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 11/25/2024
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
11/25/2024	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 (FITF) 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 09 October 2024.
☐ 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 1-17 are subject to reexamination.

1b. ☐ Claims _____ are not subject to reexamination.

2. ☐ Claims _____ have been canceled in the present reexamination proceeding.

3. ☐ Claims _____ are patentable and/or confirmed.

4. ☑ Claims 1-17 are rejected.

5. ☐ Claims _____ are objected to.

6. ☐ The drawings, filed on _____ are acceptable.

7. ☐ The proposed drawing correction, filed on _____ has been (7a) ☐ approved (7b) ☐ disapproved.

8. ☐ Acknowledgment is made of the priority claim under 35 U.S.C. 119(a)-(d) or (f).

a) ☐ All b) ☐ Some* c) ☐ None of the certified copies have

1 ☐ been received.

2 ☐ not been received.

3 ☐ been filed in Application No. _____.

4 ☐ been filed in reexamination Control No. _____.

5 ☐ been received by the International Bureau in PCT application No. _____.

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

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

10. ☐ Other: _____

cc: Requester (if third party requester)

EX PARTE REEXAMINATION NON-FINAL OFFICE ACTION

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

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

This is a second Non-Final office action due to the Examiner updating the rejections, which was not necessitated by any claim amendments.

Claims 1-17 are reexamined below.

Prior and Concurrent Proceedings and Litigation

Examiner notes related *ex parte* reexamination filings: 90/015,053 (Examiner's Answer to Appeal Brief mailed October 24, 2024) and 90/015,054 (Non-Final mailed November 5, 2024).

Examiner further notes:

- IPR2021-01444, which concluded with a Denial of Institution in which the PTAB indicated Petitioner did not show a reasonable likelihood of prevailing because Petitioner did not show persuasively that the references taught a "third-party trusted authority."
- IPR2024-00232, trial instituted.
- IPR2024-00775, pending.
- IPR2024-01326, pending.
- IPR2024-01333, pending.

The '730 Patent is also the subject of 6:21cv210, *Proxense, LLC V. Samsung Electronics Co, Ltd Et Al.*

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.

References Asserted by PO Requester as Raising SNQs of Patentability

- U.S. Pat. No. 7,188,110 to Ludtke ("Ludtke" or "Ex. 1005") available as prior art under 35 USC 102(e);
- U.S. Pub. No. 20030196084 to Okereke et al. ("Okereke" or "Ex. 1006") available as prior art under 35 USC 102(a,e);
- U.S. Pub. No. 20030177102 to Robinson ("Robinson" or "Ex. 1007") available as prior art under 35 USC 102(a,e); and
- WO 9956429 A2 to Scott ("Scott" or "Ex. 1008") available as prior art under 35 USC 102(b).

<u>Other</u>

- Declaration of Benjamin F. Goldberg ("Goldberg Dec" or "Ex. 1003").

Claim Interpretation

I. Lexicographic Definitions

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

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

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

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

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

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

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

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

Claim Rejections - 35 USC § 103

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.

Claims 1, 2, 4-9, 11, 12, and 14-17 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Ludtke and Okereke.

As per claim 1, 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)

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)

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

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)

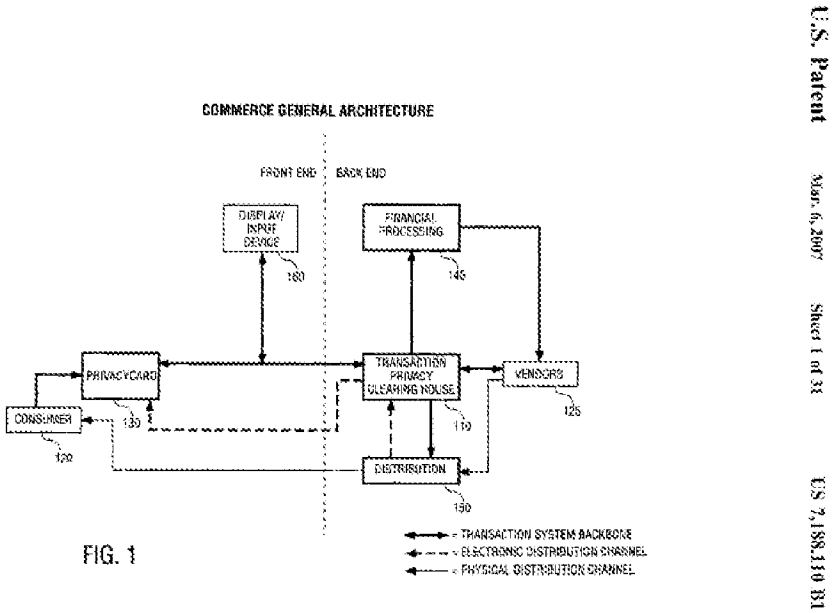

FIG. 1

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)

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.

