



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
90/015,052	06/08/2022	8352730	02198-00080	9657
142179	7590	05/20/2025		
Hard IP Professional Services LLC (General)			EXAMINER	
10 Notch Hill Drive			TARAE, CATHERINE MICHELLE	
Livingston, NJ 07039				
			ART UNIT	PAPER NUMBER
			3992	
			MAIL DATE	DELIVERY MODE
			05/20/2025	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action in Ex Parte Reexamination	Control No. 90/015,052	Patent Under Reexamination 8352730	
	Examiner C. Michelle Tarae	Art Unit 3992	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

- a. ☒ Responsive to the communication(s) filed on 08 March 2025.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

b. ☐ This action is made FINAL.

c. ☐ A statement under 37 CFR 1.530 has not been received from the patent owner.

A shortened statutory period for response to this action is set to expire 2 month(s) from the mailing date of this letter. Failure to respond within the period for response will result in termination of the proceeding and issuance of an *ex parte* reexamination certificate in accordance with this action. 37 CFR 1.550(d). **EXTENSIONS OF TIME ARE GOVERNED BY 37 CFR 1.550(c)**. If the period for response specified above is less than thirty (30) days, a response within the statutory minimum of thirty (30) days will be considered timely.

Part I THE FOLLOWING ATTACHMENT(S) ARE PART OF THIS ACTION:

- | | |
|--|---|
| 1. ☐ Notice of References Cited by Examiner, PTO-892. | 3. ☐ Interview Summary, PTO-474. |
| 2. ☐ Information Disclosure Statement, PTO/SB/08. | 4. ☐ _____. |

Part II SUMMARY OF ACTION

- 1a. ☒ Claims 1-17 are subject to reexamination.
- 1b. ☐ Claims _____ are not subject to reexamination.
2. ☐ Claims _____ have been canceled in the present reexamination proceeding.
3. ☐ Claims _____ are patentable and/or confirmed.
4. ☒ Claims 1-17 are rejected.
5. ☐ Claims _____ are objected to.
6. ☐ The drawings, filed on _____ are acceptable.
7. ☐ The proposed drawing correction, filed on _____ has been (7a) ☐ approved (7b) ☐ disapproved.
8. ☐ Acknowledgment is made of the priority claim under 35 U.S.C. 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the certified copies have
 - 1 ☐ been received.
 - 2 ☐ not been received.
 - 3 ☐ been filed in Application No. _____.
 - 4 ☐ been filed in reexamination Control No. _____.
 - 5 ☐ been received by the International Bureau in PCT application No. _____.

* See the attached detailed Office action for a list of the certified copies not received.

9. ☐ Since the proceeding appears to be in condition for issuance of an *ex parte* reexamination certificate except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte* Quayle, 1935 C.D. 11, 453 O.G. 213.
10. ☐ Other: _____

cc: Requester (if third party requester)

EX PARTE REEXAMINATION NON-FINAL OFFICE ACTION

A substantial new question (SNQ) of patentability affecting claims 1-17 of U.S. Pat. No. 8,352,730 to Giobbi (“the ‘730 Patent”) was raised by the Request for *Ex Parte* reexamination filed June 8, 2022 (“Request”) by Samsung Electronics America, Inc. (“Requester”).

Prosecution History of the instant 90/015,052

Reexamination (“the ‘052 Reexam”)

A first Non-Final office action rejecting claims 1-17 was mailed September 12, 2024.

Patent Owner (“PO”) filed a response on October 9, 2024 (“Remarks”).

A second Non-Final office action was mailed November 25, 2024.

Patent Owner (“PO”) filed a response to the second Non-Final office action on January 27, 2025 (“Remarks II”).

A Final Office Action in response to Remarks II was mailed March 3, 2025.

PO submitted after final amendments on March 8, 2025 (“March 2025 After Final Amendment”). These amendments are entered.

