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

7590 07/29/2025

Hecht Partners LLP
125 Park Avenue,
25th Floor
New York, NY 10017

EXAMINER
TARAE, CATHERINE MICHELLE

ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
07/29/2025	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.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

DO NOT USE IN PALM PRINTER

(THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS)

Quinn Emanuel Urquhart & Sullivan LLP
c/o James M. Glass
51 Madison Ave.
22nd Floor
New York, NY 10010

EX PARTE REEXAMINATION COMMUNICATION TRANSMITTAL FORM

REEXAMINATION CONTROL NO. *90/015,052* .

PATENT UNDER REEXAMINATION *8352730* .

ART UNIT *3992* .

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above identified *ex parte* reexamination proceeding (37 CFR 1.550(f)).

Where this copy is supplied after the reply by requester, 37 CFR 1.535, or the time for filing a reply has passed, no submission on behalf of the *ex parte* reexamination requester will be acknowledged or considered (37 CFR 1.550(g)).

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 30 June 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.
2. ☐ Information Disclosure Statement, PTO/SB/08.
3. ☐ Interview Summary, PTO-474.
4. ☐ _____.

Part II SUMMARY OF ACTION

1a. ☑ Claims 18-34 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 18-34 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 amendments on March 8, 2025 ("March 2025 Amendments"). These amendments have been 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 ("April 28, 2025 Order"). 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.

A Non-Final Office Action addressing amended claims 1-17 was mailed May 20, 2025. The previous rejection under Ludtke was withdrawn and a new rejection under Burger was applied.

PO submitted amendments on June 30, 2025 ("June 2025 Amendments") canceling claims 1-17 and renumbering them as 18-34. These amendments have been entered.

This is another Non-Final Office Action addressing claims 18-34 in light of PO's Remarks filed June 30, 2025 ("Remarks III") and reapplying the rejections of Ludtke and Burger in light of several Patent Trial and Appeal Board ("PTAB") proceedings identified below.

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.

Table 1: Related IPRs for U.S. Pat. No. 8,352,730

Proceeding #	IPR	References	Claims	Status[1]
1	IPR2024-01486	Burger Burger, Robinson	1, 2, 4-9, 11, 12, 14-17 3, 10, 13	Institution Denied. Discretionary denial.
2	IPR2024-01333 joined with IPR2024-00232	Ludtke Ludtke, Kon	1, 2, 4-6, 8, 9, 11, 12, 14-17 3, 10, 13	Terminated. Adverse judgement.
3	IPR2024-01326	Ludtke Ludtke, Kon	1, 2, 4-6, 8, 9, 11, 12, 14-17 3, 10, 13	Institution Denied. Petitioner asked to institute only if IPR '775 was denied. IPR '775 was instituted.
4	IPR2024-00775	Burger Burger, Robinson	1, 2, 4-9, 11, 12, 14-17 3, 10, 13	Terminated. Adverse judgement.
5	IPR2021-01444	Scott, Russell, Lapsley Scott, Russell, Lapsley, Robinson Scott, Russell, Lapsley, Rhoads Berardi, Rosen, Shreve, Kinoshita	1, 2, 4-9, 11 3, 10 6 1-2, 4-6, 8-9, and 11	Institution Denied. Petitioner did not show reasonable likelihood of prevailing.

[1] As of July 21, 2025.

Table 2: Related IPRs for U.S. Pat. No. 8,886,954

Proceeding #	IPR	References	Claims	Status[2]
6	IPR2024-01485	Burger Burger, Robinson	1, 2, 4, 5, 7-13, 15, 16, 18-24, 26-29 3, 14, 17	Institution Denied. Discretionary denial.
7	IPR2024-01334	Ludtke Ludtke, Kon	1, 2, 4-7, 10, 12, 13, 15, 16, 18, 19, 22-27 3, 14, 17	FWD. Claims unpatentable.
8	IPR2024-01327	Ludtke	1, 2, 4-7, 10, 12, 13, 15, 16, 18, 19, 22-27	Institution Denied. Discretionary denial.
9	IPR2024-00846	Burger Burger, Robinson Burger, Orsini	1, 2, 4, 5, 7-13, 15, 16, 18-24, 26-29 3, 14, 17 6, 25	Trial Instituted.
10	IPR2024-00233 joined with IPR2024-01334	Ludtke Ludtke, Kon	1, 2, 4-7, 10, 12, 13, 15, 16, 18, 19, 22-27 3, 14, 17	Pending Director Review.

[2] As of July 21, 2025.

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.[3] 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:

[3] 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 Objections

Claims 18-34 are objected to for failing to comply with 37 CFR 1.530 (f), which says,

> "Changes shown by markings. Any changes relative to the patent being reexamined which are made to the specification, including the claims, must include the following markings:
> (1) The matter to be omitted by the reexamination proceeding must be enclosed in brackets; and
> (2) The matter to be added by the reexamination proceeding must be underlined."

As such, claims 18-34 must be completely underlined to show they are new claims relative to the '730 Patent.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46

USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on nonstatutory double patenting provided the reference application or patent either is shown to be commonly owned with the examined application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement. See MPEP § 717.02 for applications subject to examination under the first inventor to file provisions of the AIA as explained in MPEP § 2159. See MPEP § 2146 *et seq.* for applications not subject to examination under the first inventor to file provisions of the AIA. A terminal disclaimer must be signed in compliance with 37 CFR 1.321(b).

The filing of a terminal disclaimer by itself is not a complete reply to a nonstatutory double patenting (NSDP) rejection. A complete reply requires that the terminal disclaimer be accompanied by a reply requesting reconsideration of the prior Office action. Even where the NSDP rejection is provisional the reply must be complete. See MPEP § 804, subsection I.B.1. For a reply to a non-final Office action, see 37 CFR 1.111(a). For a reply to final Office action, see 37 CFR 1.113(c). A request for reconsideration while not provided for in 37 CFR 1.113(c) may be filed after final for consideration. See MPEP §§ 706.07(e) and 714.13.

The USPTO Internet website contains terminal disclaimer forms which may be used. Please visit www.uspto.gov/patent/patents-forms. The actual filing date of the

application in which the form is filed determines what form (e.g., PTO/SB/25, PTO/SB/26, PTO/AIA/25, or PTO/AIA/26) should be used. A web-based eTerminal Disclaimer may be filled out completely online using web-screens. An eTerminal Disclaimer that meets all requirements is auto-processed and approved immediately upon submission. For more information about eTerminal Disclaimers, refer to www.uspto.gov/patents/apply/applying-online/eterminal-disclaimer.

Claims 18-34 are rejected on the ground of nonstatutory double patenting as being unpatentable over claims 1-29 of U.S. Patent No. 8,886,954. Although the claims at issue are not identical, they are not patentably distinct from each other because while claim 18 of the '052 Reexam recites "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 1 of the '954 Patent omits this limitation. While both claims recite receiving an access message at/by an application from the agent allowing the user access to the application, claim 18 of the '052 Reexam recites this is in response to authentication of the one or more codes and the other data values by the agent. Thus, the claims are obvious variants of each other. The table below shows the similarities in scope for each claim, using the first independent claim as exemplary.