"In so doing, a unique identifier for the wireless product to be employed is passed as at 210 to the proxy server 125 program for authorization. The wireless product 165 can be a personal digital assistant (PDA), laptop, cellular telephone or any other device capable of remote wireless communication. The unique identifier can be a serial number or SIM. 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 key exchange 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." (¶0025)

"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." (¶0026)

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. (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 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.

"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 verifying the user, the transaction device displays the collection of eCoupons that the user requested on its display screen, step 1607." (27:31-33)

Here, after the user is authenticated, the user has access to a collection of eCoupons, which are digital files.

"Secure distribution of physical (or electronic) content to the user is performed once the transaction is authorized." (29:29-30)

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

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

"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 4, Ludtke discloses **the method of claim 1, 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 5, Ludtke discloses **the method of claim 1, 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 6, Ludtke discloses **the method of claim 1, further comprising: establishing a secure communication channel prior to sending the one or more codes and the other data values for authentication.**

"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 7, Ludtke discloses **the method of claim 1, further comprising: receiving a request for the one or more codes and the other data values without a request for biometric verification; and 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 8 recites substantially similar subject matter to that of claim 1; therefore, claim 8 is rejected based on the same rationale as claim 1.

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 9, 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 11, Ludtke discloses **the integrated device of claim 8, 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:

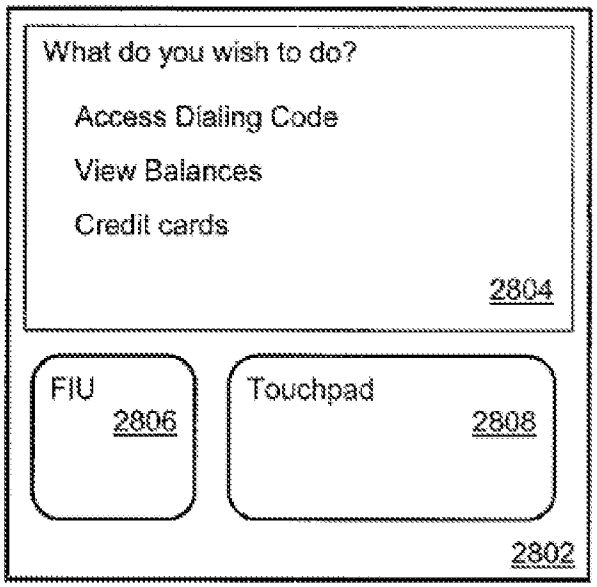

FIG. 28

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

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

"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 3, 10 and 13 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Ludtke, Okereke, and Robinson.

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

Claim Rejections - 35 USC § 102

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 –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.
>
> (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 15-17 are rejected under pre-AIA 35 U.S.C. 102(a,e) as being anticipated by Ludtke.

As per claim 15, Ludtke discloses **a system, comprising:**

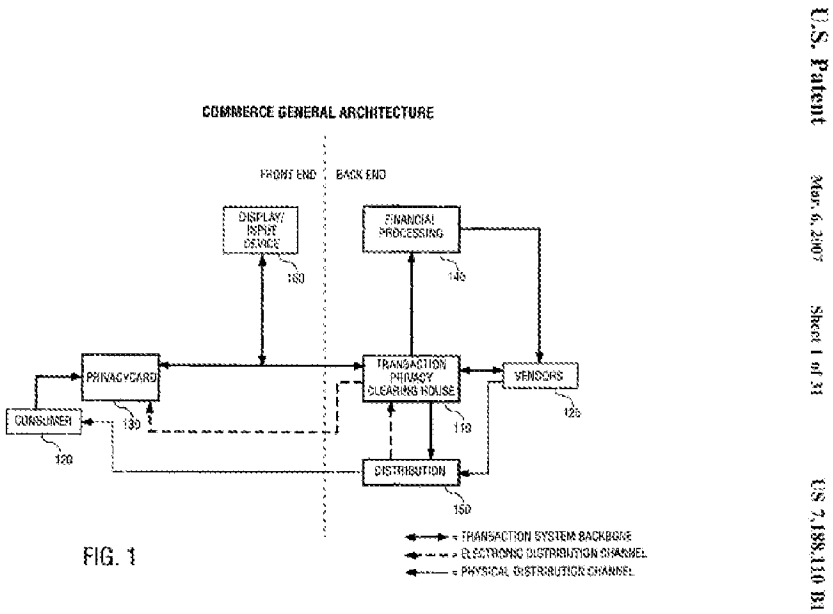

FIG. 1

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)