On March 27, 2025, the Patent Trial and Appeal Board (“PTAB”) issued an order staying the ‘052 Reexam pending termination or completion of the inter partes review trial for IPR2024-00232 (“Order Staying Reexam”).

The PTAB issued a judgment on April 28, 2025 in IPR2024-00232/IPR2024-01333 granting PO’s motion for adverse judgment and lifted the prior stay of this proceeding (“Order Lifting Reexam”). The April 28, 2025 Order further indicated that

their judgment constitutes a Final Written Decision under 35 U.S.C. § 318(a) and that Examiner assigned to 90/015,052 should consider whether estoppel under 37 C.F.R. § 42.73(d)(3)(i) would preclude Patent Owner from taking action inconsistent with this adverse judgment.

This is a Non-Final Office Action addressing amended claims 1-17. The previous rejection under Ludtke is withdrawn.

Prior and Concurrent Proceedings and Litigation

The patent owner is reminded of the continuing responsibility under 37 CFR 1.565(a) to apprise the Office of any litigation activity, or other prior or concurrent proceeding, involving the '730 Patent throughout the course of this reexamination proceeding.

The third party requester is also reminded of the ability to similarly apprise the Office of any such activity or proceedings throughout the course of this reexamination proceeding. See MPEP §§ 2207, 2282, and 2286.

Claim Interpretation

I. Lexicographic Definitions

After careful review of the original specification and unless expressly noted otherwise by the Examiner, the Examiner cannot locate any lexicographic definitions in the original specification with the required clarity, deliberateness, and precision. Because the Examiner cannot locate any lexicographic definitions in the original specification with the required clarity, deliberateness, and precision, the Examiner concludes the Patent Owner is not their own lexicographer. See MPEP § 2111.01 IV.

II. 'Source' for the 'Broadest Reasonable Interpretation'

For terms not lexicographically defined by Patent Owner, the Examiner hereby adopts the following interpretation under the broadest reasonable interpretation standard. In other words, the Examiner has provided the following interpretation simply as express *notice* of how she is interpreting particular terms under the broadest reasonable interpretation standard. Additionally, this interpretation is only a guide to claim terminology since claim terms must be interpreted in context of the surrounding claim language.¹ In accordance with *In re Morris*, 127 F.3d 1048, 1056 (Fed. Cir. 1997), the Examiner points to this other “source” to support her interpretation of the claims. Finally, the following list is not intended to be exhaustive in any way:

¹ While most interpretations are cited because these terms are found in the claims, the Examiner may have provided additional interpretations to help interpret words, phrases, or concepts found in the interpretations themselves, the '730 Patent, or in the prior art.

Third-party trusted authority. “third party n. . . . 2. One other than the principals involved in a transaction.” THE AMERICAN HERITAGE COLLEGE DICTIONARY 1433 (4th ed. 2004).

Access message: a message/notification indicating the user is allowed access, or otherwise allowing access (See at least the ‘730 Patent at 5:23-26, “Authentication module 310 can send a message to application 330, or otherwise allow access to the application, responsive to a successful authentication by trusted key authority 320.”)

Application: “1. n. a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file.” (See independent claims 1, 8, 12, and 15. See at least the ‘730 Patent at 5:27-39, “Application 330 is a resource that can be accessed by a verified and authenticated user. Application 330 can be, for example, a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file, and the like. Application 330 can execute on the same system as authentication module 310 or on another system in communication with the system of the authentication module. In one embodiment, application module 330 allows access by a user after receiving a message from authentication module 310. At that point, application 330 can allow direct use by the user, or require that communications continue to pass through authentication module 310 for continued authentication.”)

Computer software: “n. computer programs; instructions that make hardware work...” Microsoft Press Computer Dictionary, 5th Edition, Microsoft Press, Redmond, WA, 2002.

File: “n. A complete, named collection of information, such as a program, a set of data used by a program, or a user-created document...” Microsoft Press Computer Dictionary, 5th Edition, Microsoft Press, Redmond, WA, 2002.

