e.g., infrared (IR) or radio frequency (RF) links) systems. MSC-1005, ¶[0099]; MSC-1003, ¶[120].

[4]

As shown above in FIG. 7A (*see supra* [1.3], [1.4]), the Pocket Vault ID is transmitted after the Pocket Vault holder's scanned biometric data matches stored biometric data. MSC-1005, ¶¶[135], [178]-[0184]; MSC-1003, ¶[121].

Burger's chip ID or Pocket Vault ID can also be released from the Pocket Vault only after the fingerprint scanner 220 (discussed below) has successfully authenticated the identity of the holder. MSC-1005, ¶[0122], [0349], [0358]. "[T]he Pocket Vault 102 may be adapted to not release any personal or secure information, even encrypted, until the holder presents satisfactory verification of his or her identity, such as, for example, presenting the holder's fingerprint to the fingerprint scanner 220." MSC-1005, ¶[0553]. Accordingly, it would have been obvious to a POSITA that the transmission of "***the one or more codes and the other data values***" to the network server in a message would have been an indication "***that the biometric verification was successful***" because this transmission was only possible if the biometric verification was successful. MSC-1003, ¶[122]. Thus, the inclusion of "***the one or more codes and the other data values***" in a message to the network server would have in and of itself indicated "***that the biometric verification was successful***." MSC-1003, ¶[122].

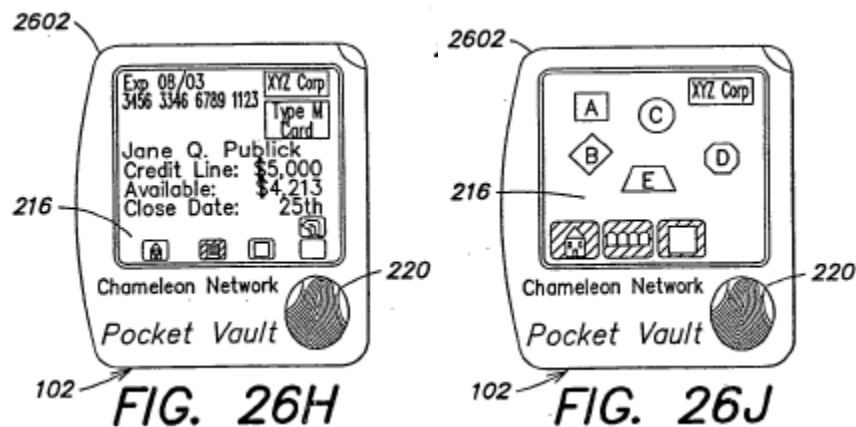
[5]

Burger discloses that that various types of biometric scans and data can be used to perform the authentication including, e.g., a fingerprint scan, retina scan, a speech pattern analysis (“*wherein the biometric data includes one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition*”). MSC-1005, ¶¶[0112], [0135]. Although the example implementation used subsequently in the mapping of Burger to the ’954 claims describes an example of fingerprint scanning, Burger’s disclosure makes obvious that user authentication could also include various suitable authentication techniques in place of fingerprint scanning, such as, e.g., retina scanning, voice recognition, hand geometry. MSC-1005, ¶¶[0112], [0135]; MSC-1003, ¶[123].

[7]

As explained above in the Use Case described in §III.A.1 and [1.3]-[1.5], when a user is interested in a financial transaction and after network server determines that the Pocket Vault is authorized to be used, e.g., by checking whether the transmitted Pocket Vault ID matches a stored ID in the network server, the network server transmits an approval message for the financial transaction. MSC-1005, FIGS. 19 (steps 1920, 1922), 24 (steps 2006, 2406, 2408), 25 (Steps 2506),

¶¶[0511]-[529], [182]. An application used in the financial transaction is then executed on the Pocket Vault. For instance, “[i]n the example of FIG. 26H, the preferred menu immediately shows the holder’s preferred credit card as the selected menu item. Should the holder opt to use this media to engage in a transaction, the holder can simply choose the media directly. Alternatively, the holder may opt to access the HOME menu or other menu items by selecting appropriate icons displayed on the screen. In the example of FIG. 26J, the preferred menu immediately shows, perhaps, a selected group of the holder’s most frequently used menu items.” MSC-1005, ¶[242]. A retailer “may verify authenticity by matching the information displayed on the token 102a [or Pocket Vault 102] with that revealed in a swipe or other token reading process.” MSC-1005, ¶[158]; MSC-1003, ¶[124].



MSC-1005, FIG. 26H, 26J.

Relatedly, it would have been obvious that computer software, a file, or a financial account (“*application*”) would have been accessed to allow the Pocket Vault to display credit card information (or other financial account information) to

complete a financial transaction with a retailer. MSC-1003, ¶[125]. For instance, if a credit card transaction is being made, it would have been obvious to a POSITA that to complete a financial transaction, a financial account or a file including financial account information (“*application*”) would have been accessed to charge an amount involved in the financial transaction. MSC-1005, step 722 in FIG. 7B, step 1026 in FIG. 10A; steps 1920, 1922 in FIG. 19, FIGS. 26H-26K, 14; ¶¶[003], [95]-[96], [105], [109], [127]-[129], [139], [149], [155]-[158], [0242], [236]-[238], [250], [255], [318]-[332], [559], [679] [95]-[96], [517]-[527], [182]-[186]; MSC-1003, ¶[125].

[8]

Burger teaches that the memory 210 in the Pocket Vault includes medical information cards, just like a wallet includes medical information cards. MSC-1005, ¶¶[127], [3]. It would have been obvious to a POSITA that in a transaction involving a medicine purchase or a health care service, a user of the Pocket Vault would have wanted to access the user’s medical information, e.g., such as a card that provides medical insurance information. MSC-1003, ¶[126]. In such cases, the user would have accessed the Pocket Vault following the method of claim 1, and the access message would have provided access to “*the application that includes a file including medical information*” so that the user can complete its transaction.

MSC-1003, ¶[126]. One example would be if a user went to a pharmacy and wanted to use the user's insurance to cover the payment for medication. The user would then access the Pocket Vault to display a file that provides medical insurance information to the pharmacy retailer to complete the transaction. MSC-1003, ¶[126].

[9]

See [7], [1.5]; MSC-1005, step 722 in FIG. 7B, step 1026 in FIG. 10A; steps 1920, 1922 in FIG. 19, FIGS. 26H-26K, 14; ¶¶[003], [95]-[96], [105], [109], [127]-[129], [139], [149], [155]-[158], [0242], [236]-[238], [250], [255], [318]-[332], [559], [679] [95]-[96], [517]-[527], [182]-[186]; MSC-1003, ¶[127].

[10]

As explained above in [1.4], after the Pocket Vault Holder's biometric scanned data has been validated, "a trust relationship may be established between the network server 114 and the Pocket Vault 102" and that a secure Internet connection ("*a secure communication channel*") is established to facilitate the registration of the Pocket Vault (FIG. 7A, Step 710), which is done prior to the Pocket Vault ID being sent for authentication (FIG. 7A, Step 713). MSC-1005, ¶[114]. Accordingly, Burger renders obvious [10] obvious. MSC-1003, ¶[128].

[11.1]

When a request to register a new Pocket Vault holder is received, the operations 1904 (FIG. 19) shown in Burger's FIG. 20 below are performed by the network server. MSC-1005, FIGS. 19, 20, ¶¶[0462]-[0464], [0476]. In particular, after a request is received to register a new Pocket Vault holder, "the network server 114 requests the interface station computer 304 to transfer the information regarding the proposed new holder to the network server 114." MSC-1005, ¶¶[0476]-[0477]. After the requisite encrypted holder registration information is received through an interface station computer 304 and the network server determines that the Pocket Vault is authorized for use, "all of the relevant information regarding the new Pocket Vault registration is logged into the database 406 of the network server 114." MSC-1005, ¶¶[0476]-[0481]. The registration information "may include, for example, the interface station operator ID, the interface unit ID, the Pocket Vault ID, and all of the relevant information relating to the new Pocket Vault holder." MSC-1005, ¶[0481]; MSC-1003, ¶[129].

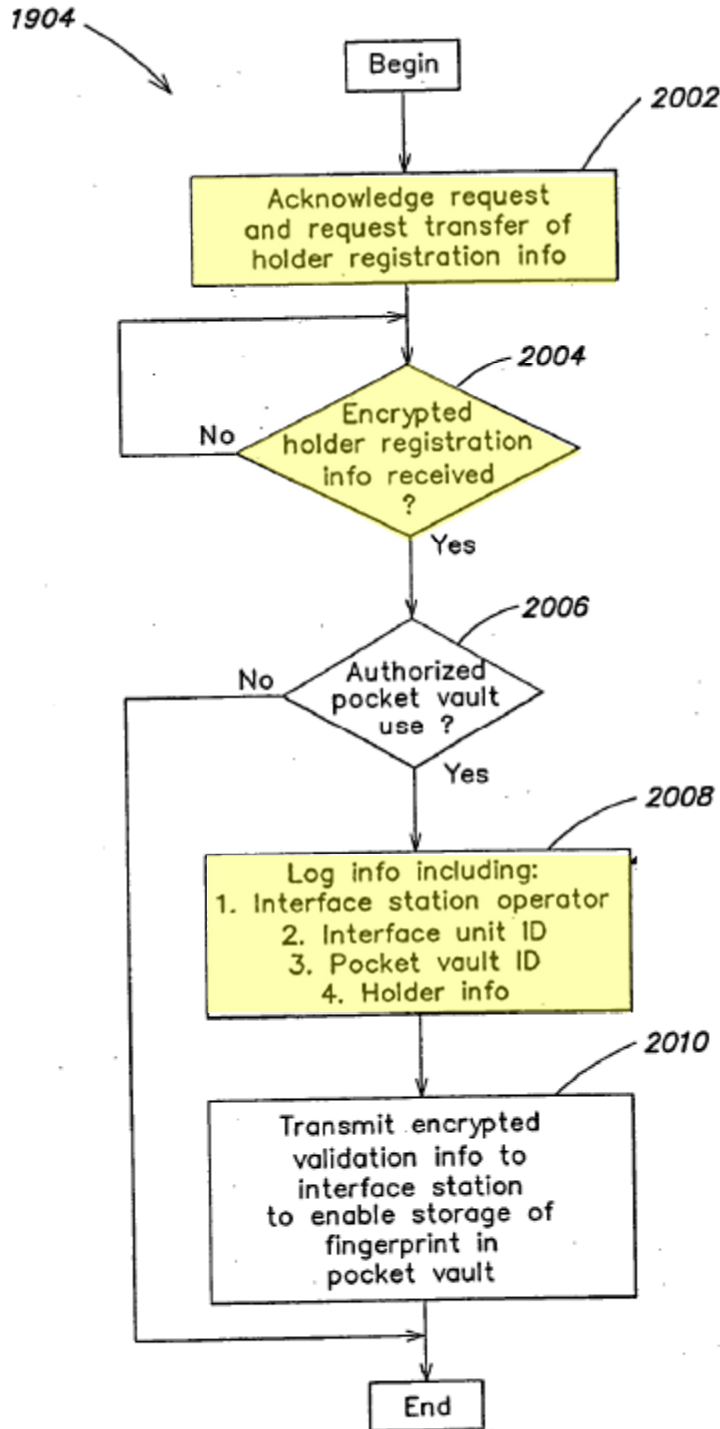


FIG. 20

MSC-1005, FIG. 20.

Although some of the communications described in FIG. 20 are described as being performed by an interface station, Burger also discloses that “in some embodiments wherein appropriate networking capabilities are provided, each Pocket Vault 102 may communicate directly with the network server 114, without the interface stations 104a-c facilitating communication therebetween.” MSC-1005, ¶¶[0101], [0562], [0573], [0585]. Thus, in such embodiments, it would have been obvious to a POSITA that the network server would have communicated directly with the Pocket Vault to obtain the registration information for a new Pocket Vault holder. MSC-1003, ¶[130].

