



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.
90/015,054	06/08/2022	10698989	2090-0003-REX	1008
142179	7590	11/05/2024	EXAMINER	
Hard IP LLC (General)			TON, MY TRANG	
10 Notch Hill Drive				
Livingston, NJ 07039				
			ART UNIT	PAPER NUMBER
			3992	
			MAIL DATE	DELIVERY MODE
			11/05/2024	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)

MARISSA R. DUCCA
1300 I STREET NW,
SUITE 900
WASHINGTON, DC 20005

***EX PARTE* REEXAMINATION COMMUNICATION TRANSMITTAL FORM**

REEXAMINATION CONTROL NO. 90/015,054 .

PATENT UNDER REEXAMINATION 10698989 .

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. 90/015,054	Patent Under Reexamination 10698989	
	Examiner MY TRANG TON	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 02 November 2022.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

b. ☐ This action is made FINAL.

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

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

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

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

Part II SUMMARY OF ACTION

- 1a. ☒ Claims 1-9 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 1-9 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

This Office action is a first Office action on the merits for the reexamination proceeding control number 90/015,054 (hereinafter the “**054 Proceeding**”). This is a reexamination of claims 1-9 of United States Patent
5 No. 10,698,989 (the “**989 Patent**”), entitled “BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION” which issued on June 30, 2020. The request for reexamination filed June 8, 2022 (hereinafter “**the Request**”) including two proposed SNQs which were accepted in the Ex Parte Order mailed August 2, 2022 (hereinafter “**the Order**”).

10

PRIORITY

After careful review of the prosecution history of the 989 Patent, Examiners find that the 989 Patent was filed on February 20, 2016 and assigned U.S. Patent Application No. 15/049,060 (hereinafter the “**060 application**”). The 060 Application is a continuation of application No.
15 14/521,982, filed on Oct. 23, 2014, now Pat. No. 9,298,905, which is a continuation of application No. 13/710,109, filed on Dec. 10, 2012, now Pat. No. 8,886,954, which is a continuation of application No. 11/314,199, filed on Dec. 20, 2005, now Pat. No. 8,352,730, which claims the benefit of a
20 provisional application No. 60/652,765, filed on Feb, 14, 2005, and a provisional application No. 60/637,538, filed on Dec. 20, 2004.

LITIGATION

After reviewing the Request, performing a litigation search and reviewing the file history of the 989 Patent, Examiners are aware of the following related litigation: IPR2021-01448.

5

REFERENCES RELIED UPON OR DISCUSSED

1. US. Patent No. 7,188,110 ("**Ludtke**")
2. U.S. Patent Publication No. 2003/0196084 ("**Okereke**")
3. International Publication Number WO 99/56429 ("**Scott**")

10

As noted in the Order:

- All of the cited references in the Request (Ludtke, Okereke and Scott) were not of record in the prosecution of the 060 Application.
- Scott was used and discussed in the prosecution of IPR2021-01448. However, the Third Party Requester alleges in SNQ 2 that 989 Patent claims are rendered obvious in light of Ludtke in view of Scott, based on an combination/interpretation other than that was the focus of IPR2021-01448. In other words, Ludtke was not previously combined with Scott during the IPR2021-01448.
- In the IPR2021-01448 proceeding, the PTAB denied institution. A denial of institution is not considered an earlier concluded proceeding for the purpose of the SNQ analysis. See MPEP § 2242 I.; *Ex parte Finjan Inc.*, Appeal No. 2018-007444 at 7-8 (PTAB Sept. 28, 2018) ("Because no trial was instituted on the inter partes review, there was

15

20

no “final holding of invalidity” or “concluded examination or review”
for SNQ purposes). To the extent Scott was considered in the
IPR2021-01448, Scott is nevertheless not “old art” as defined in the
MPEP and the PTAB’s determinations likewise do not affect the
5 Examiner’s SNQ analysis.

STATUS OF THE CLAIMS

Claims 1-9 are originally as in the 989 Patent.
Of these, claims 1, 5 and 7 are independent claims.

10

CLAIM INTERPRETATION

During examination, claims are given the broadest reasonable
interpretation consistent with the specification and limitations in the
specification are not read into the claims. See MPEP §§ 2111, 2111.01 and *In re*
15 *Yamamoto et al.*, 222 USPQ 934 (Fed. Cir. 1984). Under a broadest reasonable
interpretation, words of the claim must be given their plain meaning, unless
such meaning is inconsistent with the specification. See MPEP § 2111.01(I). It
is further noted it is improper to import claim limitations from the
specification, *i.e.*, a particular embodiment appearing in the written description
20 may not be read into a claim when the claim language is broader than the
embodiment. See MPEP 2111.01. Therefore, unless one of the exceptions
applies below, Examiners will interpret the limitations of the examined claims
using the broadest reasonable interpretation.

A. Lexicography

A first exception to the prohibition of reading limitations from the specification into the claims is when the Applicant for patent has provided a lexicographic definition for the term. See MPEP §2111.01(IV). Following an independent review of the claims in view of the specification herein, Examiners find that Patent Owner has not provided any lexicographic definitions related to claim terms with any reasonable clarity, deliberateness and precision.

B. Claim Interpretation under 35 U.S.C. §112(6th ¶)

A second exception to the prohibition of reading limitations from the specification into the claims is when the claimed feature is written as a means-plus-function or a step-plus-function. See 35 U.S.C. §112(6th ¶) and MPEP §2181-2183. As noted in MPEP §2181, a three prong test is used to determine the scope of a means-plus-function or step-plus-function limitation in a claim:

- (A) the claim limitation uses the term “means” or “step” or a term used as a substitute for “means” that is a generic placeholder (also called a nonce term or a non-structural term having no specific structural meaning) for performing the claimed function
- (B) the term “means” or “step” or the generic placeholder is modified by functional language, typically, but not always linked by the transition word “for” (e.g., “means for”) or another linking word or phrase, such as “configured to” or “so that”
- (C) the term “means” or “step” or the generic placeholder is not modified by sufficient structure, material, or acts for performing the claimed function.

B1. FL #1: “a persistent storage” (claim 5)

A first means-plus-function phrase is recited in claim 5 which recites “the persistent storage” or hereinafter FL #1. Examiners determine herein that

FL #1 meets the three prong test and thus will be interpreted as a means-plus-function limitation under 35 U.S.C. §112(6th ¶).

Examiners find that FL #1 in claim 5 recites:

“the persistent storage having an output configured to provide a first set of
5 *biometric data and the ID code for use on the smartphone*”.

“**FL #1**” – From claim 5

(B1)(a) 3-Prong Analysis Prong (A)

As an initial matter, Examiners find that FL #1 does not use the term
10 “means.” However, FL #1 meets invocation prong (A) because “means... for”
type language is recited. Examiners find that “the persistent storage” is a
generic placeholder or nonce term equivalent to “means” because the term
“persistent storage” does not convey any particular structure. Examiners
further notes that the specification of the 989 Patent does not define element
15 structure for “the persistent storage”, thus the specification of the 989 Patent
does not impart or disclose any structure for the phrase. In fact, Examiners
find that the 989 Patent merely illustrates the persistent storage as a blank box
(See 989 Patent FIG. 2, item 226) without any disclosure within the
specification as to the structures within the blank box.

20 Additionally, there is no disclosure or suggestion from the prior art or the
989 Patent that any “persistent storage” is a sufficient structure to perform the
entire function recited in FL #1. Multiple persistent storage in the related prior
art have multiple functions which do not include the function recited in FL #1.

For example: U. S Patent No. 8,706,707, claim 6 claimed: “*The system of claim 4, wherein the configuration database comprises a persistent storage for storing the network*”; U.S Patent No. 8,473,922, claim 3 claimed “... *a persistent storage capable of collecting a plurality of log data..*”; or U.S Patent No.

- 5 8,463,867, claim 4 claimed “...*said persistent storage is provided by a database stored at each of said one or more computers providing persistent storage of said interpretable storage conditions*”.

Accordingly, while there is common use of the generic term “persistent storage” the diverse functions would necessitate different structures, whether
10 hardware or software. Examiners find that each of these prior art references use persistent storage in association with distinct functions from each other and that of FL #1 which would require distinct algorithms and/or software to cause a device to perform these distinct functions. Thus, Examiners find that each of these persistent storage comprises different and distinct
15 structures/programming to perform their associated distinct functions.

Accordingly, while each of these prior art references use the term “persistent storage” they use this term generically in association with a special function to imply a special purpose persistent storage.

Accordingly, Examiners find nothing in the specification, prosecution
20 history or the prior art to construe “the persistent storage” in FL #1 as the name of a sufficiently definite structure for performing the function recited in FL #1 so as to take the overall claim limitation out of the ambit of §112(6th ¶).

See Williamson v. Citrix Online, L.L.C., 115 USPQ2d 1105, 1112 (Fed. Cir. 2015).

In light of the above, Examiners conclude that the term “persistent storage” is a generic placeholder having no specific structure associated therewith. Because “persistent storage” is merely a generic placeholder having no specific structure associated therewith, Examiners conclude that FL #1 meets invocation Prong (A).

(B1)(b) 3-Prong Analysis Prong (B)

FL #1 meets invocation prong (B) because it recites the function:
“configured to provide a first set of biometric data and the ID code for use on the smartphone”.

Examiners find that because nothing in the written description of the 989 Patent contradicts the plain language as set forth in the Function of FL #1, the terms within the Function of FL #1 will have their ordinary and accustomed meaning. Because Functional Phrase #1 includes the Function of FL #1, Examiners conclude that, Functional Phrase #1 meets Invocation Prong (B).