Claim 18 of the '052 Reexam	Claim 1 of the '954 Patent
A method for verifying a user during authentication of an integrated device, comprising the steps of:	A method comprising:
<u>persistently storing biometric data of the user and a plurality of codes and other data values</u>	<u>persistently storing biometric data of a user and a plurality of codes and other data values</u>

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;	comprising a device ID code uniquely identifying an integrated device and a secret decryption value in a tamper proof format written to a storage element on the integrated device that is not capable of being subsequently altered;
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;	
responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan;	responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan;
comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;	comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;
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	responsive to a determination that the scan data matches the biometric data, wirelessly sending one or more codes and other values from the plurality of codes and other data values for authentication to a third party that operates a trusted authority, wherein the one or more codes and other data values includes the device ID code; and
responsive to authentication of the one or more codes and the other data values by the	receiving, at an application, an access message from the trusted authority indicating

agent, receiving an access message from the agent allowing the 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.	that the trusted authority successfully authenticated the one or more codes and other data values sent to the third party and allowing the user access to the application.

Claim 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 18, 19, 21-26, 29, and 31-34 are rejected under pre-AIA 35 U.S.C. 102(e) as being anticipated by U.S. Pub. No. 2005/0050367 to Burger et al. ("Burger")

As per claim 18, 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." Burger's Pocket Vault 102 is an integrated device at least because it integrates a plurality of devices such as a finger print scanner, token/token port, a user input device, memories, and a display. See Fig. 2.

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." See 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."

[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."

[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."

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.

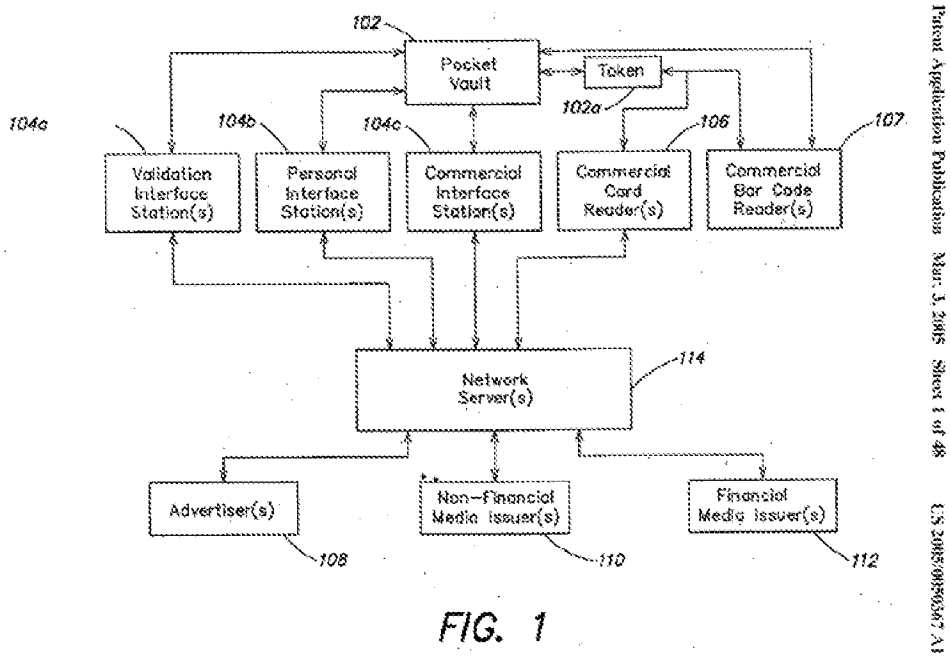


Fig. 1 of Burger

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

As evidenced by the citations below, the Pocket Vault is an application the user accesses as it contains software and files in the form of credit cards, driver's license, library card, frequent flier card, program for RFID functionality, and advertisements.

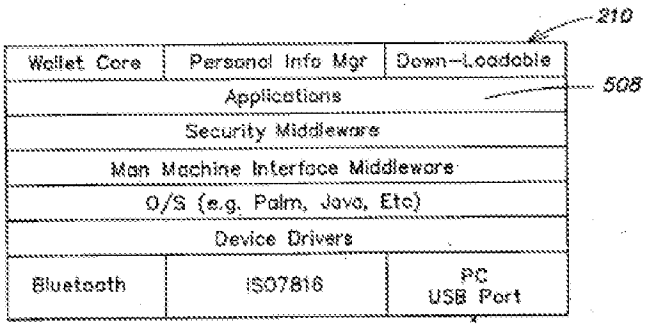


FIG. 5

Fig. 5 shows the memory of the Pocket Vault containing applications 508, Wallet Core, and Personal Info Mgr

[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. For example, in response to an interrogation signal from the RFID interrogator 116 (e.g., an interrogator of an automated toll booth), the Pocket Vault 102 (if authorized) can return an appropriate RF signal to authorize payment of the required fee for the toll. In some embodiments, the RFID functionality of the Pocket Vault 102 can be altered by the user so that user is permitted to select the personality of the RFID tag that is embodied by the device. The user may, for example, first use the Pocket Vault 102 as an RFID tag to authorize payment of a toll, and later use the same Pocket Vault 102 as an RFID tag to authorize payment at a service station."

[0109] "To permit the Pocket Vault holder to select from among the various media stored in memory of the Pocket Vault 102, the Pocket Vault 102 may comprise a display (not shown in FIG. 1). By employing either a display having a user-manipulable touch screen or a separate user input device (not shown in FIG. 1), a Pocket Vault holder can 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."

[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…"

[0238] "When, at the step 1002, it is determined that an advertisement has been scheduled, the routine 722 proceeds to a step 1004, wherein the scheduled advertisement is displayed, for example, for approximately two seconds. FIG. 26I shows an example of how the display 216 may appear when such an advertisement is displayed." See. Fig. 10A.

[0255] "When, at the step 1022, it is determined that the holder has selected a media from the displayed menu items, the routine 722 proceeds to a step 1024, wherein the selected media is displayed to the holder on the display 216. The selected media may, for example, be a particular credit card, in which case the name of the credit card and/or the logo for the credit card and any preferred advertisement, specials, etc., for the selected media may be displayed to the holder as well."

Example 2: the interface stations are applications

As evidenced by the citations below, the interface stations are applications the user accesses as they contain software and files in the form of instructions for implementing certain functionalities by the controller, credit cards, and advertisements. The interface

stations also allow the sending of information between the Pocket Vault and network server.

