

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: John J. Giobbi Attorney Docket No.: 42342-0136IP1
U.S. Patent No.: 8,352,730
Issue Date: January 8, 2013
Appl. Serial No.: 11/314,199
Filing Date: December 20, 2005
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. 8,352,730 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
D.	Level of Ordinary Skill in the Art.....	3
II.	THE '730 PATENT	4
A.	Brief Description.....	4
B.	Prosecution History.....	4
III.	THE CHALLENGED CLAIMS ARE UNPATENTABLE.....	5
A.	[GROUND 1] – Claims 1, 2, 4-9, 11, 12, and 14-17 are obvious over Burger	5
1.	Burger	5
2.	Application of Burger to the '730 Claims.....	27
B.	[GROUND 2] – Claim 3, 10, and 13 are Obvious in view of Burger and Robinson	86
1.	Robinson.....	86
2.	Combination of Burger and Robinson	90
3.	Application of Burger and Robinson to the '730 Claims.....	93
IV.	PTAB DISCRETION SHOULD NOT PRECLUDE INSTITUTION.....	95
A.	35 U.S.C. §314(a) - <i>Fintiv</i>	95
B.	35 U.S.C. §325(d) – <i>Advanced Bionics</i>	98
V.	CONCLUSION AND FEES	100
VI.	MANDATORY NOTICES UNDER 37 C.F.R § 42.8(a)(1).....	100
A.	Real Party-In-Interest Under 37 C.F.R. § 42.8(b)(1).....	100
B.	Related Matters Under 37 C.F.R. § 42.8(b)(2)	100
C.	Lead And Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3).....	101
D.	Service Information	101

EXHIBITS

MSC-1001	U.S. Patent No. 8,352,730 to John J. Giobbi (“the ’730 Patent”)
MSC-1002	Excerpts from the Prosecution History of the ’730 Patent (“the ’730 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/ (last visited April 19, 2024)
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	US Patent No. 8,200,980 (“Robinson 980”)

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	Product Identification Codes, https://www.uc.edu/content/dam/uc/ce/docs/OLLI/Page%20Content/PRODUCT%20IDENTIFICATION%20CODES%20BAR%20QR.pdf , last visited April 19, 2024
MSC-1021	RESERVED
MSC-1022	<i>Ex-Parte</i> Re-examination Request of 730 Patent; Re-examination application number 90/015,052
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 19, 2024

MSC-1027 Order Denying Motion to Transfer, *Proxense, LLC v Microsoft Corporation*, 6:23-cv-00319, W.D. Tex., April 18, 2024

LISTING OF CHALLENGED CLAIMS

Claim 1	
[1pre]	A method for verifying a user during authentication of an integrated device, comprising the steps of:
[1.1]	persistently storing biometric data of the 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 a storage element on the integrated device that is unable to be subsequently altered;
[1.2]	wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;
[1.3]	responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan,

[1.4]	comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;
[1.5]	responsive to a determination that the scan data matches the biometric data, wirelessly sending one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, wherein the one or more codes and other data values includes the device ID code; and
[1.6]	responsive to authentication of the one or more codes and the other data values by the agent, receiving an access message from the agent allowing the user access to an application,
[1.7]	wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.

Claim 2	
[2]	The method of claim 1, wherein the one or more codes and the other data values are transmitted to the agent 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 and the scan data are both based on a fingerprint scan by the user.

Claim 6	
[6]	The method of claim 1, further comprising: establishing a secure communication channel prior to sending the one or more codes and the other data values for authentication.
Claim 7	
[7.1]	The method of claim 1, further comprising: receiving a request for the one or more codes and the other data values without a request for biometric verification; and
[7.2]	responsive to receiving the request for the one or more codes and the other data values without a request for biometric verification, sending the one or more codes and the other data values without requesting the scan data.
Claim 8	
[8.pre]	An integrated device for verifying a user during authentication of the integrated device, comprising:

[8.1]	a memory 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 memory that is unable to be subsequently altered;
[8.2]	wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;
[8.3]	a verification unit, in communication with the memory, receives scan data from a biometric scan for comparison against the biometric data, and if the scan data matches the biometric data, wirelessly sends one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, wherein the one or more codes and the other data values includes the device ID code; and

[8.4]	responsive to the agent authenticating the one or more codes and the other data values, a radio frequency communicator, receives an access message from the agent allowing the user access to an application,
[8.5]	wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.

Claim 9

[9]	The integrated device of claim 8, wherein the one or more codes and the other data values are transmitted to the agent over a network.
-----	--

Claim 10

[10]	The integrated device of claim 9, wherein an age verification is registered in association with the device ID code.
------	---

Claim 11	
[11]	The integrated device of claim 8, wherein the verifier comprises: an LED to be activated for requesting the biometric scan.
Claim 12	
[12.pre]	A method for authenticating a verified user using a computer processor configured to execute method steps, comprising:
[12.1]	receiving one or more codes from a plurality of codes and other data values including a device ID code,
[12.2]	wherein the plurality of codes and the other data values comprises the device ID code uniquely identifying the integrated device and a secret decryption value associated with a biometrically verified user, the device ID code being registered with an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices;

[12.3]	requesting authentication of the one or more codes and the other data values by the agent, wherein the authentication determines whether the one or more codes and the other data values are legitimate;
[12.4]	receiving an access message from the agent; and
[12.5]	in response to a positive access message, allowing the biometrically verified user access to an application, wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.
Claim 13	
[13]	The method of claim 12, further comprising: registering a date of birth or age with the agent.

Claim 14

[14]	The method of claim 12, further comprising: establishing a secure communications channel with a biometric key, wherein the one or more codes and the other data values associated with the biometrically verified user is received from the biometric key.
------	---

Claim 15

[15.pre]	A system, comprising:
[15.1]	a biometric key stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the biometric key and a secret decryption value in a tamper proof format written to a storage element on the biometric key that is unable to be subsequently altered, and if scan data can be verified as being from the user by comparing the scan data to the biometric data, wirelessly sending, one or more codes from the plurality of codes and other data values wherein the one or more codes and the other data values include the device

	ID code,
[15.2]	and the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition; and
[15.3]	an authentication unit receives the plurality of codes and the other data values and send the plurality of codes and the other data values to agent for authentication to determine whether the one or more codes and the other data values are legitimate, wherein the agent is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, and
[15.4]	responsive to the device ID code being authenticated, the authentication unit receiving an access message from the agent allowing the user to access an application,

[15.5]	wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.
Claim 16	
[16]	The system of claim 15, wherein the biometric key receives an authentication request from the authentication unit, and in response, requests a biometric scan from the user to generate the scan data.
Claim 17	
[17]	The system of claim 15, wherein if the biometric key cannot verify the scan data as being from the user, it does not send the one or more codes and the other data values.

Microsoft Corporation (“**Petitioner**” or “**Microsoft**”) petitions for *Inter Partes* Review (“**IPR**”) of claims 1-17 (“**the Challenged Claims**”) of U.S. Patent No. 8,352,730 (“**the ‘730 Patent**”). Compelling evidence presented in this Petition demonstrates at least a reasonable likelihood that Microsoft will prevail with respect to at least one of the Challenged Claims.

I. REQUIREMENTS FOR IPR

A. Grounds for Standing

Petitioner certifies that the ‘730 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]-[166]).

Ground	Claim(s)	35 U.S.C. § 103
1	1, 2, 4-9, 11, 12, and 14-17	Burger
2	3, 10, and 13	Burger in view of Robinson

The ‘730 Patent was filed on December 20, 2005, and claims priority from

earlier applications. MSC-1001, cover. The earliest application that the '730 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 '730 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 the December 20, 2004 date of the provisional application is used as the priority date of the '730 Patent.

Reference	Filing Date	Publication Date
US 2005/0050367 (Burger or MSC-1005)	Sept. 30, 2004	Mar. 3, 2005
US Pat Pub. No. 2003/0177102 (Robinson or MSC-1006)	Feb. 19, 2003	Sept. 18, 2003

C. Claim Construction

No formal claim constructions are necessary in these proceedings 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). Nonetheless, for the sake of completeness, Petitioner notes the three phrases addressed by the Board during a prior IPR proceeding (IPR2021-01444).

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 these proceedings. MSC-1003, ¶¶[43]-[44].

Petitioner reserves the right to respond to any constructions offered by Patent Owner or adopted by 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.

D. Level of Ordinary Skill in the Art

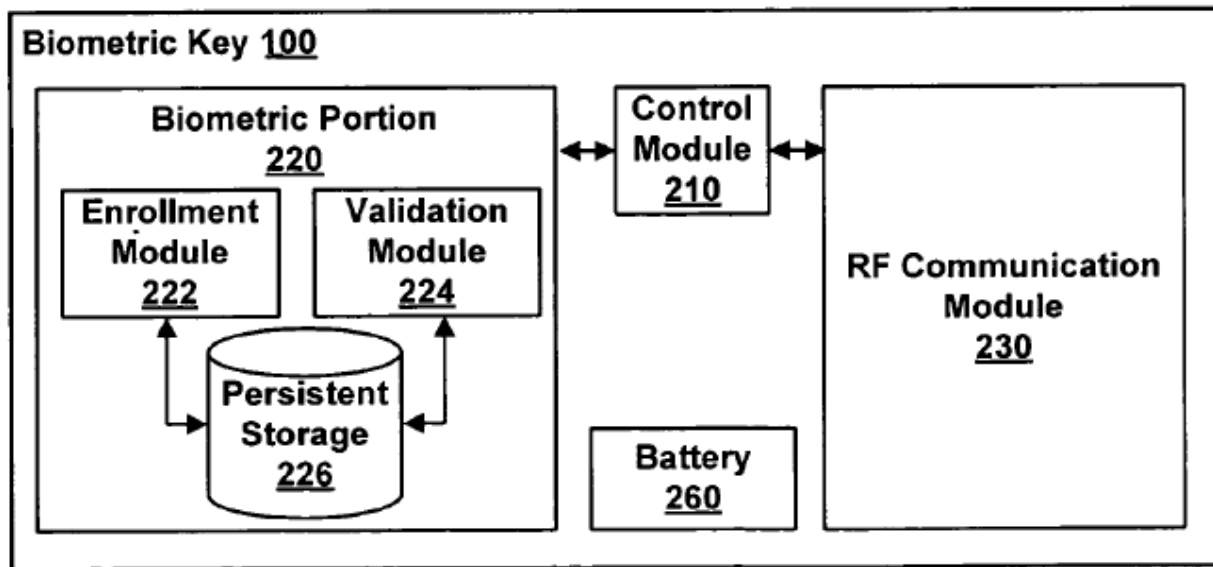
A person of ordinary skill in the art (“POSITA”) relating to the subject matter of the ‘730 Patent as of December 20, 2004 would have had (1) at least a bachelor’s degree in computer science, computer engineering, electrical engineering, or a related field, and (2) at least two years of industry experience in wireless communications security. Additional graduate education could substitute for professional

experience, and *vice versa*. MSC-1003, ¶¶[22]-[23].

II. THE '730 PATENT

A. Brief Description

The '730 patent is directed to systems and methods for performing “an authentication responsive to biometric verification of a user being authenticated.” MSC-1001, 1:15-18, Abstract, 2:60-67. In particular, the '730 patent discloses a biometric key 100, as shown in FIG. 2 below, that can be used to perform the biometric verification using a trusted key authority. MSC-1001, 3:47-5:2, 5:60-67; MSC-1003, ¶¶[45]-[48].



MSC-1001, FIG. 2.

B. Prosecution History

The '730 patent was filed as US Patent Application No. 11/314,199 (the “199 application”) on Dec. 20, 2005. MSC-1001, cover. After three RCEs, the

Examiner allowed the claims by amending the claims to add features [1.2] and [1.7] (and some other minor amendments) by virtue of an Examiner amendment attached to the notice of allowance dated August 31, 2012. MSC-1002, 31-43. However, as noted in this petition below, features [1.2] and [1.7] were well-known and would have been obvious to a POSITA. MSC-1003, ¶¶[49]-[50].

III. THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. [GROUND 1] – Claims 1, 2, 4-9, 11, 12, and 14-17 are obvious over Burger

1. Burger

Burger is related to a portable electronic authorization device it calls a “Pocket Vault.” MSC-1005, ¶[51]. The Pocket Vault is “used for producing, distributing, storing, and using the typical contents of a person’s wallet, as well as the multiple, separate transaction authorization devices.” MSC-1005, ¶[93]. Burger’s system, shown below in FIG. 1, enables “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”—the Pocket Vault. MSC-1005, ¶¶[51], [93]; MSC-1003, ¶[51].

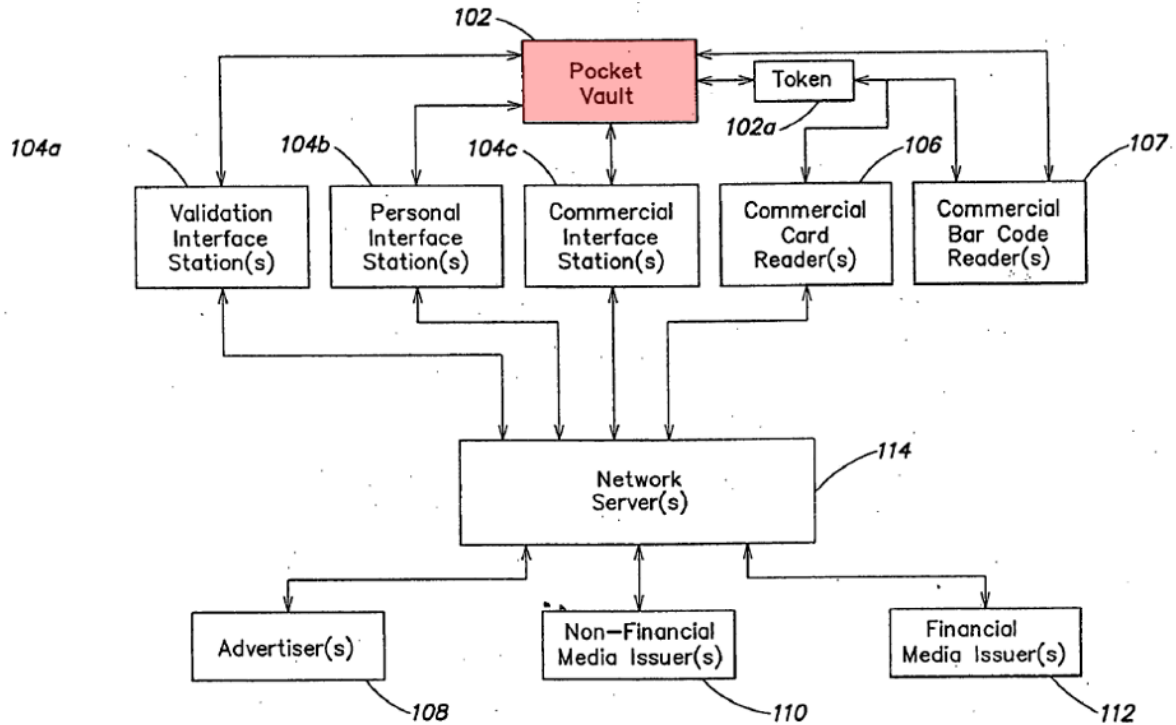


FIG. 1

MSC-1005, FIG. 1¹.

Burger's system 100 includes the Pocket Vault 102, an associated token 102a, network server(s) 114, interface stations 104a-c coupled to the network server(s) 114, 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, ¶¶[96]-[97]. Components of system 100 can be connected in a wired or wireless manner. MSC-1005, ¶¶[99]-[102]. The Pocket Vault 102 may communicate with the network server 114 directly in a wireless network or may communicate through the

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

interface stations 104a-c. MSC-1005, ¶[101]; MSC-1003, ¶[52].

An example of the Pocket Vault 102 is shown below in Burger's FIG. 2.

Burger's Pocket Vault 102 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 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 102 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]. A POSITA would have understood that device serial numbers are generally used to identify a device, and, for a device such as the Pocket Vault, would have included a Pocket Vault ID (chip ID). MSC-1003, ¶[53].

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, building security passes, etc." MSC-1005, ¶[129]; MSC-1003, ¶[54].

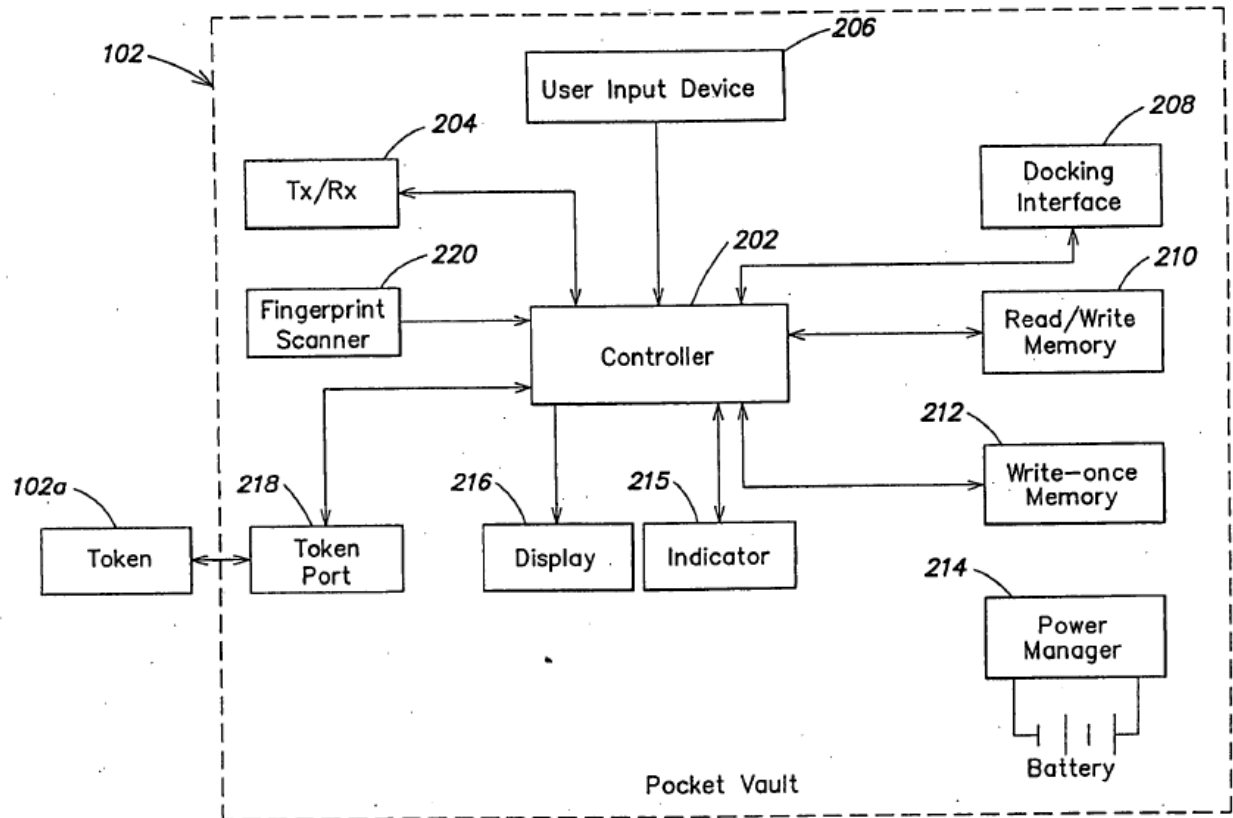


FIG. 2

MSC-1005, FIG. 2.

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 102 only after the fingerprint scanner 220 ... has successfully authenticated the identity of the holder.” MSC-1005, ¶[122]; MSC-1003, ¶[55].

The Pocket Vault 102 includes a display 216 that can be used, e.g., to dynamically display branding and advertising messages. MSC-1005, ¶[110]. In addition, the display 216 can include a “touch screen or a separate user input device” to “effectively flip through the contents of the Pocket Vault 102 to locate and select a desired media (e.g., a credit card, driver’s license, library card, frequent flier card, a particular RFID personality, etc.) much like a person can flip through the contents of his or her wallet to do the same.” MSC-1005, ¶¶[109], [132], [133]; MSC-1003, ¶[56].

The Pocket Vault 102 can also include or be coupled to 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 102 and can include a display device to display information such as credit card information and used in transactions with retailers. MSC-1005, ¶¶[103]-[104], [155]-[158]. For example, “[w]hen used by a consumer, retailers may verify authenticity by matching the information displayed on the token 102a with that revealed in the swipe or other token reading process. Without a match, the token 102a may be rejected.” MSC-1005, ¶[158]; MSC-1003, ¶[57].

Burger’s Pocket Vault 102 also includes a fingerprint scanner 220. MSC-1005, FIG. 2; ¶[135]. “[O]ther bio-metric scanning devices may also be employed to verify the identity of the holder. For example, some embodiments may employ a

charge coupled device (CCD) to serve as an iris or retina scanner, an optical sensor, and/or a voiceprint.” MSC-1005, ¶[135]; MSC-1003, ¶[58].