(B1)(c) 3- Prong Analysis Prong (C)

FL #1 meets invocation prong (C) because FL #1 does *not* recite sufficient structure for performing all the claimed function. Based upon a review of claim 5, Examiners find that FL #1 recites very little structure, if any, for performing the function as set forth of FL #1.

In view of Examiners finding above that FL #1 meets invocation prongs (A)-(C), Examiners conclude FL #1 invokes interpretation under 35 U.S.C. §112(6th ¶).

5 (B1)(d) Corresponding Structure

After a claimed phrase has been shown to invoke 35 U.S.C. §112(6th ¶), as found above, the next step is to determine the corresponding structure or material as described in the specification for performing the recited function. See MPEP §2181.

10 Based upon a review of the specification of the 989 Patent, Examiners find that the closest corresponding structure for the FL #1 can include a ROM element, a flash memory element, or any other type of non-volatile storage element (see col. 5, lines 45-50). Examiners find that the 989 Patent disclosed an algorithm for “Persistent Storage 226” in column 5, lines 43 - column 6, line
15 3 and Fig. 5:

20 *“Persistent storage 226 persistently stores biometric data from one or more users which can be provided according to specific implementations. In one embodiment, at least some of Persistent storage 226 is a memory element that can be written to once but cannot subsequently be altered. Persistent storage 226 can include, for example, a ROM element, a flash memory element, or any other type of non-volatile storage element. Persistent storage 226 is itself, and stores data in, a tamper-proof format to prevent any changes to the stored data. Tamper-proofing increases reliability of authentication because it does not allow any changes to biometric data (i.e., allows reads of stored data, but not writes to store new data or modify existing data). Furthermore, data can be stored in an encrypted form.*

25 *In one embodiment, Persistent storage 226 also stores the code that is provided by the key 100 responsive to successful verification of the user.*

5 As described above, in one embodiment the code is a device ID or other value that uniquely identifies biometric key 100. In one embodiment, the code is providing during the manufacturing process and the biometric data are provided during an enrollment of the user. In other embodiments, the code is provided during enrollment and/or the biometric data are provided during manufacturing. Further, in some embodiments Persistent storage 226 stores other data utilized during the operation of biometric key 100. For example, Persistent storage 226 can store encryption/decryption keys utilized to establish secure communications links."

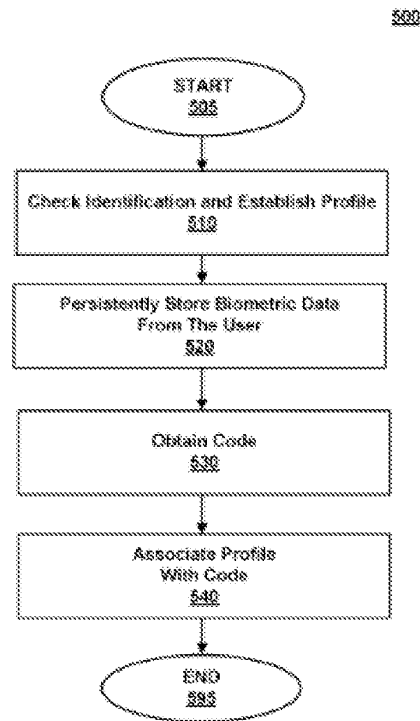


FIG. 5

Fig. 5 of the 989 Patent.

Accordingly, Examiners find the corresponding hardware structures for persistent storage to be ROM element, flash memory element, non-volatile

storage element is used in association with special instructions (Fig. 5) that enable the persistent storage to perform specific function recited in FL #1.

In view of these findings, FL #1 will be limited to the persistent storage, i.e., the ROM element, the flash memory element or the non-volatile storage element performed the algorithm discloses in, for example, Fig. 5.

B2. FL #2: “a validation module” (claim 5)

A second means-plus-function phrase is recited in claim 5 which recites “the validation module” or hereinafter FL #2. Examiners determine herein that FL #2 meets the three prong test and thus will be interpreted as a means-plus-function limitation under 35 U.S.C. §112(6th ¶).

Examiners find that FL #2 in claim 5 recites:

“a validation module, coupled to communicate with the persistent storage to receive the biometric data from the persistent storage, the validation module having a scan pad to capture scan data from a biometric scan, the validation module comparing the scan data to the biometric data to determine whether the scan data matches the biometric data”.

“FL #2” – From claim 5

(B2)(a) 3-Prong Analysis Prong (A)

As an initial matter, Examiners find that FL #2 does not use the term “means.” However, FL #2 meets invocation prong (A) because “means... for” type language is recited. Examiners find that “the validation module” is a

generic placeholder or nonce term equivalent to “means” because the term “validation module” does not convey any particular structure. Examiners further note that the specification of the 989 Patent does not define element structure for “the validation module”, thus the specification of the 989 Patent does not impart or disclose any structure for the phrase. In fact, Examiners find that the 989 Patent merely illustrates the validation module as a blank box (See 989 Patent FIG. 2, item 224) without any disclosure within the specification as to the structures within the blank box.

Additionally, there is no disclosure or suggestion from the prior art or the 989 Patent that any “validation module” is a sufficient structure to perform the entire function recited in FL #2. Multiple validation module in the related prior art have multiple functions which do not include the function recited in FL #2. For example: U. S Patent No. 8,027,658, claim 6 claimed: “*a validation module hosted by the service provider to automatically validate at least a portion of the subscriber emergency information of one or more subscribers against at least one of insurance information for the one or more subscribers and government information for the one or more subscribers*”; U.S Patent No. 7,783,554, claim 20 claimed “*a validation module stored in the computer readable storage medium and configured to compare the summary bid information to the identified summary bid requirements to validate the bid*”; U.S Patent No. 7478233, claim 15 claimed “*a validation module that validates the node based on a physical characteristic of the node, and where successful*”

validation is required prior to performing protection or authentication by the protection module and authentication module, respectively”.

Accordingly, while there is common use of the generic term “validation module” the diverse functions would necessitate different structures, whether hardware or software. While Examiners recognize the Applicant’s evidence that the validation module can comprise scan pad, something more than generic scan pad would be required to provide the function recited in FL #2.

Accordingly, Examiners find nothing in the specification, prosecution history or the prior art to construe “the validation module” in FL #2 as the name of a sufficiently definite structure for performing the function recited in FL #2 so as to take the overall claim limitation out of the ambit of §112(6th ¶). See *Williamson v. Citrix Online, L.L.C.*, 115 USPQ2d 1105, 1112 (Fed. Cir. 2015).

In light of the above, Examiners conclude that the term “validation module” is a generic placeholder having no specific structure associated therewith. Because “validation module” is merely a generic placeholder having no specific structure associated therewith, Examiners conclude that FL #2 meets invocation Prong (A).

(B2)(b) 3-Prong Analysis Prong (B)

FL #2 meets invocation prong (B) because it recites the function:

“communicate with the persistent storage to receive the biometric data from the persistent storage, the validation module having a scan pad to capture

scan data from a biometric scan, the validation module comparing the scan data to the biometric data to determine whether the scan data matches the biometric data”.

Examiners find that because nothing in the written description of the
5 989 Patent contradicts the plain language as set forth in the Function of FL #2, the terms within the Function of FL #2 will have their ordinary and accustomed meaning. Because Functional Phrase #2 includes the Function of FL #2, Examiners conclude that, Functional Phrase #2 meets Invocation Prong (B).

10 (B2)(c) 3- Prong Analysis Prong (C)

FL #2 meets invocation prong (C) because FL #2 does *not* recite sufficient structure for performing all the claimed function. Based upon a review of claim 5, Examiners find that FL #2 recites very little structure, if any, for performing the function as set forth of FL #2.

15 In view of Examiners finding above that FL #2 meets invocation prongs (A)-(C), Examiners conclude FL #2 invokes interpretation under 35 U.S.C. §112(6th ¶).

(B2)(d) Corresponding Structure

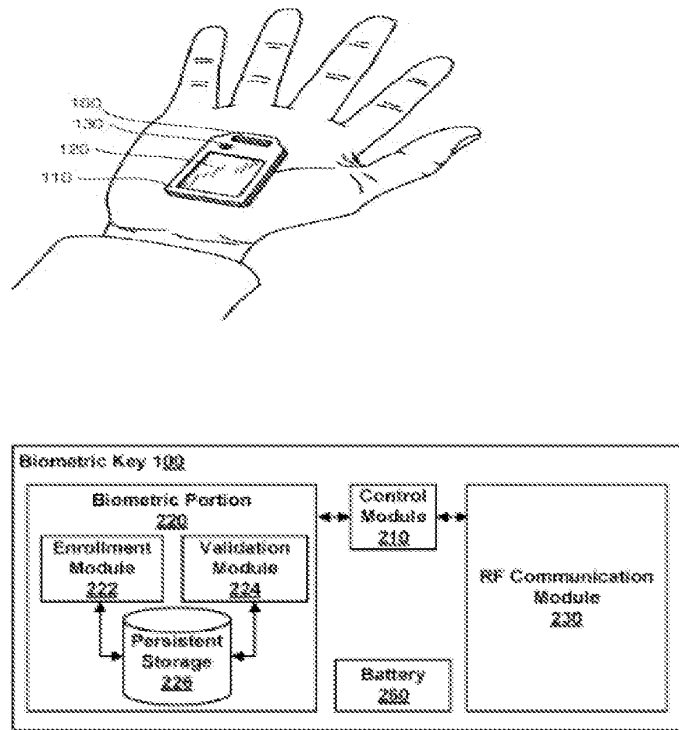
20 After a claimed phrase has been shown to invoke 35 U.S.C. §112(6th ¶), as found above, the next step is to determine the corresponding structure or material as described in the specification for performing the recited function. See MPEP §2181.