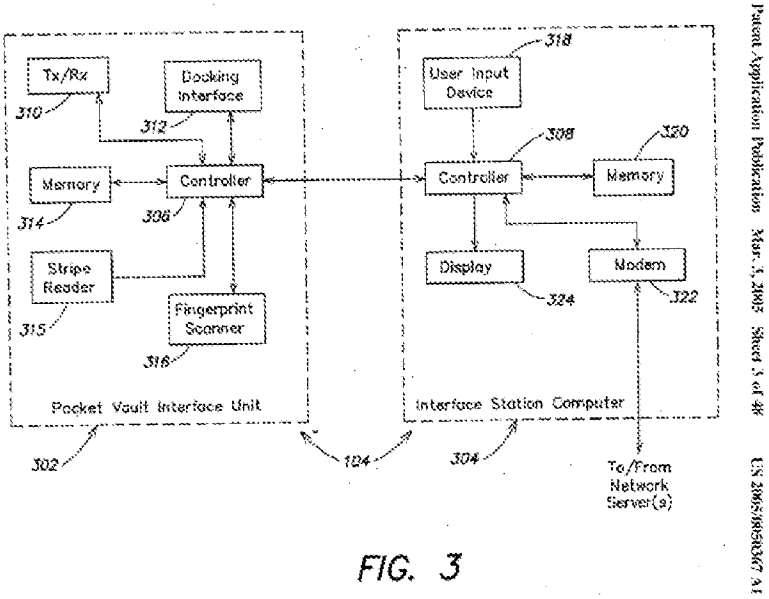


Fig. 3 shows the components of an interface station 104

[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.

[0137] "As shown in FIG. 3, each interface station 104 may include both an 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…"

[237] "The advertiser 108 (FIG. 1) may, for example, have made arrangements with the company operating the network server 114 to have certain advertising information uploaded to Pocket Vaults 102 when particular Pocket Vault holders interface their Pocket Vaults 102 with their personal interface stations 104b."

[320] "If placed in the personal interface station 104c, such account numbers may be automatically revealed (e.g., through detection of an encrypted cookie on the interface station computer 304 of the personal interface station 104c)."

[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

[0679]"If it does involve use of a Pocket Vault credit card, this card may, for example, be accessed while the Pocket Vault 102 is interfaced with the holder's personal interface station 104b."

As per claim 19, Burger discloses **the method of claim 18, 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 21, Burger discloses **the method of claim 18, 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 22, Burger discloses **the method of claim 18, 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 23, Burger discloses **the method of claim 18, 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 24, Burger discloses **the method of claim 18, 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 25 recites substantially similar subject matter to that of claim 18; therefore, claim 25 is rejected based on the same rationale as claim 18.

As per claim 26, Burger discloses **the integrated device of claim 25, wherein the one or more codes and the other data values are transmitted to the agent over a network.**

See claim 19.

Claim 29 recites substantially similar subject matter to that of claim 18; therefore, claim 29 is rejected based on the same rationale as claim 18.

As per claim 31, Burger discloses **the method of claim 29, 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 32 recites substantially similar subject matter to that of claim 18; therefore, claim 32 is rejected based on the same rationale as claim 18.

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 33, Burger discloses **the system of claim 32, 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 <u>request has been received to register a new Pocket Vault holder</u>, 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."

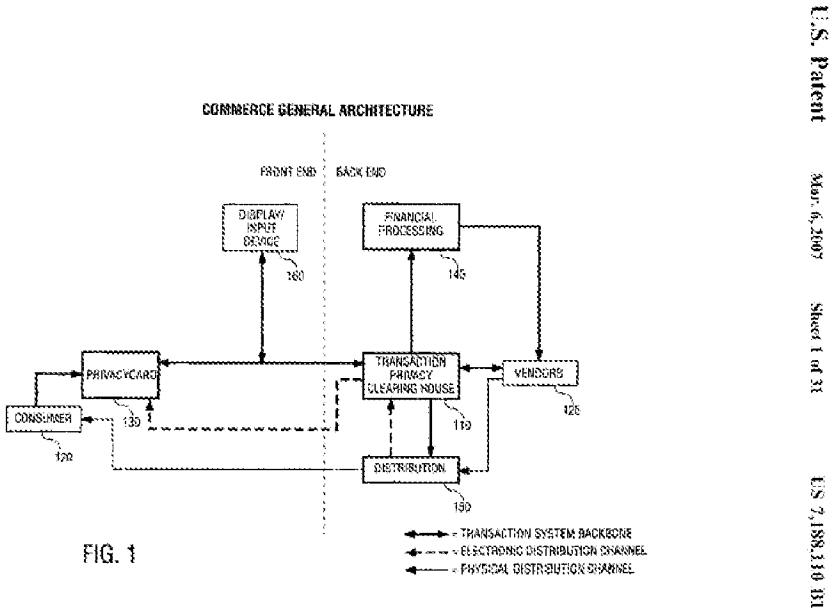
[0585] "After the step 3204, the routine 3020 proceeds to a step 3206, wherein the new holder is prompted to apply his or her fingerprint to the fingerprint scanner 220 while the Pocket Vault 102 is interfaced with the interface unit 302."

As per claim 34, Burger discloses **the system of claim 32, 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.

Claims 32-34 are rejected under pre-AIA 35 U.S.C. 102(a,e) as being anticipated by U.S. Pat. No. 7,188,110 to Ludtke et al. ("Ludtke")

As per claim 32, Ludtke discloses **a system, comprising:**



<u>Fig. 1 of Ludtke shows the system includes the transaction privacy clearing house (TPCH) (110) (i.e. third-party trusted authority), the consumer (120) and vendors (125)</u>

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 confirmation succeeds, <u>the device writes the fingerprint image data into write-once memory, or other memory that is protected from accidental modification</u>." (19:35-40)

"The user connects to and performs transactions with the eCommerce system through a transaction device which has a unique identifier (ID)." (3:32-35)

"The device may also be encoded with a secret PIN code that must be entered to begin the user-confirmation procedure." (18:61-63)

"One means of achieving this is for the transaction device to be manufactured with several hundred unique transaction device ID values stored in its permanent memory. In this embodiment, the TPCH may maintain a copy of these values, so it knows that whenever a transaction arrives with one of these values, the TPCH knows which transaction device, and hence which user, the transaction it associated with." (30:20-27)

"Another embodiment of security in a data structure is shown in FIG. 26 at 2609, where a different PKI key pair may be used for each set of password data 2616. Thus, in this structure a phone number 2610, a password ID 2612, a back-end public key 2614, and password data 2616 are maintained on an individual key basis. Thus, even if one of the key pairs were compromised, the additional keys would still protect other records in the device. Although more complex in nature, this complexity may be hidden from the user by use of automatic updates and back-end programming." (37:57-67; Fig. 26)

"In the embodiment as illustrated in FIG. 26, at 2609 there may be a one-to-one relationship between a password and a public key owned by the back-end system. A password exchange protocol may enable the back-end system to demand a password by its password ID 2612. In response, the device may encrypt the specified password using the back-end system's public key, and transmit it to the back-end system." (38:1-8)

"The device and back-end system each have one pair of session keys a public key and a private key." (38:36-38)

It is noted the term "biometric key" refers to the device the user uses (known in other claims as an "integrated device." (the '730 Patent, Figs. 1-2; Goldberg Dec, ¶108)

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, and

"At 3102 the user may start a device, such as a digital wallet (DW). At 3104 the DW checks to see if a fingerprint has been detected. If not then the DW loops back looking for a fingerprint. If a fingerprint has been detected, then at 3106 a check is made to see if it matches a stored authorized fingerprint." (39:49-54)