In this example of registering a new Pocket Vault holder, no request for biometric verification is made. However, the Pocket Vault still receives a request (“*a request for the one or more codes and the data values*”) for pocket holder registration information including “the Pocket Vault ID, and all of the relevant information relating to the new Pocket Vault holder.” MSC-1005, ¶[0481]. Accordingly, Burger renders obvious “*receiving a request for the one or more codes and other data values without a request for biometric verification.*”² MSC-1003,

² Recall from [1.1] above that Burger’s Pocket Vault ID and other data in the transmitted encrypted message satisfies “the plurality of codes and the other data values.”

¶[131].

[11.2]

As explained above in [11.1], in response to receiving the request for registration information (“**responsive to receiving the request**”), the Pocket Vault sends all the Pocket Vault registration information, including the Pocket Vault ID, to the network server to be logged into the database 406 of the network server without requesting or performing any biometric scan (“**sending the one or more codes and the other data values without requesting the scan data**”). MSC-1005, ¶¶[0476]-[0481]; MSC-1003, ¶[132].

[12.pre]

To the extent the preamble of claim 12 is limiting, Burger’s Pocket Vault is an “**integrated device**,” as explained in [1.1]. MSC-1005, ¶¶[0002], [0010], [0127]-[0128], [0118], [0134], [0094]-[0095]; MSC-1003, ¶[133].

[12.1]

As explained above in [1.1], Burger’s Pocket Vault includes a write-once memory 212 or any suitable memory device that permits only a single write operation to store data such as the Pocket Vault ID and user fingerprints (“**a persistent storage media that stores biometric data of a user and a plurality of codes and**

other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to the persistent storage media and not capable of being subsequently altered”).

See [1.1]; MSC-1005, ¶¶[0112]-[0114], [0118], [0122], [0127], [0129], [0134], [0154], [0182], [0551]-[0552], [0094]-[0095], FIG. 2; MSC-1003, ¶[134].

[12.2]

See [1.1]-[1.4]; MSC-1005, ¶¶[0112]-[0114], [0122], [0135], [0146], [0178]-[0184], [0186], FIGS. 7A, 2.

The fingerprint scanner 220 (or any biometric scanner used instead of the scanner 220), the controller 202, the transceiver 204, the display 216, and the indicator 215 are the “*validation module*” that is “*coupled to communicate with the persistent storage media*” and performs the recited operations. MSC-1005, ¶¶[0122], FIG. 2 (reproduced below). Because the scanner 220 obtains stored copies of biometric data from the memory to perform the comparison with scanned biometric data, it would have been obvious to a POSITA that the scanner 220 would be “*coupled to communicate with the persistent storage media.*” MSC-1003, ¶¶[135]-[136]. Moreover, the controller 202 is coupled to the memory and transceiver 204 to send and receive any data from the Pocket Vault.

[1.1]-[1.4] explain how Burger renders obvious “receives scan data ...” and

the remaining features in [12.2]. MSC-1003, ¶[137].

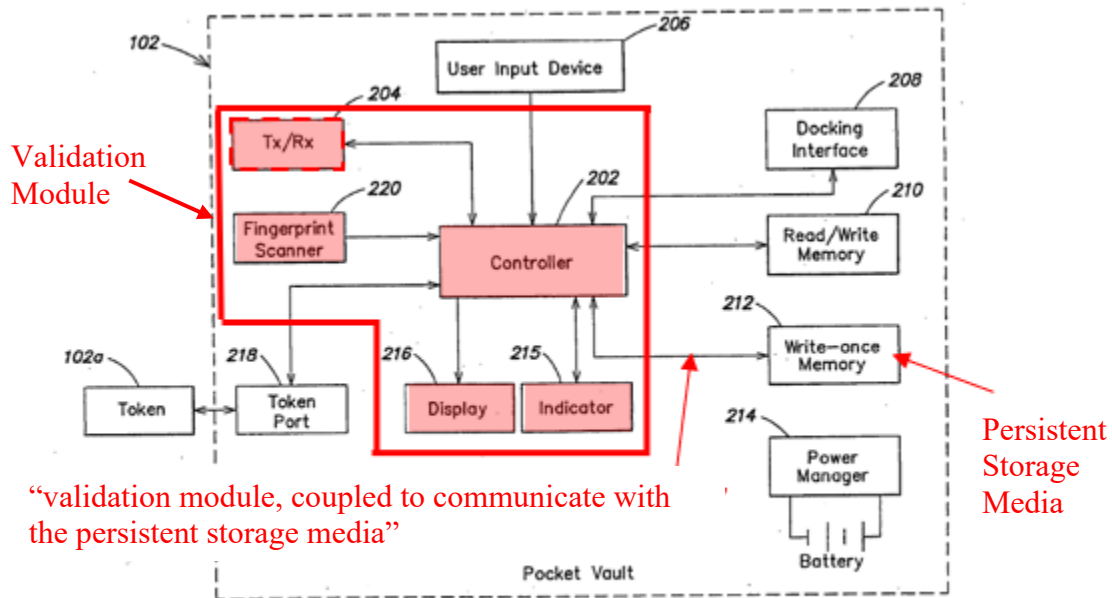


FIG. 2

MSC-1005, FIG. 2.

[12.3]

See [1.5]; MSC-1005, FIGS. 7A, 7B, 10A, 19, 24, 26H-26K; ¶¶[0109], [517]-[527], [182]-[186], [0095]-[0096], [0320], [0194], [0101]-[103], [0125], [0236]-[0238], [0155]-[0158].

The “one or more antennas” of the transceiver 204 (alternatively the transceiver 204 itself) are the “*radio frequency communication module*” as the antennas perform the transmitting and receiving of data using RF signals for the Pocket Vault. MSC-1005, ¶[0123]; MSC-1003, ¶¶[138]-[139].

Note that claim 12 does not require that the “*radio frequency communication module*” be separate from the “*validation module*,” thus mapping the transceiver 204 to the “*radio frequency communication module*” within the “*validation module*” is consistent with the claims and “the principle that in [an] obviousness analysis, a single element, feature, or mechanism can ordinarily satisfy multiple claim limitations, including by performing multiple claimed functions.”

Google LLC v. Personal Audio, LLC, No. 2017-1162, 12 (Fed. Cir, 2018) (non-precedential) (affirming PTAB Decision in IPR2015-00845) (citing *Linear Tech. Corp. v. ITC*, 566 F.3d 1049, 1055 (Fed. Cir. 2009); *Rodime PLC v. Seagate Tech., Inc.*, 174 F.3d 1294, 1305 (Fed. Cir. 1999); *In re Kelley*, 305 F. 2d 909, 915-16 (CCPA 1962)); MSC-1003, ¶[140].

To the extent, the “*radio frequency communication module*” is understood to not be part of the “*validation module*,” the antennas of the transceiver correspond to the “*radio frequency communication module*” and the fingerprint scanner 220 (or any biometric scanner used instead of the scanner 220), the controller 202, and parts of the transceiver 204 other than the antennas are the “*validation module*.” MSC-1003, ¶[141].

[13]

See [2]; MSC-1005, ¶¶[0186], [114], [122], [146], [0099], FIGS. 7A, 27;

MSC-1003, ¶[142].

[15]

Burger discloses that output devices, such as LEDs and a display, can be used to provide information to a Pocket Vault holder and prompt user input options. MSC-1005, ¶¶[0133], [0177]. An indicator 215 can be “any device capable of generating a perceptible indication to a holder.” MSC-1005, ¶[0131], FIG. 2. For example, the indicator 215, can include a LED and beeper, to prompt the Pocket Vault holder to apply a fingerprint on the fingerprint scanner 220 and a “beep” is emitted after each fingerprint is applied. MSC-1005, ¶¶[0204], [0206], [0133]; *see also* ¶¶[0232], [0355], [0384], [0585], [0598]. Although the prompting of a user to scan the user’s fingerprints is not part of the method shown in FIG. 7A, it would have been obvious to a POSITA that there are multiple ways of the Pocket Vault obtaining a fingerprint scan. MSC-1003, ¶[143]. One of the methods to obtain a fingerprint scan is to wait for the user to apply the user’s finger on the fingerprint scanner 220 (as shown in Burger’s FIG. 7A), but another obvious and predictable option is for the Pocket Vault to prompt the user to apply the user’s fingerprint through the use of an Indicator 215 (that includes a LED). The prompting for additional fingerprint scans can also be made when one fingerprint scan has been completed but scans of additional fingerprints are still needed. MSC-1005, ¶[0204].

Accordingly, it would have been obvious to a POSITA that Burger renders obvious

“[t]he integrated device ... comprising: an LED to be activated for requesting the biometric scan.” MSC-1003, ¶[143].

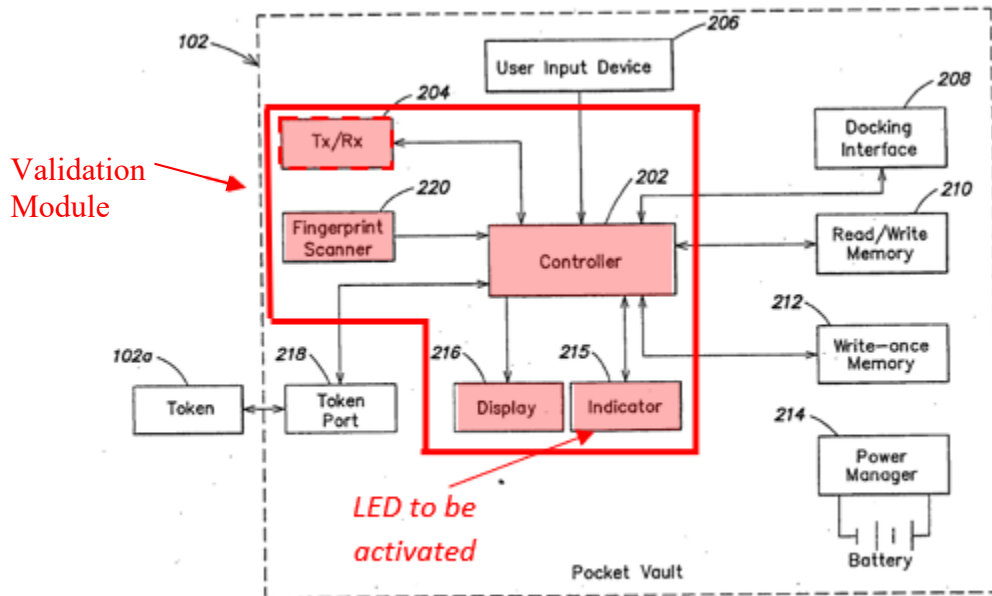


FIG. 2

MSC-1005, FIG. 2.

[16.pre]

For reasons similar to those noted above with respect to claim 1 and in particular [1.pre], Burger renders obvious [16.pre]. MSC-1005, ¶¶[0002], [0010], [0127]-[0128], [0118], [0134], [0094]-[0095]; MSC-1003, ¶[144]. The '954 patent's specification does not explicitly recite a "computer processor." However, a POSITA would have understood that the recited "computer processor" may refer to

one or more computer system modules configured to perform processing steps corresponding to the features of claims 16-21. MSC-1003, ¶[144]. For instance, claim 19 recites that the “application includes one or more of a casino machine, ... garage door opener, an ATM machine ...” clearly indicating that the recited application, and therefore the “computer processor” that “receive[s], at an application” (in addition to the wirelessly receiving and requesting authentication steps in claim 16) is located at different devices. MSC-1001, 11:24-12:3. And because the claimed steps can be implemented in various devices and the “steps can be performed in any order,” the “computer processor” would not have been understood to be limited to one particular device. MSC-1001, 8:26-44. As explained below, the claimed “*computer processor*” may correspond to the controller 402 of the network server and the controller 122 of the Pocket Vault. MSC-1003, ¶[144].