Based upon a review of the specification of the 989 Patent, Examiners find that the closest corresponding structure for the FL #2 can comprise scan pad 120 (Fig. 1) to capture scan data from a use's fingerprint (col. 5, lines 27-42). However, Examiners find that the scan pad 120 itself is not sufficient
5 corresponding structures for perform the entire function. A generic scan pad would not readily perform all recited function. Rather Examiners find that scan pad 120 is used in association with special instructions (Steps 605-695 of Fig. 6) would be required to perform the function recited in FL #2.

Examiners find that the 989 Patent disclosed an algorithm for the
10 validation module 224 at col. 5, lines 27-42:

15 *“Validation module 224 can comprise scan pad 120 (FIG. 1) to capture scan data from a user's fingerprint (e.g., a digital or analog representation of the fingerprint). Using the scan data, validation module 224 determines whether the user's fingerprint matches the stored biometric data from enrollment. Conventional techniques for comparing fingerprints can be used. For example, the unique pattern of ridges and valleys of the fingerprints can be compared. A statistical model can be used to determine comparison results. Validation module 224 can send comparison results to control module 210.*

20 *In other embodiments, Validation module 224 can be configured to capture biometric data for other human characteristics. For example, a digital image of a retina, iris, and/or handwriting sample can be captured. In another example, a microphone can capture a voice sample.”*



Figs. 1-2 of 989 Patent

In view of these findings, FL #2 will be limited to the validation module
5 comprises scan pad to capture scan data from a user's fingerprint and having
special programming therein for comparing the scanned data to the stored
fingerprint to determine whether the scanned data matches the stored data (i.e.,
steps 605-650 of Fig. 6).

10 **B3. FL #3: "a smartphone" (claim 7)**

A third means-plus-function phrase is recited in claim 7 (and included in
dependent claim 8), which recites "the smartphone" or hereinafter FL #3.

Examiners determine herein that FL #3 meets the three prong test and thus will be interpreted as a means-plus-function limitation under 35 U.S.C. §112(6th ¶).

Examiners find that FL #3 in claim 7 recites:

5 *“the smartphone configured to indicate that a biometric authentication is requested, the smartphone configured to wirelessly send the ID code to the third party trusted authority for authentication responsive to determining that scan data from a biometrics scan performed using the smartphone matches the biometric data of the legitimate user”*

10 **“FL#3”** – From claim 7

(B3)(a) 3-Prong Analysis Prong (A)

As an initial matter, Examiners find that FL #3 does not use the term “means.” However, FL #3 meets invocation prong (A) because “means... for”
15 type language is recited. Examiners find that “the smartphone” is a generic placeholder or nonce term equivalent to “means” because the term “smartphone” does not convey any particular structure. Examiners further note that the specification of the 989 Patent does not define “the smartphone”, thus the specification of the 989 Patent does not impart or disclose any
20 structure for the phrase.

Additionally, there is no disclosure or suggestion from the prior art or the 989 Patent that any “smartphone” is a sufficient structure to perform the entire functions recited in FL #3. Multiple smartphone in the related prior art have

multiple functions which do not include the functions recited in FL #3. For example: U. S. Patent No. 6,683,851, claim 4 claimed: “*wherein said first plurality of modules are application modules within a smartphone*”; U. S. Patent No. 6,434,371, claim 33 claimed “*wherein said system operates in*
5 *SMARTPHONE mode when said first portion is detached from said second portion*”; or U. S. Patent No. 6,246,862, claim 16 claimed “... *to control the smartphone to perform one of a radiotelephone function and a personal computer or personal digital assistant function; ... when the smartphone is positioned in close proximity to a user*”.

10 Accordingly, while there is common use of the generic term “smartphone” the diverse functions would necessitate different structures, whether hardware or software. While Examiners recognize the Applicant’s evidence that the biometric key 100 is integrated into a mobile phone (e.g. a cellular phone or smartphone), tablet, laptop, mp3 player, mobile gaming
15 device, watch, key fob or other mobile device, something more than generic mobile phone (i.e., hardware, firmware, or software) would be required to perform the entire functions recited in FL #3.

 Accordingly, Examiners find nothing in the specification, prosecution history or the prior art to construe “the smartphone” in FL #3 as the name of a
20 sufficiently definite structure for performing the functions recited in FL #3 so as to take the overall claim limitation out of the ambit of §112(6th ¶). See *Williamson v. Citrix Online, L.L.C.*, 115 USPQ2d 1105, 1112 (Fed. Cir. 2015).

In light of the above, Examiners conclude that the term “smartphone” is a generic placeholder having no specific structure associated therewith.

Because “the smartphone” is merely a generic placeholder having no specific structure associated therewith, Examiners conclude that FL #3 meets

5 invocation Prong (A).

(B3)(b) 3-Prong Analysis Prong (B)

FL #3 meets invocation prong (B) because it recites the functions:

- “*configured to indicate that a biometric authentication is requested,*

10 [**“Sub-Function #3-1”**]

- “*configured to wirelessly send the ID code to the third party trusted authority for authentication responsive to determining that scan data from a biometrics scan performed using the smartphone matches the biometric data of the legitimate user*”.

15 [**“Sub-Function #3-2”**]

Examiners find that because nothing in the written description of the 989 Patent contradicts the plain language as set forth in the Function of FL #3, the terms within the Function of FL #3 will have their ordinary and accustomed meaning. Because Functional Phrase #3 includes the Function of FL #3,

20 Examiners conclude that, Functional Phrase #3 meets Invocation Prong (B).

(B3)(c) 3- Prong Analysis Prong (C)

FL #3 meets invocation prong (C) because FL #3 does *not* recite sufficient structure for performing all the claimed function. Based upon a review of claim

7, Examiners find that FL #3 recites very little structure, if any, for performing the function as set forth of FL #3.

In view of Examiners finding above that FL #3 meets invocation prongs (A)-(C), Examiners conclude FL #3 invokes interpretation under 35 U.S.C.

5 §112(6th ¶).

(B3)(d) Corresponding Structure

After a claimed phrase has been shown to invoke 35 U.S.C. §112(6th ¶), as found above, the next step is to determine the corresponding structure or
10 material as described in the specification for performing the recited function. See MPEP §2181(II).

Based upon a review of the specification of the 989 Patent, Examiners find that the closest corresponding structure for the FL #3 is a smart phone. However, Examiners find that the smart phone itself is not sufficient
15 corresponding structures for perform the Sub-Functions #3-1 and #3-2 . A generic smart phone would not readily perform the recited function. Rather Examiners find that software program as shown in Figs. 6-7 would be required to perform the Sub-Functions #3-1 and #3-2.

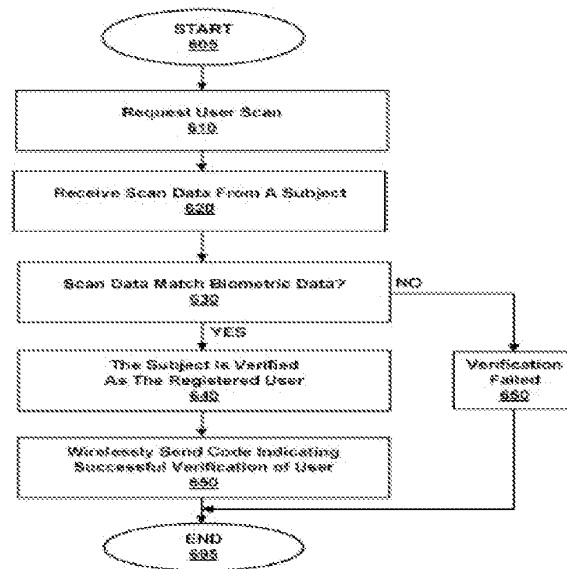


FIG. 6

Fig. 6 of the 989 Patent.

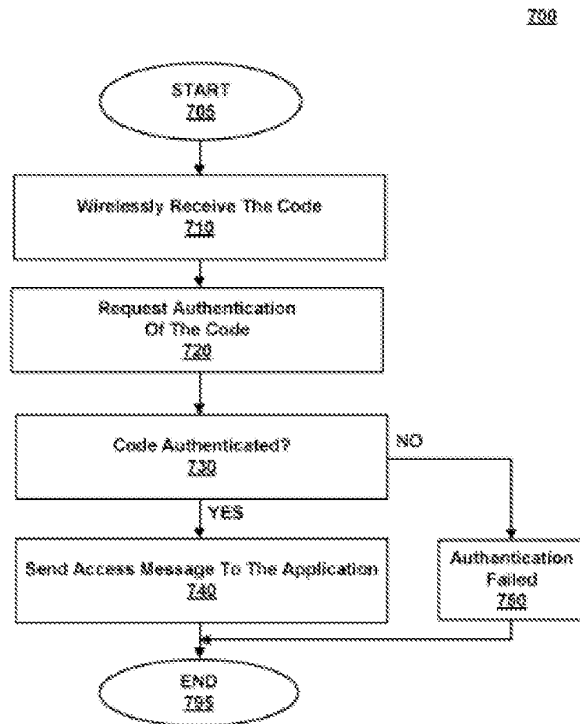


Fig. 7 of the 989 Patent.