Claim Rejections - 35 USC § 102

In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis (i.e., changing from AIA to pre-AIA) for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

The following is a quotation of the appropriate paragraphs of pre-AIA 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 2, 4-9, 12, and 14-17 are rejected under pre-AIA 35 U.S.C. 102(e) as being anticipated by Burger.

As per claim 1, Burger discloses a method for verifying a user during authentication of an integrated device, comprising the steps of:

[0010] “According to another aspect, a method for using an apparatus comprises steps of using the apparatus to authenticate an identity of a user of the apparatus, and after

the apparatus has authenticated the identity of the user, enabling a transponder of the apparatus to emit a wireless signal representing information stored in the apparatus in response to a wireless interrogation signal.”

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;

[0112] “One suitable user authentication technique that may be employed is the analysis of a bio-metric feature of the individual attempting use of the device (e.g., a fingerprint scan, retina scan, a speech pattern analysis, keystroke rhythm, etc.), and validating the identity of the individual on that basis... 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, 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.”

[0114] “As discussed below, 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.”

[0122] “The controller 202 may include a software-programmable and encryption-protected or hard-wired unique chip ID. In one embodiment, this chip ID is released from the Pocket Vault 102 only after the fingerprint scanner 220 (discussed below) has successfully authenticated the identity of the holder.”

[0127] “Similarly, any suitable memory device that permits a only single write operation to take place may be employed as the write-once memory 212.”

[0182] “[T]he 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, as described below.”

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;

[0112] “One suitable user authentication technique that may be employed is the analysis of a bio-metric feature of the individual attempting use of the device (e.g., a fingerprint scan, retina scan, a speech pattern analysis, keystroke rhythm, etc.), and validating the identity of the individual on that basis.”

responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan;

[0180] “When, at the step 702, it is determined that the holder has applied his/her fingerprint to the fingerprint scanner 220, the routine 700 proceeds to a step 704, wherein the power manager 214 powers on the Pocket Vault 102.” Fig. 7

comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;

[0182] “After the step 706, the routine 700 proceeds to a step 708, wherein it is determined whether the Pocket Vault 102 has been validated. 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, as described below.”

[0184] “When, at the step 708, it is determined that the Pocket Vault 102 has already been validated, the routine 700 proceeds to a step 712, wherein 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.”

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

[0113] “It should be appreciated that, for some applications, it may be desirable to receive and store authentication information (e.g., fingerprint data) of some or all Pocket Vault holders in the network server 114. Accordingly, in some embodiments, such authentication information may be maintained by the network server 114. This authentication information may be transmitted to the network server 114, for example, when Pocket Vaults 102 are first validated.”

[0114] “As discussed below, 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

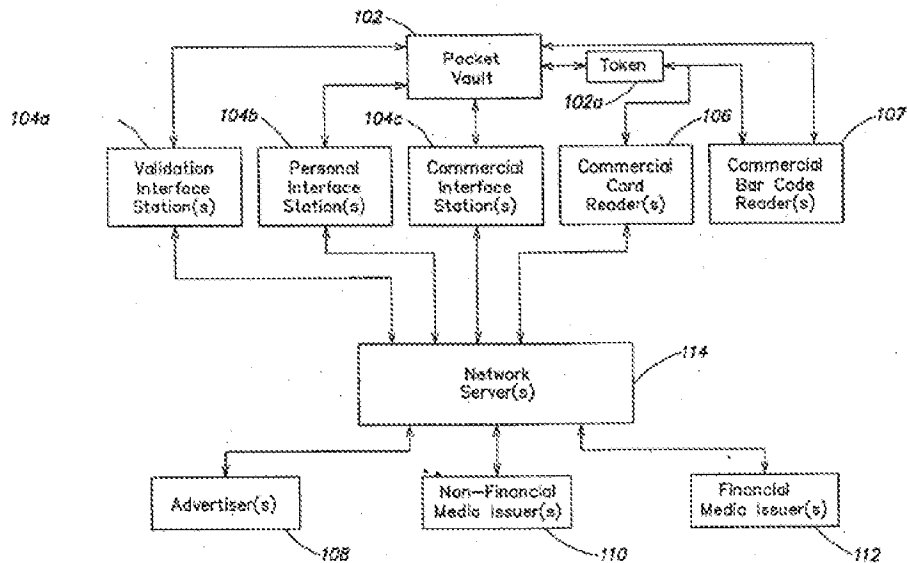
the Pocket Vault 102 to permanently store the Pocket Vault holder's authentication information.”