"The consumer access device 2802 has an LCD screen 2804 showing text, a biometric identification unit, in this embodiment as a Fingerprint Identification Unit (FIU) 2806 and a touchpad 2808 for user input. The user of the consumer access device 2802 would be authorized access to the device 2802 if the device recognized the user after the user had pressed his finger against the FIU 2806." (39:21-27; Figs. 28 and 31)

"One means of achieving this is for the transaction device to be manufactured with several hundred unique transaction device ID values stored in its permanent memory. In this embodiment, the TPCH may maintain a copy of these values, so it knows that whenever a transaction arrives with one of these values, the TPCH knows which transaction device, and hence which user, the transaction it associated with." (30:20-27, where the unique transaction device ID value is the one or more codes that is wirelessly sent)

"In order to maintain confidentiality of the identity of the user, the transaction device information does not provide user identification information. Thus, the vendor or other entities do not have user information but rather transaction device information. The TPCH 110 maintains a secure database of transaction device information and user information." (6:45-51)

"The user connects to and performs transactions with the eCommerce system through a transaction device which has a unique identifier (ID)… The transaction device, e.g., the privacy card, is the identity that may be known to a vendor. The highly secured location, accessible through or part of a transaction processing clearing house (TPCH), provides the transaction processing clearing house the information necessary to authorize a transaction. For example, the transaction processing clearing house may access relevant account information to authorize transactions. However, the identity of the user

is not revealed externally so that confidentiality of the user's identity is maintained." (3:32-47)

"In this embodiment, a transaction privacy clearing house (TPCH) 110 interfaces a user 120 and a vendor 125. In this particular embodiment, a transaction device, e.g., a privacy card 130, is used to maintain the privacy of the user while enabling the user to perform transactions. The transaction device information is provided to the TPCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed." (6:36-44)

"One embodiment of the TPCH 600 is illustrated by FIG. 6. The incoming communications mechanism 605 and outgoing communications mechanism 610 are the means of communicating with external retailers and vendors, as well as the transaction device such as the digital wallet. A variety of communication devices may be used, such as the Internet, direct dial-up modem connections, wireless or cellular signals, etc." (9:35-42)

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

"The identification by the biometric device may be achieved in a variety of ways, as discussed above. For example, biometric identification, may be, fingerprint, retinal scan, voice, DNA, hand profile, face recognition, etc." (35:61-64)

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

"In order to maintain confidentiality of the identity of the user, the transaction device information does not provide user identification information. Thus, the vendor or other entities do not have user information but rather transaction device information. The TPCH 110 maintains a secure database of transaction device information and user information." (6:45-51)

"The user connects to and performs transactions with the eCommerce system through a transaction device which has a unique identifier (ID)… The transaction device, e.g., the privacy card, is the identity that may be known to a vendor. The highly secured location, accessible through or part of a transaction processing clearing house (TPCH), provides the transaction processing clearing house the information necessary to authorize a transaction. For example, the transaction processing clearing house may access relevant account information to authorize transactions. However, the identity of the user is not revealed externally so that confidentiality of the user's identity is maintained." (3:32-47)

"In this embodiment, a transaction privacy clearing house (TPCH) 110 interfaces a user 120 and a vendor 125. In this particular embodiment, a transaction device, e.g., a privacy card 130, is used to maintain the privacy of the user while enabling the user to perform transactions. The transaction device information is provided to the TPCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed." (6:36-44)

"One embodiment of the TPCH 600 is illustrated by FIG. 6. The incoming communications mechanism 605 and outgoing communications mechanism 610 are the means of communicating with external retailers and vendors, as well as the transaction device such as the digital wallet. A variety of communication devices may be used, such as the Internet, direct dial-up modem connections, wireless or cellular signals, etc." (9:35-42)

"Authentication unit" is software executed by a processor on the integrated device that is responsible for sending the device ID code or additional code to the third party trusted authority to authenticate the user and device. (the '730 Patent at 5:9-26; Goldberg Dec, ¶110)

responsive to the device ID code being authenticated, the authentication unit receiving an access message by an application from the agent allowing the user to access the 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.

"transaction device information is provided to the TPCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed" (6:41-44).

"TPCH, at step 1520, confirms the transaction and provides the confirmation to the vendor and the user. At step 1525, the vendor completes the transaction without the knowledge of the user" (27:13-16)

"After validating that the transaction device is in good standing and that the selected account has sufficient funds for the transaction, the TPCH issues a transaction confirmation back to the personal POS terminal. The personal POS terminal reflects the transaction confirmation back to the web browser and the transaction device. The transaction device may display a transaction confirmation to the user and may additionally record the transaction in its local storage. . . Secure distribution of physical (or electronic) content to the user is performed once the transaction is authorized." (29:15-30) Here, the transaction confirmation is the "access message" and the content the user can access at the web browser is the "application."

"If the product purchased is electronic in nature (e.g., software, content such as digital images, stock purchases, etc.) electronic distribution may be used. In one embodiment of electronic distribution, the TPCH 110 functions as the middleman of the distribution channel. This allows the TPCH 110 to retain user privacy by not exposing addressing information and possibly email addresses to third parties. In an embodiment which utilizes a POS terminal and a POS terminal is used for distribution, the content may be encrypted at the source and distributed via the system to the POS terminal wherein the POS terminal subsequently decrypts the distributed material. The POS terminal may then pass the data to an appropriate place desired by the user, for example, to a user controlled device such as PC storage, a digital wallet or a privacy card." (7:42-56)

In the above embodiment, the user would have access to the digital product after they have been authenticated. The digital product can include software and digital images.

"[T]he transaction device can adapt to new services and functionality, either automatically by the transaction device or manually by the user. For example, on a web site the user might click a button that causes new functionality to be downloaded to the transaction device for access at a future time... For example, when arriving at a new airport, the transaction device might download a new service that provides instructions for how to buy a train ticket to certain destinations…For example, once a user has carried out a typical transaction to purchase electronic content, or has used the transaction device to register as a user of digital content that is delivered periodically, the content provider knows the transaction device ID and the electronic content distribution servers." (31:11-52)

Signals 8–11 of Fig. 17 correspond to an access message received by an application (e.g., a webpage with new content).

As per claim 33, Ludtke discloses **the system of claim 32, 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.**

"At 3102 the user may start a device, such as a digital wallet (DW). At 3104 the DW checks to see if a fingerprint has been detected. If not then the DW loops back looking for a fingerprint. If a fingerprint has been detected, then at 3106 a check is made to see if it matches a stored authorized fingerprint." (39:49-54)

"The consumer access device 2802 has an LCD screen 2804 showing text, a biometric identification unit, in this embodiment as a Fingerprint Identification Unit (FIU) 2806 and a touchpad 2808 for user input. The user of the consumer access device 2802 would be authorized access to the device 2802 if the device recognized the user after the user had pressed his finger against the FIU 2806." (39:21-27; Figs. 28 and 31)

As per claim 34, Ludtke discloses **the system of claim 32, 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.**

Item 3110 in Fig. 31 shows an error message if the detected fingerprint does not match with stored data (i.e., cannot be verified).