When a user is interested in using the device, the user’s biometric feature (e.g., fingerprint scan, retina scan, etc.) 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 and/or PIN code) is stored within the to-be-accessed device,” 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]. Burger explains that “great care may be taken to ensure that only authorized individuals are permitted to validate Pocket Vaults 102 by having their authentication information (e.g., their fingerprint data or PIN codes) stored therein. Therefore, after it has been confirmed that the holder’s authentication information has been properly stored in the Pocket Vault 102, 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." MSC-1005, ¶[116]; MSC-1003, ¶[59].

Burger's network server(s) 114 can "serve as: (1) a repository of information for the network, (2) the entity that controls access to the stored information by the other network devices, and (3) a service provider for financial and non-financial media issuers, advertisers, as well as Pocket Vault holders." MSC-1005, ¶¶[98], [117], FIG. 1. In one example shown in FIG. 4 (reproduced below), the network server 114 may include a database 406 that stores "a real-time record of critical reference data along with transaction histories, back-up files, and security audit trail information for key events. 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, ¶[60].

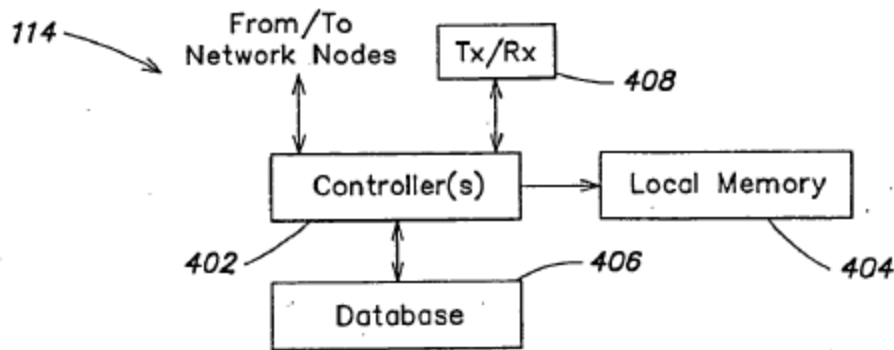


FIG. 4

MSC-1005, FIG. 4.

FIG. 27 (shown below) depicts another example implementation of a network server 114 that includes “one or more controllers 402 and a database 406, as described above in connection with FIG. 4. In addition, the network server 114 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, ¶[61].

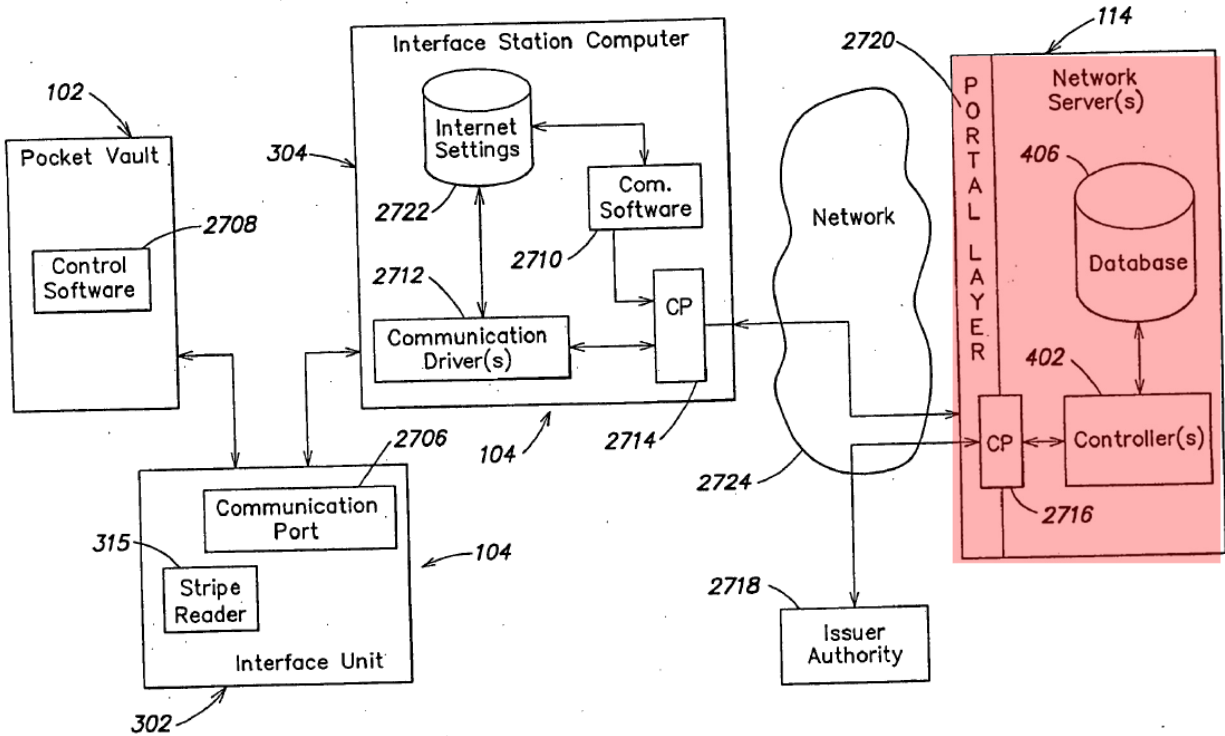
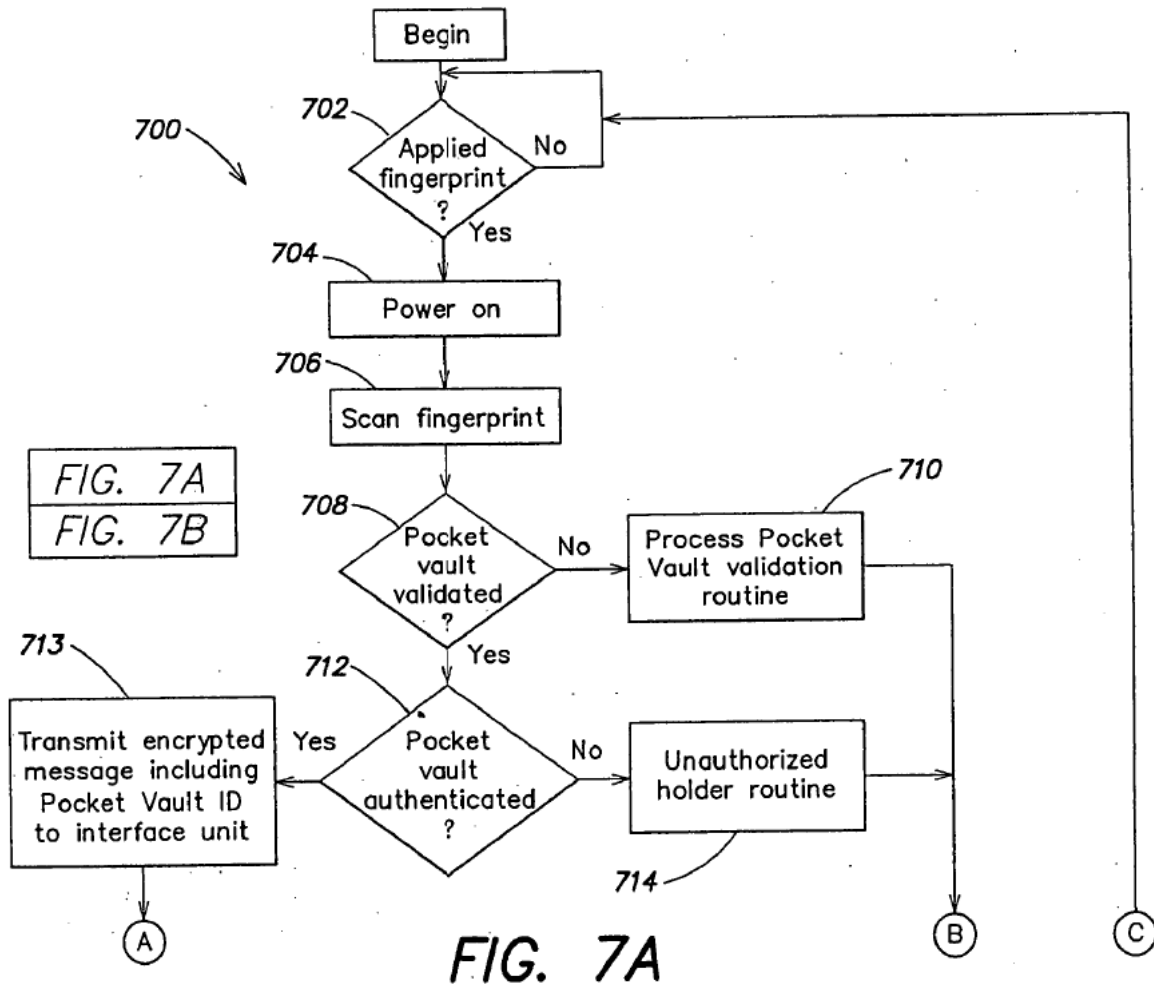


FIG. 27

MSC-1005, FIG. 27.

An example method of using Burger's Pocket Vault 102 to perform user and device authentication is shown in FIG. 7A below. When a user's fingerprint is applied to the fingerprint scanner 220, the power manager 214 powers on the Pocket Vault 102. 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 102 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, ¶[62].



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 114 at step 713. MSC-1005, ¶¶[185]-[186], [101], [114]-[116]; MSC-1003, ¶[63].

Burger then teaches that a check can be performed to ensure that components used to interface the Pocket Vault 102 with the other components in the network 100 are in place and operating correctly, and subsequently, a Pocket Vault holder is granted access to the contents of his or her Pocket Vault 102. MSC-1005, ¶[187]; MSC-1003, ¶[64].

In some embodiments, after the unique Pocket Vault chip ID is transmitted and a token 102a (e.g., Chameleon Card) is determined to be on-board the Pocket Vault 102, 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 102 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, ¶[65].

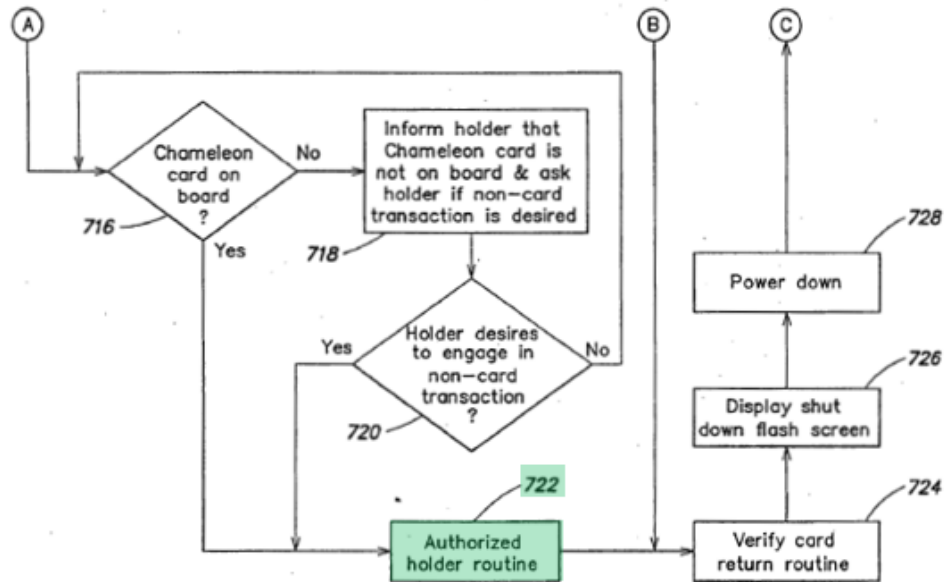


FIG. 7B

MSC-1005, FIG. 7B.

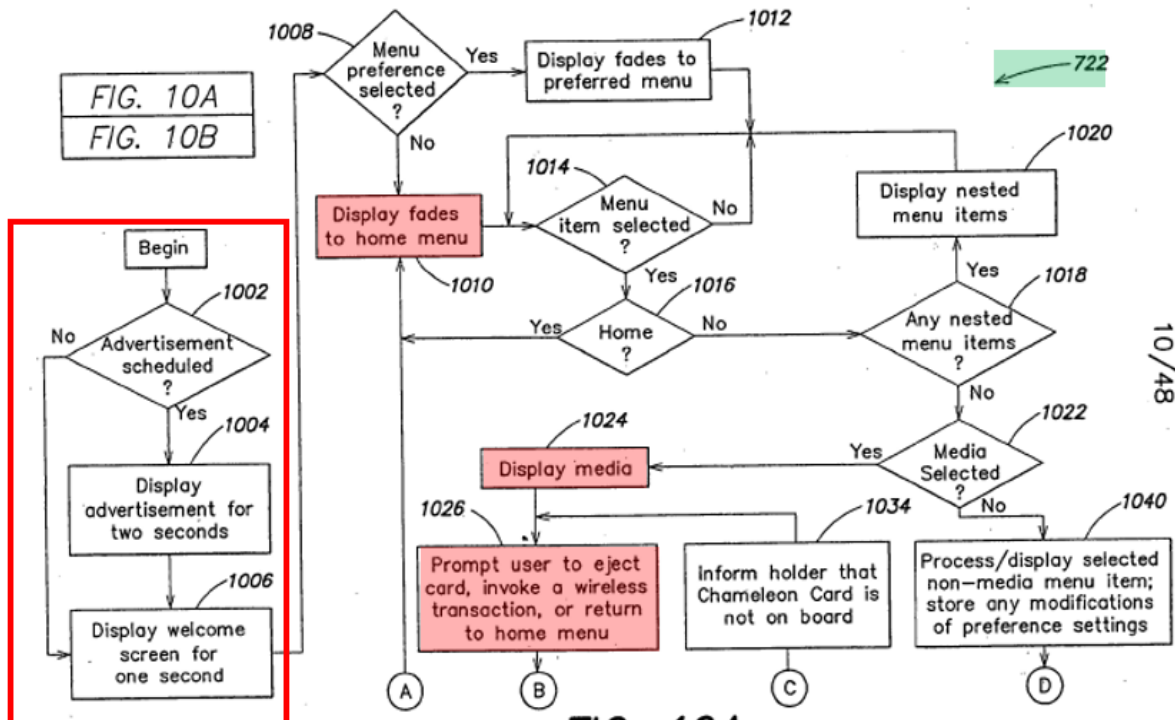


FIG. 10A

MSC-1005, FIG. 10A.

Burger's Pocket Vault 102 can be used as a "wallet replacement" to execute a transaction. MSC-1005, FIGS. 19, 24, 25, ¶[93]. For example, when a request to authorize a transaction has been made, Burger's network server 114 implements the operations depicted in FIGS. 24 and 25 (reproduced below). MSC-1005, FIG. 19, ¶[0474]; MSC-1003, ¶[66].

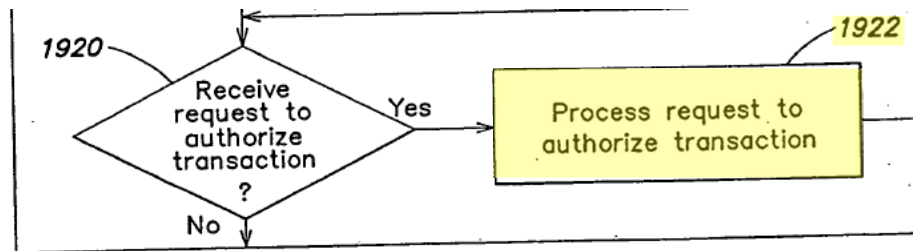


FIG. 19

MSC-1005, FIG. 19.

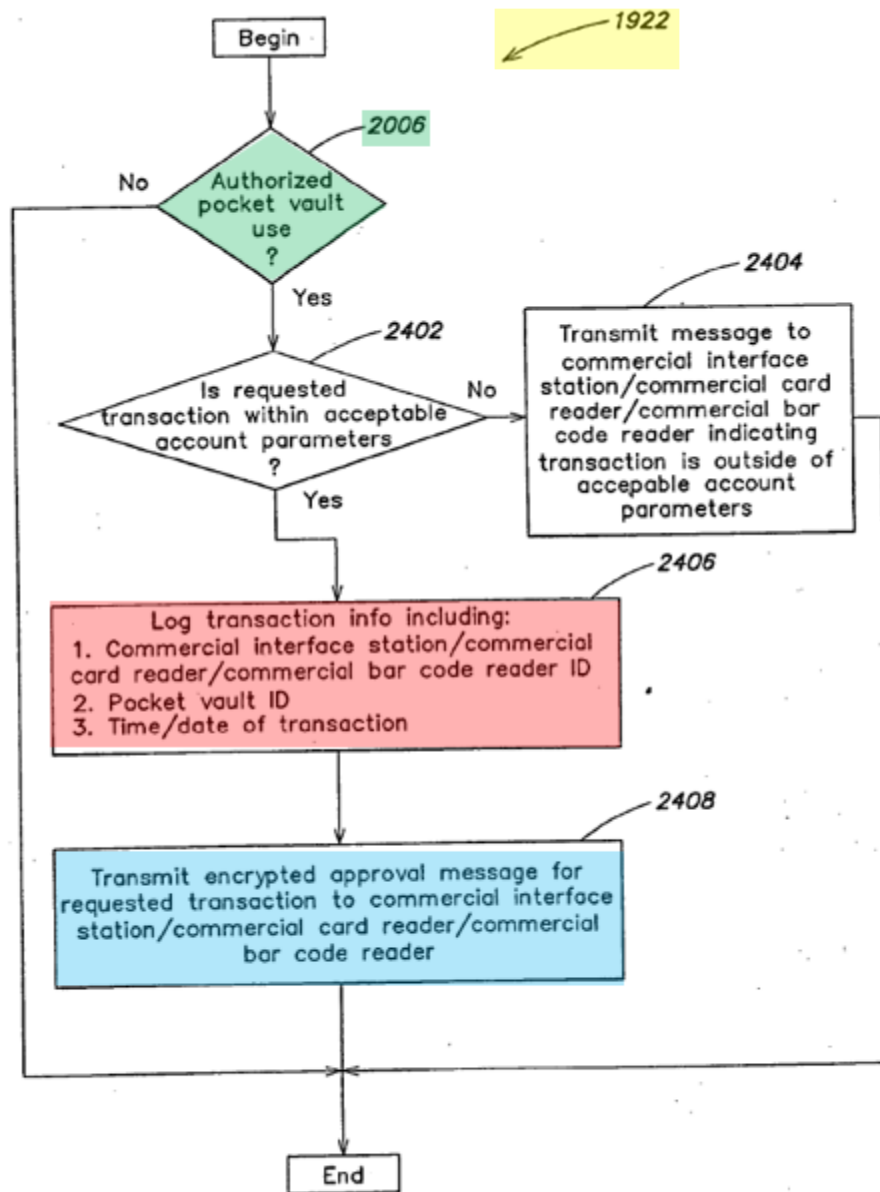
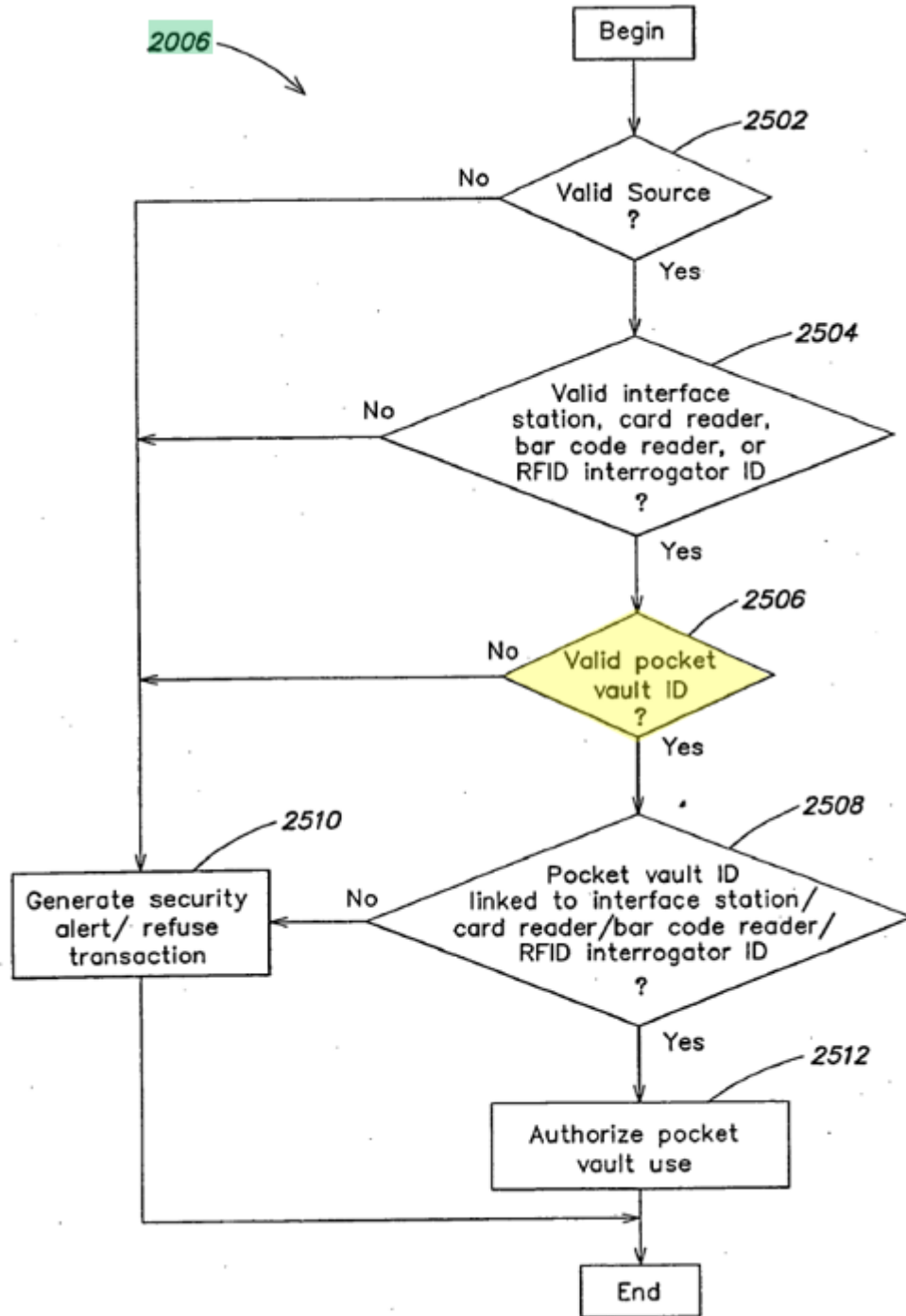


FIG. 24

MSC-1005, FIG. 24.