[0186] “When, at the step 712, it is determined that the Pocket Vault 102 has been properly authenticated, the routine 700 proceeds to a step 713, wherein an encrypted message including the unique Pocket Vault chip ID is transmitted to the pocket vault interface unit 302, in the event that the Pocket Vault 102 is interfaced or in communication with such a device.”

[0146] “The database 406 may, for example, comprise a relational database, and may be used to store the majority, if not all, of the data maintained by the network server 114. The database 406 may, for example, keep 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 and appropriate contact information for each; records regarding the versions of software loaded onto each Pocket Vault 102, each pocket vault interface unit 302, and each interface station computer 304; a list of currently authorized or registered Pocket Vaults 102, identified by chip ID and linked to the holder list...”

[0116] “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.”

The network server is the third-party trusted authority between the user of the Pocket Vault and advertisers, non-financial media issuers and financial media issuers as shown in Fig. 1.



Patent Application Publication Mar. 3, 2005 Sheet 1 of 48 U.S. 2005/005367 A1

Fig. 1 of Burger

responsive to authentication of the one or more codes and the other data values by the agent, receiving an access message by an application from the agent allowing the user access to the application,

[0439] "When, at the steps 1730 and 1732, it is determined that an encrypted transaction approval message has been received in a timely manner, the routine 1414 proceeds to a step 1734, wherein a message is forwarded to the pocket vault interface unit 302 indicating that the requested transaction has been approved. This message may also be used to update information on the Pocket Vault 102, and/or to cause the Pocket Vault 102 to generate an indication (e.g., an audio tone) that the transaction has been approved."

[0440] "After the step 1734, the routine proceeds to a step 1738, wherein a message is displayed on the display 324 indicating that the requested transaction has been approved."

[0518] "After the step 2406, the routine 1922 proceeds to a step 2408, wherein an encrypted approval message is transmitted to the entity with which the transaction is

being attempted (e.g., a commercial interface station 104C, a card reader 106, or a barcode reader 107).” Fig. 24

[0100] As shown in FIG. 1, the Pocket Vault 102 may be interfaced with any of the interface stations 104a-c so as to permit information to be uploaded from the network server 114 to the Pocket Vault 102, or to be downloaded from the Pocket Vault 102 to the network server 114.

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.

As discussed above in the previous limitation, the access message may be received by the pocket vault and/or the interface stations. The following are examples of how the pocket vault and the interface stations can be interpreted as applications.

Example 1: the Pocket Vault is an application

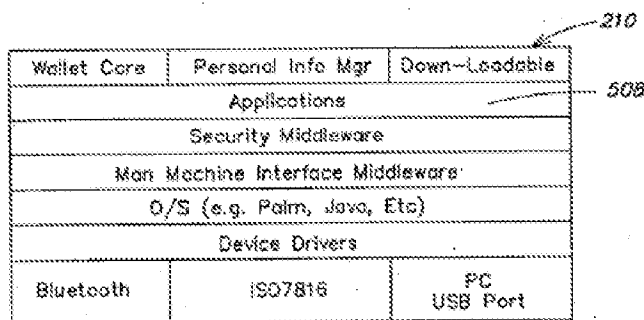


FIG. 5

Fig. 5 shows the memory of the Pocket Vault containing applications 508

[0178] “FIG. 7 is a flow diagram illustrating an example implementation of a primary routine 700 that may be executed by the controller 202 of the Pocket Vault 102. Instructions for the routine 700 may be stored, for example, in the "applications" section 508 of the memory 210 of the Pocket Vault 102.”