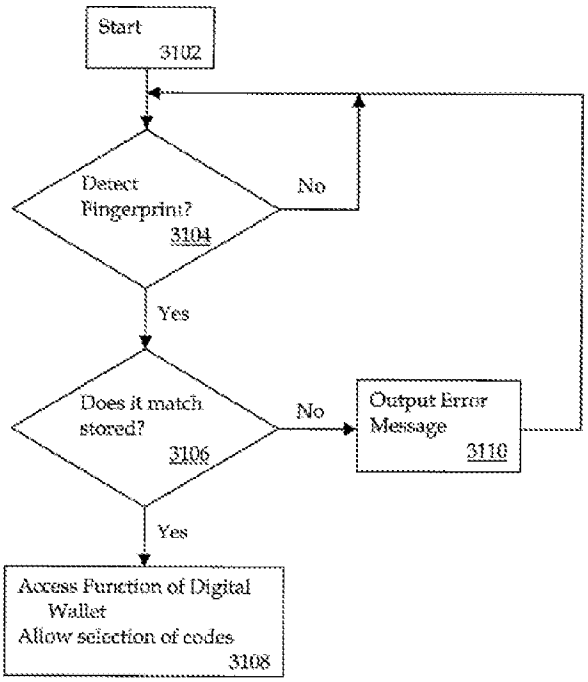


FIG. 31

Fig. 31 of Ludtke describes the process to verify a user of the integrated device using biometric authentication

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

As per claim 28, Burger discloses **the integrated device of claim 25, 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 <u>provide information to the Pocket Vault holder. For example, light emitting diodes (LEDs)</u>, 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 20, 27, and 30 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 20, Burger does not expressly disclose **the method of claim 18, 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 27 and 30 recite substantially similar subject matter to that of claim 20; therefore, claims 10 and 13 are rejected based on the same rationale as claim 20.

Claims 18, 19, 21-26, 28, 29, and 31 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Ludtke and U.S. Pub. No. 2003/0196084 to Okereke et al. ("Okereke")

As per claim 18, Ludtke discloses **a method for verifying a user during authentication of an integrated device, comprising the steps of:**

"A method of identifying an authorized user with a biometric device and enabling the authorized user to access private information over a voice network is disclosed." (abstract) Also see Figs. 7B-7C as examples of an integrated device.

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;

"If confirmation succeeds, the device writes the fingerprint image data into write-once memory, or other memory that is protected from accidental modification." (19:35-40)

"The user connects to and performs transactions with the eCommerce system through a transaction device which has a unique identifier (ID)." (3:32-35)

"The device may also be encoded with a secret PIN code that must be entered to begin the user-confirmation procedure." (18:61-63)

"One means of achieving this is for the transaction device to be manufactured with several hundred unique transaction device ID values stored in its permanent memory. In this embodiment, the TPCH may maintain a copy of these values, so it knows that whenever a transaction arrives with one of these values, the TPCH knows which transaction device, and hence which user, the transaction it associated with." (30:20-27)

"Another embodiment of security in a data structure is shown in FIG. 26 at 2609, where a different PKI key pair may be used for each set of password data 2616. Thus, in this structure a phone number 2610, a password ID 2612, a back-end public key 2614, and password data 2616 are maintained on an individual key basis. Thus, even if one of the key pairs were compromised, the additional keys would still protect other records in the device. Although more complex in nature, this complexity may be hidden from the user by use of automatic updates and back-end programming." (37:57-67; Fig. 26)

"In the embodiment as illustrated in FIG. 26, at 2609 there may be a one-to-one relationship between a password and a public key owned by the back-end system. A password exchange protocol may enable the back-end system to demand a password by its password ID 2612. In response, the device may encrypt the specified password using the back-end system's public key, and transmit it to the back-end system." (38:1-8)

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;

"The identification by the biometric device may be achieved in a variety of ways, as discussed above. For example, biometric identification, may be, fingerprint, retinal scan, voice, DNA, hand profile, face recognition, etc." (35:61-64)

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

"At 3102 the user may start a device, such as a digital wallet (DW). At 3104 the DW checks to see if a fingerprint has been detected. If not then the DW loops back looking for a fingerprint. If a fingerprint has been detected, then at 3106 a check is made to see if it matches a stored authorized fingerprint." (39:49-54)

"The consumer access device 2802 has an LCD screen 2804 showing text, a biometric identification unit, in this embodiment as a Fingerprint Identification Unit (FIU) 2806 and a touchpad 2808 for user input. The user of the consumer access device 2802 would be authorized access to the device 2802 if the device recognized the user after the user had pressed his finger against the FIU 2806." (39:21-27; Figs. 28 and 31)

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

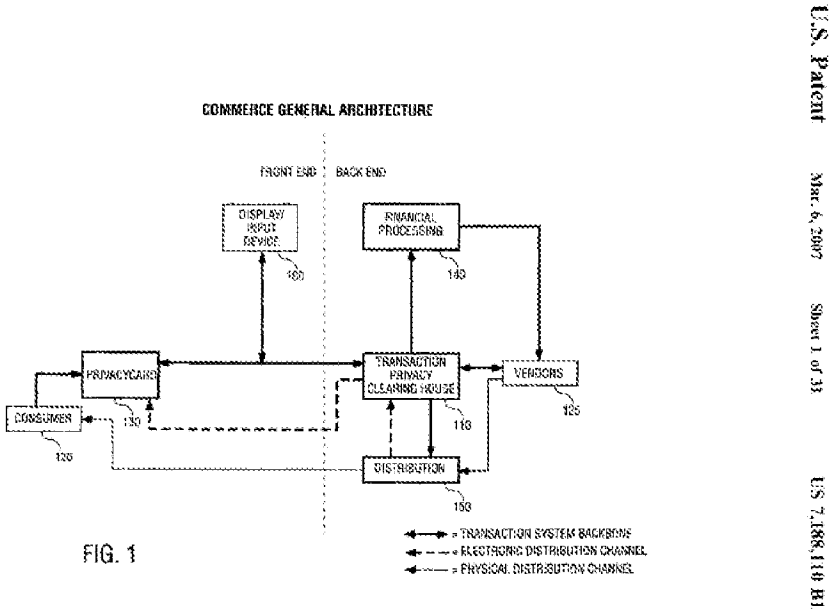
"One means of achieving this is for the transaction device to be manufactured with several hundred unique transaction device ID values stored in its permanent memory. In this embodiment, the TPCH may maintain a copy of these values, so it knows that whenever a transaction arrives with one of these values, the TPCH knows which transaction device, and hence which user, the transaction it associated with." (30:20-27, where the unique transaction device ID value is the one or more codes that is wirelessly sent)

"In order to maintain confidentiality of the identity of the user, the transaction device information does not provide user identification information. Thus, the vendor or other entities do not have user information but rather transaction device information. The TPCH 110 maintains a secure database of transaction device information and user information." (6:45-51)