Consistent with this understanding, Burger discloses a method of authenticating a verified Pocket Vault holder (“*user*”) using a controller 402 (“*computer processor*”) of the network server. MSC-1005, FIG. 4, ¶¶[0144]-[0145], [0540]. The network server also includes a local memory 404 that has “instructions stored therein which, when executed by the controller 402, cause the controller 402 to implement the routines described ... in connection with FIGS. 19-25 and/or FIGS. 30-39.” *Id.*; MSC-1003, ¶[145]. As noted below, the method including features [16.1]-[16.4] are rendered obvious by Burger. MSC-1003, ¶[145].

[16.1]

As explained above in [1.5], the controller of the network server “*wirelessly receiv[es] one or more codes and other data values from a plurality of codes and other data values including a device ID code*” from the Pocket Vault. MSC-1005, ¶¶[0112]-[0114], [0122], [0135], [0146], [0178]-[0184], [0186], FIGS. 7A, 2.

Remaining features are rendered obvious for the same reasons noted above in [1.2]-[1.5]. MSC-1005, ¶¶[0112]-[0114], [0118], [0122], [0127], [0129], [0135], [0146], [0154], [0178]-[0184], [0186], [0551]-[0552], FIGS. 7A, 2; MSC-1003, ¶¶[146]-[147].

[16.2]

See [1.4], [1.5]. As explained above in §III.A.1, [1.4], and [1.5], Burger discloses that the controller 122 (“*computer processor*”) of the Pocket Vault controls the transmission of (step 713) of an encrypted message including the unique Pocket Vault chip ID to the network server. MSC-1005, ¶¶[0186], [0113]-[114], [122], [146], FIG. 7A. In a request to authorize a transaction, e.g., as disclosed in Burger’s FIGS. 19 (steps 1920, 1922), 24 (steps 2006, 2406, 2408), 25 (Steps 2506), a POSITA would have understood that the request involves a request to authenticate the pocket vault ID (step 2506) using the device ID code in the en-

encrypted message from the Pocket Vault (“*requesting authentication of the integrated device using the one or more codes and other data values*”). MSC-1005, ¶¶[0511]-[529], [182]; MSC-1003, ¶[148].

Moreover, as explained above in [1.4], it would have been obvious to a POSITA that the network server or controller 402 and database 406 within the network server, collectively, are “*the trusted authority*” that authenticates the Pocket Vault ID or authorize the Pocket Vault by confirming that the Pocket Vault ID is valid before sending the access message to the Pocket Vault. MSC-1005, FIGS. 19, 24, 25; ¶¶[517]-[527], [182]-[186]; MSC-1003, ¶[149].

[16.3]

See [1.5], [7]; MSC-1003, ¶[150].

[16.4]

As described above in [1.1]-[1.3] and [1.5] and in the example use case in §III.A.1, (1) after a user has been biometrically verified when the Pocket Vault determines that scanned user biometric data matches stored biometric data, and (2) after the controller 402 and database 406 of the network server authenticate the Pocket Vault ID, the user is granted access to the Pocket Vault and can then select a transaction from a displayed menu. MSC-1005, steps 708, 712, 713 in FIG. 7A,

step 722 in FIG. 7B (reproduced below); step 1026 in FIG. 10A (reproduced below); steps 1920, 1922 in FIG. 19 (reproduced below); ¶¶[320], [189], [95]-[96], [125], [236]-[238], [155]-[158]. Ultimately, the Pocket Vault or token coupled to the Pocket Vault displays a credit card information to be used by a retailer. MSC-1005, ¶¶[0320], [0158], [0095]. Burger teaches that the token coupled to the Pocket Vault “may be used by the Pocket Vault holder to engage in a transaction.” MSC-1005, ¶[103]. A display in the token can “be configured to display information that is typically embossed or printed on such cards.” MSC-1005, ¶¶[0155]-[0158]; MSC-1003, ¶[151].

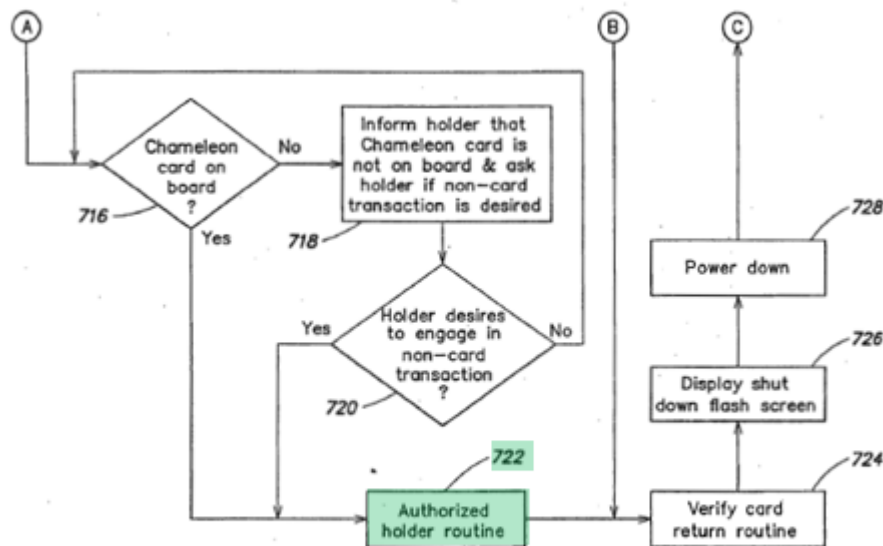


FIG. 7B

MSC-1005, FIG. 7B

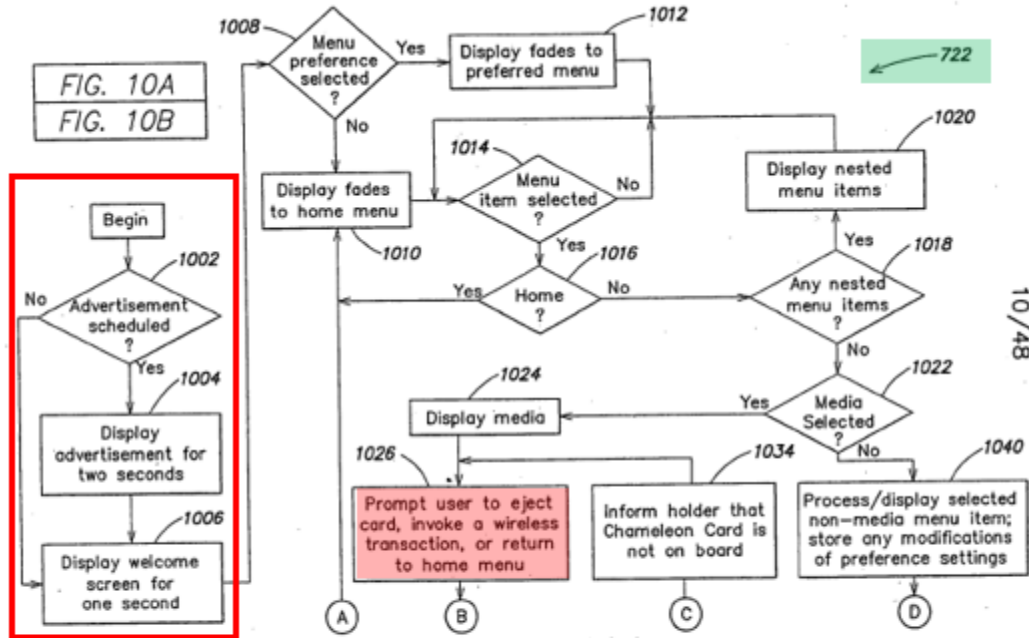


FIG. 10A

As part of the Authorized Holder Routine 722 in FIG. 7B, an advertisement is displayed and subsequently a user can select a wireless transaction to be conducted.

MSC-1005, FIG. 10A.

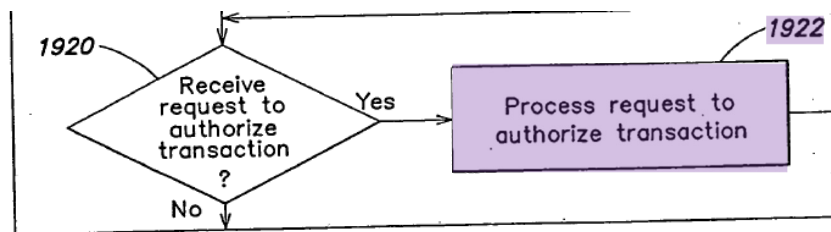


FIG. 19

When a request to conduct a transaction is received, the request is processed as shown in step 1922 in FIGS. 19, 24, and 25.

MSC-1005, FIG. 19.

Relatedly, the controller 202 of the Pocket Vault receives an encrypted approval message from the controller 402 of the network server in operation 2408 after the Pocket Vault is authorized by confirming that the Pocket Vault ID is valid (step 2006 in FIG. 24 (reproduced below); step 2506 in FIG. 25 (reproduced below)). MSC-1005, ¶¶[517]-[527], [182]-[186]. After the approval message is received, access to the application is granted, as explained above in [1.5]. Because this encrypted approval message (“*access message*”) is received by the Pocket Vault in response to the Pocket Vault ID being successfully authenticated by the network server and after the user has been biometrically verified, Burger also discloses “*in response to receiving the access message, allowing the biometrically verified user access to the application.*” MSC-1003, ¶[152].

Although operation 2408 indicates that the encrypted approval message is transmitted to an interface station (e.g., 104c, 106, 107), Burger also discloses that, in some cases, the communications may be directly between the Pocket Vault and the network server, and thus, it would have been obvious that the encrypted approval message could be sent to the Pocket Vault in addition to or instead of being sent to the interface stations. MSC-1005, ¶[101]; MSC-1003, ¶[153]. This may particularly be the case when a credit or debit card just needs to be displayed by the Pocket Vault or token coupled to the Pocket Vault.