In view of these findings, FL #3 will be limited to a generic smartphone
5 having special programming therein for performing steps 605-650 of FIG. 6 and
steps 705-750 in FIG. 7.

B4. FL #4: “a third party trusted authority” (claim 7)

A fourth means-plus-function phrase is recited in claim 7, which recites
10 “the third party trusted authority” or hereinafter FL #4. Examiners determine

herein that FL #4 meets the three prong test and thus will be interpreted as a means-plus-function limitation under 35 U.S.C. §112(6th ¶).

Examiners find that FL #4 in claim 7 recites:

*“the third-party trusted authority operated by a third party, the third-party
trusted authority storing a plurality of legitimate ID codes and
authenticating the ID code received based on a comparison of the ID code
received and the legitimate ID codes included in the plurality of the
legitimate ID codes.”*

“FL#4” – From claim 7

(B4)(a) 3-Prong Analysis Prong (A)

As an initial matter, Examiners find that FL #4 does not use the term “means.” However, FL #4 meets invocation prong (A) because “means... for” type language is recited. Examiners find that “the third party trusted authority” is a generic placeholder or nonce term equivalent to “means” because the term “third party trusted authority” does not convey any particular structure. Examiners further note that the specification of the 989 Patent does not define “the third party trusted authority”, thus the specification of the 989 Patent does not impart or disclose any structure for the phrase. In fact, Examiners find that the 989 Patent merely illustrates the third party trusted authority as a blank box (See 989 Patent FIG. 3, item 320) without any disclosure within the specification as to the structures within the blank box.

Additionally, there is no disclosure or suggestion from the prior art or the 989 Patent that any “third party trusted authority” is a sufficient structure to perform the entire functions recited in FL #4. Multiple third party trusted authority in the related prior art have multiple functions which do not include
5 the functions recited in FL #4. For example: Patent No. CN 1656769, claim 5 claimed: “a second function (H) is previously provided to the receiver by the trusted third party for verifying the function of the result of the first function is determined by the trusted third party”; U.S 20060075245, claim 26 claimed “the digital signature comprises a time stamp from a trusted third party or a trusted
10 authority”, claim 34 claimed “the re-signed hash information data comprises a time stamp from a trusted third party or a trusted authority”.

Accordingly, while there is common use of the generic term “third-party trusted authority” the diverse functions would necessitate different structures, whether hardware or software. Examiners find nothing in the specification,
15 prosecution history or the prior art to construe “the third party trusted authority” in FL #4 as the name of a sufficiently definite structure for performing the functions recited in FL #4 so as to take the overall claim limitation out of the ambit of §112(6th ¶). *See Williamson v. Citrix Online, L.L.C.*, 115 USPQ2d 1105, 1112 (Fed. Cir. 2015).

20 In light of the above, Examiners conclude that the term “third-party trusted authority” is a generic placeholder having no specific structure associated therewith. Because “the third-party trusted authority” is merely a

generic placeholder having no specific structure associated therewith,

Examiners conclude that FL #4 meets invocation Prong (A).

(B4)(b) 3-Prong Analysis Prong (B)

5 FL #4 meets invocation prong (B) because it recites the functions:

“storing a plurality of legitimate ID codes and authenticating the ID code received based on a comparison of the ID code received and the legitimate ID codes included in the plurality of the legitimate ID codes.”

“FL #4” – From claim 7

10 Examiners find that because nothing in the written description of the 989 Patent contradicts the plain language as set forth in the Function of FL #4, the terms within the Function of FL #4 will have their ordinary and accustomed meaning. Because Functional Phrase #4 includes the Function of FL #4, Examiners conclude that, Functional Phrase #4 meets Invocation Prong (B).

15

(B4)(c) 3- Prong Analysis Prong (C)

FL #4 meets invocation prong (C) because FL #4 does *not* recite sufficient structure for performing all the claimed function. Based upon a review of claim 7, Examiners find that FL #4 recites very little structure, if any, for performing
20 the function as set forth of FL #4.

In view of Examiners finding above that FL #4 meets invocation prongs (A)-(C), Examiners conclude FL #4 invokes interpretation under 35 U.S.C. §112(6th ¶).

(B4)(d) Corresponding Structure

After a claimed phrase has been shown to invoke 35 U.S.C. §112(6th ¶), as found above, the next step is to determine the corresponding structure or material as described in the specification for performing the recited function.

5 See MPEP §2181(II).

Based upon a review of the specification of the 989 Patent, Examiners find that the closest corresponding structure for the FL #4 is a server or other computerized device. However, Examiners find that the server or other computerized device itself is not sufficient corresponding structures for perform
10 the function. Rather Examiners find that software program as shown in Fig. 7 would be required to perform the above function.

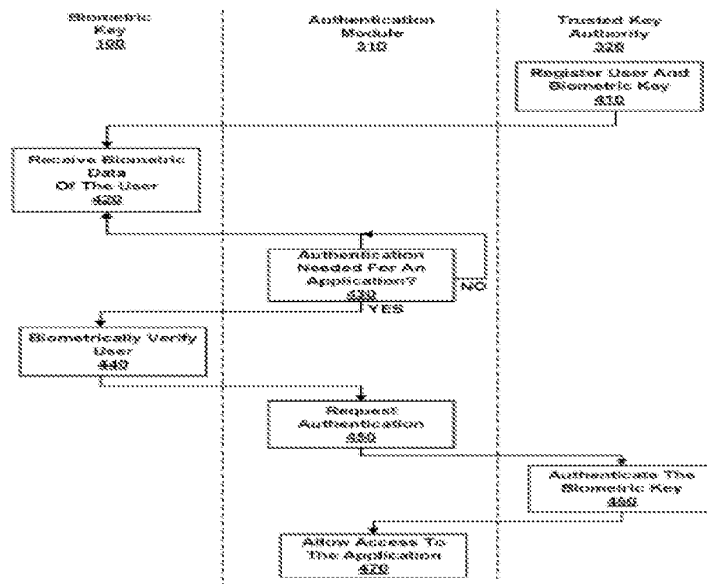
Examiners finds that the 989 Patent disclosed an algorithm for the trusted key authority 320 at col. 6, line 59- col. 7, line 53:

15 *“Trusted key authority 320 is a third-party authority that is present in some embodiments in order to provide enhanced security. In one embodiment, Trusted key authority 320 verifies that a code from a biometric key is legitimate. To do so, the Trusted key authority 320 stores a list of codes for legitimate biometric keys. The list can be batched or updated each time a new user/ key is enrolled. In one embodiment,*
20 *Trusted key authority 320 can also store a profile associated with a biometric key. The profile describes the user associated with the key, the key itself, the trusted key authority, and/or other relevant information. In one embodiment, the functionality of trusted key authority 320 is provided by a server or other computerized device.”*

25 The 989 Patent also discloses in col. 8, lines 33-46:

“FIG. 7 is a flow chart illustrating a method 700 for authenticating a biometric key according to one embodiment of the present invention. The code is wirelessly received 710. A request for authentication of the code is sent to the trusted key authority 720 . The trusted key

5 authority determines whether the code is authentic 730 (i.e., it was created through an established enrollment process) and has a valid status (e.g., has not expired). If authentication is successful, the trusted key authority sends an access message to the application to allow user access and/or provide additional information from the profile 740 (such as the user's age). If authentication is not successful, authentication fails 750 and the message to the application indicates that the user should be denied access."



10

Fig. 4 of the 989 Patent.

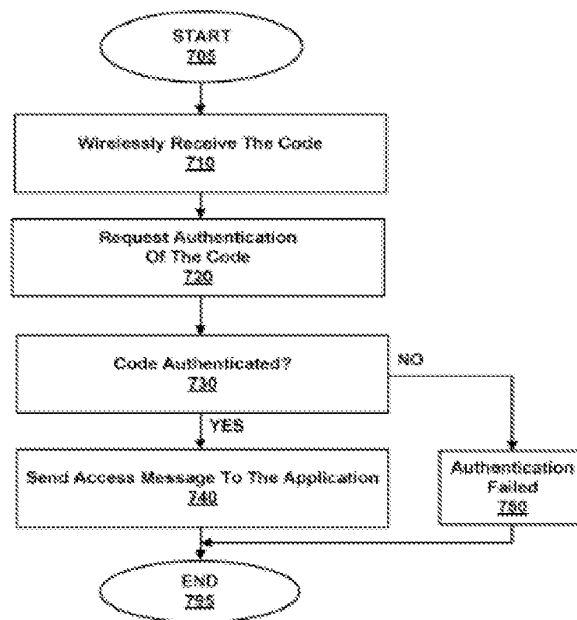


Fig. 7 of the 989 Patent.

In view of these findings, FL #4 will be limited to a server or other
5 computerized device software program that stores ID codes and has
programming that performs the steps 705-795 of FIG. 7.

C. Conclusion of Claim Interpretation

In view of the forgoing, Examiners will interpret FL #1 - FL #4 under 35
10 U.S.C. §112 (6th ¶) as discussed above. Since no further limitations invoke
interpretation under 35 U.S.C. §112(6th ¶) and no further limitations are
lexicographically defined, the remaining limitations will be interpreted applying
the broadest reasonable interpretation.

CLAIM REJECTIONS – RELEVANT STATUTE

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 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.

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.

CLAIM INTERPRETATION

- Limitation “third party trusted authority” is interpreted to mean “trusted authority that is an entity or party separate from the principal parties to a transaction” consistent with the PTAB (IPR2021-01448 Decision, page 10, last paragraph).
- Limitation “ID code” is interpreted to mean “a unique code identifying a device” consistent with court’s Final Construction (6:21-CV-00210-ADA Jury Trial Demand), page 2.