[0108] “Moreover, as is also discussed in more detail below, the Pocket Vault 102 may be configured or programmed to function as an RFID tag that can be used only by an authorized user of the Pocket Vault 102.”

[0127] “The memory 210 may have instructions stored therein which, when executed by the controller 202, cause the controller 202 to implement the routines/software described below in connection with FIGS. 7-12 and/or FIG. 28. Of course, the memory 210 may also contain a suitable operating system (e.g., Palm OS, Microsoft's Windows CE, Microsoft's Windows for Smartcards, or some similar offering), appropriate device drivers, and other software employed in connection with the controller 202 and/or the peripherals thereof. “

[0176] “As mentioned above, FIGS. 7-12 are flow diagrams illustrating an example implementation of software that may be executed by the controller 202 of the Pocket Vault 102. As described below, this or additional proprietary software may enable menu structures, handle preference management, provide the data on and safeguard the programmability of the virtual magnetic stripe 610 (if so equipped), and ensure proper encryption data management. In one embodiment, local software for each Pocket Vault 102 and pocket vault interface station 104 may be upgraded from time to time by automatic download from the network server 114.”

[0146] “...records regarding the versions of software loaded onto each Pocket Vault 102, each pocket vault interface unit 302, and each interface station computer 304...”

Example 2: the interface stations are applications

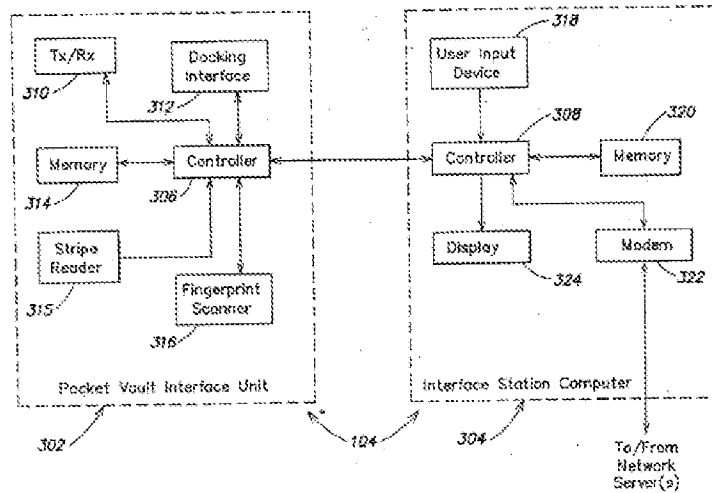


FIG. 3

Fig. 3 shows the memory of the interface stations

[0137] “As shown in FIG. 3, each interface station 104 may include both an the interface station computer 304 and a pocket vault interface unit 302. The interface station computer 304, for example, may be a standard desktop personal computer (PC), and may, as shown, comprise a controller 308, a user input device 318, a memory 320, a modem 322, and a display 324. These components are well known in the art and therefore will not be described in detail herein. The memory 320 of the interface station computer 304 may have instructions stored therein which, when executed by the controller 308, cause the controller to implement the routine described below in connection with FIGS. 14-18 as well as any other software, e.g., a browser, drivers, etc., executing on the interface station computer 304.”

[0146] “...records regarding the versions of software loaded onto each Pocket Vault 102, each pocket vault interface unit 302, and each interface station computer 304...”

[0364] “FIG. 14 is a flow diagram illustrating example implementation of a primary routine 1400 that may be executed by the controller 308 of the interface station computer 304 of FIG. 3.”