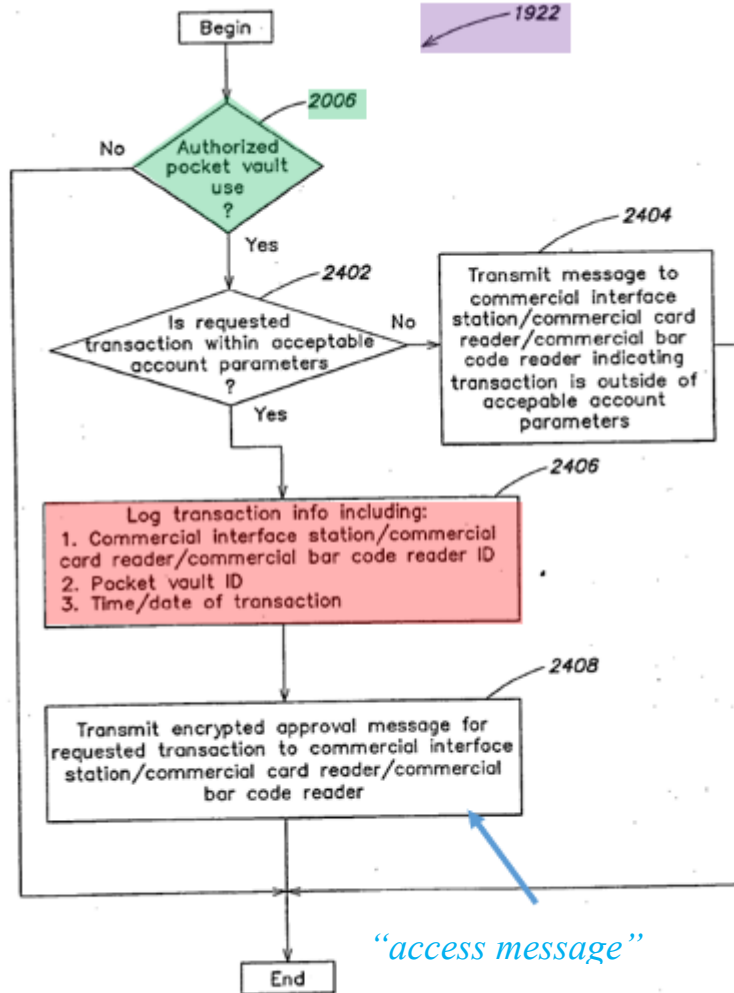
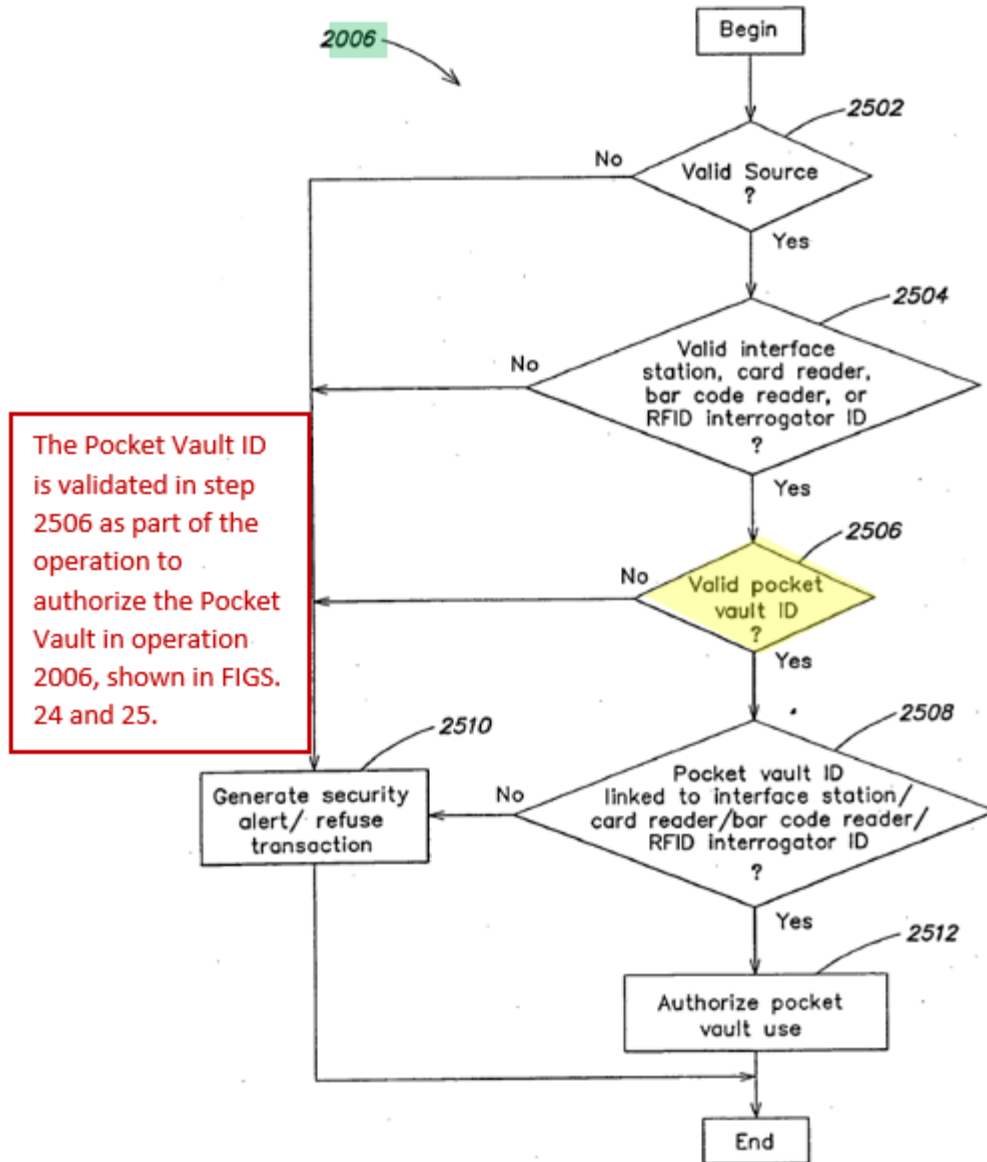


FIG. 24

MSC-1005, FIG. 24.



MSC-1005, FIG. 25.

Under another example implementation of the authorized holder routine 722 in Burger, an advertising message based on an advertisement received from the network server and a welcome screen are displayed in response to authentication of the Pocket Vault. MSC-1005, ¶¶[0194], [0236]-[237], FIG. 7B, 10A (reproduced below). The user can then access *an application*, such as an advertisement. MSC-

1005, ¶[0242], FIGS. 26H-26K, 14. Again, it would have been obvious that for the Pocket Vault to be allowed to display the advertisements and home menu, the Pocket Vault would have received an access message from the network server (“*in response to receiving the access message*”) to “*allow[] the biometrically verified user access to the application*” after and conditioned on the network server successfully authenticating the Pocket Vault ID that was sent to the network server. MSC-1003, ¶[154].

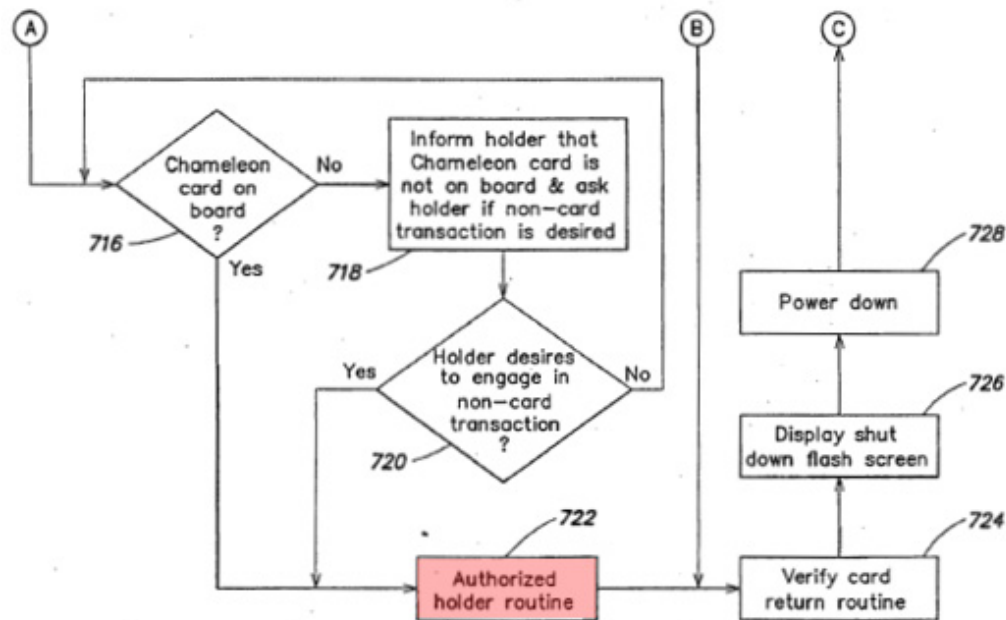


FIG. 7B

MSC-1005, FIG. 7B.

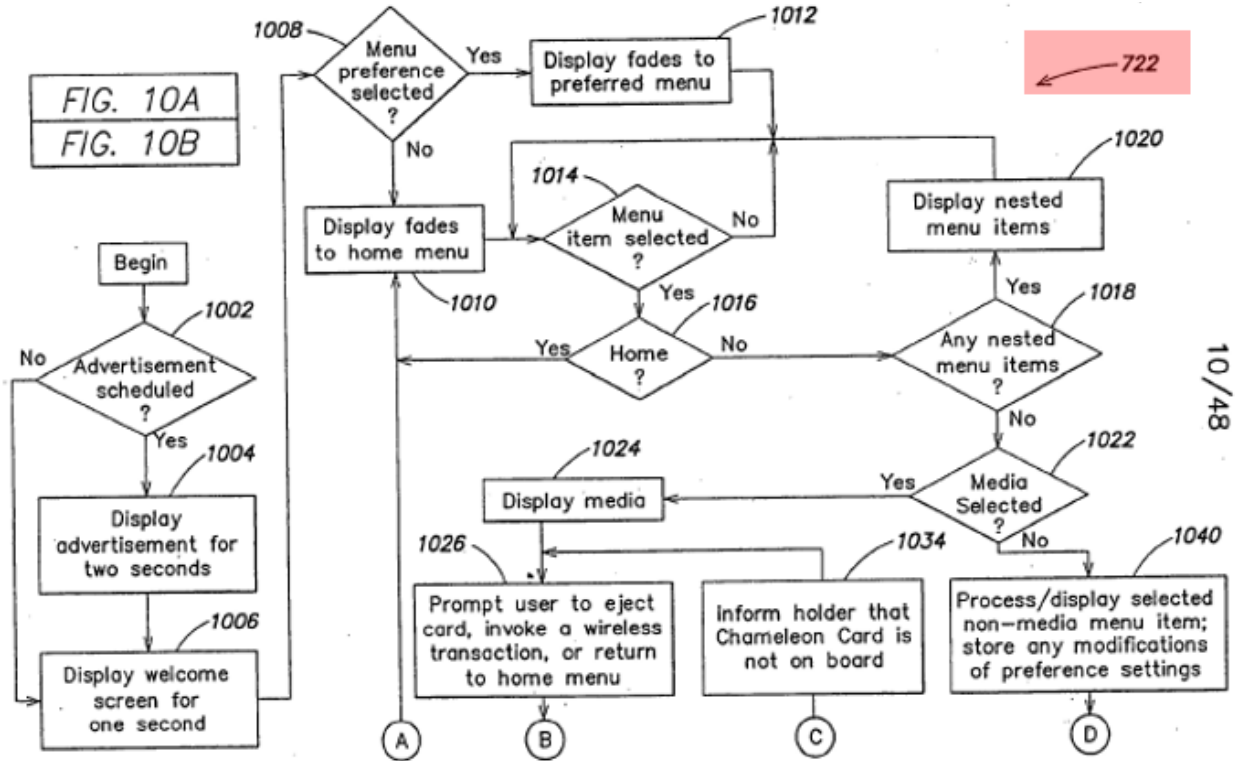
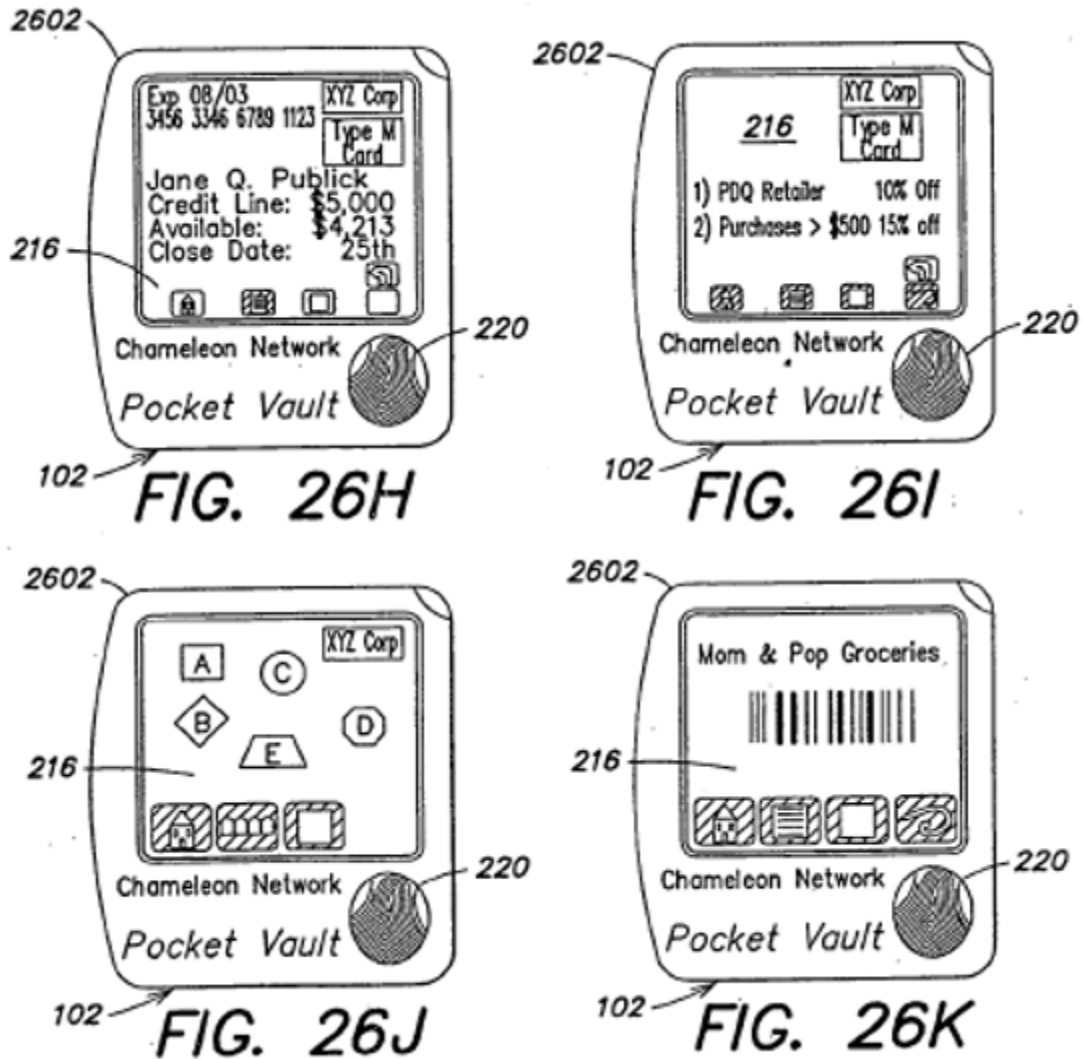