DISCUSSED CLAIM REJECTIONS

1/ Claims 1-9 are rendered obvious under 35 U.S.C. §103 over Ludtke in view with Okereke.

Ludtke teaches in Fig. 1 a method comprising:

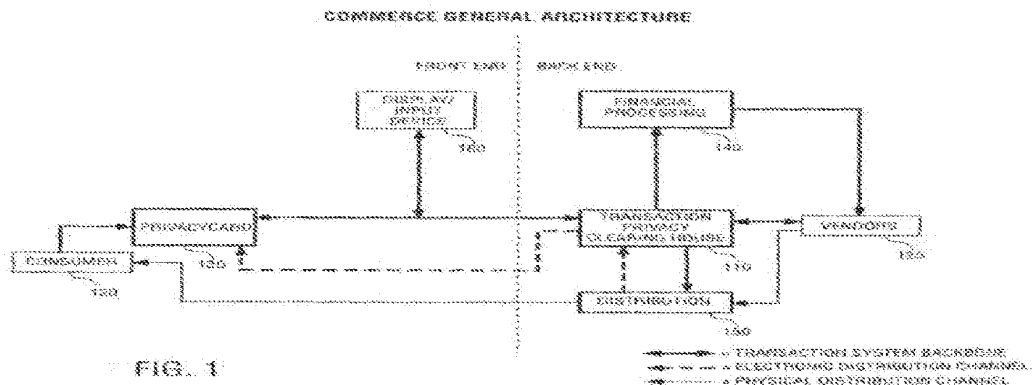


FIG. 1

Fig. 1 of Ludtke.

receiving, at a smartphone (Ludtke discloses “the transaction device may contain wireless data communication...” ¶5:40-41, “cell phone functionality built-in” ¶18:3-4, “another portable device such as a cell phone” ¶34:21. Fig. 28 shows “consumer access device” having functions allowing the user to see balances and credit cards, and also to “Access Dialing Codes” is inherently seen as the smartphone), **an identification (ID) code from a third-party trusted authority** (Ludtke discloses a transaction device (PRIVACYCARD 130) provide information to a TRANSACTION PRIVACY CLEARING HOUSE 110 for authorization for the transaction between a consumer 120 and vendor 125 to be performed: “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 TPOCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed.” ¶6:36-44). The TPOCH 110 is not part of the transaction, but rather functions a third-party middleman of the transaction: “In one embodiment of electronic distribution, the TPOCH 110 functions as the middleman of the distribution channel. This allows the TPOCH 110 to retain user privacy by not exposing addressing information and possibly email addresses to third parties.” ¶7:44-48. This ensures that sensitive information is not shared with the vendor 125), **the ID code uniquely identifying the smartphone among a plurality of smartphones** (Ludtke discloses the TPOCH 110 having “transaction device information” that is maintained in a secure database by the TPOCH 110: “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 transaction. However, the identity of the user is not revealed externally so that confidentiality of the user’s identity is maintained” ¶3:40-47). It would therefore be obvious that the ID code originate from the list of device information maintained by the TPOCH 110 and communicated to the smartphone. The TPOCH 110 would include the ID code in communications to the smartphone to ensure verification);

persistently storing biometric data and an ID code on a smartphone

(Ludtke discloses a storage location “*In one embodiment, the TPCCH allows users to backup data that is generated directly on the transaction device, such as a telephone book and appointment information, into a storage location managed by the TPCCH.*” ¶ 10:46-49; “*In addition, it may provide an alternative, non-PC based location from which to securely execute utility applications and to store data, thus enhancing data security and protection from danger such as PC viruses and hard disk crashes.*” ¶ 24:61-65; and the importance of maintaining the confidentiality of private information: “*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*” ¶ 3:40-47; “*For example, any type of demographic questionnaire can be created by a vendor and distributed to users of this system while retaining their individual privacy. The data can be collected and returned to the vendor along with the means of identifying the specific target transaction devices that may subsequently receive the appropriate promotional materials. However, the identity of the user is not revealed. Thus, direct marketing is available to vendors even though user identity confidentiality is maintained. Additionally, the eCommerce system may automatically collect any type of data that can be obtained through use of this system and subsequently sold to third parties.*”

However, individual privacy is always maintained.” ¶5:23-35, “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

5 *information. The TPC 110 maintains a secure database of transaction device information and user information.” ¶6:45-51. Ludtke also describes persistently storing the fingerprint data on the integrated device that cannot be afterward altered: “The fingerprint data entry process may be performed at least twice, to confirm that the user has entered the correct data (using the correct fingerprint).*

10 *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), wherein the biometric data is one selected from a group consisting of facial recognition, a finger-print scan, and a retinal scan of a legitimate user (Ludtke describes: “*The identification by the biometric device*

15 *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);*

receiving, at the smartphone, scan data from a biometric scan using the smartphones (Ludtke describes using biometric verification including a

20 fingerprint to verify the user of the device. Figure 28 shows a device with a Fingerprint Identification Unit (FIU) 2806 and a touchpad 2808 for user input: “*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);

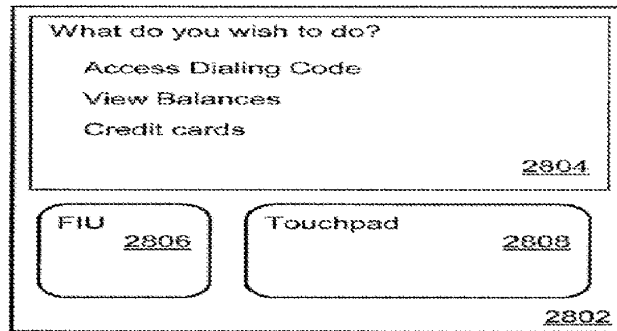


FIG. 28

Fig. 28 of Ludtke.

comparing, using the smartphone, the scan data to the biometric data (Fig. 31 of Ludtke describes the process to verify the user of the device.

As can be seen in the flow chart, the device is continuously looking for a request for verification (“Detect fingerprint 3104”). In response to that request,

it will receive scan data from the touchpad so it can determine whether the fingerprint matches (3106): “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. If a match does not occur, then at 3110 an error message is output and the DW returns to checking to see if a fingerprint has been detected

3104. If the fingerprint does match a stored one, then at 3108 the DW allows access to functions of the DW and access to a selection of codes.” ¶39:49-59).

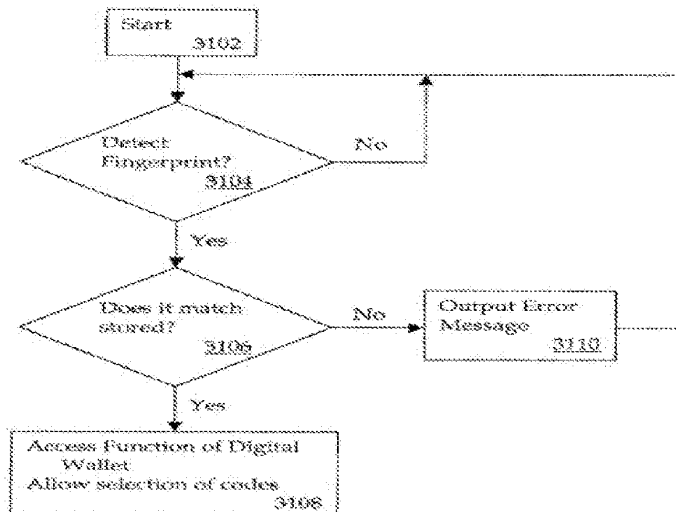


Fig. 31 of Ludtke

5 **responsive to a determination that a scan data matches the**
biometric data (Ludtke describes: “If a fingerprint has been detected, then at
3106 a check is made to see if it matches a stored authorized fingerprint. If a
match does not occur, then at 3110 an error message is output and the DW
returns to checking to see if a fingerprint has been detected 3104. If the
10 fingerprint does match a stored one, then at 3108 the DW allows access to
functions of the DW and access to a selection of codes.” ¶39:52-59), **wirelessly**
sending from the smartphone (Ludtke discloses “... In addition, the
transaction device may contain wireless data communication, data storage and
communication protocols for selectively communicating with outside devices such
15 as a digital wallet described herein, point of sale (POS) terminal or personal

computer (PC) and digital televisions (DTV). ¶5:39-44, and “A variety of communication devices may be used, such as the Internet, direct dial-up modem connections, wireless or cellular signals, etc.” ¶9:39-42), the ID code for comparison by the third-party trusted authority against one or more

5 **previously registered ID codes** (Ludtke discloses the TPCCH 110 includes information that can be compared with information from the consumer 120 and the consumer’s device so the TPCCH 110 can determine whether the consumer 120 is authorized to complete a transaction with the vendor 125: “The transaction device information is provided to the TPCCH 110 that then

10 *indicates to the vendor 125 and the user 120 approval of the transaction to be performed.” ¶6:41-44) maintained by the third-party trusted authority* (Ludtke describes: “The TPCCH 110 maintains a secure database of transaction device information and user information. In one embodiment, the TPCCH 110 interfaces to at least one financial processing system 140 to perform associated

15 *financial transactions, such as confirming sufficient funds to perform the transaction, and transfers to the vendor 125 the fees required to complete the transaction” ¶6:49-55), a transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code* (Ludtke teaches once the TPCCH 110 authenticates the ID code, it provides

20 *notice to the parties and the transaction can be performed and completed: “The transaction device information is provided to the TPCCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed” ¶6:41-44), wherein the transaction being completed includes accessing*

**one or more from a group consisting of a casino machine, a keyless lock,
an ATM machine, a web site, a file and a financial account** (Ludtke teaches:

*“A variety of user interfaces may be used. In one embodiment, an input device
may be incorporated on the transaction device. Alternately or supplementally an
5 input device may be coupled to the transaction device. In one embodiment, an
input device may be provided on a digital wallet coupled to a privacy card. User
inputs may be provided on the POS terminals including a personal POS terminal.”*

¶5:65- ¶6:4. Since Ludtke describes the transaction device as including “a
digital wallet”, a POSITA would recognize as files that allow the user to digitally
10 store credit card and other payment information and to make transactions with
that card. Moreover, the POSITA would recognize that giving access to the
digital wallet is providing access to a financial account) as called for in claim 1.