MSC-1005, FIG. 25.

In response to the request to authorize a transaction, the network server 114 determines whether the Pocket Vault 102 is authorized. MSC-1005, FIGS. 24, 25;

¶¶[0511]-[513]. To determine whether the Pocket Vault 102 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;

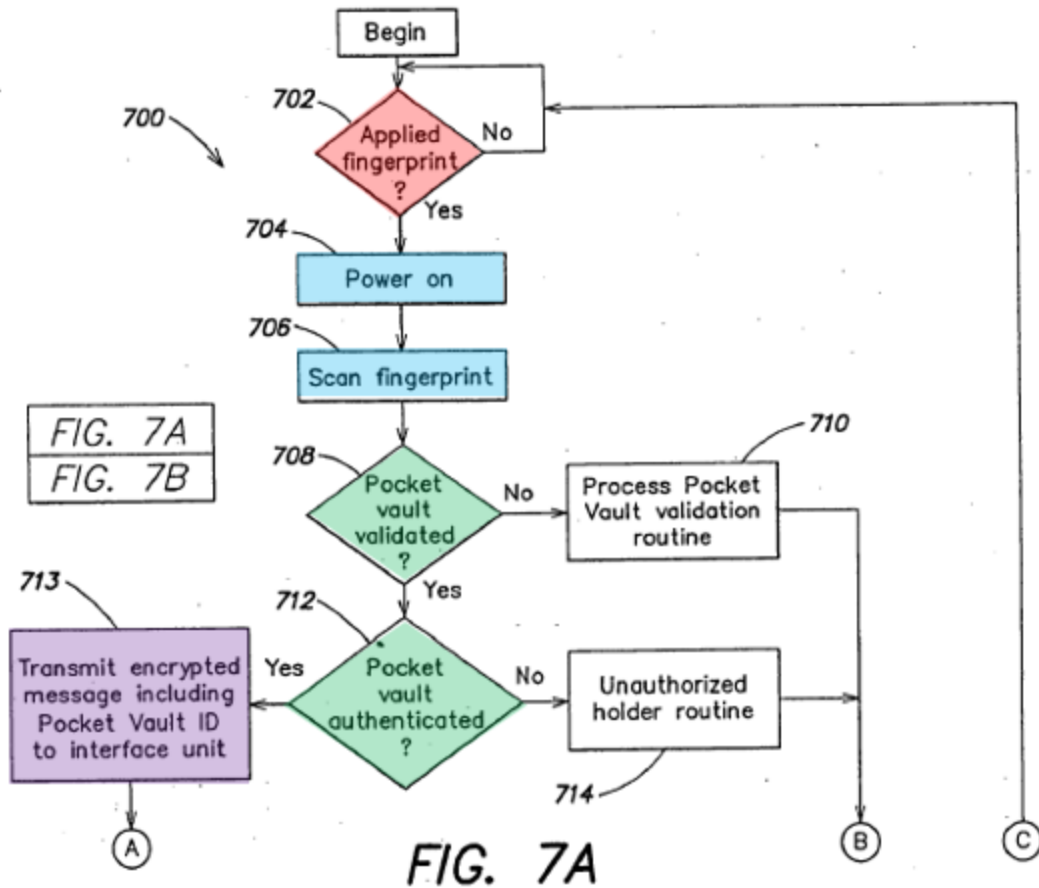
¶¶[0520]-[523]. If the network server 114 determines that there is a valid source and the ID is valid, the network server proceeds to determine whether the Pocket Vault ID is valid, and upon, doing so, determines that the Pocket Vault is authorized. MSC-1005, FIG. 25; ¶¶[0524]-[529], [182]; MSC-1003, ¶[67].

Once the Pocket Vault 102 use is authorized, “it is determined whether the requested transaction is within acceptable account parameters.” MSC-1005, FIG. 24; ¶[0514]. “When ... it is determined that the requested transaction is within acceptable account parameters, information regarding the transaction is logged into the database 406 of the network server 114 (FIG. 4). As shown [in FIG. 24], the logged information may include the identification of the entity with which the transaction took place, the Pocket Vault ID (if available), and the time and date of the transaction.” MSC-1005, FIG. 24; ¶¶[0511]-[513]. “[A]n 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; ¶[0518]; MSC-1003, ¶[68].

Example Use Case

Dr. Traynor describes an example implementation (noted hereinbelow) of one use case of Burger's system. MSC-1003, ¶¶[69]-[74].

When a user is interested in using the Pocket Vault 102 for a transaction (e.g., at a grocery or retail store), the user places their 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). MSC-1005, FIG. 7A. 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 114 (*see* purple annotated rectangle in FIG. 7A below). MSC-1005, FIG. 7A. A check is then performed to ensure that the components used to interface the Pocket Vault 102 with the other components in the network 100 (either wirelessly or directly) are in place and operating correctly. MSC-1005, FIGS. 7A, 7B, ¶[187]; MSC-1003, ¶[70].



MSC-1005, FIG. 7A.

Next, after the Pocket Vault holder determines that the Pocket Vault includes a token 102a (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. 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, ¶[71].

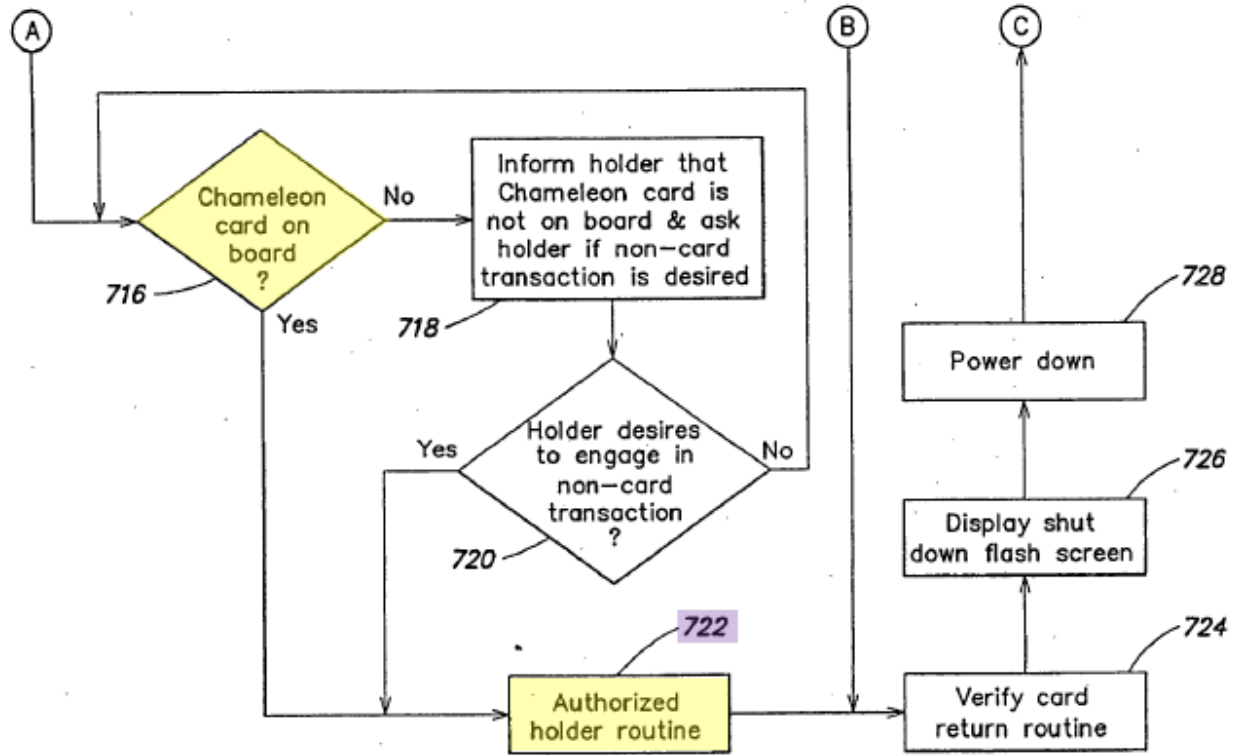
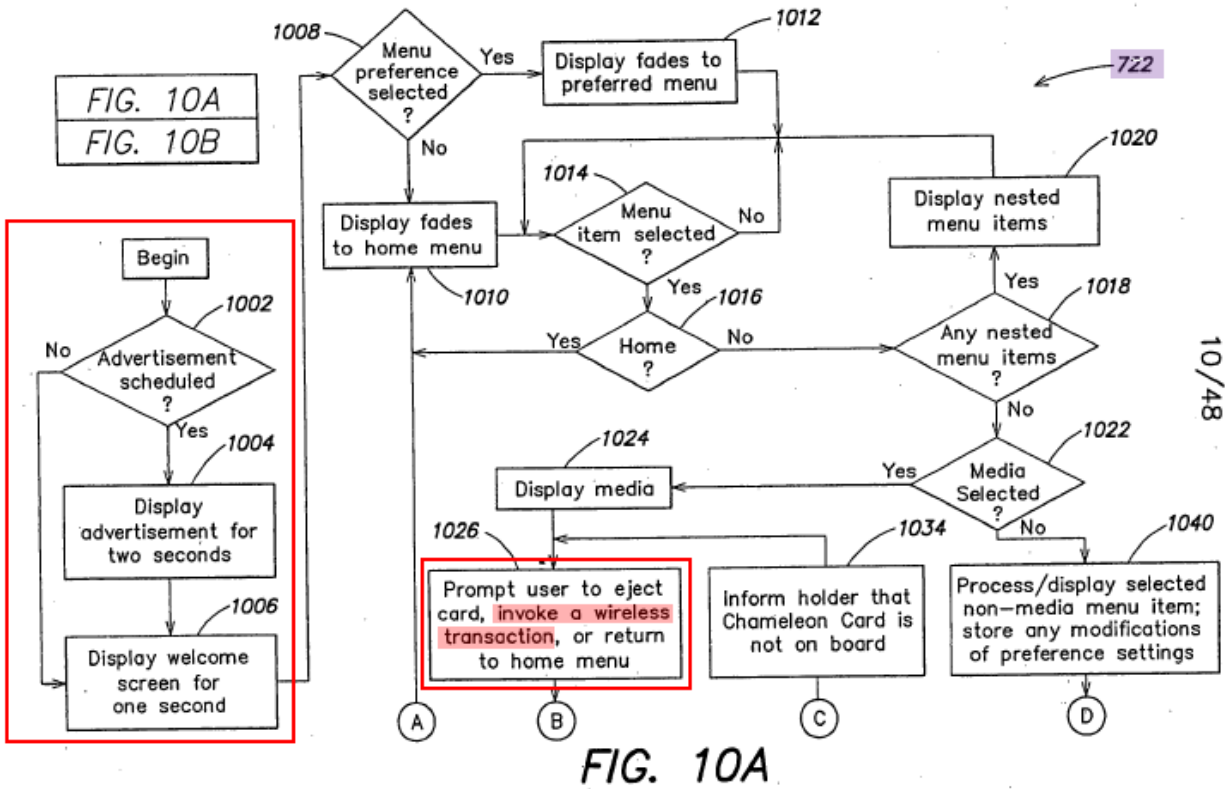


FIG. 7B

MSC-1005, FIG. 7B.



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

The network server 114 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, ¶[72].

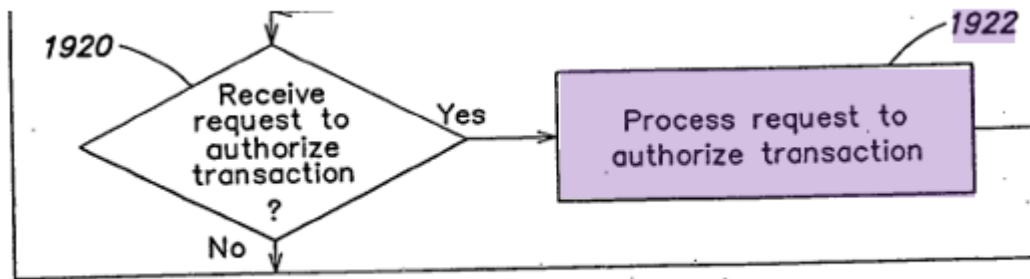


FIG. 19

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

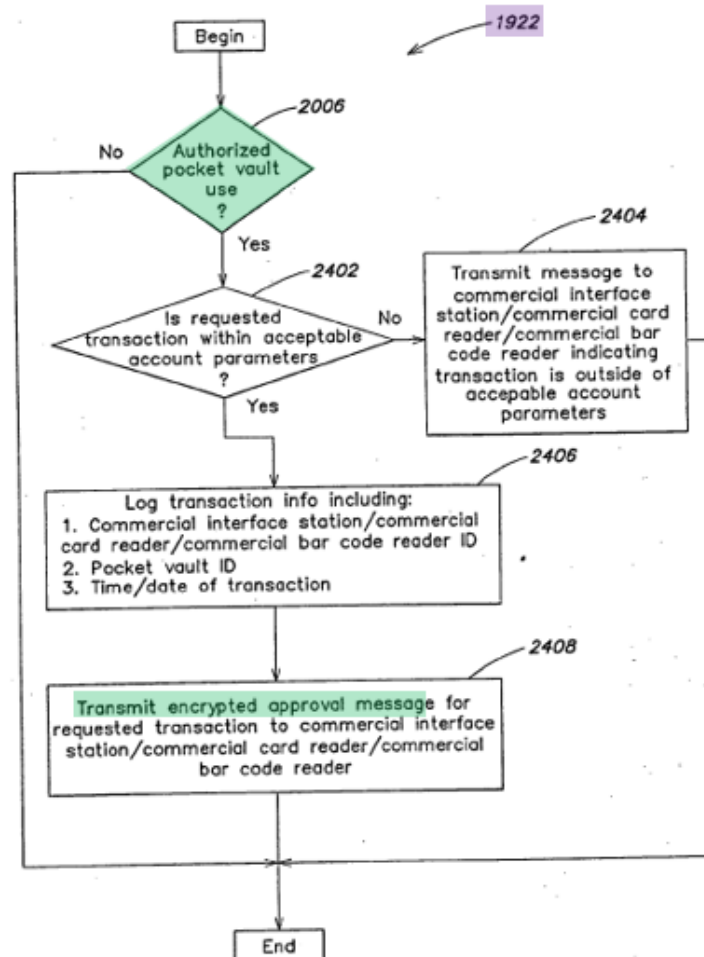


FIG. 24

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

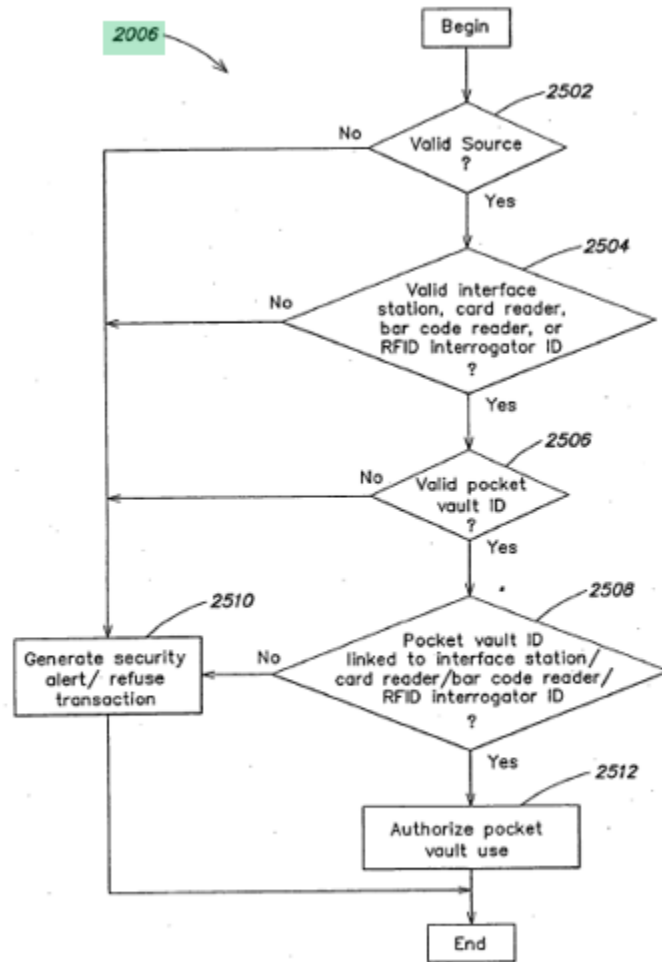
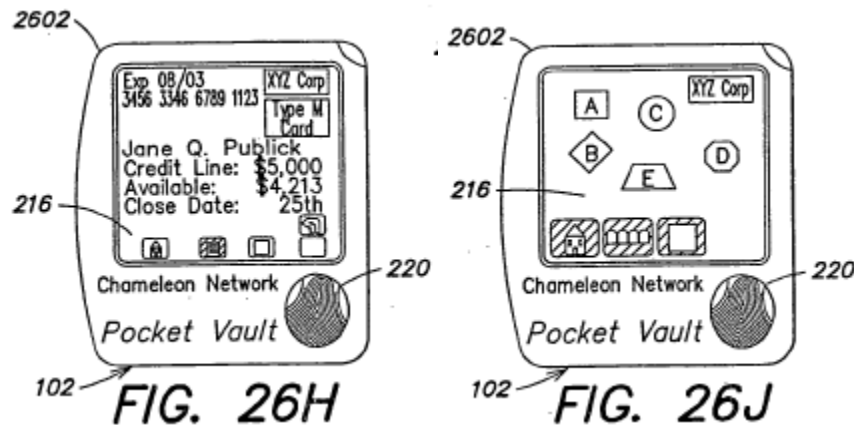


FIG. 25

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

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, ¶¶[73]-[74].



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

2. Application of Burger to the '730 Claims

[1.pre]

To the extent the preamble is limiting, Burger renders it obvious. Burger teaches systems, methods, and apparatus directed to “*verifying a user during authentication of an integrated device.*” MSC-1005, ¶[0010]. As explained below in [1.1]-[1.7], Burger discloses verifying a Pocket Vault holder (“*user*”) during authentication of a Pocket Vault 102 (“*integrated device*”) for transactions involving financial and/or non-financial media. MSC-1005, ¶¶[0002], [0127]-[0128]; MSC-1003, ¶[82].

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]. “Because the device may incorporate many different media that are commonly stored in a person's wallet or elsewhere, possibly including both financial and non-financial media,” the device may also be referred to as a multi-purpose “point-of-transaction” device. MSC-1005, ¶[0094]. The Pocket Vault 102 is self-contained with a set of authentication security features to ensure privacy. MSC-1005, ¶[0095]; MSC-1003, ¶[83].