"The user connects to and performs transactions with the eCommerce system through a transaction device which has a unique identifier (ID)… The transaction device, e.g., the privacy card, is the identity that may be known to a vendor. The highly secured location, accessible through or part of a transaction processing clearing house (TPCH), provides the transaction processing clearing house the information necessary to authorize a transaction. For example, the transaction processing clearing house may access relevant account information to authorize transactions. However, the identity of the user is not revealed externally so that confidentiality of the user's identity is maintained." (3:32-47)

"In this embodiment, a transaction privacy clearing house (TPCH) 110 interfaces a user 120 and a vendor 125. In this particular embodiment, a transaction device, e.g., a privacy card 130, is used to maintain the privacy of the user while enabling the user to perform transactions. The transaction device information is provided to the TPCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed." (6:36-44)

"One embodiment of the TPCH 600 is illustrated by FIG. 6. The incoming communications mechanism 605 and outgoing communications mechanism 610 are the means of communicating with external retailers and vendors, as well as the transaction device such as the digital wallet. A variety of communication devices may be used, such as the Internet, direct dial-up modem connections, wireless or cellular signals, etc." (9:35-42)



<u>Fig. 1 of Ludtke showing the transaction privacy clearing house (TPCH) (110) (i.e. third-party trusted authority) separate from the consumer (120) and vendors (125)</u>

Ludtke discloses use of a device ID, secret PIN codes, and private keys to authorize users as discussed above. Ludtke further discloses sending the device ID to the TPCH as part of the transaction as discussed above; however, if Ludtke is seen as not describing the specific "transaction device information" that is provided to the TPCH or storing the secret decryption value, Okereke discloses this.

[Okereke ¶0025] "In so doing, a <u>unique identifier for the wireless product to be employed is passed as at 210 to the proxy server 125 program for authorization</u>. The wireless product 165 can be a personal digital assistant (PDA), laptop, cellular telephone or any other device capable of remote wireless communication. The <u>unique identifier can be a serial number or SIM</u>. number, for example. If the unique identifier is one which the proxy server program identifies as being acceptable, the proxy server program will send approval as at 220 to the desktop 140, which executes functionality to make a <u>key exchange</u> as at 225, such as, for example, a Diffie Hellman Key Exchange. This key is used to encrypt information sent to the server using AES (Advanced

Encryption Standard)… In another embodiment, this key is used as part of a shared secret between the server and the client. This shared secret is used to generate a session key. The new session key ensures that conversations cannot be eavesdropped if the key has been compromised."

[Okereke ¶0026] "The wireless device 165 is provided with a memory, processor, and input/output means as is commonly known. Using the session key, the user can then encrypt credential information, its PKI certificate 180 and private key, and forward this information to the proxy server 125 as at 230 in FIGS. 4 and 5. In one embodiment of the invention, the encrypted information is sent to the proxy server via secure IP network. The credential information or authentication measure can be something the user has (such as a swipe card), something the user is (such as represented by a fingerprint scan), or something the user knows (such as a password or pass phrase). In one embodiment, the credential information is a user name and password."

Okereke and Ludtke are analogous references as both are concerned with user/device authentication and secure communications/transactions. (Ludtke, abstract; Okereke, abstract)

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to modify Ludtke to have the "transaction device information" include a device ID as well as store secret decryption value as doing so provides additional data with which to authenticate the user/device before allowing subsequent transactions, thereby enhancing the security of the transaction. (Ludtke, 37:29-43, "Because of the sensitive nature of the information being transferred, such as access codes, PINs, etc., it may be desired to use a secure communication means and/or encryption to lessen the possibility of unauthorized use of the information.")

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, 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.

"transaction device information is provided to the TPCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed" (6:41-44).

"TPCH, at step 1520, confirms the transaction and provides the confirmation to the vendor and the user. At step 1525, the vendor completes the transaction without the knowledge of the user" (27:13-16)

"After validating that the transaction device is in good standing and that the selected account has sufficient funds for the transaction, the TPCH issues a transaction confirmation back to the personal POS terminal. The personal POS terminal reflects the transaction confirmation back to the web browser and the transaction device. The transaction device may display a transaction confirmation to the user and may additionally record the transaction in its local storage. . . Secure distribution of physical (or electronic) content to the user is performed once the transaction is authorized." (29:15-30) Here, the transaction confirmation is the "access message" and the content the user can access at the web browser is the "application."

"If the product purchased is electronic in nature (e.g., software, content such as digital images, stock purchases, etc.) electronic distribution may be used. In one embodiment of electronic distribution, the TPCH 110 functions as the middleman of the distribution channel. This allows the TPCH 110 to retain user privacy by not exposing addressing information and possibly email addresses to third parties. In an embodiment which utilizes a POS terminal and a POS terminal is used for distribution, the content may be encrypted at the source and distributed via the system to the POS terminal wherein the POS terminal subsequently decrypts the distributed material. The POS terminal may then pass the data to an appropriate place desired by the user, for example, to a user controlled device such as PC storage, a digital wallet or a privacy card." (7:42-56)

In the above embodiment, the user would have access to the digital product after they have been authenticated. The digital product can include software and digital images.

"[T]he transaction device can adapt to new services and functionality, either automatically by the transaction device or manually by the user. For example, on a web site the user might click a button that causes new functionality to be downloaded to the transaction device for access at a future time... For example, when arriving at a new airport, the transaction device might download a new service that provides instructions for how to buy a train ticket to certain destinations...For example, once a user has carried out a typical transaction to purchase electronic content, or has used the transaction device to register as a user of digital content that is delivered periodically, the content provider knows the transaction device ID and the electronic content distribution servers." (31:11-52)

Signals 8–11 of Fig. 17 correspond to an access message received by an application (e.g., a webpage with new content).

As per claim 19, Ludtke discloses **the method of claim 18, wherein the one or more codes and the other data values are transmitted to the agent over a network.**

"One means of achieving this is for the transaction device to be manufactured with several hundred unique transaction device ID values stored in its permanent memory. In this embodiment, the TPCH may maintain a copy of these values, so it knows that whenever a transaction arrives with one of these values, the TPCH knows which transaction device, and hence which user, the transaction it associated with." (30:20-27, where the unique transaction device ID value is the one or more codes that is transmitted to the agent over the network)

"One embodiment of the TPCH 600 is illustrated by FIG. 6. The incoming communications mechanism 605 and outgoing communications mechanism 610 are the means of communicating with external retailers and vendors, as well as the transaction device such as the digital wallet. A variety of communication devices may be used, such

as the Internet, direct dial-up modem connections, wireless or cellular signals, etc." (9:35-42)

"One embodiment of a system is illustrated in FIG. 1. In this embodiment, a transaction privacy clearing house (TPCH) 110 interfaces a user 120 and a vendor 125. In this particular embodiment, a transaction device, e.g., a privacy card 130, is used to maintain the privacy of the user while enabling the user to perform transactions. The transaction device information is provided to the TPCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed." (6:36-44)

As per claim 21, Ludtke discloses **the method of claim 18, wherein the one or more codes and the other data values indicate that the biometric verification was successful.**