Although Ludtke discloses “transaction device information” that is
communicated from the consumer’s transaction device (PRIVACYCARD 130) to
15 the TPC 110 for authorization, the storage location for this information and
the importance of maintaining the confidentiality of private information.
However, Ludtke does not specifically indicate that this “transaction device
information” is unique (“ID code” that is unique) to the consumer’s transaction
device, and storage of secret information in the user’s device.

20 Nevertheless, Okereke teaches “... *systems that perform electronic
financial transactions or electronic commerce must protect against unauthorized
access to confidential records and unauthorized modification of data*” ¶[0003].
Okereke discloses “a secret key” that is maintained by the user, and can be

used to encrypt and decrypt information communicated to the user.

Specifically, Okereke discloses the device ID code information in the form of a unique serial number or SIM number for the user device: “... *The proxy server program then awaits the initiation of a request 210 from the desktop to establish*
5 *secure wireless access capabilities using the system of the present invention. 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*
10 *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 148, 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*
15 *using AES (Advanced Encryption Standard)... ¶[0025]. Okereke also teaches “With PKI, a public and a private key are created simultaneously using the same algorithm by a certificate authority... The private key is never shared with anyone or sent across the network...” ¶[0007].*

It would have been obvious to a person of ordinary skill in the art
20 (POSITA) at the time the invention was filed to combine Ludtke’s system with the teachings of Okereke’s unique Device ID, and would have recognized that the “transaction device information” disclosed within Ludtke would include the unique device information taught in Okereke which would ensure that the

information used to authenticate the device only identifies the authorized device. The POSITA would have expected this to yield the predictable result of the option to use PKI-compliant encryption and decryption with a private key (secret information), as well as the ability to ensure authentication of an

5 authorized device using unique device identifying information such as the serial number or SIM. Moreover, Ludtke includes the persistent storage area of the device where the ID code can be stored. The POSITA would have Ludtke's financial system storing the secret information in Ludtke's memory because this is important information that needs to be maintained in the device and

10 using the unique device ID disclosed in Okereke as the transaction device information. Examiners find this combination would be predictable because the use of PKI encryption which taught by Okereke would make the system of Ludtke even more secure. Examiners find this combination is merely the use of a known technique to improve similar devices in a similar way. See MPEP

15 §2143(I)(C). The combination is not seen to create a greater expenditure of time, effort or other resources nor do the references even vaguely include a teaching away of the proposed modification.

In addition, the POSITA would have been motivated to combine Ludtke and Okereke because they are both in the same field of endeavor:

20 authentication of the user and device, including use of biometric information, for the purpose of exchanging sensitive information over network. (Ludtke discloses "*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). Okereke discloses *"In order to begin using the system via wireless device, the user may be required to provide additional forms of authentication to the CPS, such as a password or biometric signature. When the user is authenticated, a secure channel is established between the device*
5 *and the CPS. All user requests to access secure resources are then handled via the CPS, which presents the appropriate user's certificate on their behalf as required."* ¶[0031]).

Regarding claim 2: The method of claim 1, further comprising:

10 **Receiving a request for biometric verification** (Ludtke describes using biometric verification including the fingerprint to verify the user of the device. Figure 28 shows the device with the Fingerprint Identification Unit (FIU) 2806 and the 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*
15 *user after the user had pressed his finger against the FIU 2806."* ¶[39:24-27),
and responsive to a determination that the scan data does not match the biometric data, indicating the smartphone cannot verify the scan data as being from the legitimate user, the smartphone does not send the ID code
(As can be seen in the flow chart shown in Fig. 31 of Ludtke, the device is
20 continuously looking for a request for verification ("Detect fingerprint"). In response to that request, it will receive scan data from the touchpad so it can determine whether the fingerprint matches (3106). If the scan data does not match the stored data (i.e., the device cannot authenticate the user), it will

output an error message, and not allow access to the digital wallet or selection of codes: *“If a fingerprint has been detected, then at 3106 a check is made to see if it matches a stored authorized fingerprint. If a match does not occur, then at 3110 an error message is output and the DW returns to checking to see if a*
5 *fingerprint has been detected 3104. If the fingerprint does match a stored one, then at 3108 the DW allows access to functions of the DW and access to a selection of codes.”* ¶39:52-59).

Regarding claim 3: The method of claim 1, wherein completing the
10 **transaction includes accessing an application** (In Ludtke, access would be given applications of either computer software, a file or both. Ludtke describes the transaction device as including the “digital wallet”. The POSITA would recognize as an application and files that allow the user to digitally store credit card and other payment information and to make transactions with that card.
15 Figs. 5A-5B).

Regarding claim 4: The method of claim 1, wherein the transaction
being completed responsive to the third-party trusted authority
successfully authenticating the ID code includes the third party trusted
20 **authority sending an indication that the third party trusted authority**
authenticated the ID code to another party (Ludtke teaches once the TPC 110 notifies both the user 120 and the vendor 125 (another party) that the TPC 110 authenticated the ID code, the transaction can be completed: *“The*

transaction device information is provided to the TPCCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed."

¶6:41-44)

5 Regarding claim 5: A smartphone (Ludtke discloses "*the transaction device may contain wireless data communication*" ¶5:40-41, "*cell phone functionality built-in*" ¶18:3-4, "*another portable device such as a cell phone*" ¶34:21. Fig. 28 shows "consumer access device" having functions allowing the user to see balances and credit cards, and also to "Access Dialing Codes" is
10 inherently seen as the smartphone), **comprising:**

a persistent storage having an input that receives an identification (ID) code (Ludtke discloses a storage location "*In one embodiment, the TPCCH allows users to backup data that is generated directly on the transaction device, such as a telephone book and appointment information, into a storage location*
15 *managed by the TPCCH.*" ¶10:46-49; "*In addition, it may provide an alternative, non-PC based location from which to securely execute utility applications and to store data, thus enhancing data security and protection from danger such as PC viruses and hard disk crashes.*" ¶24:61-65; and the importance of maintaining the confidentiality of private information: "*The highly secured location,*
20 *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 ¶3:40-47; *“For example, any type of demographic questionnaire can be created by a vendor and distributed to users of this system while retaining their individual privacy. The data can be collected and returned*
5 *to the vendor along with the means of identifying the specific target transaction devices that may subsequently receive the appropriate promotional materials. However, the identity of the user is not revealed. Thus, direct marketing is available to vendors even though user identity confidentiality is maintained. Additionally, the eCommerce system may automatically collect any type of data*
10 *that can be obtained through use of this system and subsequently sold to third parties. However, individual privacy is always maintained.”* ¶5:23-35, *“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*
15 *information. The TPC 110 maintains a secure database of transaction device information and user information.”* ¶6:45-51. Ludtke also describes persistently storing the fingerprint data on the integrated device that cannot be afterward altered: *“The fingerprint data entry process may be performed at least twice, to confirm that the user has entered the correct data (using the correct fingerprint).*
20 *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. It is noted that the storage described in Ludtke would necessarily include an input (through which it receives the data that is stored there)), **from**

a third-party trusted authority (the transaction device (PRIVACYCARD 130) provide information to the TRANSACTION PRIVACY CLEARING HOUSE 110 for authorization for the transaction between the consumer 120 and vendor 125 to be performed: “One embodiment of a system is illustrated in FIG. 1. In this

5 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

10 the transaction to be performed.” ¶6:36-44. The TPCH 110 is not part of the transaction, but rather functions the third-party middleman of the transaction: “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

15 third parties.” ¶7:44-48. This ensures that sensitive information is not shared with the vendor 125), **and biometric data** (Ludtke discloses “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