[0518] “After the step 2406, the routine 1922 proceeds to a step 2408, wherein an encrypted approval message is transmitted to the entity with which the transaction is

being attempted (e.g., a commercial interface station 104C, a card reader 106, or a barcode reader 107).” Fig. 24

As per claim 2, Burger discloses the method of claim 1, wherein the one or more codes and the other data values are transmitted to the agent over a network.

[0099] “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).”

See Fig. 27 showing a network 2724 between the network server 114 and the pocket vault interface station computer 104.

As per claim 4, Burger discloses the method of claim 1, wherein the one or more codes and the other data values indicate that the biometric verification was successful.

[0122] “The controller 202 may include a software-programmable and encryption-protected or hard-wired unique chip ID. In one embodiment, this chip ID is released from the Pocket Vault 102 only after the fingerprint scanner 220 (discussed below) has successfully authenticated the identity of the holder.”

[0349] “When, at the step 1310, it is determined that the scanned fingerprint does match that of an authorized operator of the interface unit 302, the routine 1300 proceeds to a step 1312, wherein a second encrypted message, including an ID of the pocket vault

interface unit 302 that is released only after a successful fingerprint match, is transmitted to the interface station computer 304.”

As per claim 5, Burger discloses the method of claim 1, wherein the biometric data and the scan data are both based on a fingerprint scan by the user.

[0112] “One suitable user authentication technique that may be employed is the analysis of a bio-metric feature of the individual attempting use of the device (e.g., a fingerprint scan, retina scan, a speech pattern analysis, keystroke rhythm, etc.), and validating the identity of the individual on that basis... 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, 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.”

[0184] “When, at the step 708, it is determined that the Pocket Vault 102 has already been validated, the routine 700 proceeds to a step 712, wherein 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.”

As per claim 6, Burger discloses 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.

[0114] “As discussed below, 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.

**As per claim 7, Burger discloses 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**

[0477] “As shown, the routine 1904 begins at a step 2002, wherein a request received from the interface station computer 304 to register a new Pocket Vault holder is acknowledged, and the network server 114 requests the interface station computer 304 to transfer the relevant information regarding the proposed new holder to the network server 114.”

Item 2002 in Fig. 20 where holder registration information is requested.

[0481] “When, the routine 2006 has determined that the proposed Pocket Vault use is authorized, the routine 1904 proceeds to a step 2008, wherein all of the relevant information regarding the new Pocket Vault registration is logged into the database 406 of the network server 114 (FIG. 4). As shown in FIG. 20, this 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.”

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.

[0479] “When, at the step 2004, it is determined that all of the requisite holder registration information has been received from the interface station computer 304...

[0481] When, the routine 2006 has determined that the proposed Pocket Vault use is authorized, the routine 1904 proceeds to a step 2008, wherein all of the relevant information regarding the new Pocket Vault registration is logged into the database 406 of the network server 114 (FIG. 4). As shown in FIG. 20, this 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.”

**Claim 8 recites substantially similar subject matter to that of claim 1;
therefore, claim 8 is rejected based on the same rationale as claim 1.**

As per claim 9, Burger discloses 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.

See claim 2.

**Claim 12 recites substantially similar subject matter to that of claim 1;
therefore, claim 12 is rejected based on the same rationale as claim 1.**

As per claim 14, Burger discloses 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.

[0114] “As discussed below, 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.

[0186] "When, at the step 712, it is determined that the Pocket Vault 102 has been properly authenticated, the routine 700 proceeds to a step 713, wherein an encrypted message including the unique Pocket Vault chip ID is transmitted to the pocket vault interface unit 302, in the event that the Pocket Vault 102 is interfaced or in communication with such a device."

**Claim 15 recites substantially similar subject matter to that of claim 1;
therefore, claim 15 is rejected based on the same rationale as claim 1.**

Further, with regard to the authentication unit that "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," Burger discloses a communication protocol layer 2716 ("authentication unit") "which provides low-level communication functions to server communications software." ([540]). See FIG. 27, 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.