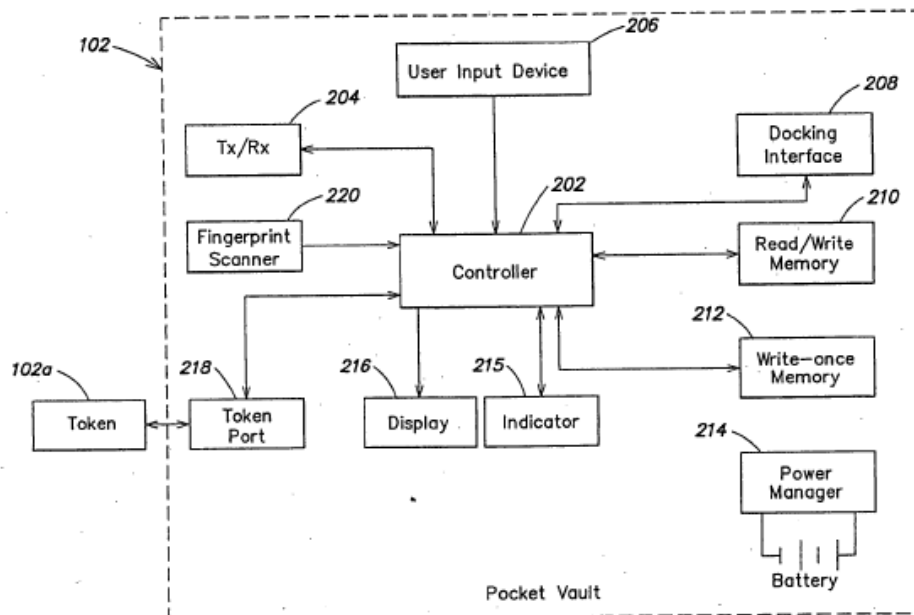


FIG. 2

MSC-1005, FIG. 2.

[1.1]

Like the 730 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 102 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 unable to be subsequently altered*”). MSC-1005, ¶¶[127], [182], FIG. 2 (reproduced below); MSC-1003, ¶[84].

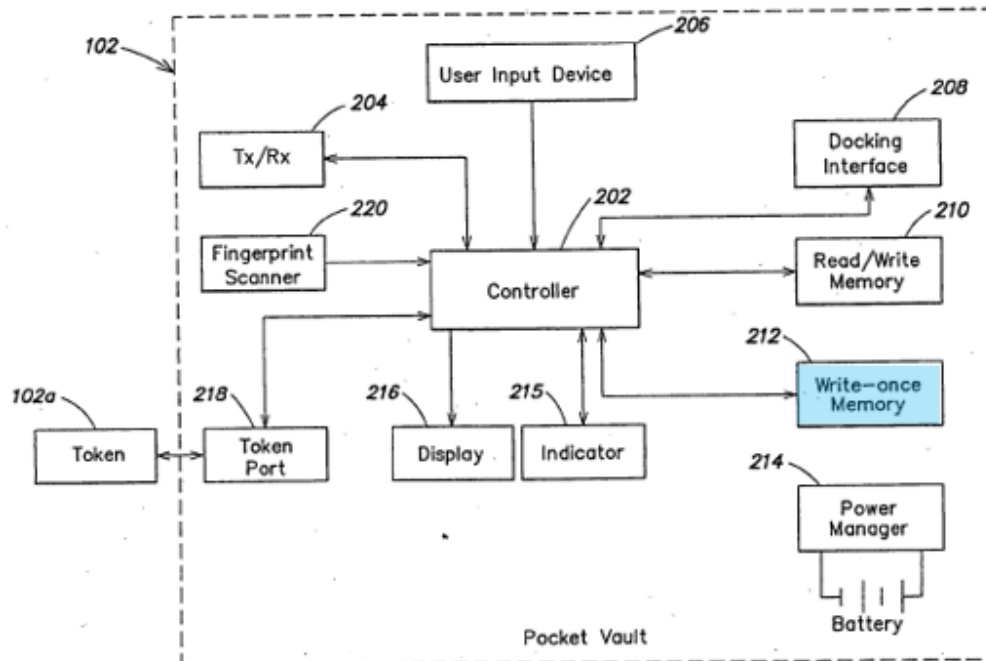


FIG. 2

MSC-1005, FIG. 2.

The Pocket Vault 102 stores authentication information, such as user fingerprints (“*biometric data of the user*”), device serial numbers such as a Pocket Vault ID (chip ID), and encryption/decryption information (“*a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value*”). MSC-1005, ¶¶[0112], [114], [118], [122], [127], [129]. Indeed, Burger teaches that the network server 114 provides the PKI certificate to the Pocket Vault 102 and grants the Pocket Vault authority to permanently store authentication information (“*persistently storing biometric data ...*”). MSC-1005, ¶¶[114], [182]; MSC-1003, ¶[85].

In particular, a 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 devices. MSC-1003, ¶[86]. 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 the integrated device.*” MSC-1003, ¶[87]. The ’730 patent suggests that a device ID code can be both the “plurality of codes” and “other data values.” MSC-1001, 7:24-31. Consistent with the description in the ’730 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.*”

Alternatively, it was also known and would have been obvious to a POSITA that a device serial number (Pocket Vault ID) 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, ¶[87]. Neither the claims nor the specification impose any restriction as to the individual contents of the “*plurality of codes*” or the “*other data values*.”

It was also known and would have been obvious to a POSITA that a device serial number includes different parts that respectively provide different type of information about the device. MSC-1003, ¶[88]. For instance, MSC-1020 describes various types of product serial numbers and provides several examples in which a device serial number includes different parts, such as a manufacture code and a product code. MSC-1020, 4, 17, 18. In the context of Burger, it would have been obvious to a POSITA that a device serial number would include manufacturer and product codes of the Pocket Vault. MSC-1003, ¶¶[88]. In his declaration, Dr. Traynor also provides additional examples that further corroborate that Burger’s device serial number renders obvious “*a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device.*” MSC-1003, ¶¶[86]-[88].

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]. Various 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, ¶[89]. 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, ¶[89]. 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 un-

authorized 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, ¶[89].

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, ¶[90]. This is similar to the 730 patent’s description of tamper-proof, which states that “[t]amper-proofing increases reliability of authentication because it does not allow any changes to biometric data (i.e., allows reads of stored data, but not writes to store new data or modify existing data).” MSC-1001, 4:29-43; MSC-1003, ¶[90].

While Burger explicitly discloses storing a user’s biometric data, like fingerprints, 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 [in] a storage element on the integrated device that is unable to be subsequently altered.*” MSC-1003, ¶[91]. 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 device serial number and encryption/decryption information is not tampered with and is kept secure. *Id.* Moreover, a POSITA would have understood or recognized 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 Pocket Vault ID would not typically be modified to another number (otherwise there could be multiple devices with the same number). As such, it would have been obvious to a POSITA to persistently store this data (e.g., user's biometric data, device ID number, and private key) in the tamper proof memory of the Burger system because of the sensitivity of this information and the fact that this information is typically meant to be unchangeable after it is written once. *Id.*

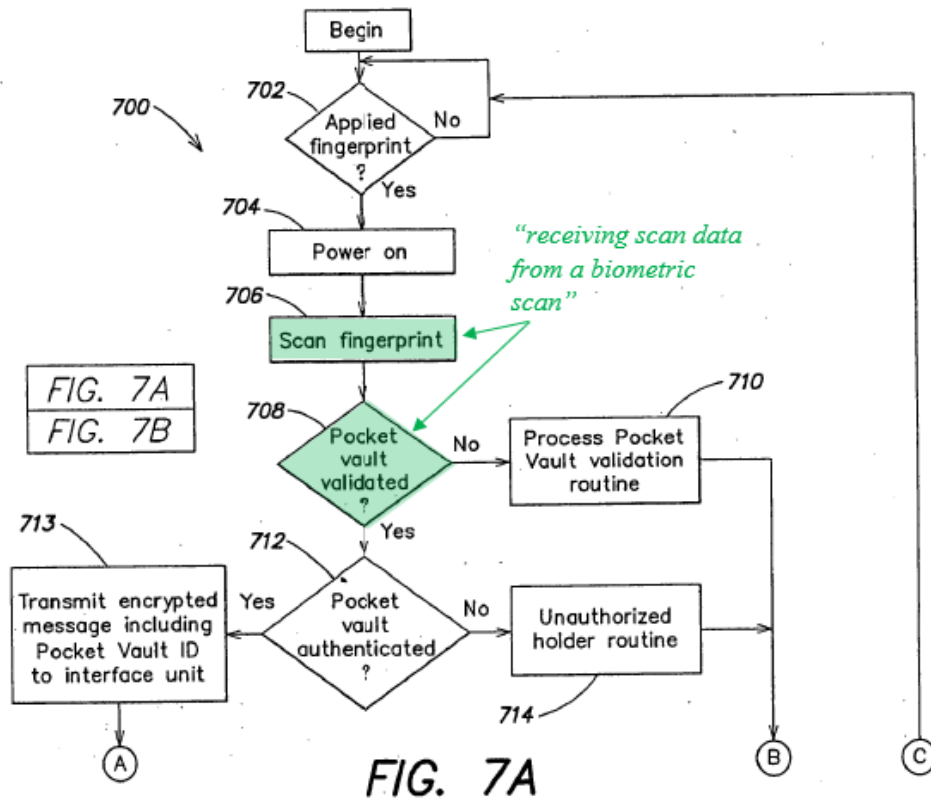
[1.2]

Burger discloses 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 is selected from a group consisting of a 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

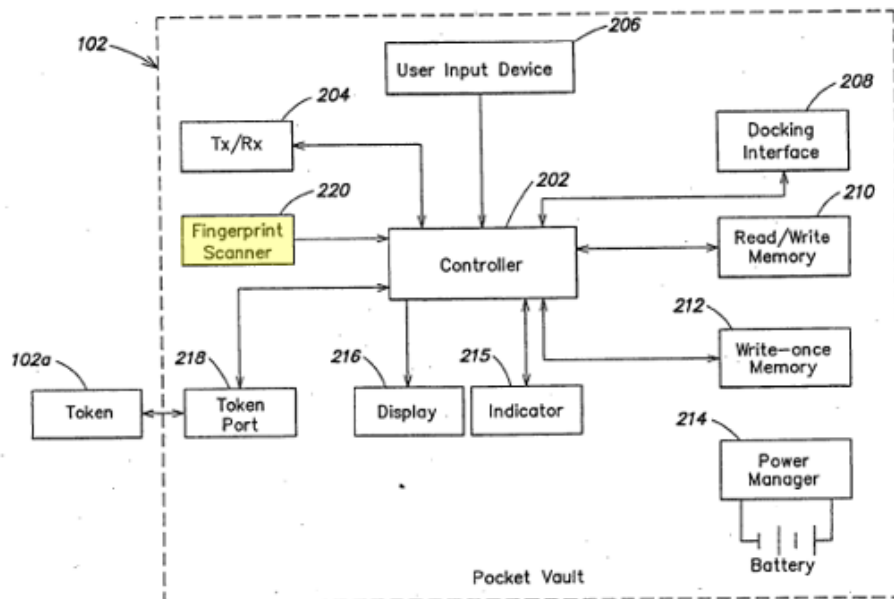
mapping of Burger to the 730 claims describes an example of fingerprint scanning, Burger's disclosure makes obvious that user authentication could include various suitable authentication techniques in place of fingerprint scanning, such as, e.g., retina scanning, voice recognition, hand geometry. MSC-1005, ¶¶[0112], [0135]; MSC-1003, ¶[92].

[1.3]

As depicted below in Burger's FIGS. 7A and 2, Burger discloses that 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 102 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 Pocket Vault 102 or the controller 202 in the Pocket Vault 102 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, ¶[93].



MSC-1005, FIG. 7A.



MSC-1005, FIG. 2.

As noted below, although the example of Burger's mapping to the 730 claims is of fingerprint scanning, Burger's disclosure makes obvious that user authentication could 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, ¶[94].

[1.4]

After receiving the scan data from the biometric scan, the user's scanned data (e.g., fingerprints) are compared to biometric data (e.g., fingerprints) 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, ¶[95].

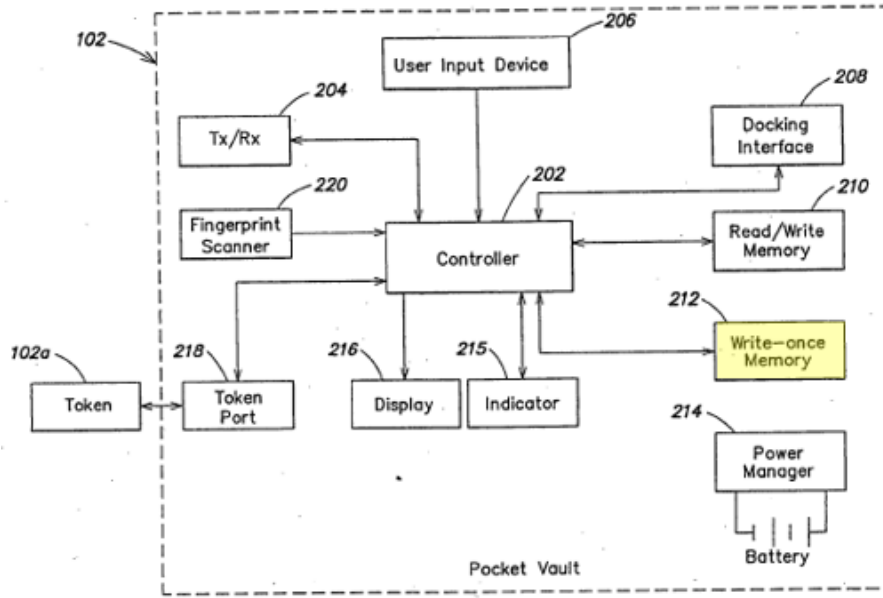
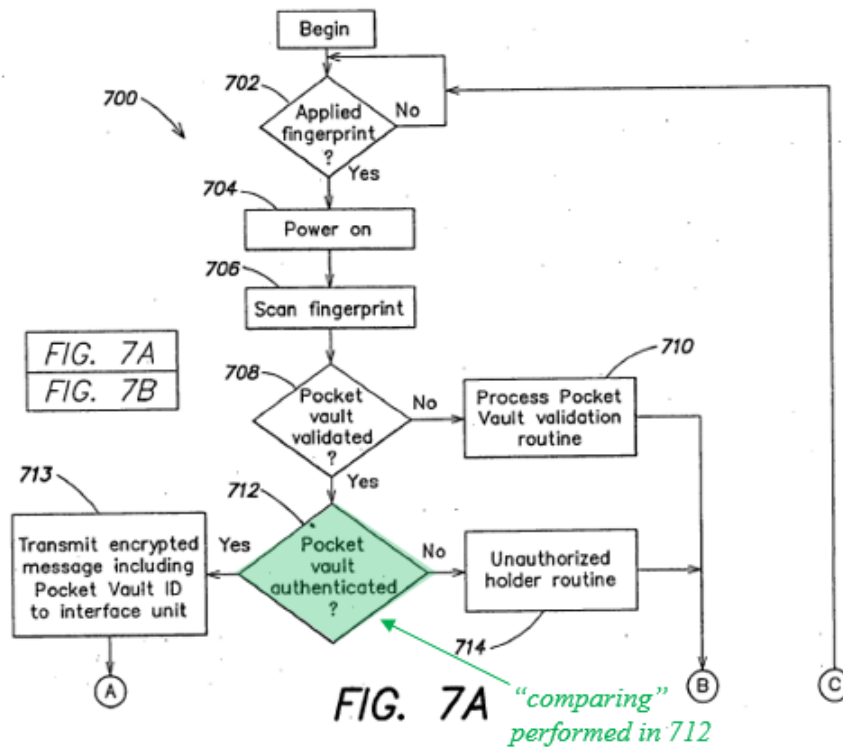


FIG. 2

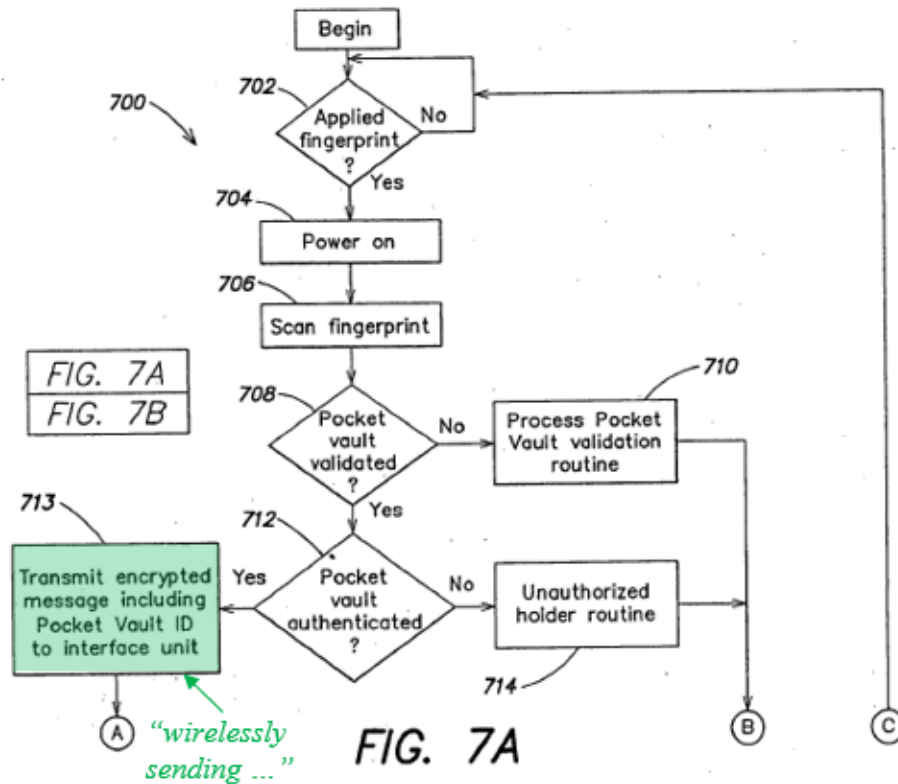
MSC-1005, FIG. 2.



MSC-1005, FIG. 7A.

[1.5]

As shown in FIG. 7A, 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]. And “*responsive to a determination that the scan data matches the biometric data*” (step 712), the Pocket Vault 102 wirelessly sends (step 713) an encrypted message including the unique Pocket Vault chip ID (“*wirelessly sending one or more codes 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, ¶[96].



MSC-1005, FIG. 7A.

In related disclosure, Burger teaches that authentication information, such as the encrypted message including the unique Pocket Vault chip ID, are transmitted to the network server 114. 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, ¶[97].

Communication between the various network elements, e.g., between the Pocket Vault 102, interface stations 104a-c, and network server 114 can be wireless, and the Pocket Vault 102 can communicate directly with the network server 114. MSC-1005, ¶¶[0099]-[0101], [0097], [0123], FIG. 1 (reproduced below); MSC-1003, ¶[98].

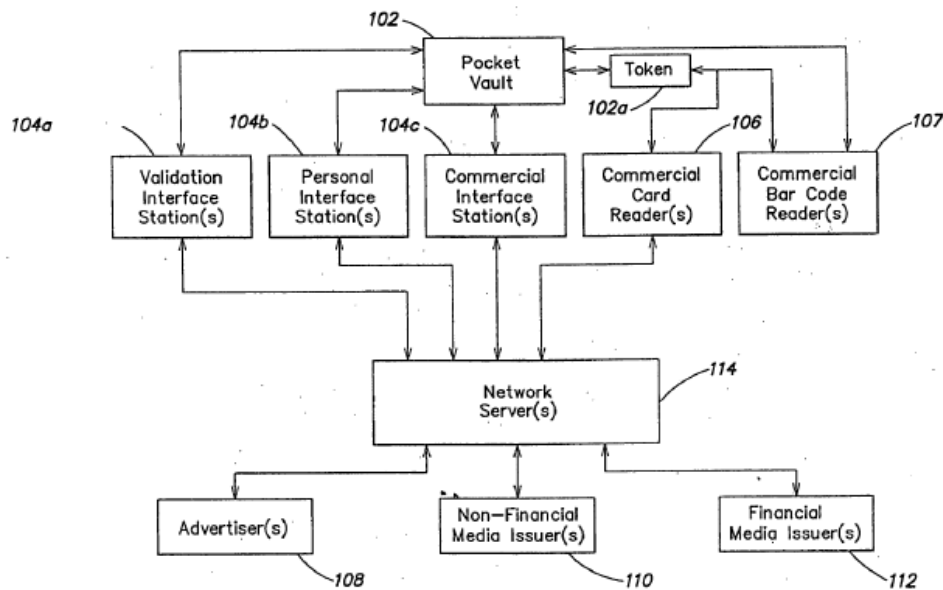


FIG. 1

MSC-1005, FIG. 1.