20 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), **where the biometric data is one selected from a group consisting of facial recognition, a fingerprint scan, and a retinal scan, of a**

legitimate user (Ludtke describes: “*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), **the ID code uniquely identifying**
5 **the smartphone among a plurality of smartphones** (Ludtke discloses the TPOCH 110 having “transaction device information” that is maintained in the secure database by the TPOCH 110: “*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*
10 *transaction. For example, the transaction processing clearing house may access relevant account information to authorize transaction.*” ¶3:40-45. It would therefore be obvious that the ID code originate from the list of device information maintained by the TPOCH 110 and communicated to the smartphone. The TPOCH 110 would include the ID code in communications to
15 the smartphone to ensure verification among the plurality of smartphone);

the persistent storage storing the biometric data and the ID code, the persistent storage having an output (the storage described in Ludtke would necessarily include an output: where the data can be retrieved from the
20 memory for use) **configured to provide a first set of biometric data and the ID code for use on the smartphone** (Examiners interpreting this under 112(6th ¶) as above and this limitation is limited to the ROM, flash memory or other non-volatile memory, etc. and the related programming. Ludtke discloses

the storage: *"In one embodiment, the TPCCH allows users to backup data that is generated directly on the transaction device, such as a telephone book and appointment information, into a storage location managed by the TPCCH."* ¶10:46-49; *"In addition, it may provide an alternative, non-PC based location from which*
5 *to securely execute utility applications and to store data, thus enhancing data security and protection from danger such as PC viruses and hard disk crashes."* ¶24:61-65; and the importance of maintaining the confidentiality of private information: *"The highly secured location, accessible through or part of a transaction processing clearing house (TPCH), provides the transaction*
10 *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"* ¶3:40-47; *"For example, any type of demographic questionnaire can*
15 *be created by a vendor and distributed to users of this system while retaining their individual privacy. The data can be collected and returned to the vendor along with the means of identifying the specific target transaction devices that may subsequently receive the appropriate promotional materials. However, the identity of the user is not revealed. Thus, direct marketing is available to vendors*
20 *even though user identity confidentiality is maintained. Additionally, the eCommerce system may automatically collect any type of data that can be obtained through use of this system and subsequently sold to third parties. However, individual privacy is always maintained."* ¶5:23-35, *"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 TPC 110 maintains a secure database of transaction device information and user information.” ¶6:45-51. Ludtke also describes persistently storing the fingerprint data on the integrated device that cannot be afterward altered: “The fingerprint data entry process may be performed at least twice, to confirm that the user has entered the correct data (using the correct fingerprint). 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);

a validation module (portion of the device that receives the scan and verifies the biometric information), **coupled to communicate with the persistent storage to receive the biometric data from the persistent storage, the validation module having a scan pad to capture scan data from a biometric scan** (Examiners interpreting this under 112(6th ¶) as above and this limitation is limited to the scan pad and the related programming. Figure 28 of Ludtke shows the device with the Fingerprint Identification Unit (FIU) 2806 and the touchpad 2808 for user input: “*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), **the validation module comparing the scan data to the biometric data to determine whether the scan data matches the biometric data** (Fig. 31 of

5 Ludtke describes the process to verify the user of the integrated device. As can be seen in the flow chart, the device is continuously looking for a request for verification (“Detect fingerprint 3104”). In response to that request, it will receive scan data from the touchpad so it can determine whether the fingerprint matches (3106): “At 3102 the user may start a device, such as a
10 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. If a match does not occur, then at 3110 an error message is output and the DW returns to checking to see if a fingerprint has been detected
15 3104. If the fingerprint does match a stored one, then at 3108 the DW allows access to functions of the DW and access to a selection of codes.” ¶39:49-59);
and

a wireless transceiver (Ludtke discloses “In one embodiment, the transaction device may be configured to closely resemble a standard credit card.
20 More particularly, the card may have a magnetic stripe or a smart card chip that functions similarly to standard credit cards. In addition, the transaction device may contain wireless data communication, data storage and communication protocols for selectively communicating with outside devices such as a digital

wallet described herein, point of sale (POS) terminal or personal computer (PC) and digital televisions (DTV).” ¶5:36-44; and “A variety of communication devices may be used, such as the Internet, direct dial-up modem connections, wireless or cellular signals, etc.” ¶9:39-42), **that, responsive to a determination that the**

5 **scan data matches the biometric data, sends the ID code for comparison by the third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority**

(Ludtke describes: “If a fingerprint has been detected, then at 3106 a check is made to see if it matches a stored authorized fingerprint. If a match does not

10 occur, then at 3110 an error message is output and the DW returns to checking to see if a fingerprint has been detected 3104. If the fingerprint does match a stored one, then at 3108 the DW allows access to functions of the DW and access to a selection of codes.” ¶39:52-59), **a transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code**

15 (Ludtke teaches once the TPC 110 authenticates the ID code, it provides notice to the parties and the transaction can be completed: “The transaction device information is provided to the TPC 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed” ¶6:41-44),

wherein the transaction being completed includes accessing one or more

20 **from a group consisting of a casino machine, a keyless lock, an ATM**

machine, a web site, a file and a financial account (Ludtke teaches: “A variety of user interfaces may be used. In one embodiment, an input device may be incorporated on the transaction device. Alternately or supplementally an input

device may be coupled to the transaction device. In one embodiment, an input device may be provided on a digital wallet coupled to a privacy card. User inputs may be provided on the POS terminals including a personal POS terminal."

¶5:65- ¶6:4. Since Ludtke describes the transaction device as including "a
5 digital wallet", the POSITA would recognize as files that allow the user to digitally store credit card and other payment information and to make transactions with that card. Moreover, the POSITA would recognize that giving access to the digital wallet is providing access to the financial account) as called for in claim 5.

10 Although Ludtke discloses "transaction device information" that is communicated from the consumer's transaction device (PRIVACYCARD 130) to the TPC 110 for authorization, the storage location for this information and the importance of maintaining the confidentiality of private information. However, Ludtke does not specifically indicate that this "transaction device
15 information" is unique ("ID code" that is unique) to the consumer's transaction device, and storage of secret information in the user's device.

Nevertheless, Okereke teaches "... *systems that perform electronic financial transactions or electronic commerce must protect against unauthorized access to confidential records and unauthorized modification of data*" ¶[0003].

20 Okereke discloses "a secret key" that is maintained by the user, and can be used to encrypt and decrypt information communicated to the user.

Specifically, Okereke discloses the device ID code information in the form of a unique serial number or SIM number for the user device: "... *The proxy server*

program then awaits the initiation of a request 210 from the desktop to establish secure wireless access capabilities using the system of the present invention. 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

5 *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 148, which executes*

10 *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)... ¶[0025]. Okereke also teaches “With PKI, a public and a private key are created simultaneously using the same algorithm by a certificate authority... The private key is never shared with*

15 *anyone or sent across the network...” ¶[0007].*

It would have been obvious to the POSITA at the time the invention was filed to combine Ludtke’s system with the teachings of Okereke’s unique Device ID, and would have recognized that the “transaction device information” disclosed within Ludtke would include the unique device information taught in

20 Okereke which would ensure that the information used to authenticate the device only identifies the authorized device. The POSITA would have expected this to yield the predictable result of the option to use PKI-compliant encryption and decryption with the private key (secret information), as well as

the ability to ensure authentication of the authorized device using unique device identifying information such as the serial number or SIM. Moreover, Ludtke includes the persistent storage area of the device where the ID code can be stored. The POSITA would have Ludtke's financial system storing the secret information in Ludtke's memory because this is important information that needs to be maintained in the device and using the unique device ID disclosed in Okereke as the transaction device information. Examiners find this combination would be predictable because the use of PKI encryption which taught by Okereke would make the system of Ludtke even more secure.

Examiners find this combination is merely the use of a known technique to improve similar devices in a similar way. See MPEP §2143(I)(C). The combination is not seen to create a greater expenditure of time, effort or other resources nor do the references even vaguely include a teaching away of the proposed modification.

In addition, the POSITA would have been motivated to combine Ludtke and Okereke because they are both in the same field of endeavor: authentication of the user and device, including use of biometric information, for the purpose of exchanging sensitive information over network. (Ludtke discloses "*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). Okereke discloses "*In order to begin using the system via wireless device, the user may be required to provide additional forms of authentication to the CPS, such as a password or biometric signature. When*

the user is authenticated, a secure channel is established between the device and the CPS. All user requests to access secure resources are then handled via the CPS, which presents the appropriate user's certificate on their behalf as required.” ¶[0031]).

5

Regarding claim 6: **The smartphone of claim 5, wherein the ID code is transmitted to the third-party trusted authority over a network** (Ludtke discloses “The *transaction device information is provided to the TPC 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to* be performed” ¶6:41-44), and “The *incoming communication 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.”* ¶9:36-42).

10

15

Regarding claim 7: **A system, comprising:**

a smartphone (Examiners interpreting this under 112(6th ¶) as above and this limitation is limited to the smartphone and the related programming. Ludtke discloses “*the transaction may contain wireless data communication*” ¶5:40-41, “*cell phone functionality built-in*” ¶18:3-4, “*another portable device such as a cell phone*” ¶34:21. Fig. 28 discloses “consumer access device” having functions allowing the user to see balances and credit cards, and also to

20

“Access Dialing Codes” is inherently seen as the smartphone) **that persistently stores biometric data and an ID code** (Ludtke discloses the storage “*In one embodiment, the TPOCH allows users to backup data that is generated directly on the transaction device, such as a telephone book and appointment information,*
5 *into a storage location managed by the TPOCH.*” ¶10:46-49; “*In addition, it may provide an alternative, non-PC based location from which to securely execute utility applications and to store data, thus enhancing data security and protection from danger such as PC viruses and hard disk crashes.*” ¶24:61-65; and the importance of maintaining the confidentiality of private information:
10 “*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*
15 *externally so that confidentiality of the user's identity is maintained*” ¶3:40-47; “*For example, any type of demographic questionnaire can be created by a vendor and distributed to users of this system while retaining their individual privacy. The data can be collected and returned to the vendor along with the means of identifying the specific target transaction devices that may subsequently receive*
20 *the appropriate promotional materials. However, the identity of the user is not revealed. Thus, direct marketing is available to vendors even though user identity confidentiality is maintained. Additionally, the eCommerce system may automatically collect any type of data that can be obtained through use of this*

system and subsequently sold to third parties. However, individual privacy is always maintained.” ¶5:23-35, “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 TPC 110 maintains a secure database of transaction device information and user information.” ¶6:45-51. Ludtke also describes persistently storing the fingerprint data on the integrated device that cannot be afterward altered: “The fingerprint data entry process may be performed at least twice, to confirm that the user has entered the correct data (using the correct fingerprint). 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), **wherein the biometric data is one selected from a group consisting of facial recognition, a fingerprint scan, and a retinal scan data of a legitimate user** (Ludtke describes: “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.” ¶35:60-64), **and the ID code is received from a third-party trusted authority** (Ludtke discloses the transaction device (PRIVACYCARD 130) provide information to the TRANSACTION PRIVACY CLEARING HOUSE 110 for authorization for the transaction between the consumer 120 and vendor 125 to be performed: “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 TPCCH 110 that then indicates to the vendor 125 and the user 120 approval of the