FIG. 10A

MSC-1005, FIG. 10A.



MSC-1005, FIGS. 26H-26K.

[18.1]

Burger discloses that after the Pocket Vault Holder's biometric scanned data has been validated, "a trust relationship may be established between the network server 114 and the Pocket Vault 102" and that a secure Internet connection ("*a secure communications channel*") is established to facilitate the registration of the

Pocket Vault (FIG. 7A, Step 710), which is done prior to the Pocket Vault ID being sent for authentication (FIG. 7A, Step 713). MSC-1005, ¶[114]. Accordingly, Burger renders obvious [18.1]. MSC-1003, ¶[155].

[18.2]

See [1.4], [16.4]; MSC-1003, ¶[156].

[19]

See [7]; MSC-1003, ¶[157].

[20]

See [8]; MSC-1003, ¶[158].

[21]

See [7], [9], [19]; MSC-1003, ¶[159].

[22.pre]

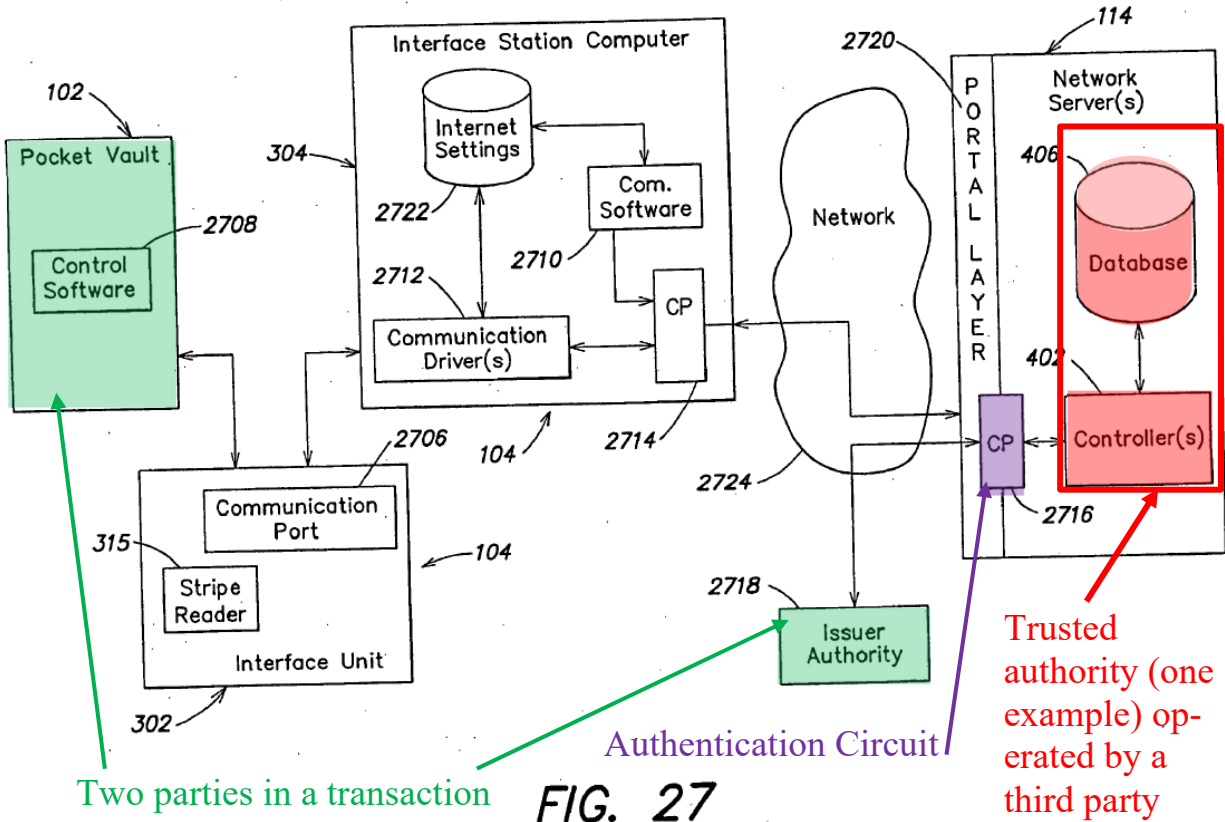
See [1.pre]; MSC-1005, ¶¶[0002], [0010], [0127]-[0128], [0118], [0134], [0094]-[0095]; MSC-1003, ¶[160].

[22.1]

See [1.1], [1.3]-[1.5]; MSC-1005, ¶¶[0112]-[0114], [0118], [0122]-[123], [0127], [0129], [0134]-[0135], [0146], [0154], [0178]-[0184], [0186], [209]-[210], [0551]-[0552], [0099]-[0101], FIGS. 7A, 2; MSC-1003, ¶[161].

[22.2]

As shown in Burger's annotated FIG. 27 below, Burger discloses "a communication protocol layer 2716, which provides low-level communication functions to server communications software." MSC-1005, ¶[540]. As is obvious from Burger's FIG. 27, communications (e.g., device ID codes) between the network server's controller(s) 402 and database 406 and external elements (e.g., network 2724, Pocket Vault, or issuer authority 2718) all pass through the communication protocol layer 2716. MSC-1003, ¶[162].



MSC-1005, FIG. 27.

Accordingly, it would have been obvious to a POSITA that Burger renders obvious *“an authentication circuit³ that receives the one or more codes and other data*

³ Notably, the “authentication circuit” recited in claim 22 is not recited as directly performing any type of “authentication.” Rather, the extent of the “authentication” function ascribed to the recited “authentication circuit” by the claim is merely that it receives and sends the one or more codes and other data values to a third party “for authentication.” Given the breadth of this claim language, therefore, Burger’s

values and sends the one or more codes and the other data values to a third party that operates a trusted authority for authentication.” For the reasons noted above in [1.5] and [16.4], Burger also renders obvious the remaining features of [22.2]. See [1.5], [16.4]; MSC-1005, FIGS. 7A, 7B, 10A, 19, 26H-26K; ¶¶[0320], [0189], [0095]-[0096], [0101], [0125], [0236]-[0238], [0155]-[0158], [0103], [517]-[527], [182]-[189], [0194]; MSC-1003, ¶[163]. For example, because the network server uses communication protocol layer 2716 for communications between its controller 402 and any other network element, it would have been obvious to a POSITA that when the network server sends the access message to Pocket Vault, the com-

“communication protocol layer 2716,” which similarly receives and sends such data to an entity “for authentication” (i.e., to controller(s) 402 and database 406), is an “authentication circuit.” MSC-1003, footnote 3. Specifically, communication protocol layer 2716 receives and sends this information “for authentication” by the controller(s) 402 and the database 406. Moreover, because the communication protocol layer 2716 is involved in receiving and transmitting data to other network elements, it would have been understood that by a POSITA that the communication protocol layer 2716 also includes “circuitry” to perform the receiving and transmitting. *Id.*

munications protocol layer 2716 (“*authentication circuit*”) also “*receives an access message from the trusted authority*” (e.g., controller 402) “*indicating that the trusted authority successfully authenticated the one or more codes and other data values to the third party and allows the user to access an application.*”

MSC-1003, ¶[163].

[23]

When a request to register a new Pocket Vault holder is received, the operations 1904 shown in Burger’s FIG. 20 below are performed by the network server.

MSC-1005, ¶¶[0464], [0476]; MSC-1003, ¶[164].

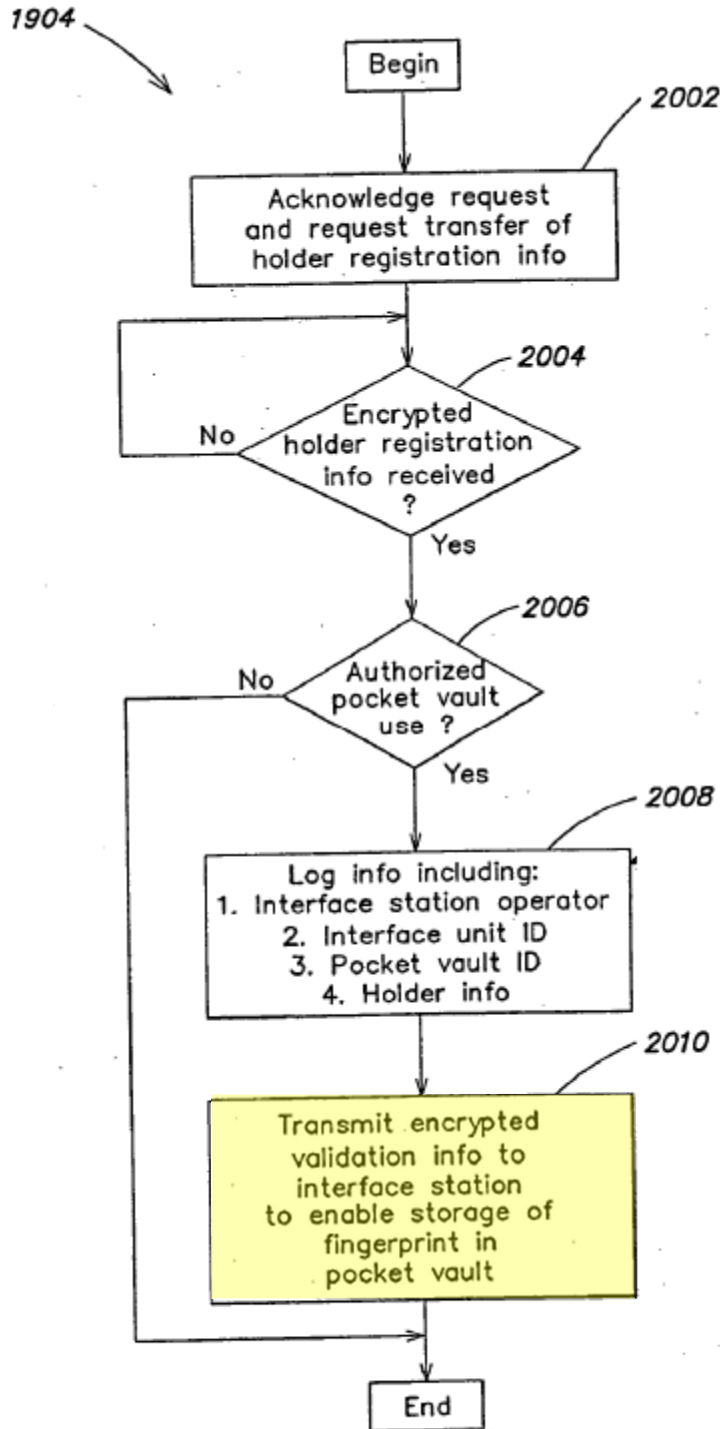


FIG. 20

MSC-1005, FIG. 20.