As per claim 16, Burger discloses 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.

[0464] “When, at the step 1902, it is determined that a request has been received to register a new Pocket Vault holder, the routine 1900 proceeds to a step 1904, wherein the request to register the new Pocket Vault holder is processed. An example of a routine that may be employed to implement the step 1904 is discussed in more detail below in connection with FIG. 20.”

[0482] “After the step 2008, the routine 1904 proceeds to a step 2010, wherein 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.”

[0575] “After completion of the NEW POCKET VAULT HOLDER routine 3020, the routine 1422 proceeds to a step 3022, wherein it is determined whether a new holder was successfully validated.”

[0585] “After the step 3204, the routine 3020 proceeds to a step 3206, 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.”

As per claim 17, Burger discloses 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.

[0211] “When, at the step 811, it is determined that the fingerprint scanned at the step 706 does not match any of the stored fingerprints, the routine 710 proceeds to a step 818, wherein an indication (e.g., a message on the display 216 or an audio signal from

the indicator 215) is generated to inform the holder that the validation attempt was unsuccessful."

Item 811 in Fig. 8B.

Claim Rejections - 35 USC § 103

In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis (i.e., changing from AIA to pre-AIA) for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claim 11 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Burger.

As per claim 11, Burger discloses the integrated device of claim 8, wherein the verifier comprises: an LED to be activated for requesting the biometric scan.

[0133] "As mentioned above in connection with the description of the indicator 215, in addition to or in lieu of the display 216, other user output devices may also be employed to provide information to the Pocket Vault holder. For example, light emitting diodes

(LEDs), a beeper or buzzer, a speech synthesizer, a vibrator, etc., may be employed in some embodiments of the Pocket Vault 102.”

[0138] “The pocket vault interface unit 302 is coupled to the interface station computer 304 such that a controller 306 of the pocket vault interface unit 302 can communicate with the controller 308 of the interface station computer 304. The communications interface between these devices may, for example, comprise a Smartcard, Bluetooth or USB interface. As shown, in addition to the controller 306, the pocket vault interface unit 302 may comprise a transceiver 310, a docking interface 312, a finger print scanner 316, a stripe reader 315, and a memory 314. Further, although not shown in FIG. 3, the pocket vault interface unit 302 may also comprise a display and/or another device used to provide feedback to the operator, e.g., an audio indicator or LED.”

[0232] “After the step 918, the routine 714 proceeds to a step 920, wherein after a delay of a certain period of time (e.g., thirty seconds), the holder is prompted to reapply his/her fingerprint within a particular period of time (e.g., ten seconds) to avoid shut down of the Pocket Vault 102.”

If Burger is seen as not disclosing this limitation, at the time of the invention, it would have been obvious to a person of ordinary skill in the art to use the LED as disclosed in Burger to prompt the Pocket Vault user to apply a fingerprint on the fingerprint scanner as there are a number of ways to prompt a user to do so and Burger could have employed its LED, which is already used to provide information to the user of the Pocket Vault.

Claims 3, 10, and 13 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Burger and U.S. Pub. No. 2003/0177102 to Robinson (“Robinson”).

As per claim 3, Burger does not expressly disclose the method of claim 1, further comprising:

registering an age verification for the user in association with the device ID code.

Robinson discloses this:

[0009] One aspect of the present invention is that it provides a reliable system and method that conducts age verification of individuals for access to age-restricted areas, goods, and services.

[0010] It is also an aspect of the current invention to offer verifiers (individuals verifying another individual's age) and presenters (individuals trying to verify their own age) a convenient, reliable, and secure way to conduct an age verification in an age-restricted transaction with the use of a biometric read (such as a fingerprint) and a system ID (SID) number entry and without the use of any age-verifying token(s).