In Burger's system depicted above, the parties involved in a transaction (consistent with the Use Case above in §III.A.1) involve a Pocket Vault (first party) user who wants to buy from a retailer, as noted in the table below. MSC-1003, ¶[99].

Second party	Third party	Agent that is a third-party trusted authority
Retailer	Party/company operating the network server 114	The network server 114, as a whole, or, in some cases, a portion (a controller 402 and database 406) of the network server 114. The “agent” may also refer to the entity operat- ing the network server.

As Dr. Traynor explains, it would also have been obvious to a POSITA that Burger’s disclosure is not limited to the above-noted parties and transaction, and that Burger contemplates several possible transactions between different parties, as noted in the table below. MSC-1003, ¶[100]. In each example below, the first party is the Pocket Vault holder (user).

Transaction	Second party	Third party	Agent that is a 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/company operating the network server 114	The network server 114, as a whole, or, in some cases, a portion (a controller 402 and database 406) of the network server 114. The agent may also refer to the entity operating the network server.
Obtaining authorization to enter a secure building or facility	Non-financial media issuer 110 (e.g., hotel card key issuer, library, building management for company)		
Obtaining advertisement content	Advertiser(s) 108		

or related information			
------------------------	--	--	--

MSC-1005, ¶¶[94], [98], [103]-[104], [110]-[111], [117], [128]-[129], [155]-[158], [237]-[240], [255], [324]-[328], [0511]-[513], [679]; MSC-1003, ¶[101].

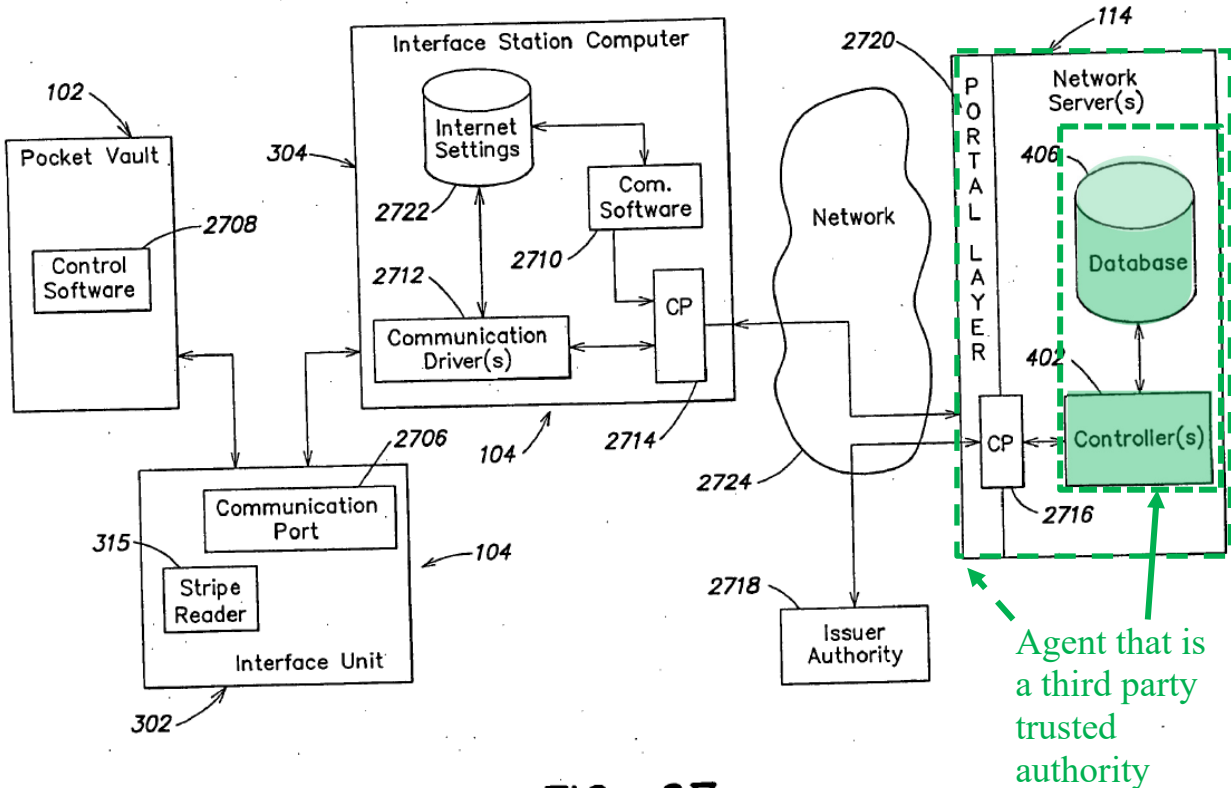
“[A]gent that is a Third-Party Trusted Authority”

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, Burger discloses “*an agent that is a third-party trusted authority*” in several different ways, as explained below. MSC-1003, ¶[102].

The network server 114 includes a controller 402 and database 406. MSC-1005, ¶¶[146], [0531]-[0543], FIG. 27. The database 406 stores 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 102 a, identified by chip ID and linked to the holder list (“*possessing a list of device ID codes uniquely identifying legitimate integrated devices*”). 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].

Accordingly, it would have been obvious to a POSITA that the controller 402 and database 406 of the network server 114 (or the network server 114 as a whole) can operate as “***an agent that is a third-party trusted authority***” under several different example implementations. MSC-1003, ¶¶[103]-[104]. For example, the controller 402 and database 406 of the network server 114 may operate as “***an agent that is a third-party trusted authority***” in a transaction between the Pocket Vault holder/user and a retailer, as noted above in the Use Case. MSC-1005, FIG. 19, ¶[0474]; FIGS. 24, 25; ¶¶[0511]-[513], [320], [158], [95]. It would also have been obvious to a POSITA that the company or entity owning the network server 114 can be the “***agent***” because the network server 114 or components thereof effectively operate on behalf of the company. MSC-1003, ¶[104].



MSC-1005, FIG. 27.

In another example, the controller 402 and database 406 of the network server 114 (or the network server 114 as a whole) may be “*an agent that is a third-party trusted authority*” when there is a transaction between a Pocket Vault holder/user and an entity such as the advertiser 108. MSC-1003, ¶¶[110], [105]. For instance, an advertiser may send information to the network server 114, which is then forwarded to a Pocket Vault 102 for display upon successful authentication of the user and Pocket Vault ID. MSC-1005, ¶¶[110], [0117], [0146], [237], [541], FIG. 1 (reproduced below).

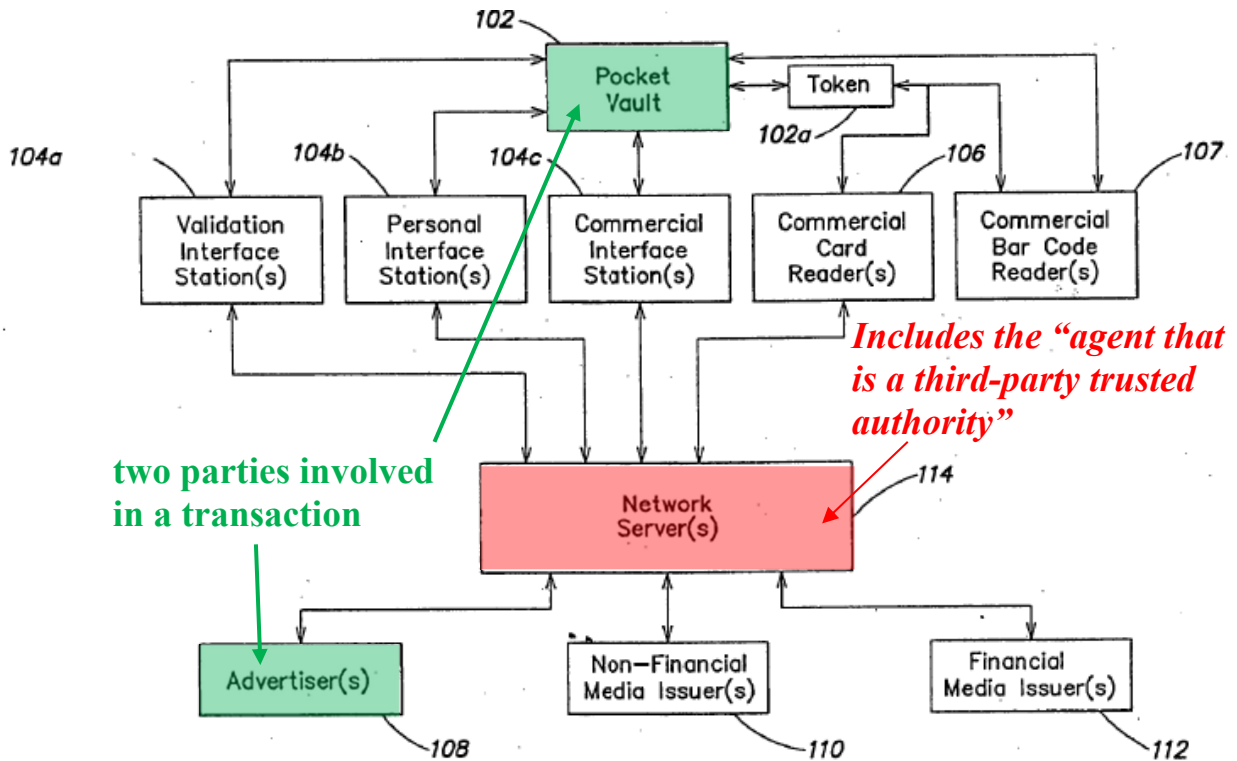
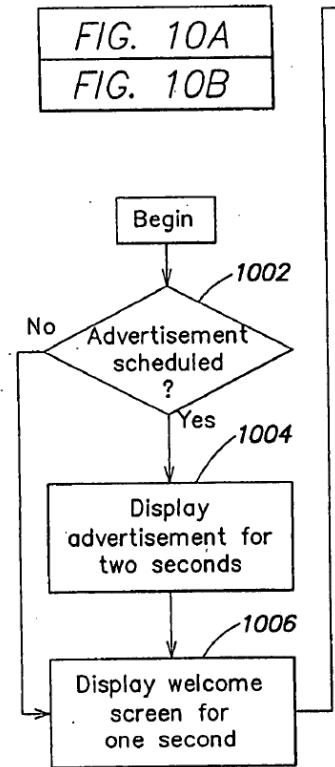


FIG. 1

MSC-1005, FIG. 1.

In some embodiments, after the unique Pocket Vault chip ID is transmitted and a token 102a (e.g., Chameleon Card) is determined to be on-board the Pocket Vault 102, advertisements sent from an advertiser 108 to the network server 104 can be provided to the Pocket Vault 102 for display. MSC-1005, ¶¶[236]-[238], FIG. 10 (reproduced below); MSC-1003, ¶[106].



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 above Use Case and consistent with Burger’s disclosure, the controller 402 and database 406 of the network server 114 (or the network server 114 as a whole) serve as “*an agent that is a third-party 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, ¶[107]. 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-1005, ¶¶[110], [0117], [0147], [0038]; 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 102 and the advertiser 108, the controller 402 and database 406 of the network server 114 (or the network server 114 as a whole) are “*an agent that is a third-party trusted authority*,” as they have a secure and trusted connection with at least the Pocket Vault 102 and operate as an intermediary device that facilitates information exchange between the advertiser 108 and the Pocket Vault 102. MSC-1003, ¶¶[107]-[108].

[1.6]

As described in the example use case above in §III.A.1, after the controller 402 and database 406 of the network server 114 authenticate the Pocket Vault ID (“*responsive to authentication of the one or more codes and the other data values by the agent*”), the user is granted access to the Pocket Vault 102 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 102 or token 102a coupled to the Pocket Vault 102 displays a credit card information to be used by a retailer. MSC-1005, ¶¶[0320], [0158], [0095]. Burger teaches that the token 102a coupled to Pocket Vault 102 “may be used by the Pocket Vault holder to engage in a transaction.” MSC-1005, ¶[103]. A display in the token 102a can “be configured to display information that is typically embossed or printed on such cards.” MSC-1005, ¶¶[0155]-[0158]; MSC-1003, ¶[109].

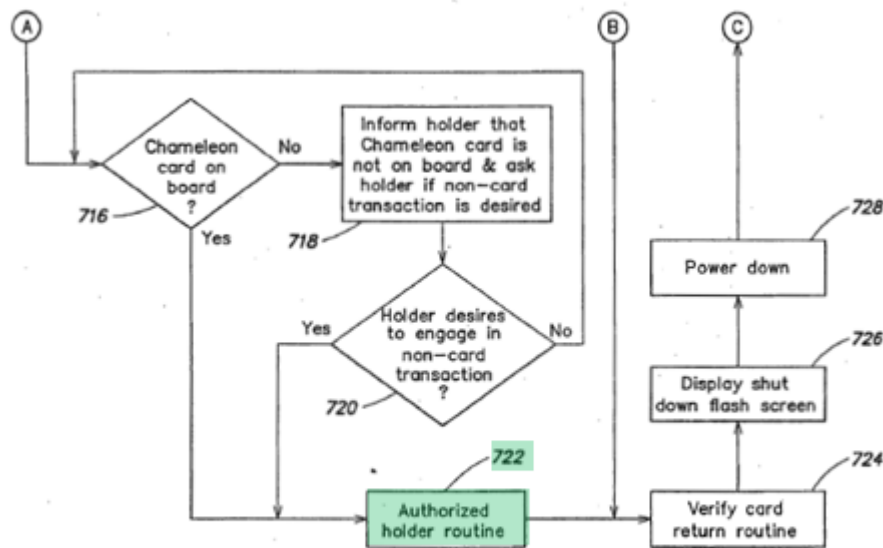
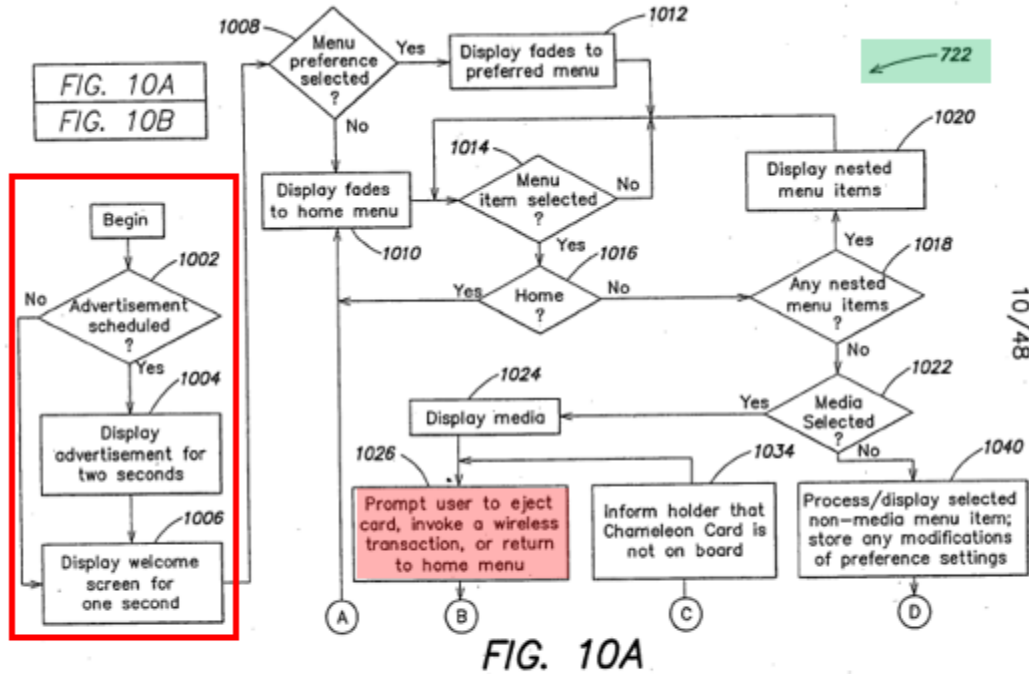


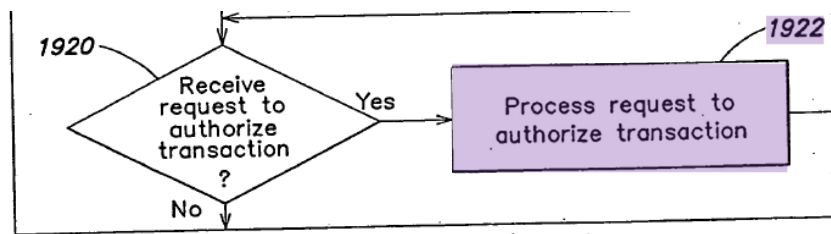
FIG. 7B

MSC-1005, FIG. 7B.



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.



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.

It would have been obvious that the Pocket Vault 102 would have received

an access message from the controller 402 of the network server 114 (“***receiving an access message from the agent***”) to “***allow[] the user access to an application***” after the controller 402 and database 406 of the network server 114 authenticated the Pocket Vault ID that was sent to the network server 114 (“***responsive to authentication of the one or more codes and the other data values by the agent***”) 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, ¶[110].

For the mapping of “***application***,” please see the remarks below for feature [1.7]. MSC-1003, ¶[111].

As noted above, the controller 402 of the network server 114 also transmits an encrypted approval message in operation 2408 after the Pocket Vault 102 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***”) is received by the Pocket Vault 102 in response to the Pocket Vault ID being successfully authenticated by the network server 114, Burger also discloses “***responsive to authentication of the one or more codes and the other data values by the agent, receiving an access message from the agent allowing the user access to an application***” in this additional way. 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 102 and the network server 114, and thus, it would have been obvious that the encrypted approval message could be sent to the Pocket Vault 102 in addition to or instead of being sent to the interface stations. MSC-1005, ¶[101]; MSC-1003, ¶[112]. This may particularly be the case when all that is desired is for a credit or debit card to be displayed by the Pocket Vault 102 or token 102a coupled to the Pocket Vault 102. *Id.*