"At 3102 the user may start a device, such as a digital wallet (DW). At 3104 the DW checks to see if a fingerprint has been detected. If not then the DW loops back looking for a fingerprint. If a fingerprint has been detected, then at 3106 a check is made to see if it matches a stored authorized fingerprint." (39:49-54)

"The consumer access device 2802 has an LCD screen 2804 showing text, a biometric identification unit, in this embodiment as a Fingerprint Identification Unit (FIU) 2806 and a touchpad 2808 for user input. The user of the consumer access device 2802 would be authorized access to the device 2802 if the device recognized the user after the user had pressed his finger against the FIU 2806." (39:21-27; Figs. 28 and 31)

As per claim 22, Ludtke discloses **the method of claim 18, wherein the biometric data and the scan data are both based on a fingerprint scan by the user.**

"The identification by the biometric device may be achieved in a variety of ways, as discussed above. For example, biometric identification, may be, fingerprint, retinal scan, voice, DNA, hand profile, face recognition, etc." (35:61-64)

As per claim 23, Ludtke discloses **the method of claim 18, further comprising: establishing a secure communication channel prior to sending the one or more codes and the other data values for authentication.**

"The security management function 620 ensures secure communications among the components internal to the TPCH 600 and the entities external to the TPCH 600. This function includes participating in secure communications protocols to open and maintain secure connections. This ensures that only authorized entities are allowed access to data and that only authorized transaction devices can execute transactions against a user's account." (9:52-59)

As per claim 24, Ludtke discloses **the method of claim 18, further comprising: receiving a request for the one or more codes and the other data values without a request for biometric verification; and 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.**

Per the Goldberg Dec, Ludtke envisions using different forms of authentication other than biometric information. In the situation where a PIN was used, there would be no need for a request for biometric information. (¶90)

"The transaction device enhances security by authenticating the user of the card prior to usage such that if a card is lost or stolen, it is useless in the hands of an unauthorized person. One means of authentication is some kind of PIN code entry. Alternately, authentication may be achieved by using more sophisticated technologies such as a biometric solution (e.g., fingerprint recognition)." (4:65-5:1)

Claim 25 recites substantially similar subject matter to that of claim 18; therefore, claim 25 is rejected based on the same rationale as claim 18.

Further, the "verification unit" will be the portion of memory and instructions that verify the biometric information. (Goldberg Dec ¶94). A POSITA would recognize that the verification unit would be in communication with the memory, since the biometric information that the verification unit compares with received biometric information is stored in the memory for comparison. (*Id.*)

As per claim 26, Ludtke 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.

As per claim 28, Ludtke discloses **the integrated device of claim 25, wherein the verifier comprises: an LED to be activated for requesting the biometric scan.**

Per the Goldberg Dec, Ludtke discloses notifications to request a biometric scan and it would be obvious to use an LED. In describing the fingerprint scanner, Ludtke indicates that at "various times during interaction, the user is prompted to supply a fingerprint recognition sample." (14:40-42) A POSITA would recognize that the prompt can be in a number of ways that would be consistent with alerts on a mobile device. One of the common alert mechanisms in a mobile device is an LED. (Goldberg Dec ¶97)

Ludtke further discloses a user interface (Fig. 28) with a screen asking the user what they wish to do:

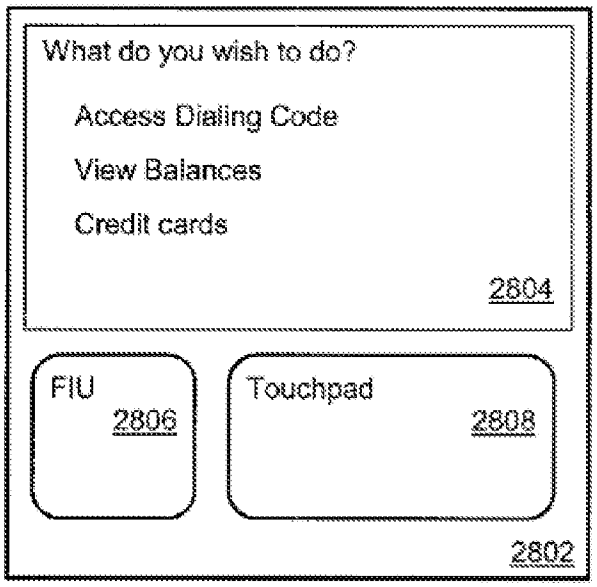


FIG. 28

A POSITA would have recognized that user interface screens such as these are very often implemented with an LED screen, and an LED screen would be the obvious and well known choice for alerting the user.

Claim 29 recites substantially similar subject matter to that of claim 18; therefore, claim 29 is rejected based on the same rationale as claim 18.

Further, since the claim does not indicate what "receives" the one or more codes, the receiver can be the device itself, a memory or processor on the device, or another device receiving codes. (Goldberg Dec, ¶101) Additionally, users are biometrically verified through the use of fingerprint data to secure the device. (*Id.*)

As per claim 31, Ludtke discloses **the method of claim 29, 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.

"The transaction device enhances security by authenticating the user of the card prior to usage such that if a card is lost or stolen, it is useless in the hands of an unauthorized person. One means of authentication is some kind of PIN code entry. Alternately, authentication may be achieved by using more sophisticated technologies such as a biometric solution (e.g., fingerprint recognition)." (4:65-5:1)

Claims 20, 27 and 30 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Ludtke, Okereke, and U.S. Pub. No. 2003/0177102 to Robinson. ("Robinson")

As per claim 20, Ludtke and Okereke do 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:

"A presenter presents a biometric sample obtained from the presenter's person and the presenter's system ID number to conduct age verifications for purchase of or access to age-restricted goods or services. This data is used to authenticate the presenter's age and authorize access to purchase or obtain age-restricted goods or services by matching the presented transaction biometric with at least one registered biometric template and without the use of a man-made identity token." (abstract)

"Referring to FIG. 1, a general architecture overview of a system for age verification using biometric and system ID matching is illustrated. The system includes a verifier

database 124, wherein age verification records are stored, as well as information about authorized points of verification (POVs). The age verification records contain information related to individuals seeking age verification (that is, presenters). Various other records and databases may also be held in the verifier's database." (¶0026)

See also ¶¶0027-29, 32, 66 and 67.

Ludtke, Okereke, and Robinson are analogous references as each seeks to provide user authentication for transactions. (Ludtke, Okereke, and Robinson abstracts)

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to modify the combination of Ludtke and Okereke to include registering an age verification for the user in association with the device ID code as doing so would enhance the authentication process by enabling vendors to add age restrictions to certain transactions. (Robinson, ¶0008 "Since age verification in such a system would be tied to an individual's biometric rather than a token, the chances are minimized that an individual can successfully present false age verification, or that a careless employee can bypass the system. Additionally, such a system would present a form of age verification that could not be lost, stolen, or fabricated.")

Claims 27 and 30 recite substantially similar subject matter to that of claim 20; therefore, claims 27 and 30 are rejected based on the same rationale as claim 20.