[0014] To register in the system, an individual presents at least one biometric sample, identity-verifying information, and age-verifying information. The biometric sample may be, for example and without limitation, a fingerprint, a retinal scan, a face geometric scan, or a voice print. The identity-verifying information may be, for example and without limitation, a name, a home address, a telephone number, or a government ID number and state of issue. 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.

At the time of the invention, it would have been obvious to a person of ordinary skill in the art 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 by the user such as 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.

Claims 10 and 13 recite substantially similar subject matter to that of claim 3; therefore, claims 10 and 13 are rejected based on the same rationale as claim 3.

ESTOPPEL

37 CFR 42.73(d)(3) states in part:

(3) Patent applicant or owner. A patent applicant or owner is precluded from taking action inconsistent with the adverse judgment, including obtaining in any patent: (i) A claim that is not patentably distinct from a finally refused or canceled claim. See MPEP 2190 II.

Amended claims 1-17 are rejected under 37 CFR 42.73(d)(3) as not being patentably distinct from finally refused originally issued claims 1-17.

In IPR2024-00775, the Board issued a final written decision on April 28, 2025, holding that original issued claims 1-17 were finally unpatentable over Burger. As stated above, the newly added limitation of "receiving an access message by an application

from the agent allowing the user access to the application” in amended claims 1-17 is expressly disclosed by the Burger reference (see at least ¶¶100, 439, 440, 518). Thus, amended claims 1-17 are estopped as not being patentably distinct from original claims 1-17 which were finally refused in IPR2024-00775.

Amendment in Reexamination Proceedings

Patent owner is notified that any proposed amendment to the specification and/or claims in this reexamination proceeding must comply with 37 CFR 1.530(d)-(j), must be formally presented pursuant to 37 CFR §1.52(a) and (b), and must contain any fees required by 37 CFR § 1.20(c). See MPEP §2250(IV) for examples to assist in the preparation of proper proposed amendments in reexamination proceedings.

Service of Papers

After the filing of a request for reexamination by a third party requester, any document filed by either the patent owner or the third party requester must be served on the other party (or parties where two or more third party requester proceedings are merged) in the reexamination proceeding in the manner provided in 37 CFR 1.248. See 37 CFR 1.550.

Future Correspondence

If attempts to reach Examiner C. Michelle Tarae by telephone at 571-272-6727 are unsuccessful, the examiner’s supervisor, Andrew J. Fischer, can be reached on 571-272-6779.

Information regarding the status of published reexamination applications may be obtained from Patent Center. Unpublished application information in Patent Center is available to registered users. To file and manage patent submissions in Patent Center, visit: <https://patentcenter.uspto.gov>. Visit <https://www.uspto.gov/patents/apply/patent-center> for more information about Patent Center and <https://www.uspto.gov/patents/docx> for information about filing in DOCX format.

For additional questions, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000. For general inquiries, the CRU main number is 571-272-7705.

All correspondence relating to this *ex parte* reexamination proceeding may be submitted via:

Electronically: Registered users may submit via Patent Center
<https://patentcenter.uspto.gov/>.

By Mail to: Mail Stop *Ex Parte* Reexam
Central Reexamination Unit
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

By FAX to: (571) 273-9900
Central Reexamination Unit

By hand: Customer Service Window
Knox Building
501 Dulany Street
Alexandria, VA 22314

For Patent Center transmissions, 37 CFR 1.8(a)(1)(i)(C) and (ii) states that correspondence (except for a request for reexamination and a corrected or replacement request for reexamination) will be considered timely filed if (a) it is transmitted via the Office's electronic filing system in accordance with 37 CFR 1.6(a)(4) , and (b) includes a certificate of transmission for each piece of correspondence stating the date of transmission, which is prior to the expiration of the set period of time in the Office action.

Signed:

/C. Michelle Tarae/
Reexamination Specialist, Art Unit 3992

Conferees:

/JEFFREY D CARLSON/
Primary Examiner, Art Unit 3992

/ANDREW J. FISCHER/
Supervisory Patent Reexamination Specialist, Art Unit 3992