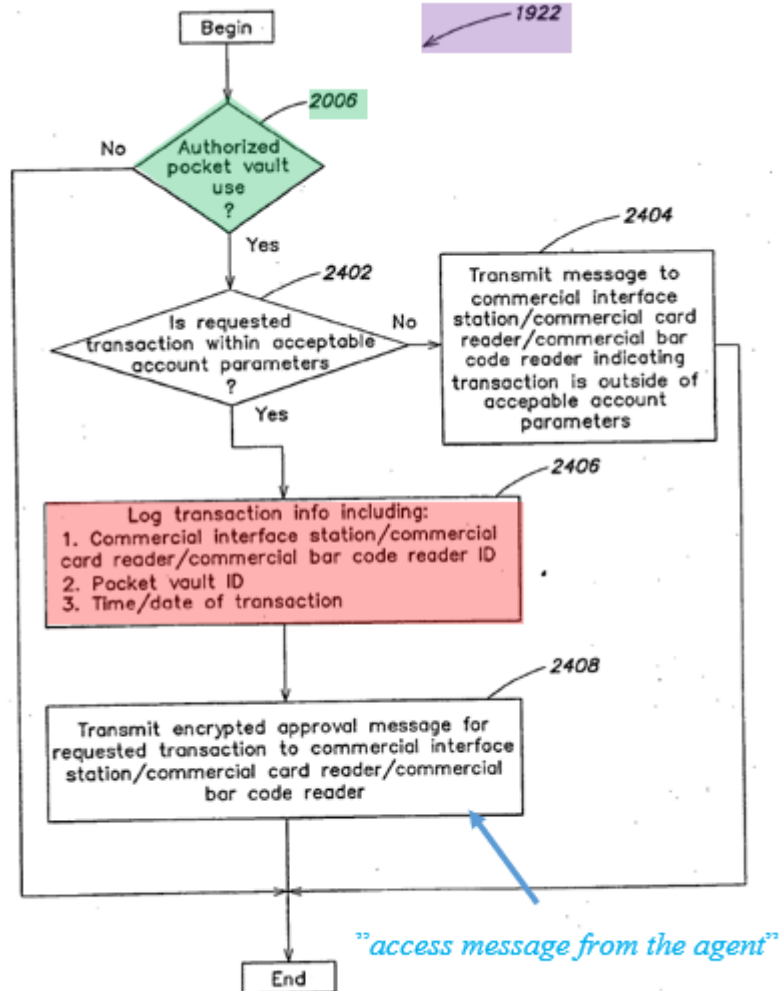
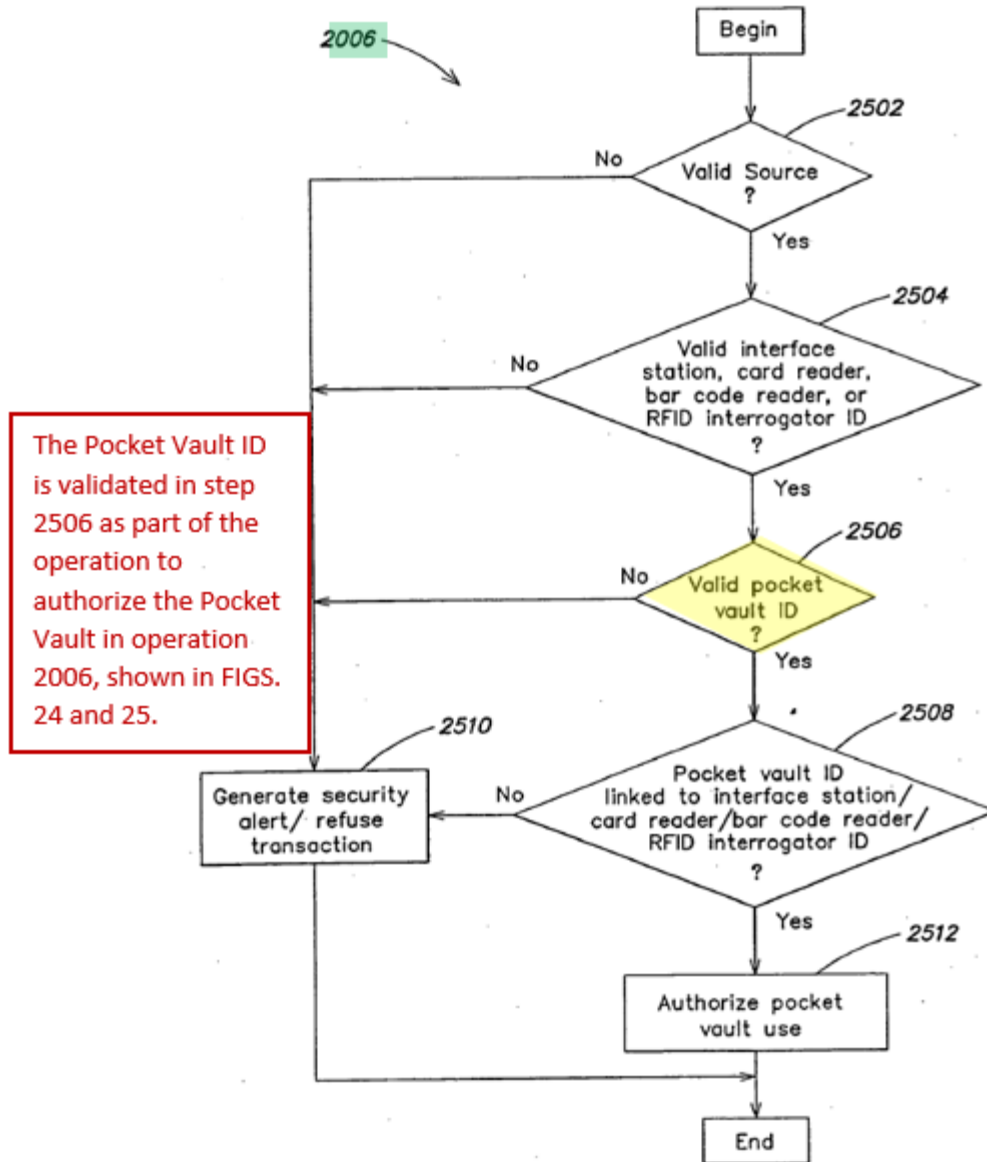


FIG. 24

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 114 and a welcome screen are displayed in response to authentication of the Pocket Vault. MSC-1005, ¶¶[0194], [0236]-[237], [110], FIG. 7B, 10A (reproduced below). Thereafter, the user can access *an application*, such as a file

or software for an advertisement, or a website (link) thereto. 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, the Pocket Vault 102 would have re-

ceived an access message from the network server 114 (*“receiving an access mes-*

sage from the agent”) to *“allow[] the user access to an application”* after and

conditioned on the network server 114 successfully authenticating the Pocket Vault

ID that was sent to the network server 114 (*“responsive to authentication of the*

one or more codes and the other data values by the agent”). MSC-1003, ¶[113].

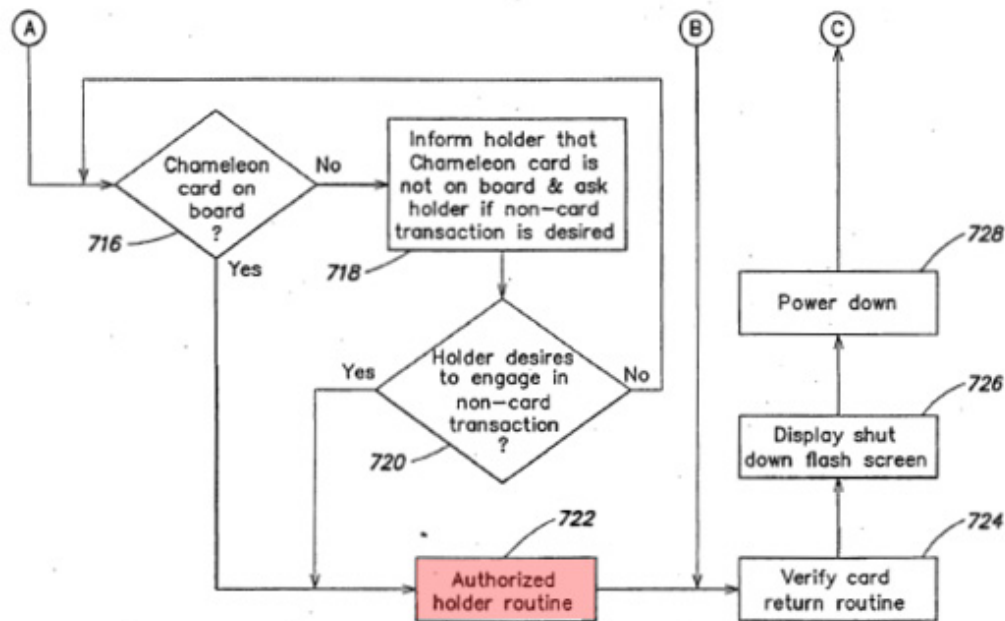
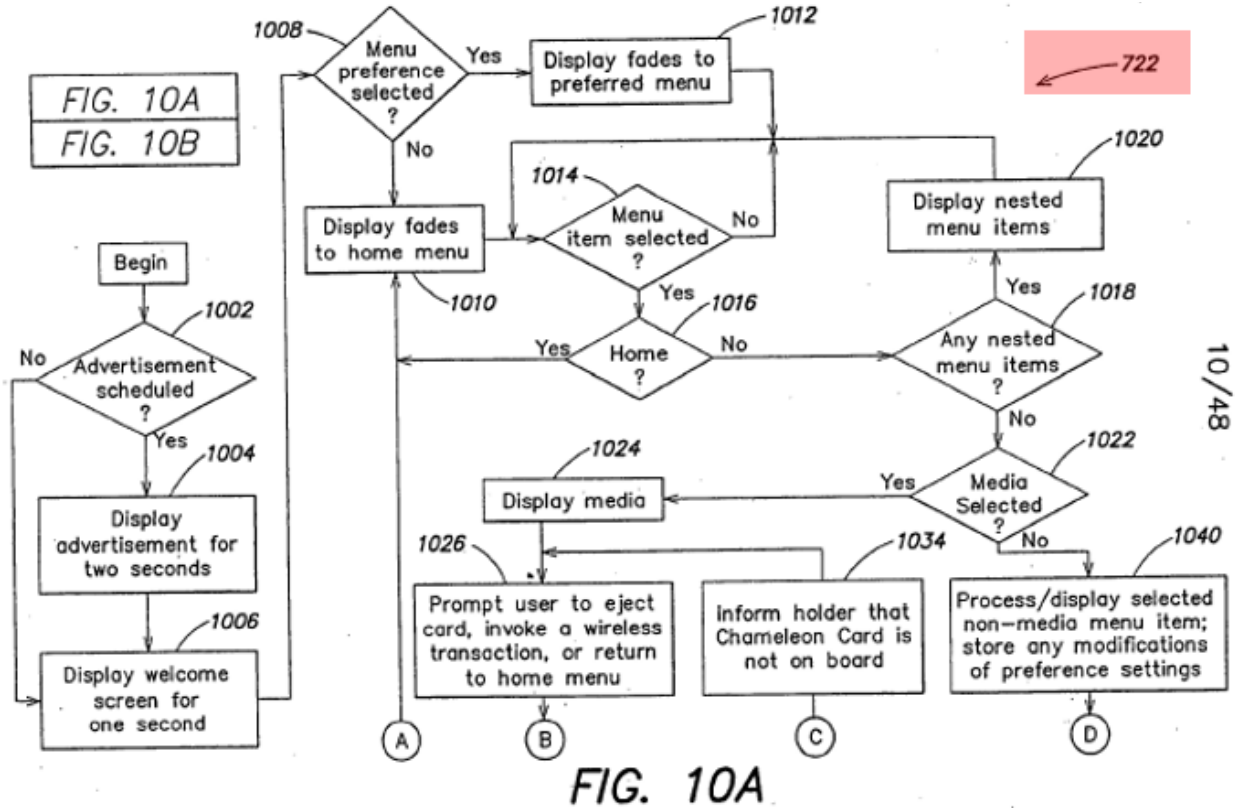
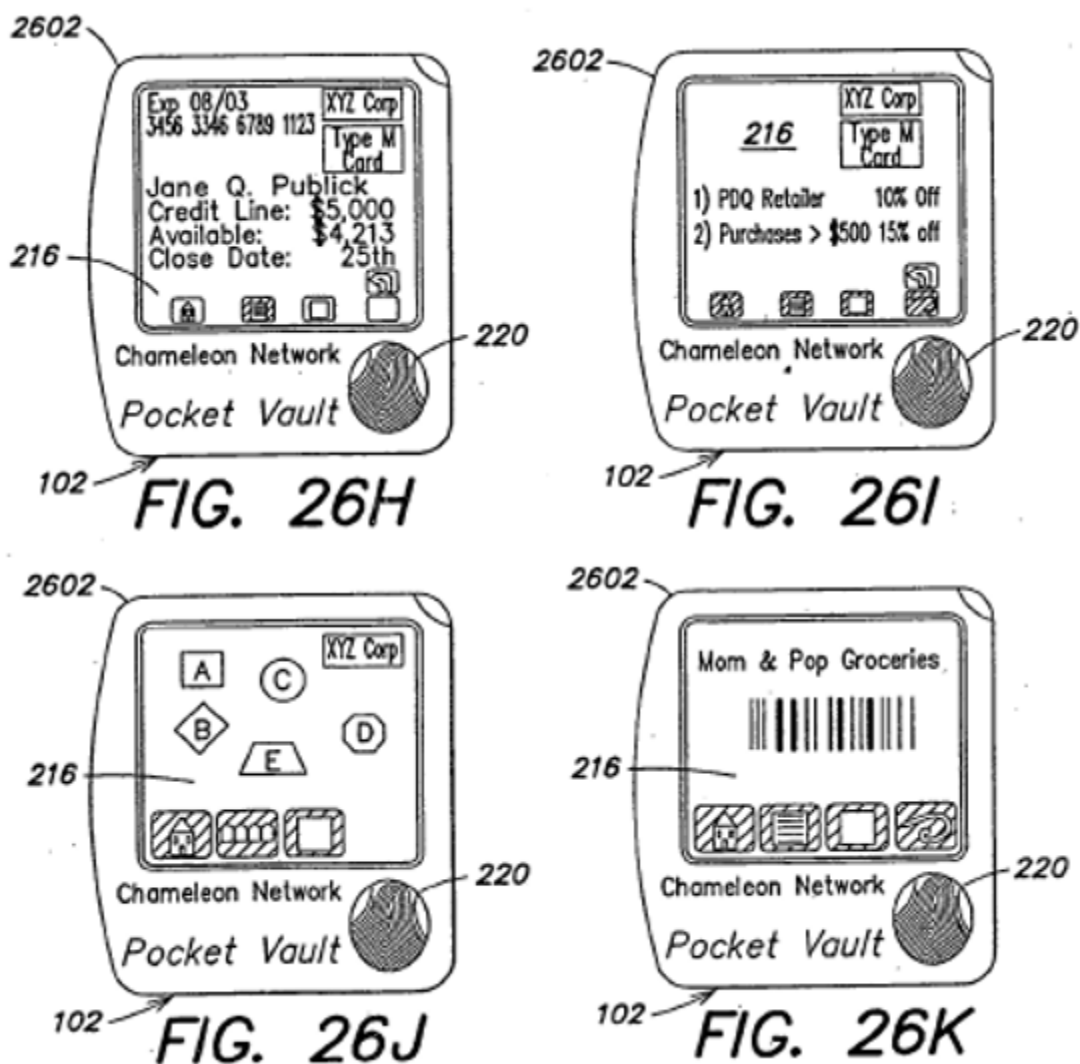


FIG. 7B

MSC-1005, FIG. 7B.



MSC-1005, FIG. 10A.



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

[1.7]

As explained in [1.6] and noted in the table below, Burger's Pocket Vault can be used in different scenarios and implementations, each of which demonstrate that Burger renders obvious [1.6] and [1.7]. See citations in [1.6] (MSC-1005, step 722 in FIG. 7B, step 1026 in FIG. 10A; steps 1920, 1922 in FIG. 19; ¶¶[320],

[189], [95]-[96], [110], [125], [236]-[238], [155]-[158], [517]-[527], [182]-[186],
[101], [0242], FIGS. 26H-26K, 14), ¶[250]; MSC-1003, ¶[114].

“application”	Implementation in Burger (after the Pocket Vault 102 has been authenticated by the network server 114)
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 website (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. ¶¶ [679]-[680]; <i>see generally</i> [94] [102] [128] [129] (re “building security” or “building access cards”)

Thus, Burger's "*application*" "*is selected from a group consisting of*" "*a computer software,*" "*a file,*" "*keyless lock,*" or "*web site.*" A POSITA would have understood that a user would only be allowed access to the computer software, file, keyless lock, or web site ("*application*") for displaying the above-noted content after the network server 114 sends a message back to the Pocket Vault 102 indicating that the Pocket Vault 102 has been authenticated by the network server 114. MSC-1003, ¶¶[114]-[115].

[2]

As noted above in [1.5], Burger discloses that an encrypted message including the Pocket Vault ID ("*the one or more codes and the other data values*") is wirelessly transmitted to the controller 402 and/or database 406 of the network server 114 ("*agent*"). MSC-1005, ¶¶[0186], [114], [122], [146], FIG. 7A; MSC-1003, ¶[116].

The transmission can be made over any one of various suitable networks, such as network 2724 in FIG. 27. For example, as disclosed in Burger's ¶[0099], "[a]ny of a number of techniques may be used to interconnect the various elements of the network system 100, and *the invention is not limited to any particular networking technique*. In one illustrative embodiment, for example, *the network*

server 114 is coupled to the other elements in the network system 100 via the Internet or similar packet-switched communication system. Alternatively, dedicated or selectively established (e.g., using a dial-up modem) communication channels or time slots thereof may be employed between the respective devices. The connections between most of the network devices may be either hardwired (including fiber optic connections) or wireless (e.g., infrared (IR) or radio frequency (RF) links)." Accordingly, it would have been obvious to a POSITA that Burger teaches ***"wherein the one or more codes and the other data values are transmitted to the agent over a network."*** MSC-1003, ¶[117].

[4]

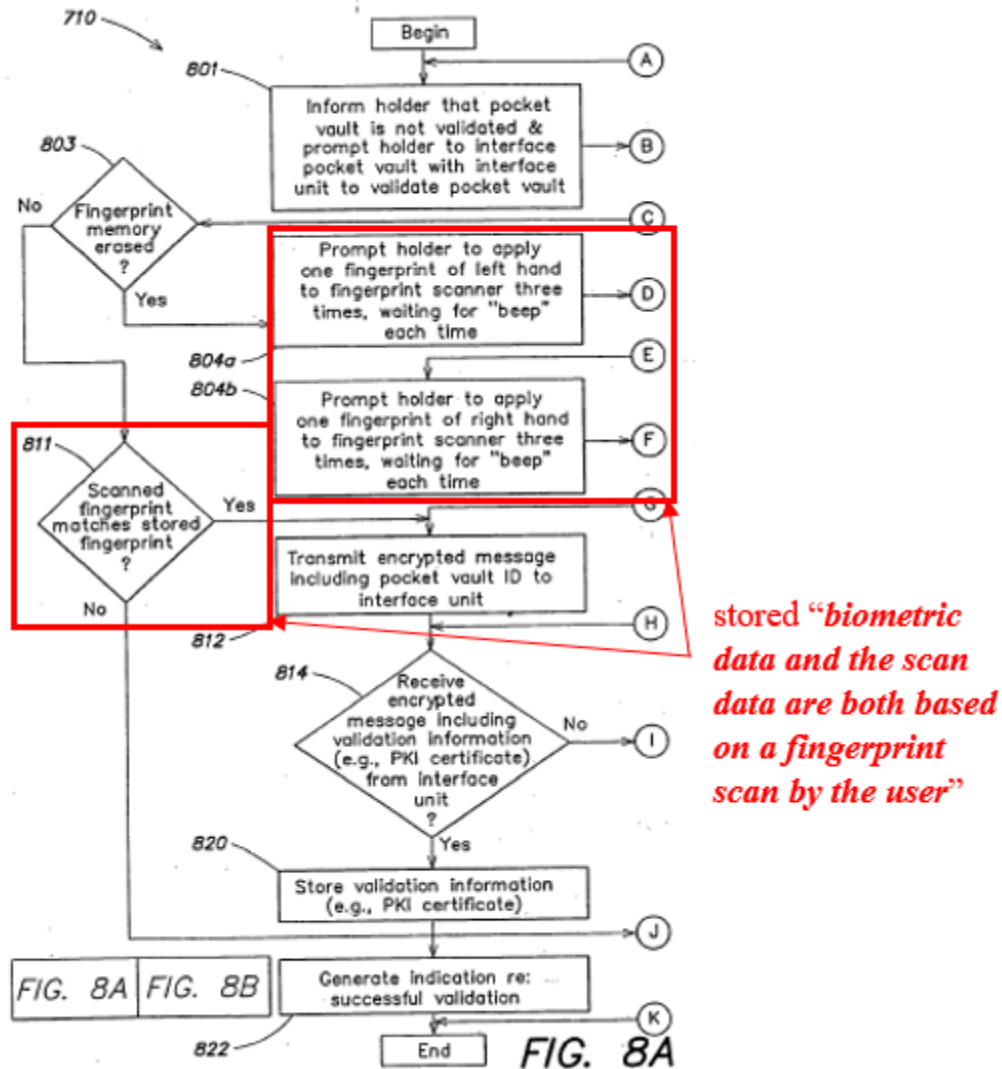
As shown above in FIG. 7A and noted above with respect to [1.3] and [1.4], the Pocket Vault ID is transmitted after the Pocket Vault holder's scanned biometric data matches stored biometric data. MSC-1005, ¶¶[135], [178]-[0184]; MSC-1003, ¶[118].

Burger also discloses, in several embodiments, that the chip ID or Pocket Vault ID is released from the Pocket Vault 102 only after the fingerprint scanner 220 (discussed below) has successfully authenticated the identity of the holder. MSC-1005, ¶[0122], [0349], [0358]. In some cases, "the 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 114 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, ¶[119]. Thus, the inclusion of "*the one or more codes and the other data values*" in a message to the network server 114 would have in and of itself indicated "*that the biometric verification was successful*." MSC-1003, ¶[119].

[5]

As explained above in [1.3], [1.4], and [4], in some implementations, Burger discloses comparing scanned fingerprint data ("*scan data*") of a user with stored fingerprint data ("*biometric data*") previously stored. *See also* MSC-1005, FIGS. 8A (reproduced below), 8B (step 808b), ¶¶[0199]-[0209]. Thus, "*the biometric data and the scan data are both based on a fingerprint scan by the user*." MSC-1003, ¶[120].



MSC-1005, FIG. 8A.

[6]

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*" is established to facilitate the registration of the Pocket Vault 102 (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 *“establishing a secure communication channel prior to sending the one or more codes and the other data values for authentication.”* MSC-1003, ¶[121].

[7.1]

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 114. 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 114 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, ¶[122].