As shown in FIG. 20, after the requisite encrypted holder registration information is received through an interface station computer 304 or directly from the Pocket Vault and the network server determines that the Pocket Vault is authorized for use, “all of the relevant information regarding the new Pocket Vault registration is logged into the database 406 of the network server 114.” MSC-1005, ¶¶[0476]-[0481]. Next, in operation 2010, “the network server 114 transmits encrypted validation information to the interface station computer 304, which then may be passed on to the pocket vault interface unit 302, and then to the Pocket Vault 102, so as to enable the new holder’s fingerprint to be stored in the memory of the Pocket Vault 102.” MSC-1005, ¶[0482], FIG. 20; MSC-1003, ¶[165].

In this example, the validation information sent from the communication protocol layer 2716⁴ (“*authentication circuit*”) in the network server and received by the Pocket Vault (“*the integrated hardware device*”) is the “*authentication request from the authentication circuit*,” and, in response to receiving this information, the Pocket Vault is enabled to “*request[] a biometric scan*” (e.g., fingerprints) “*from the user to generate scan data*.” MSC-1005, ¶[0482], FIG. 20;

⁴ As shown in Burger’s FIG. 27, it would have been obvious to a POSITA that the communication protocol layer 2716 (“*authentication circuit*”) sends and receives data between the Pocket Vault and the network server. MSC-1003, footnote 4.

MSC-1003, ¶[166].

In another example, as part of a new Pocket Vault holder routine, shown below in FIG. 32, after a new holder's identity is verified (operation 3218) or a new holder account is created, instructions are sent to the Pocket Vault "wherein the new holder is prompted to apply his or her fingerprint to the fingerprint scanner 220 while the Pocket Vault 102 is interfaced with the interface unit 302. The user is further prompted to follow the directions on the Pocket Vault 102." MSC-1005, ¶¶[0575], [0585], FIG. 32; MSC-1003, ¶[167].

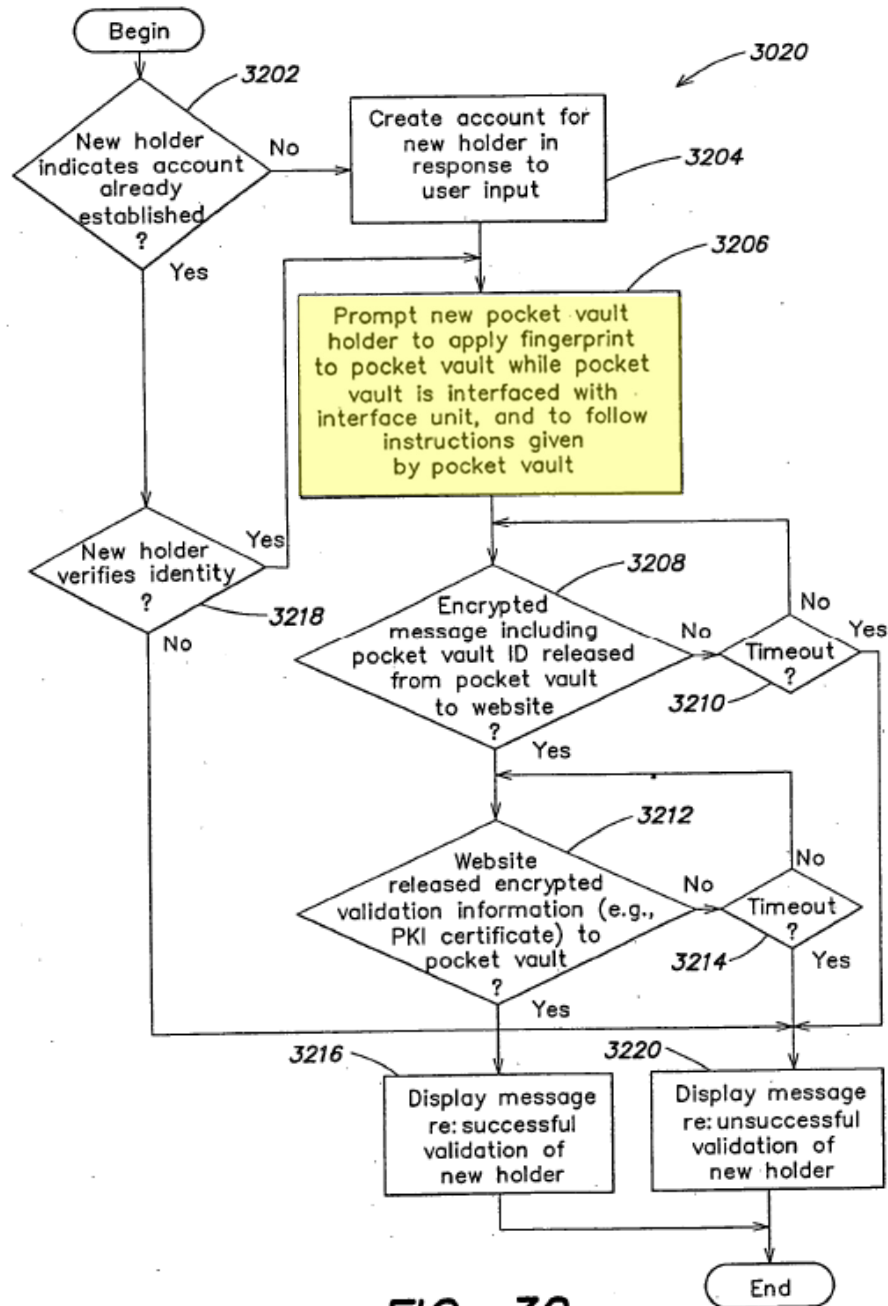


FIG. 32

MSC-1005, FIG. 32.

Although FIG. 32 is described as being performed by an interface station, “in some embodiments wherein appropriate networking capabilities are provided, each Pocket Vault 102 may communicate directly with the network server 114,

without the interface stations 104a-c facilitating communication therebetween.”

MSC-1005, ¶¶[0101], [0562], [0573], [0585]. Thus, in such embodiments, it would have been obvious to a POSITA that the communication protocol layer 2716 in the network server (“*authentication circuit*”) would have communicated directly with the Pocket Vault and sent a message (“*an authentication request*”) to request the Pocket Vault to prompt the new holder to apply the holder’s fingerprints. MSC-1003, ¶[168]. In this additional way, Berger renders obvious [23]. *Id.*

Under both examples noted above, when the scanned fingerprints do not match stored fingerprints in the Pocket Vault, the Pocket Vault does not send the Pocket Vault ID and takes other action, such as launching an unauthorized holder routine (“*when the integrated hardware device cannot verify scan data as being from the user, the integrated hardware device does not send the one or more codes and other data values,*” as recited in claim 24). MSC-1005, ¶¶[0184], [0185], [0585], FIG. 7A; MSC-1003, ¶[169].

[24]

See [23]; MSC-1003, ¶[170].

[26]

See [5]; MSC-1003, ¶[171].

[27]

See [7]; MSC-1003, ¶[172].

[28]

See [8]; MSC-1003, ¶[173].

[29]

See [9]; MSC-1003, ¶[174].

**B. [GROUND 2] – Burger and Robinson Render Obvious
Claims 3, 14, 17**

1. Robinson

Robinson relates to “a reliable system and method that conducts age verification of individuals for access to age-restricted areas, goods, and services” and for use in “verification [of] *an age-restricted transaction with the use of a biometric read* (such as a fingerprint) and a system ID (SID) number entry.” MSC-1006, ¶¶[0009]-[0010]; MSC-1003, ¶[74]. “[I]ndividuals trying to verify their own age” are referred to as “presenters” in Robinson. MSC-1006, ¶[0010]. Robinson explains that:

To register in the system, an individual presents at least one biometric sample, identity-verifying information, and *age-verifying*

information. ... The age-verifying information may be, for example and without limitation, age, date of birth, or a driver's license scan. The individual also registers with the system a system identification number (SID) that is used in conjunction with their biometric scan for age verification.

MSC-1006, ¶¶[0014]-[0015].

To implement the age-verification method, Robinson discloses a system that includes a verifier database 124 that contains age verification records or a central database 102 that stores data related to presenters and authorized points of verification (POVs). MSC-1006, ¶¶[0026]-[0027], [0030], FIG. 1. “Age verifying records hold presenter age verifying and identity verifying information, such as a presenter's age, date of birth, government ID number and state of issue, home address, or a telephone number; at least one biometric template; and *at least one ID number (SID)* that identifies the presenter within the system.” MSC-1006, ¶[0028]. “The SID is a number used to help identify registered individuals in the invention's system. ... The SID may be a unique number (a number with no chance of being honestly duplicated, e.g. social security number), reasonably unique number (a number with a statistically small chance of being duplicated, e.g. phone number), or a non-unique number (a number with a large chance of being duplicated).” MSC-1006, ¶[0043]; MSC-1003, ¶[75].

The age verification can be conducted by “verifier devices connected to a

verifier database 124, such as a register 130 or presenter service computer 126” or devices such as kiosks, vending machines, PCs, or a wireless device attached to a biological identification device (BID). MSC-1006, ¶¶[0035], [0030]. Robinson’s FIG. 3 depicts one example method for performing age verification. As shown in FIG. 3, “[t]he presenter enters their SID and their biometric sample (herein referred to as the “transaction biometric”) and transaction information, which is then sent to the verifier database 304 where the presenter’s age is verified. MSC-1006, ¶¶[0054]-[0057], FIG. 3. After the presenter’s age has been verified (or declined), the verifier device outputs the verification result, e.g., through a digital display or printed receipt. MSC-1006, ¶¶[0057]-[0058], [0048], FIG. 3. Robinson’s “verification [method] allows the system to track verifier behavior within the system, so that if a particular verifier falls under suspicion of fraudulent verification activity, each enrollment that verifier has confirmed may be evaluated.” MSC-1006, ¶[0048]; MSC-1003, ¶¶[76]-[77].