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 18-34 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 <u>by an application</u> from the agent allowing the user access to <u>the</u> application" in amended claims 18-34 is expressly disclosed by the Burger reference (see at least ¶¶100, 439, 440, 518). Thus, amended claims 18-34 are estopped as not being patentably distinct from original claims 1-17 which were finally refused in IPR2024-00775.

Response to Arguments

I. <u>Arguments related to Burger</u>

PO's arguments filed June 30, 2025 have been fully considered but they are not persuasive.

A. <u>In the Remarks III, PO argues that Burger does not disclose an access message</u>. (Remarks III at p. 11)

Examiner respectfully disagrees. Although not binding, Examiner hereby adopts the PTAB's rationale from IPR2024-00846 for Granting Institution of *Inter Partes* Review ("IPR-2024-00846 GIIPR") of related U.S. Pat. No. 8,886,954 ("the '954 Patent") dated November 18, 2024.

Although the claims are different, the '954 Patent claim 1 shares similar scope relating to the access message limitation with claim 18 of the '730 Patent. The similar limitations are:

'730 Patent, claim 18	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
'954 Patent, claim 1	receiving, at an application, an access message from the trusted authority indicating that the trusted authority successfully authenticated the one or more codes and other data values sent to the third party and allowing the user access to the application

Table 3: identifying the similar limitations between the '730 Patent and the '954 Patent

After the network server authenticates the user's Pocket Vault ID, the user is granted access to the pocket vault and can then perform a variety of transactions, where the pocket vault is an application since a user can access computer software and files on the pocket vault to enable the user to perform the transactions. (Burger at ¶¶ 108, 109, 114, 127; Figs. 7A-7B, 10A; IPR-2024-00846 GIIPR at pp. 19-25) After authentication, the access message is sent to the pocket vault or to the interface stations indicating the user can access the pocket vault. (Burger at ¶¶ 186, 439, 440, 518; Figs. 7, 24; IPR-2024-00846 GIIPR at pp. 22-24)

Examiner notes the claims do not expressly recite how authentication is performed. Claim 18 recites, in part, "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." This merely recites that "one or more codes" are sent "for authentication," but how the one or more codes are authenticated is not expressly recited.

B. In the Remarks III, PO argues that Burger does not disclose the parties to be a user and an application as required by the claims. (Remarks III at p. 45)

Examiner respectfully disagrees. The claims do not require the parties to be a user and an application. Rather, claim 18 requires a third party trusted authority, where the access message is sent to the application from the agent (of the third party trusted authority). The parties could be the user and the application or could be, for example, the user and vendors, advertisers, non-financial media issuers and financial media issuers. In the case where one of the parties is a vendor, advertiser, non-financial media issuer or financial media issuer, the user requires access to the application to conduct a transaction therewith. This is also consistent with the PTAB's claim interpretation[4].

[4] IPR2024-00775 Granting Institution of *Inter Partes* Review dated Nov. 18, 2024, p. 10, "IPR2024-00232, Paper 10 at 21. There, we determined preliminarily that the entity the petitioner had identified as a third-party trusted authority, regardless of whether it was an active participant in some way in the transaction, was not the user or the vendor/retailer, which was the second party with the application being accessed in the petitioner's theory." IPR2024-00232 Granting Institution of *Inter Partes* Review dated July 24, 2024, p. 11, "Although the trusted key authority in this example is not a principal party to the transaction (here, those parties are the user and the

As discussed above, Burger discloses the network server is the third-party trusted authority between the user of the Pocket Vault (where the user utilizes the Pocket Vault to conduct the transaction) and advertisers, non-financial media issuers and financial media issuers as shown in Fig. 1. Thus, Burger can be viewed as having the parties be a user and the advertisers, non-financial media issuers and financial media issuers; or the user and the Pocket Vault (i.e., the application).

II. Arguments related to Ludtke

PO's arguments filed January 27, 2025 have been fully considered but they are not persuasive.

C. In the Remarks II, PO argues that Ludtke does not disclose an access message. (Remarks II at p. 4)

1. Claim Interpretation for Access Message

As discussed above in the office action, Examiner's broadest reasonable claim interpretation ("BRI") of "access message" utilizes the specification of the '730 Patent as a source for the BRI. The '730 Patent at col. 5, lines 23-26 says, "[a]uthentication 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)… However, despite the trusted key authority's active participation, the parties to such a transaction are the customer and the grocery store, not trusted key authority 320."

IPR2024-00233 Final Written Decision dated June 17, 2025, p. 11, "Thus, the plain language of claim 1 does not limit the parties to a transaction between the user and an application, or require that one of the parties to a transaction be the application ultimately accessed." Again, Examiner notes that while claim 1 of the '730 Patent is different from claim 1 of the '954 Patent, they are similar in scope with respect to the limitation involving the access message.

As such, Examiner finds "access message" to be "a message/notification indicating the user is allowed access, or otherwise allowing access." That is, an access message can be either: 1) "a message/notification indicating the user is allowed access" OR 2) "otherwise allowing access."

PO has not refuted this claim interpretation to date.

2. Arguments Outside the Scope of the Claim Language

To support their argument that Ludtke does not disclose an access message, PO argues the TPCH has neither control over nor knowledge of whether the vendor completes the transaction (i.e., providing access to the electronic product). (beginning on p. 7 of Remarks II)

Based on the claim language, Examiner finds that the vendor completing the transaction is outside the scope of the claim language for the following reasons:

1. With regard to at least independent method claim 18 of the '730 Patent, the preamble recites the transitional term "comprising," thus making the claim open-ended, which does not exclude additional, unrecited elements or method steps.

2. The claim language is "receiving an access message by an application from the agent allowing the user access to the 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."

Thus, based on the claim interpretation, Examiner finds that the claim requires a message/notification to an application indicating the user is allowed access, or otherwise allowing access, to the 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.

3. Completing a transaction or shipping/delivering products to the user/customer is not required for a message/notification indicating the user is allowed access to an application.

3. Based on the Examiner's Findings Above, Examiner further finds Ludtke Does Disclose an Access Message in the TPCH's Transaction Confirmation

The TPCH confirming the transaction and providing the confirmation to the vendor and the user (as outlined above in the rejection) is a message indicating the user is allowed access to the product being purchased. This is consistent with the PTAB's findings in IPR2024-00233 Final Written Decision dated June 17, 2025[5].

[5] IPR2024-00233 FWD, p. 31, "Thus, Ludtke describes a webpage receiving a message that both enables and announces access to the additional functionality, software, and services. We find that this is an example of receiving, at an application (web browser or webpage), an access message (transaction confirmation) from the trusted authority (TPCH) indicating that the trusted authority successfully authenticated the codes from the transaction device and allowing the user access to the application (new electronic content available on the webpage)."
IPR2024-00233 FWD, p. 34, "We find that the TPCH sends (and the application receives) an access message (Ludtke's transaction confirmation) that indicates that the TPCH successfully authenticated codes from the transaction device and that allows the user access to the train ticket, software, etc. Ex. 1005, 29:15–31, 31:11–52; Ex. 1003 ¶¶ 110–114. Accordingly, Ludtke teaches claim limitations 1d and 1e."

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 parities 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 Examiner, Art Unit 3992