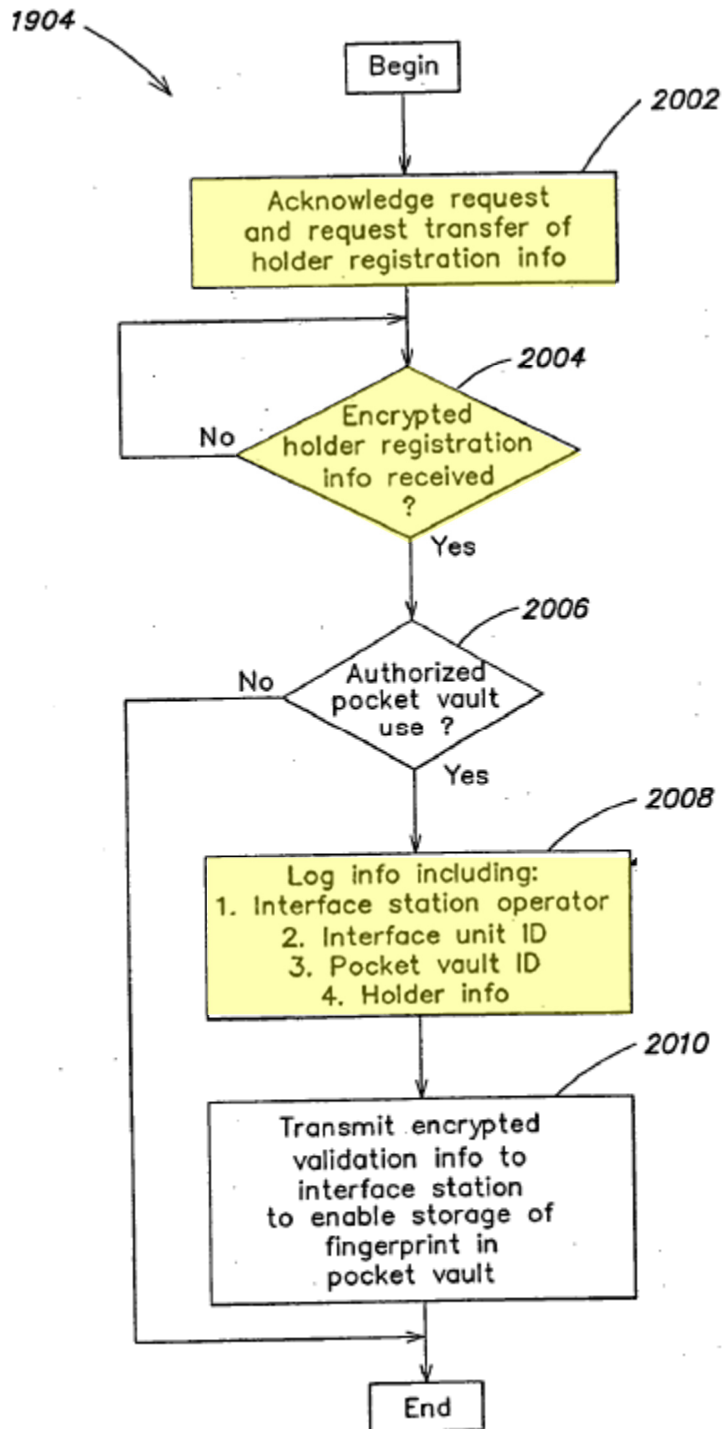


FIG. 20

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 114 would have communicated directly with the Pocket Vault 102 to obtain the registration information for a new Pocket Vault holder. MSC-1003, ¶[123].

In this example of registering a new Pocket Vault holder, no request for biometric verification is made. However, the Pocket Vault 102 still receives a request (“*a request for the one or more codes and the other 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 the other data values without a request for biometric verification.*”² MSC-1003, ¶[124].

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

[7.2]

As explained above in [7.1], in response to receiving the request for registration information (“*responsive to receiving the request*”), the Pocket Vault 102 sends all the Pocket Vault registration information, including the Pocket Vault ID, to the network server 114 to be logged into the database 406 of the network server 114 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]. Accordingly, Burger also renders obvious “*responsive to receiving the request for the one or more codes and the other data values without a request for biometric verification, sending the one or more codes and the other data values without requesting the scan data.*” MSC-1003, ¶[125].

[8.pre]

Burger’s Pocket Vault 102 is an “*integrated device.*” See [1.pre]; MSC-1005, ¶¶[0002], [0010], [0127]-[0128], [0118], [0134], [0094]-[0095]; MSC-1003, ¶[126].

[8.1]

[8.1]’s “memory” corresponds to [1.1]’s “storage element,” which is rendered obvious for the reasons noted above in [1.1]. See [1.1]; MSC-1005, ¶¶[0112], [0114], [0118], [0122], [0127], [0129], [0154], [0182], [0551]-[0552],

FIG. 2; MSC-1003, ¶[127].

[8.2]

See [1.2]; MSC-1005, ¶¶[0112], [0135]; MSC-1003, ¶[128].

[8.3]

See [1.3]-[1.5]; MSC-1005, ¶¶[0112]-[0114], [0122], [0135], [0146], [0178]-[0184], [0186], FIGS. 7A, 2; MSC-1003, ¶[129].

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 “*verification unit*” that is “*in communication with the memory*” 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 “*in communication with the memory.*” MSC-1003, ¶[130]. Moreover, the controller 202 is coupled to the memory and transceiver 204 to send and receive any data from the Pocket Vault 102. *Id.*

[1.3]-[1.5] explain how Burger renders obvious “receives scan data ...” and the remaining features in [8.3]. MSC-1003, ¶[131].

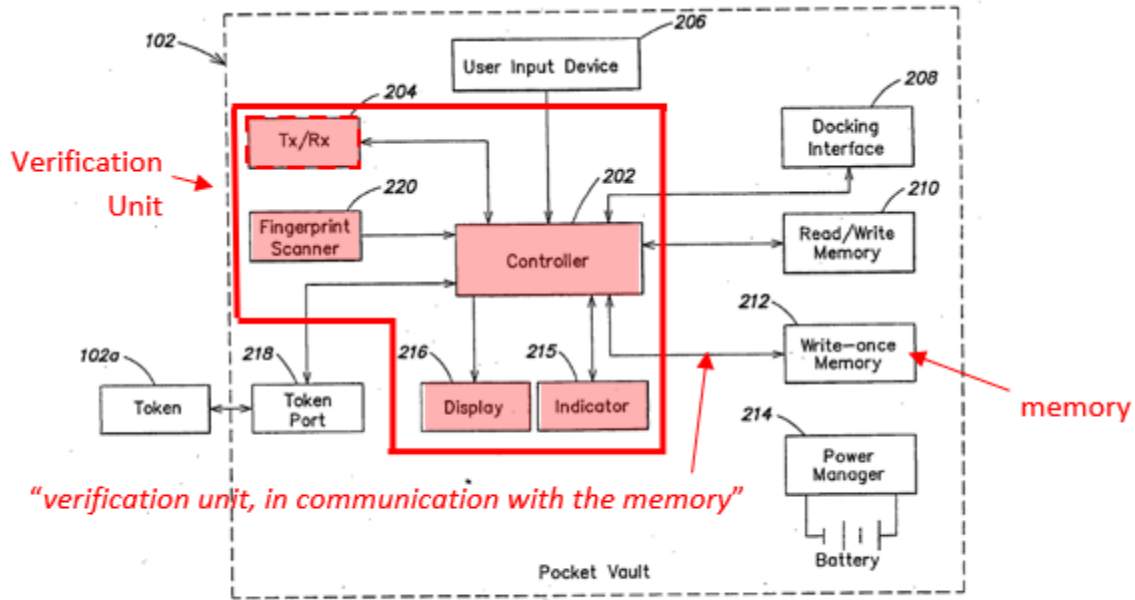


FIG. 2

MSC-1005, FIG. 2.

[8.4]

See [1.6]; MSC-1005, FIGS. 7A, 7B, 10A, 19, 26H-26K; ¶¶[0320], [0189], [0095]-[0096], [0101], [0125], [0236]-[0238], [0155]-[0158], [0103], [517]-[527], [182]-[186], [0194]; MSC-1003, ¶[132].

The “one or more antennas” of the transceiver 204 (alternatively the transceiver 204 itself) are the “*radio frequency communicator*” as the antennas perform the transmitting and receiving of data using RF signals for the Pocket Vault 102. MSC-1005, ¶[0123]; MSC-1003, ¶[133].

Note that claim 8 does not require that the “*radio frequency communicator*” be separate from the “*verification unit*,” thus mapping the transceiver 204 to the

“radio frequency communicator” within the **“verification unit”** is consistent with the claims. “[T]he 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)). To the extent, the **“radio frequency communicator”** is understood to not be part of the **“verification unit,”** the antennas of the transceiver correspond to the **“radio frequency communicator”** 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 **“verification unit.”** MSC-1003, ¶¶[134]-[135].

[8.5]

See [1.7], [8.4]; MSC-1005, FIGS. 7A, 7B, 10A, 19, 26H-26K; ¶¶[0320], [0189], [0095]-[0096], [0101], [0125], [0236]-[0238], [0155]-[0158], [0103], [517]-[527], [182]-[186], [0194], [0250]; MSC-1003, ¶[136].

[9]

See [2]; MSC-1005, ¶¶[0099], [0186], [114], [122], [146], FIG. 7A; MSC-1003, ¶[137].

[11]³

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

³ There is a typo or an antecedent basis issue in this claim because claim 8 does not recite a “*verifier*.” The “*verifier*” is likely referring to the “*verification unit*” of claim 8. For purposes of this IPR, Petitioner treats the “*verifier*” to be the same as the “*verification unit*.”

Vault 102 obtaining a fingerprint scan. MSC-1003, ¶[138]. 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 102 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 requested. MSC-1005, ¶[0204]. Accordingly and because the verification unit includes the indicator 215, it would have been obvious to a POSITA that Burger renders obvious *“the verifier compris[ing]: an LED to be activated for requesting the biometric scan.”* MSC-1003, ¶[138].

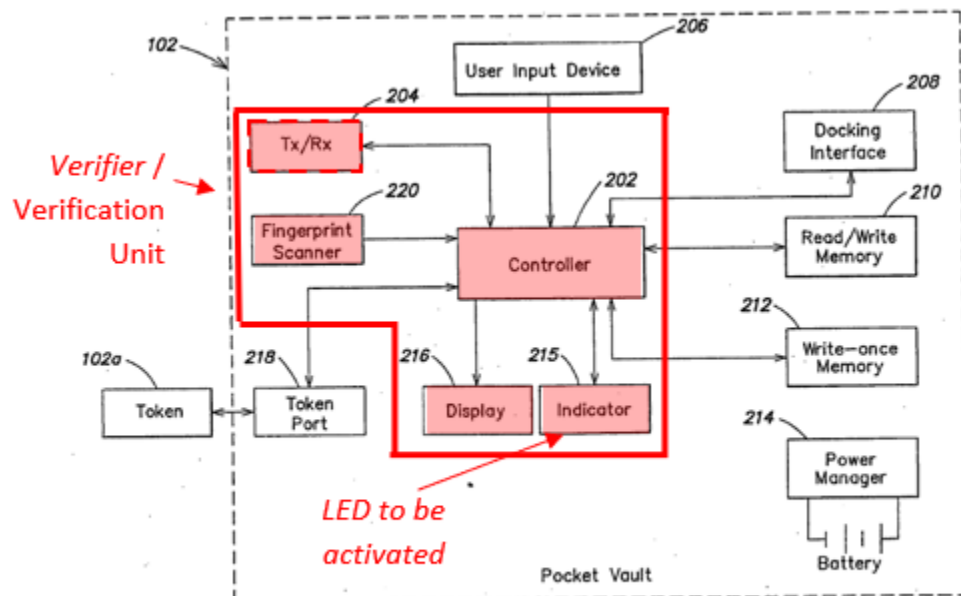


FIG. 2

MSC-1005, FIG. 2.

[12.pre]

For reasons similar to those noted above with respect to claim 1 and in particular [1.pre], Burger renders obvious a “**method for authenticating a verified user using a computer processor configured to execute method steps**,” as recited in [12.pre]. MSC-1005, ¶¶[0002], [0010], [0127]-[0128], [0118], [0134], [0094]-[0095]. For example, Burger discloses a method of authenticating a verified Pocket Vault holder (“**user**”) using a controller 402 (“**computer processor**”) of the network server 114. MSC-1005, FIG. 4, ¶¶[0144]-[0145], [0540]. The network server 114 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.” MSC-1005, ¶[145]. Although Burger does not explicitly describe the controller 402 as a computer processor, a POSITA would have understood that controller 402 is a computer processor that, as described in Burger, is configured to execute Instructions to Implement operations configured to be performed by the network sever 114, just like a computer processor would. MSC-1005, FIG. 4, ¶¶[0144]-[0145]; MSC-1003, ¶[139]. As noted below, the method including features [12.1]-[12.5] are rendered obvious by Burger. *Id.*

[12.1]

As explained above in [1.5], the network server 114 “*receiv[es] one or more codes from a plurality of codes and other data values including a device ID code*” from the Pocket Vault 102. MSC-1005, ¶¶[0112]-[0114], [0122], [0135], [0146], [0178]-[0184], [0186], FIGS. 7A, 2; MSC-1003, ¶[140].

[12.2]

See [1.5], [1.1]; MSC-1005, ¶¶[0112]-[0114], [0118], [0122], [0127], [0129], [0135], [0146], [0154], [0178]-[0184], [0186], [0551]-[0552], FIGS. 7A, 2; MSC-1003, ¶[141].

[12.3]

See [1.5], [1.6]. As explained above in §III.A.1, [1.5], and [1.6], Burger’s network server 114 includes a database 406, controller(s) 402, local memory 404, and a communications protocol layer 2716. FIGS. 4, 27. Burger’s database 406 stores “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 102 a, identified by chip ID and linked to the holder list.” MSC-1005, ¶[146]. The controller 402 executes instructions stored in memory 404 “to implement the routines described ... in connection with FIGS. 19-25 and/or FIGS. 30-39.” MSC-1005, ¶[145]; MSC-1003, ¶[142].

Turning to FIGS. 19, 24, and 25, as explained above in [1.5], it would have been obvious to a POSITA that the controller 402 and database 406 (collectively “*the agent*”) authenticate the Pocket Vault ID or authorize the Pocket Vault 102 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, ¶[143]. To perform these steps, it would have been obvious to a POSITA that the stored instructions include instructions to “*request[] authentication of the one or more codes and the other data values by the agent*” [controller 402 and database 406], as recited in [12.3]. *Id.* And because the Pocket Vault ID is part of “*the one or more codes and the other data values are legitimate,*” a POSITA would have understood that by authenticating the Pocket Vault ID, the network server 114 would determine “*whether the one or more codes and the other data values are legitimate.*” *Id.*

[12.4]

See [1.6]; MSC-1003, ¶[144].

[12.5]

See [1.6], [1.7]; MSC-1003, ¶[145].

[14]

Claims 6 and 14 recite similar features. However, claim 6 recites that the secure communications channel is established “prior to sending the one or more codes and the other data values for authentication.” *See* [6]. Claim 14 does not recite the “prior to” limitation but recites that the secure communications channel established “with a biometric key, wherein the one or more codes and the other data values associated with the biometrically verified user is received from the biometric key.” As explained above in [1.5] and [6], Burger’s network server 114 establishes a secure connection with the Pocket Vault 102 (“*biometric key*”) and receives the Pocket Vault ID from the Pocket Vault 102 (“*wherein the one or more codes and the other data values associated with the biometrically verified user is received from the biometric key.*”) *See* [6], [1.5]. MSC-1005, ¶¶[0097]-[0101], [0186], [113]-[114], [122]-[123], [146], FIGS. 1, FIG. 7A; MSC-1003, ¶[146].

[15.pre]

See [1.pre]; MSC-1005, ¶¶[0002], [0010], [0127]-[0128], [0118], [0134], [0094]-[0095]; MSC-1003, ¶[147].

[15.1]

See [1.1], [1.3]-[1.5]; MSC-1005, ¶¶[0112]-[0114], [0118], [0122], [0127], [0129], [0135], [0146], [0154], [0178]-[0184], [0186], [0551]-[0552], FIGS. 7A, 2;

MSC-1003, ¶[148].

[15.2]

See [1.2]; MSC-1005, ¶¶[0112], [0135]; MSC-1003, ¶[149].

[15.3]

As explained above and shown in Burger’s annotated FIG. 27 below, Burger discloses a communication protocol layer 2716 (“***authentication unit***”) “which provides low-level communication functions to server communications software.” MSC-1005, ¶[540]. As is obvious from Burger’s FIG. 27 below, communications (e.g., device ID codes) between the network server 114’s controller(s) 402 and database 406 (collectively “***agent***”) and external elements (e.g., network 2724, Pocket Vault 102, or issuer authority 2718) all pass through the communication protocol layer 2716. MSC-1003, ¶[150].

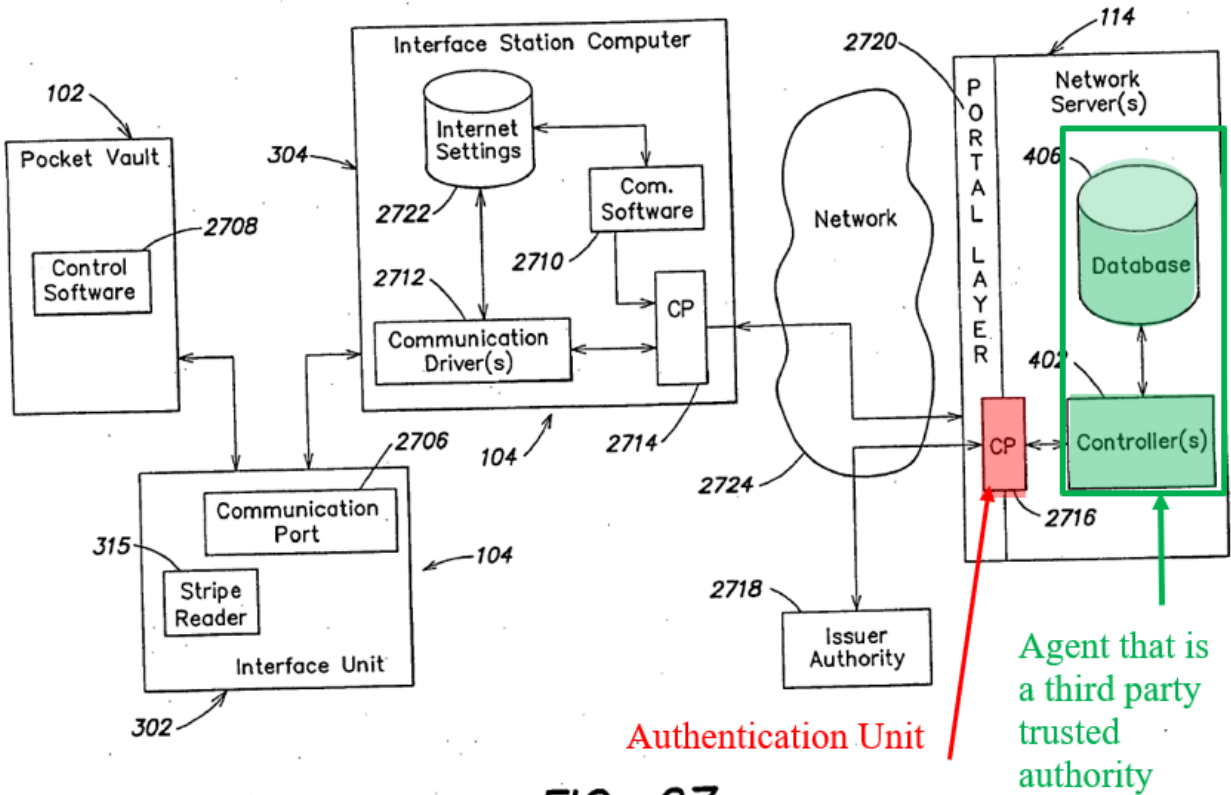


FIG. 27

MSC-1005, FIG. 27.

Accordingly, it would have been obvious to a POSITA that Burger renders obvious *“an authentication unit⁴ [that] receives the plurality of codes and the*

⁴ Notably, the “authentication unit” recited in claim 15 is not recited as directly performing any type of “authentication.” Rather, the extent of the “authentication” function ascribed to the recited “authentication unit” by the claim is merely that it receives and sends the plurality of codes and other data values to a third party “for authentication,” i.e., the recited “agent” or “third-party trusted authority.” Given

other data values and send the plurality of codes and the other data values to

agent.” MSC-1003, ¶[151]. For the reasons noted above in [1.5], Burger also renders obvious the remaining features of [15.3]. *Id.*

[15.4]

See [1.6]; MSC-1005, FIGS. 7A, 7B, 10A, 19, 26H-26K; ¶¶[0320], [0189], [0095]-[0096], [0101], [0125], [0236]-[0238], [0155]-[0158], [0103], [517]-[527], [182]-[186], [0194]. In addition, because the network server 114 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 114 sends the access message to Pocket Vault 102, the communications protocol layer 2716 (“*authentication unit*”) also “*receiv[es] an access message from the agent allowing the user to access an application.*” See [1.6]; MSC-1003, ¶[152].

the breadth of this claim language, therefore, Burger’s “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 unit.” Specifically, layer 2716 receives and sends this information “for authentication” by the controller(s) 402 and the database 406. MSC-1003, footnote 4.