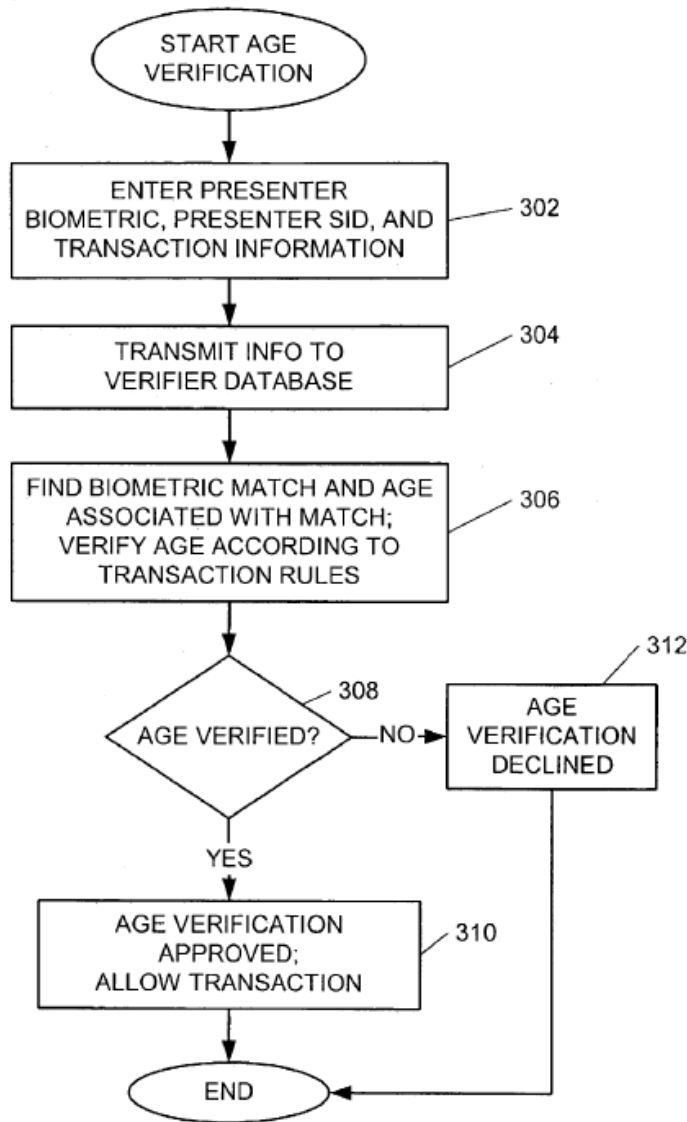


FIG. 3

MSC-1006, FIG. 3.

2. Combination of Burger and Robinson

Burger discloses a device and user authentication system that uses user biometric data, like fingerprint or retina scan, for various applications and transac-

tions. MSC-1005, FIG. 7. Robinson explains that “both the employee and merchant” of a business selling an age-restricted item, “may suffer monetary penalties and/or the merchant may even have their license to sell age-restricted goods revoked as a result of their employee's careless behavior.” MSC-1006, ¶[0005]. Accordingly, it would have been obvious to a POSITA to incorporate the age verification method of Robinson in Burger so that Burger’s system can be used by businesses interested in conducting transactions that require age-verification. MSC-1003, ¶[78]. Examples of such transactions include, e.g., buying alcohol or tobacco products, obtaining a driver’s license or passport at a government office, entering or playing certain games at a casino.

Combining the teachings of Burger and Robinson would have simply involved combining prior art elements according to known methods to yield predictable results and/or applying a known technique to a known device ready for improvement to yield predictable results. *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 415-421, 82 USPQ2d 1385, 1395-97 (2007); MSC-1003, ¶[79]. In particular, a POSITA would have understood that Robinson’s age-verification method would have been implemented in Burger’s system by allowing a user to present age-verifying information along with biometric sample and identity-verifying information, and *age-verifying information* when enrolling a user into an age-verification program. MSC-1003, ¶[79]. The age-verification information would have been

stored in the database 406 of Burger's network server, which includes the verifier database described in Robinson. When a user is involved in a transaction that requires age verification, the user enters the user's SID and biometric sample at a verifier device (e.g., a device used by the retailer). MSC-1006, ¶¶[0054]-[0057], FIG. 3. The verifier device sends the entered information to the network server, which verifies the user's age. MSC-1006, ¶¶[0054]-[0057], FIG. 3. If the user's age is authenticated, a confirmation message is then output by the verifier device. MSC-1006, ¶¶[0057]-[0058], [0048], FIG. 3; MSC-1003, ¶[79].

The above-described combination would have been predictable and had a reasonable expectation of success because it merely involves combining known elements in a manner that would have been easily implemented and obvious to a POSITA. MSC-1003, ¶[80]. For instance, it would have been well-within the capabilities of a POSITA to receive user age-verification information at a verifier device, implement a database in a network server that stores age-verification information, send age-verification information from the verifier device to the network server, and perform age-verification by comparing the age-verification information provided by the verifier device to information stored in the network server. MSC-1003, ¶[80]. The combination would also have been predictable and obvious because, as described by Robinson, businesses selling age-restricted items could be penalized or have their licenses revoked if they did not verify a user's age. MSC-

1006, ¶[0005]; MSC-1003, ¶[80]. Thus, a POSITA would have been motivated to combine the teachings of Burger and Robinson in the above-noted matter to provide a simple solution to perform age-verification when selling age-restricted goods. *Id.*

3. Application of Burger and Robinson to the '954 Claims

[3]

As explained above, in the Burger-Robinson system, age-verification can be performed by receiving a user's information (including age information) at a verifier device, sending that information to the network server, verifying the user's age at the network server, and then outputting a result of the age verification. The Burger-Robinson combination renders [3] obvious in several ways. MSC-1003, ¶[175].

First, a user registers with the system by presenting at least one biometric sample, identity-verifying information, and *age-verifying information*. MSC-1006, ¶¶[0014]-[0015]. This information is subsequently stored in the database 406 (verifier database) of network server. In this manner, Burger-Robinson renders obvious “*registering an age verification for the user.*” MSC-1003, ¶[176].

Second, when the age verification is performed, Robinson teaches that the results of the verifications are tracked. MSC-1006, ¶[0048]. That is, a result of the age verification is registered. MSC-1003, ¶[177].

Robinson also teaches that age-verification records include “*at least one ID number (SID)* that identifies the presenter within the system.” MSC-1006, ¶[0028]. Robinson explains that the “SID is a number used to help identify registered individuals in the invention's system. ... The SID may be a unique number (a number with no chance of being honestly duplicated, e.g., social security number), reasonably unique number (a number with a statistically small chance of being duplicated, e.g., phone number), or a non-unique number (a number with a large chance of being duplicated).” MSC-1006, ¶[0043]. It would have been obvious to a POSITA that the user’s Pocket Vault device ID is also a number “that can be used to identify registered individuals” and that the user’s Pocket Vault device ID would be a device ID code. MSC-1003, ¶[178]. At least because the age verifying information registered for a presenter or user includes a SID and identity-verifying information such as the Pocket Vault device ID, Burger-Robinson renders obvious “*registering an age verification for the user in association with the device ID code.*” MSC-1006, ¶¶[0014]-[0015]; MSC-1003, ¶[178].

[14]

See [3]; MSC-1003, ¶[179].

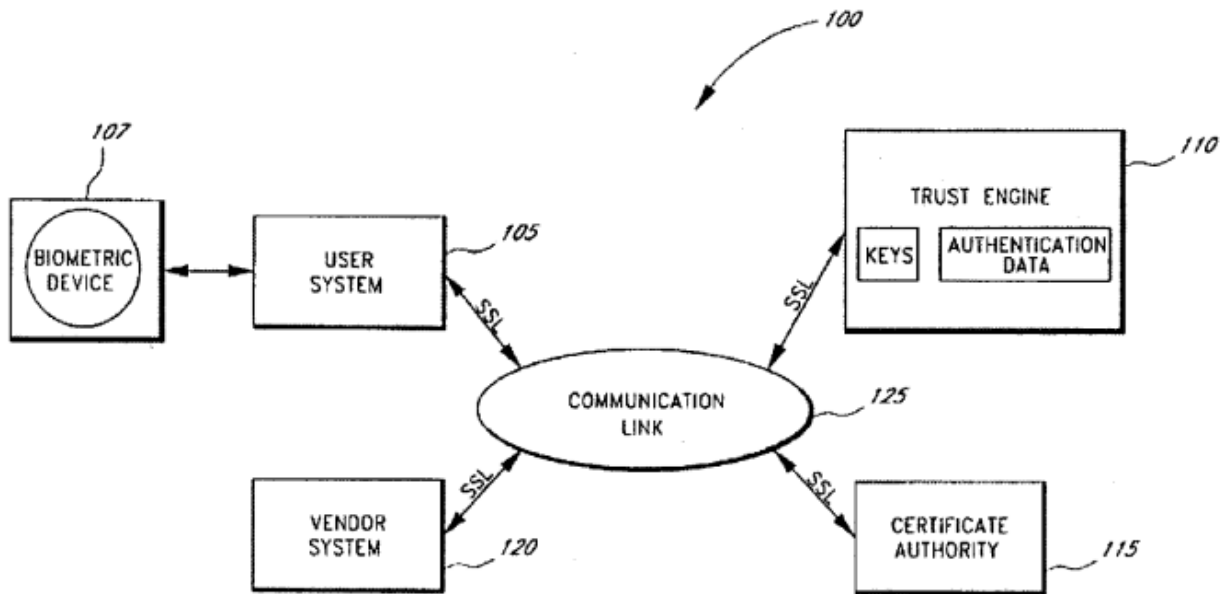
[17]

As explained above in [3], the Burger-Robinson combination registering age-verification information, such as a date of birth or age, with the database 406 (“*the trusted authority*”) in the network server. MSC-1006, ¶¶[0014]-[0015]; MSC-1003, ¶[180].

C. [GROUND 3] – Burger and Orsini Render Obvious Claims 6 and 25

1. Orsini

Orsini relates to “a method and system for securing sensitive data from unauthorized access or use.” MSC-1021, Abstract. As shown in Orsini’s FIG. 1 below, Orsini’s system involves a user system 105, a vendor system 120, and a trust engine 110. MSC-1021, ¶[62]. “[T]he user system 105 may include, but is not limited to, ... a personal mobile computing device, such as a digital assistant, mobile phone, laptop, or the like.” MSC-1021, ¶[65]; MSC-1003, ¶[81].



MSC-1021, FIG. 1.

Orsini's user system 105 includes a biometric device 107 that "may advantageously capture a user's biometric [data]." MSC-1021, ¶[63]. Orsini also discloses that "where the user produces biometric data, the user provides a physical characteristic, such as, but not limited to, facial scan, hand scan, ear scan, iris scan, retinal scan, vascular pattern, DNA, a fingerprint, writing or speech, to the biometric device 107. The biometric device advantageously produces an electronic pattern, or biometric, of the physical characteristic." MSC-1021, ¶[67]; MSC-1003, ¶[82].

2. Combination of Burger and Orsini

Burger explains that its "system may enable individuals to replace nearly all of the paper and plastic contents of their wallets and all of their other transaction

authorization implements with a single, hand-held portable electronic authorization device.” MSC-1021, ¶[93]. This single, hand-held portable electronic authorization device is described in Burger as the Pocket Vault 102, which is described as employing components similar to those used in *modern personal digital assistants and palm top computers*. MSC-1005, ¶[118]. It would therefore have been obvious that a POSITA would have implemented the Pocket Vault such that it comprises a mobile phone or laptop—devices that are similar and, in some cases, the same as modern personal digital assistants and palm top computers—as disclosed by Orsini. MSC-1003, ¶[83].