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, 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)

"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." (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 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

"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 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

"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)

"Authentication unit" is code on 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. (Goldberg Dec, ¶110)

responsive to the device ID code being authenticated, the authentication unit receiving an access message from the agent allowing the user to access an application, 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 verifying the user, the transaction device displays the collection of eCoupons that the user requested on its display screen, step 1607." (27:31-33)

Here, after the user is authenticated, the user has access to a collection of eCoupons, which are digital files.

"Secure distribution of physical (or electronic) content to the user is performed once the transaction is authorized." (29:29-30)

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

As per claim 16, Ludtke discloses **the system of claim 15, wherein the biometric key receives an authentication request from the authentication unit, and in response, requests a biometric scan from the user to generate the scan data.**

"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 17, Ludtke discloses **the system of claim 15, wherein if the biometric key cannot verify the scan data as being from the user, it does not send the one or more codes and the other data values.**

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

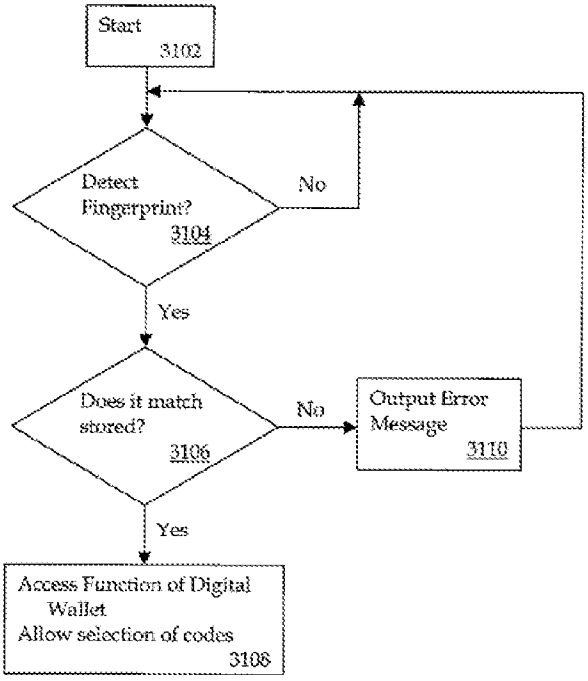

FIG. 31

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

Response to Arguments

Third-party trusted authority

In the Remarks, PO argues the third-party trusted authority must be a third-party with respect to a user and application being accessed. (p. 4 of Remarks)

All that is required of the third-party trusted authority is that it is "one other than the principals involved in a transaction." The updated rejections reflect the embodiment where a user is authorized prior to accessing a digital product (i.e., software, digital images). In this case, the third-party trusted authority is one other than the user and digital product involved in a transaction. Additionally, Examiner notes that Fig. 7 of the '730 Patent indicates that the access message is sent to the application (item 740). Examiner submits that the claims do not recite the access message being sent to the application; therefore, the claims are broader in scope than what is depicted in Fig. 7.

35 USC 112, sixth paragraph

In the Remarks, PO argues "verification unit" and "authentication unit" do not invoke 35 USC 112, sixth paragraph as the respective algorithms are fully manifested in claims 8 and 15. (p. 8 of Remarks)

Examiner finds this argument persuasive and the 35 USC 112, sixth paragraph claim interpretation for claims 8 and 15 is withdrawn.

The TPCH is the application being accessed

In the Remarks, PO argues the TPCH is the application being accessed to perform the function of a clearing house. (p. 14 of Remarks)

This argument is moot in view of the updated rejections.

The TPCH does not send an access message allowing the user to access an application

In the Remarks, PO argues the TPCH does not send an access message allowing the user to access an application. (p. 17 of Remarks)

This argument is moot in view of the updated rejections.

Extension of Time

Extensions of time under 37 CFR 1.136(a) will not be permitted in these proceedings because the provisions of 37 CFR 1.136 apply only to “an applicant” and not to parties in a reexamination proceeding. Additionally, 35 U.S.C. 305 requires that *ex parte* reexamination proceedings "will be conducted with special dispatch" (37 CFR 1.550(a)). Extensions of time in *ex parte* reexamination proceedings are provided for in 37 CFR 1.550(c).

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.

Signed:

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

Conferees:

/JEFFREY D CARLSON/
Primary Examiner, Art Unit 3992

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