[15.5]

See [1.7], [8.4]; MSC-1005, FIGS. 7A, 7B, 10A, 19, 26H-26K; ¶¶[0320], [0189], [0095]-[0096], [0101], [0125], [0236]-[0238], [0155]-[0158], [0103], [517]-[527], [182]-[186], [0194], [0250]; MSC-1003, ¶[153].

[16]

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 114. MSC-1005, ¶¶[0464], [0476]; MSC-1003, ¶[154].

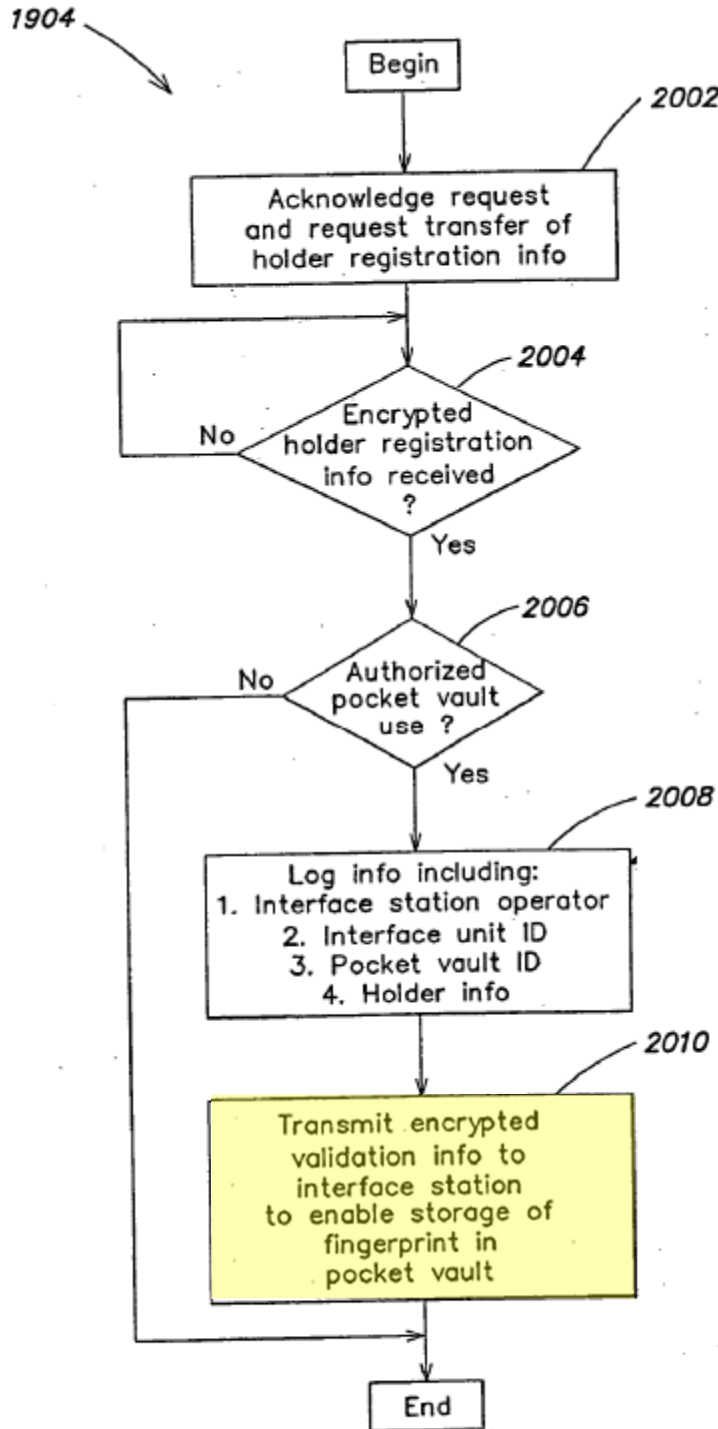


FIG. 20

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 114 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, ¶[155].

In this example, the validation information sent from the communication protocol layer 2716⁵ in the network server 114 to the Pocket Vault 102 is the “*authentication request from the authentication unit*” that is received by the Pocket Vault 102 (“*biometric key*”), and, in response to receiving this information, the Pocket Vault 102 is enabled to *request a biometric scan (e.g., fingerprints) from*

⁵ As shown in Burger’s FIG. 27, it would have been obvious to a POSITA that the communication protocol layer 2716 (“*authentication unit*”) sends and receives data between the Pocket Vault 102 and the network server 114. MSC-1003, footnote 5.

the user to generate and store scan data. MSC-1005, ¶[0482], FIG. 20. In this manner, Burger renders [16] obvious. MSC-1003, ¶[156].

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 102 "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, ¶[157].

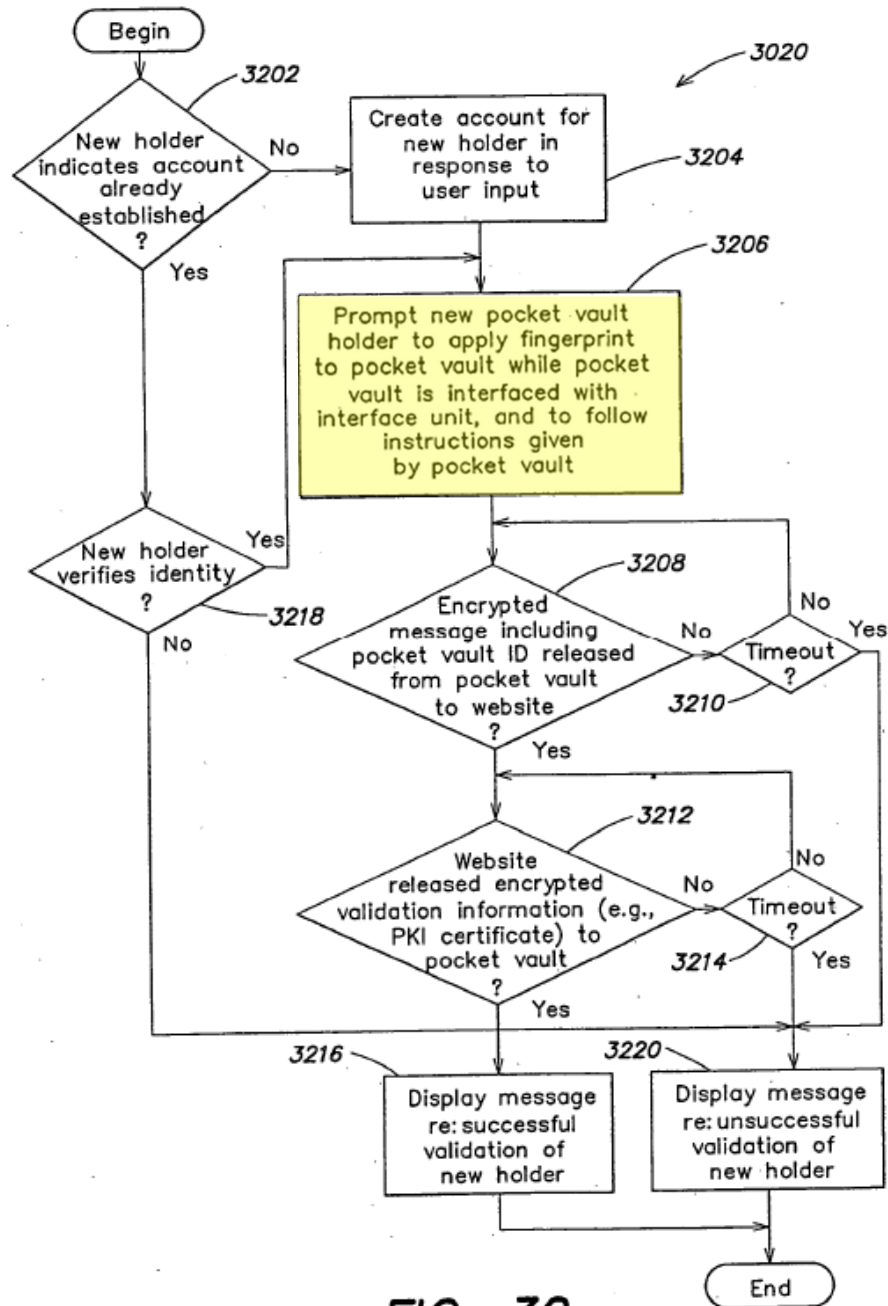


FIG. 32

MSC-1005, FIG. 32.

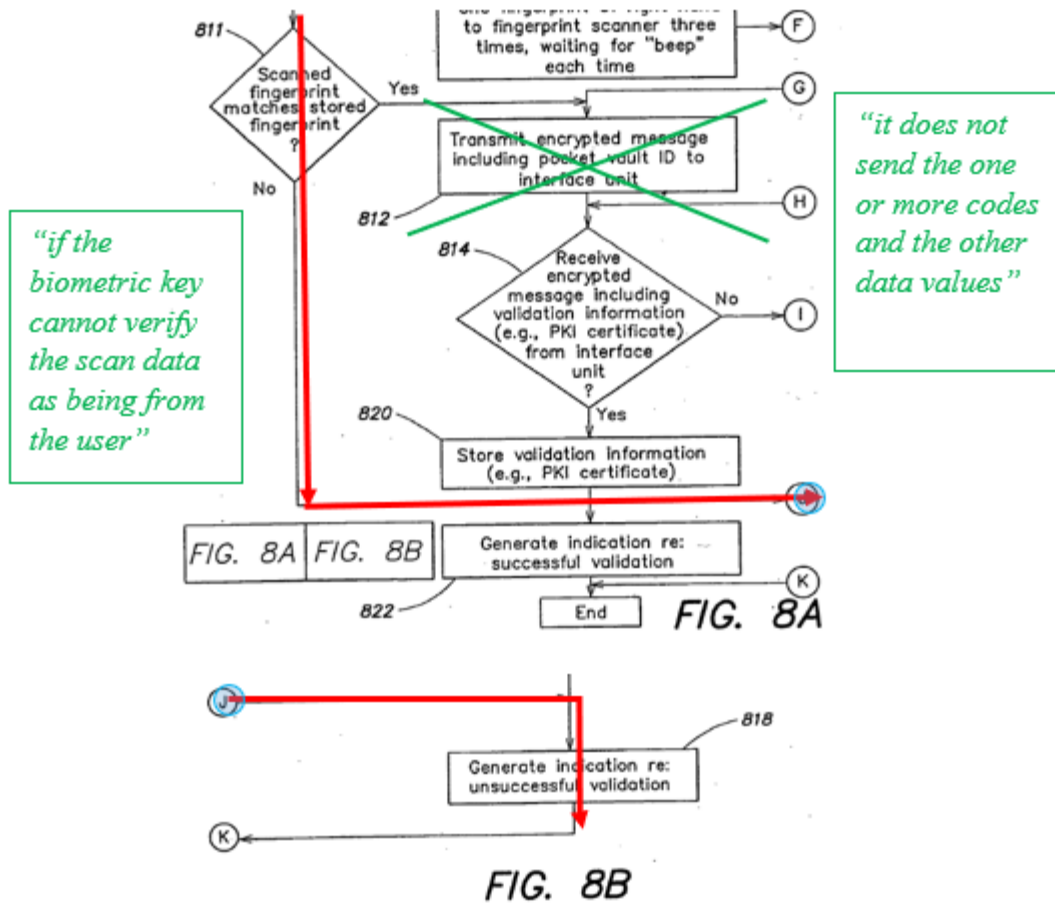
Although FIG. 32 is described as being performed by an interface station, “in some embodiments wherein appropriate networking capabilities are provided, each Pocket Vault 102 may communicate directly with the network server 114,

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 (“**authentication unit**”) in the network server 114 would have communicated directly with the Pocket Vault 102 and sent a message (“**an authentication request**”) to request the Pocket Vault 102 to prompt the new holder to apply the holder’s fingerprints. MSC-1003, ¶[158]. In this additional way, Berger renders obvious “**wherein the biometric key receives an authentication request from the authentication unit, and in response, requests a biometric scan from the user to generate the scan data,**” as recited in claim 16. *Id.*

[17]

Burger teaches that when scanned fingerprints do not match stored fingerprints, an indication of unsuccessful validation is generated and no encrypted message including codes or other data values are sent. MSC-1005, FIGS. 7A, 8A, 8B, ¶[0211]. A marked-up example is shown below in FIG. 8B, in which Burger’s system “**does not send the one or more codes and the other data values**” (steps 818, 820) “**if the biometric key cannot verify the scan data as being from the user**” (step 811). MSC-1003, ¶[159].



MSC-1005, FIG. 8B.

B. [GROUND 2] – Claim 3, 10, and 13 are Obvious in view of Burger and Robinson

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, ¶[75]. “[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.

An individual who has already registered in the system may verify their age at any participating POV by entering the individual's SID and biometric sample. This information is sent to a database where it is used to find the individual's age verifying record. Once the age verifying record is found, the individual's age is evaluated to determine whether or not it is at or above the level pre-set for the particular verification. If the individual's age is at or above the pre-set level, the individual's age is verified, and the individual is granted access. This access may be used for (but is not limited to) purchasing age-restricted goods, accessing age-restricted areas, or purchasing age-restricted services.

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, ¶[76].

Presenters who want to participate in age-verification can pre-enroll with the age-verification system. MSC-1006, ¶¶[0032], [0034]. Pre-enrollment records can be stored in the verifier database 124 and/or the central database 102. MSC-1006, ¶[0032]. The enrollment process can include a check with other databases, such as a state or government database, to obtain presenter information such as driver's license data or employment data. MSC-1006, ¶¶[0034], [0040]; MSC-1003, ¶[77].

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, ¶[78].

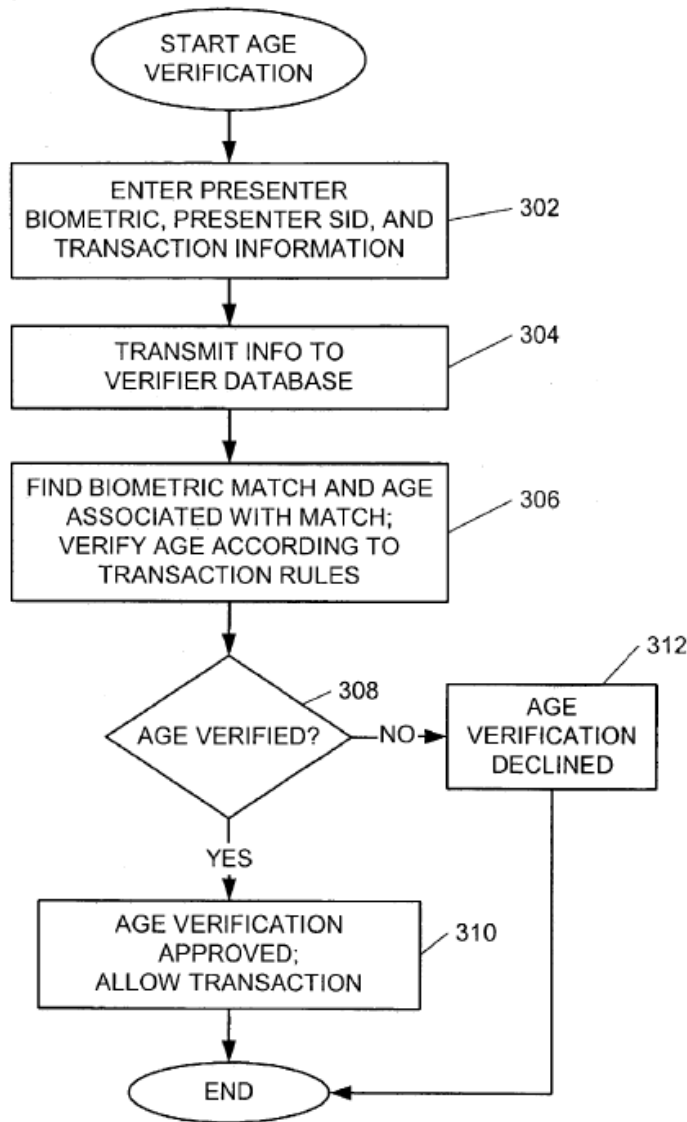


FIG. 3

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, ¶[79]. 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, or being shown an advertisement for alcohol, tobacco, or gambling.

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, ¶[80]. 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. *Id.* The age-verification information would have been stored in the database 406 of Burger's network server 114, 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, ¶[80].

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, ¶[81]. 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. *Id.*

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, ¶[81]. 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 '730 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, ¶[160].

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 114. In this manner, Burger-Robinson renders obvious “*registering an age verification for the user.*” MSC-1003, ¶[161].

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, ¶[162].

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, ¶[163]. 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.*” *Id.*; MSC-1006, ¶¶[0014]-[0015].

[10]

See [3]; MSC-1003, ¶[164].

[13]

Similar to the explanation above in [3], the Burger-Robinson combination registering age-verification information, such as a date of birth or age, with the database 406 (“*the agent*”) in the network server 114. MSC-1006, ¶¶[0014]-[0015]; MSC-1003, ¶[165].

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 months⁶ 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 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

⁶ Obtained from <https://www.uscourts.gov/statistics-reports/analysis-reports/federal-court-management-statistics>

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*

The '730 patent issued after seven years of prosecution involving multiple RCEs and amendments to overcome US Patent No. 6,041,410 (“Hsu”)-based 102 and 103 rejections. After issuance, IPR2021-01444 was filed in August 2021 asserting grounds based on International Patent Application Publication No. WO 99/56429 (“Scott”) and U.S. Patent No. 7,239,226 B2 (“Berardi”) as primary references, and IPR2024-00232 was filed in January 2024 asserting grounds based on U.S. Patent No. 7,188,110 (“Ludtke”) and U.S. Patent Application Publication No. 2002/0046336 (“Kon”). Yet, none of the references previously asserted against the '730 patent are cumulative to Burger. Indeed, Burger is a robust 91-page reference with no equivalent seen during prosecution or the earlier IPR proceedings. 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 '730 Patent.

Moreover, 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).

The '730 patent is the subject of a re-examination request (application number 90/015,052) that does not involve any of the references in these proceedings other than Robinson, which is relied upon in combination with the Ludtke and Okereke (US Patent Pub No. 2003/0196084) references to challenge claim 3, 10, and 13 in the reexamination proceedings. MSC-1022, 85. Ludtke and Okereke do not resemble or disclose the claimed features in the same or similar manner as Burger. Thus, the challenge of dependent claims 3, 10, and 13 in the reexamination proceedings is based on vastly different prior art combinations than the combination asserted in this petition. At worst, even if the use of Robinson gave rise to similar issues (which Petitioner does not concede), this Petition challenges all the '730 claims and raises other grounds with no overlap with the re-examination proceedings or prosecution history. Thus, institution should not be denied simply because one secondary reference, Robinson, is asserted for a subset of dependent claims (claims 3, 10, and 13) in this IPR petition and the reexamination proceeding, whereas numerous other grounds, references, and issues have no overlap.

Moreover, the Challenged Claims were allowed based on the Examiner's mistaken conclusion (made in without the benefit of Burger's rich disclosure) that

the claims included certain allowable subject matter. MSC-1002, 36-45. The Examiner's failure to 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 '730 Patent is the subject of several civil actions:

- *Proxense, LLC v Microsoft Corporation*, 6:23-cv-00319, W.D. Tex., filed May 02, 2023 (MSC-1004);
- *Proxense, LLC v. Google LLC et al*, 6-23-cv-00320 (WDTX) filed May 2, 2023;
- *Proxense, LLC v. Apple, Inc.*, 6-24-cv-00143 (WDTX) filed March 18, 2024; and
- *Proxense, LLC v. Samsung Electronics Co., Ltd. et al.*, 6-21-cv-00210 (WDTX) filed March 5, 2021 (settled January 19, 2023).

The '730 patent is also the subject of:

- *Samsung Electronics America, Inc. v. Proxense, LLC*, IPR2021-01444 filed August 26, 2021, institution denied;
- *Google LLC v Proxense, LLC*, IPR2024-00232 filed Jan. 17, 2024);
- and
- A pending *ex-parte* re-examination request (application 90/015,052).

Petitioner is not aware of any other disclaimers, reexamination certificates, or IPR petitions addressing the '730 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: IPR42342-0136IP1@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 IPR42342-0136IP1@fr.com

(referencing No. 42342-0136IP1 and cc'ing PTABInbound@fr.com, axf-ptab@fr.com, devoto@fr.com and khan@fr.com).

Attorney Docket No. 42342-0136IP1

IPR of U.S. Patent No. 8,352,730

Respectfully submitted,

Dated 4-19-24

/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. IPR2024-00775)

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 13,776 words, which is less than the 14,000 allowed under 37 CFR § 42.24.

Dated 4-19-24

/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 19, 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