Indeed, a POSITA would have combined Burger and Orsini because doing so would have merely involved combining prior art elements according to known methods to yield predictable results. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 415-421, 82 USPQ2d 1385, 1395-97 (2007); MSC-1003, ¶[84]. Here, Burger’s disclosure already contemplates a Pocket Vault that includes mobile devices, such as personal digital assistance and palm top computers. MSC-1005, ¶[118]. Orsini’s user system 105 is similar to Burger’s Pocket Vault in that Orsini’s user system 105 is also a mobile device that includes a scanner capable of obtaining a user’s biometric data. MSC-1021, ¶[67]. Thus, combining Burger and Orsini’s teachings would have been obvious and predictable to a POSITA. MSC-1003, ¶[84].

Moreover, the Burger-Orsini combination would have simply involved implementing known prior art elements, such as a mobile phone or laptop components and functions, in a Pocket Vault device, which, as noted above, already contemplated including similar components. MSC-1005, ¶[118]; MSC-1003, ¶[85].

The Burger-Orsini combination would also have been obvious and predictable because both prior art references are related to the same field and describe similar devices. MSC-1003, ¶[86]. For instance, Burger and Orsini are focused on securing data from unauthorized access. MSC-1021, ¶[3]; MSC-1005, ¶¶[93]-[95]. Burger and Orsini both describe a mobile user system (Pocket Vault in Burger) that can be used to obtain biometric scans of a user. MSC-1021, ¶¶[63], [67]; MSC-1005, ¶¶[112], [116]. Orsini explicitly notes that, in some implementations, the mobile user system can be a mobile phone or laptop. MSC-1021, ¶[65]. In both Burger and Orsini, the mobile user system communicates with a trusted authority (e.g., Burger's network server (or components therein), Orsini's trust engine 110). And while some of the security protocols described in Burger and Orsini are different, a POSITA using Burger's system would have turned to and combined the teachings of similar systems, like Orsini, that are reasonably pertinent to the same problem being addressed by Burger, e.g., securely storing biometric data. MSC-1003, ¶[86].

The Burger-Orsini combination would have offered several advantages. For

instance, as the use of mobile phones became more ubiquitous and mobile phones were being adopted for use for multiple purposes, including making mobile payments and web browsing to conduct electronic transaction, it would have been beneficial for the pocket value to be a mobile phone or include a mobile phone, so that the Pocket Vault could be widely and easily used by customers who had a mobile phone. MSC-1003, ¶[87] (citing MSC-1028, MSC-1029). Integrating the Pocket Vault with the mobile phone would also allow a user to carry one less device thereby increasing user convenience. Similar benefits would be attained when implementing the Pocket Vault as a laptop, which was well known in the art to be used for e-commerce and banking, even before the ubiquity of smartphones. MSC-1003, ¶[87].

The Burger-Orsini combination would also have a foreseeable chance of success. As noted above, Burger already contemplated including components similar to those used in modern personal digital assistants and palm top computers. MSC-1005, ¶[118]. Because the designs and functions of mobile phones and laptops were well-known in the art and because the Burger and Orsini combination would have been predictable to a POSITA, the combination of a Pocket Vault with mobile devices such as a mobile phone or laptop, as described above, would have had a foreseeable chance of success and would have been well within the capabilities of a POSITA. MSC-1003, ¶[88].

3. Application of Burger and Orsini to the '954 Claims

[6]

As explained above in §III.C.2, it would have been obvious to a POSITA that Burger-Orsini's Pocket Vault comprises a mobile phone or laptop. MSC-1021, ¶[65]; MSC-1003, ¶[181].

[25]

See [6]; MSC-1003, ¶[182].

IV. PTAB DISCRETION SHOULD NOT PRECLUDE INSTITUTION

A. 35 U.S.C. §314(a) - *Fintiv*

As demonstrated below, a holistic analysis of the *Fintiv* framework favors institution. *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11, 6 (PTAB Mar. 20, 2020) (precedential) ("*Fintiv*").

Factor 1 favors institution or, at worst, is neutral. Petitioner was already granted a stay pending resolution of Petitioner's motion to transfer, which was filed in August, 2023. MSC-1023; MSC-1024; MSC-1025. On April 18, 2024 the District Court issued a decision denying transfer and lifting the stay. MS-1027. Petitioner intends to request a second stay from the District Court if an IPR is instituted. Yet, because the Board does "not attempt to predict" how a district court

might adjudicate a future motion to stay, this factor is neutral, at worst. *See Fintiv*, 12; *Sand Revolution II, LLC v. Cont'l Intermodal Group – Trucking LLC*, IPR2019-01393, Pap. 24, 7 (June 16, 2020)(“*Sand Revolution*”)(informative); *Sotera Wireless Inc. v. Masimo Corporation*, IPR2020-01019 Pap. 12, 14 (PTAB Dec. 1, 2020)(“*Sotera*”) (precedential).

Factor 2 weighs against discretionary denial. The District Court schedule remains in flux, and even the *Director’s Guidance* recognizes that “scheduled trial dates are unreliable and often change.” MSC-1016, 8. Here, the motion to transfer was recently decided and no new schedule has been issued.

The projected statutory deadline for the PTAB’s Final Written Decision (FWD) in this proceeding is October 2025. In comparison, the District Court’s median time-to-trial of 28.3 months⁵ yields an estimated trial date in September 2025. Based on the estimated time to trial, the FWD will likely issue earlier or around the same time as the trial date. Yet, because no new schedule has been issued and the trial date is uncertain, Factor 2 does not favor discretionary denial due to the uncertain nature of the District Court litigation.

Factor 3 weighs against discretionary denial. Co-pending litigation has not

⁵ Obtained from <https://www.uscourts.gov/statistics-reports/analysis-reports/federal-court-management-statistics>

advanced for months and is in its early stages. The parties have not conducted a *Markman* hearing and Microsoft's still-pending motion to dismiss seeks dismissal of Proxense's Complaint because it fails to specify which Microsoft product is accused of infringement, much less how it allegedly infringes the asserted claims. MSC-1017. Proxense instead accuses an amorphous concept—a "password-less architecture"—not descriptive of any specific Microsoft product. MSC-1018. This lingering lack of clarity in how the claims are being asserted impeded Microsoft's ability to fully develop its invalidity defenses in the litigation context. If an IPR is instituted, subsequent investments in the district court litigation can further be minimized (*e.g.*, through a motion to stay pending resolution of this IPR).

Factor 4 weighs against discretionary denial. As noted above, the District Court has not issued a schedule and final invalidity grounds have yet to be determined. Given the uncertainty in the trial schedule and in the final invalidity grounds that will be at issue during trial in the District Court, Petitioner reserves the right to request further briefing and/or submit additional evidence after the parties gain more clarity regarding the District Court schedule and grounds. Because the amount of issue overlap between this petition and the litigation is unclear, Factor 4 does not merit discretionary denial.

For Factor 5, Petitioner is a defendant in the co-pending litigation.

Factor 6 heavily weighs against discretionary denial due to the particularly

strong merits of this Petition, which outweigh any inefficiencies born of parallel litigation.

B. 35 U.S.C. §325(d) – *Advanced Bionics*

During prosecution, the claims were rejected in view of US Pat. 6,041,410; US Pub. 2005/0074126; US Pub. 2002/0129262; US Pub. 2004/0128162; and US Pub. 2004/0129787. MSC-1002, 172-200, 99-112. After several rounds of amendments, an interview, and Examiner amendments, the application was allowed. MSC-1002, 130-150, 72-90, 62-64, 22-34. In January 2024, IPR2024-00233 was filed challenging the '954 patent based on U.S. Patent No. 7,188,110 ("Ludtke") and U.S. Patent Application Publication No. 2002/0046336 ("Kon").

None of the references previously asserted against the '954 patent resemble or are cumulative to Burger. Indeed, Burger is a robust 91-page reference with no equivalent seen during prosecution or the pending IPR proceeding. Accordingly, the invalidity challenge based on the prior art references asserted in this Petition is not the same as, or substantially similar to, art and arguments previously presented to the Office in connection with the '954 patent.

To the extent Robinson's use as a secondary reference in an IPR proceeding (IPR2021-01447) and an *ex parte* re-examination request (application number 90/015,053 (*see* MSC-1022)) against US Patent No. 9,298,905, a child of the '954 patent, is considered, this Petition challenges the '954 claims and raises other

grounds with no overlap with any re-examination proceedings, IPR, or prosecution history. MSC-1022, 1654 (21); *Samsung Electronics America, Inc. v. Proxense, LLC*, IPR2021-01447, Paper 12, 7 (PTAB Feb. 28, 2022). Indeed, institution should not be denied simply because one secondary reference, Robinson, is asserted for a subset of dependent claims (claims 3, 14, and 17) in this IPR petition, whereas numerous other grounds, references, and issues have no overlap.

And, even if any of these references were somehow considered cumulative to references considered by the Examiner, during prosecution, none of the claims were examined in view of the asserted combinations of prior art applied in this petition. Thus, neither condition of the first prong of the *Advanced Bionics* framework is met, and there is no need to reach the second prong to resolve against discretionary denial under Section 325(d). *See, e.g., Oticon Medical AB et. al. v. Cochlear Ltd.*, IPR2019-00975, Paper 15 at 20 (PTAB Oct. 16, 2019) (precedential).

Moreover, the Challenged Claims were allowed based on the Examiner's mistaken conclusion (made without the benefit of Burger's rich disclosure) that the claims included certain allowable subject matter. MSC-1002, 22-32. That the Examiner did not consider obviousness of the Challenged Claims over the references asserted in this Petition constitutes material error.

V. CONCLUSION AND FEES

The Challenged Claims are unpatentable. Petitioner authorizes charge of fees to Deposit Account 06-1050.

VI. MANDATORY NOTICES UNDER 37 C.F.R § 42.8(a)(1)

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

Microsoft Corporation is the real party-in-interest.

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

The ‘954 Patent is or has been the subject of the following civil actions:

- *Proxense, LLC v Microsoft Corporation*, 6:23-cv-00319, W.D. Tex., filed May 2, 2023 (MSC-1004);
- *Proxense, LLC v. Google LLC et al*, 6-23-cv-00320 (WDTX) filed May 2, 2023; and
- *Proxense, LLC v. Apple, Inc.*, 6-24-cv-00143 (WDTX) filed March 18, 2024.

One IPR petition is pending against the ‘954 patent (*Google LLC v. Proxense, LLC*, IPR2024-00233 filed January 17, 2024).

Petitioner is not aware of any other disclaimers, reexamination certificates, or IPR petitions addressing the ‘954 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
W. Karl Renner, Reg. No. 41,265 Fish & Richardson P.C. 60 South Sixth Street, Suite 3200 Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 Email: IPR42342-0137IP1@fr.com	Roberto J. Devoto, Reg. No. 55,108 Usman Khan, Reg. No. 70,439 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 IPR42342-0137IP1@fr.com

(referencing No. 42342-0137IP1 and cc'ing PTABInbound@fr.com, axf-ptab@fr.com, devoto@fr.com and khan@fr.com).

Respectfully submitted,

Dated 4-26-24

/Roberto J. Devoto/
W. Karl Renner, Reg. No. 41,265
Roberto J. Devoto, Reg. No. 55,108
Usman Khan, Reg. No. 70,439
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

(Control No. IPR2024-00846)

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 13,956 words, which is less than the 14,000 allowed under 37 CFR § 42.24.

Dated 4-26-24

/Roberto J. Devoto/

W. Karl Renner, Reg. No. 41,265
Roberto J. Devoto, Reg. No. 55,108
Usman Khan, Reg. No. 70,439
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
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 26, 2024, a complete and entire copy of this Petition for *Inter Partes* Review and all supporting exhibits were provided by Federal Express, to the Patent Owner, by serving the correspondence address of record as follows:

Patent Law Works/Proxense
Greg Sueoka
4516 South 700 East, Suite 290
Salt Lake City, UT 84107

/Diana Bradley/
Diana Bradley
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
(858) 678-5667