5 *transaction to be performed”.*¶6:36-44. The TPCCH 110 is not part of the transaction, but rather functions a third-party middleman of the transaction:

“In one embodiment of electronic distribution, the TPCCH 110 functions as the middleman of the distribution channel. This allows the TPCCH 110 to retain user privacy by not exposing addressing information and possibly email addresses to

10 *third parties.”* ¶7:44-48. This ensures that sensitive information is not shared with the vendor 125), **the ID code uniquely identifying the smartphone among a plurality of smartphones** (Ludtke discloses the TPCCH 110 having “transaction device information” that is maintained in a secure database by the TPCCH 110: “*The highly secured location, accessible through or part of a*

15 *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 transaction.”* ¶3:40-45. It would therefore be obvious that the ID code originate from the list of device information

20 maintained by the TPCCH 110 and communicated to the smartphone. The TPCCH 110 would include the ID code in communications to the smartphone to ensure verification among the plurality of smartphones), **the smartphone configured to indicate that a biometric authentication is requested** (Ludtke describes

using biometric verification including the fingerprint to verify the user of the device. Figure 28 shows the device with the Fingerprint Identification Unit (FIU) 2806 and the touchpad 2808 for user input: “*The consumer access device 2802 has an LCD screen 2804 showing text, a biometric identification unit, in this*
5 *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), **the smartphone configured to wirelessly send the ID code to the third-party trusted**
10 **authority** (Examiners interpreting this under 112(6th ¶) as above and this limitation is limited to the server or other computerized device software program. Ludtke discloses “*In one embodiment, the transaction device may be configured to closely resemble a standard credit card. More particularly, the card may have a magnetic stripe or a smart card chip that functions similarly to*
15 *standard credit cards. In addition, the transaction device may contain wireless data communication, data storage and communication protocols for selectively communicating with outside devices such as a digital wallet described herein, point of sale (POS) terminal or personal computer (PC) and digital televisions (DTV).*” ¶5:36-44, and “*A variety of communication devices may be used, such as*
20 *the Internet, direct dial-up modem connections, wireless or cellular signals, etc.*” ¶9:39-42) **for authentication responsive to determining that scan data from a biometric scan performed using the smartphone matches the biometric data of the legitimate user** (Fig. 31 of Ludtke describes the process

to verify the user of the integrated device. As can be seen in the flow chart, the device is continuously looking for a request for verification ("Detect fingerprint 3104"). In response to that request, it will receive scan data from the touchpad so it can determine whether the fingerprint matches (3106): "At 3102 the user
5 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. If a match does not occur, then at 3110 an error message is output and the DW returns to checking to see if a
10 fingerprint has been detected 3104. If the fingerprint does match a stored one, then at 3108 the DW allows access to functions of the DW and access to a selection of codes." ¶39:49-59), **wherein a transaction is completed responsive to successful authentication of the ID code by the third-party trusted authority** (Ludtke teaches once the TPC 110 authenticates the ID
15 code, it provides notice to the parties and the transaction can be completed: "The transaction device information is provided to the TPC 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed" ¶6:41-44), **wherein the transaction being completed includes accessing one or more from a group consisting of a casino machine, a
20 keyless lock, an ATM machine, a web site, a file and a financial account** (Ludtke teaches: "A variety of user interfaces may be used. In one embodiment, an input device may be incorporated on the transaction device. Alternately or supplementally an input device may be coupled to the transaction device. In one

embodiment, an input device may be provided on a digital wallet coupled to a privacy card. User inputs may be provided on the POS terminals including a personal POS terminal.” ¶5:65- ¶6:4. Since Ludtke describes the transaction device as including “a digital wallet”, the POSITA would recognize as files that

5 *allow the user to digitally store credit card and other payment information and to make transactions with that card. Moreover, the POSITA would recognize that giving access to the digital wallet is providing access to the financial account); and*

the third-party trusted authority operated by a third party (Ludtke

10 *discloses the transaction device (PRIVACYCARD 130) provides information to the TRANSACTION PRIVACY CLEARING HOUSE 110 for authorization for the transaction between the consumer 120 and vendor 125 to be performed: “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*

15 *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. The TPCH 110 is not part of the*

20 *transaction, but rather functions a third-party middleman of the transaction: “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.” ¶7:44-48. This ensures that sensitive information is not shared with the vendor 125), **the third-party trusted authority storing a plurality of legitimate ID codes and authenticating the ID code received based on a comparison of the ID code received and the legitimate ID codes included**

5 **in the plurality of the legitimate ID codes** (Ludtke discloses the TPCH 110 includes information that can be compared with information from the consumer 120 and the consumer’s device so the TPCH 110 can determine whether the consumer 120 is authorized to complete a transaction with the vendor 125: “The *transaction device information is provided to the TPCH 110*

10 *that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed.*” ¶6:41-44, 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

15 *see if it matches a stored authorized fingerprint. If a match does not occur, then at 3110 an error message is output and the DW returns to checking to see if a fingerprint has been detected 3104. If the fingerprint does match a stored one, then at 3108 the DW allows access to functions of the DW and access to a selection of codes.*” ¶39:49-59) as called for in claim 7.

20 Although Ludtke discloses “transaction device information” that is communicated from the consumer’s transaction device (PRIVACYCARD 130) to the TPCH 110 for authorization, the storage location for this information and the importance of maintaining the confidentiality of private information.

However, Ludtke does not specifically indicate that this “transaction device information” is unique (“ID code” that is unique) to the consumer’s transaction device, and storage of secret information in the user’s device.

Nevertheless, Okereke teaches “... *systems that perform electronic*
5 *financial transactions or electronic commerce must protect against unauthorized*
access to confidential records and unauthorized modification of data” ¶[0003].
Okereke discloses “a secret key” that is maintained by the user, and can be
used to encrypt and decrypt information communicated to the user.
Specifically, Okereke discloses the device ID code information in the form of a
10 unique serial number or SIM number for the user device: “... *The proxy server*
program then awaits the initiation of a request 210 from the desktop to establish
secure wireless access capabilities using the system of the present invention. 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
15 *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 148, which executes
20 *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)... ¶[0025]). Okereke also teaches
“With PKI, a public and a private key are created simultaneously using the same

algorithm by a certificate authority... The private key is never shared with anyone or sent across the network...” ¶[0007]”.

It would have been obvious to a person of ordinary skill in the art (POSITA) at the time the invention was filed to combine Ludtke’s system with
5 the teachings of Okereke’s unique Device ID, and would have recognized that the “transaction device information” disclosed within Ludtke would include the unique device information taught in Okereke which would ensure that the information used to authenticate the device only identifies the authorized device. The POSITA would have expected this to yield the predictable result of
10 the option to use PKI-compliant encryption and decryption with the private key (secret information), as well as the ability to ensure authentication of an authorized device using unique device identifying information such as the serial number or SIM. Moreover, Ludtke includes the persistent storage area of the device where the ID code can be stored. The POSITA would have Ludtke’s
15 financial system storing the secret information in Ludtke’s memory because this is important information that needs to be maintained in the device and using the unique device ID disclosed in Okereke as the transaction device information. Examiners find this combination would be predictable because the use of PKI encryption which taught by Okereke would make the system of
20 Ludtke even more secure. Examiners find this combination is merely the use of a known technique to improve similar devices in a similar way. See MPEP §2143(I)(C). The combination is not seen to create a greater expenditure of

time, effort or other resources nor do the references even vaguely include a teaching away of the proposed modification.

In addition, the POSITA would have been motivated to combine Ludtke and Okereke because they are both in the same field of endeavor:

5 authentication of the user and device, including use of biometric information, for the purpose of exchanging sensitive information over network. (Ludtke discloses “*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). Okereke discloses “*In order to begin using the*
10 *system via wireless device, the user may be required to provide additional forms of authentication to the CPS, such as a password or biometric signature. When the user is authenticated, a secure channel is established between the device and the CPS. All user requests to access secure resources are then handled via the CPS, which presents the appropriate user's certificate on their behalf as*
15 *required.*” ¶[0031]).

Regarding claim 8: **The system of claim 7, wherein the smartphone receives an authentication request, and in response, requests biometric scan from a user to generate the scan data and, when the smartphone**
20 **cannot verify the scan data as being from the legitimate user, the smartphone does not send the ID code** (As can be seen in the flow chart shown in Fig. 31 of Ludtke, the device is continuously looking for a request for verification (“Detect fingerprint”). In response to that request, it will receive

scan data from the touchpad so it can determine whether the fingerprint matches (3106). If the scan data does not match the stored data (i.e., the device cannot authenticate the user), it will output an error message, and not allow access to the digital wallet or selection of codes: *"If a fingerprint has been*
5 *detected, then at 3106 a check is made to see if it matches a stored authorized fingerprint. If a match does not occur, then at 3110 an error message is output and the DW returns to checking to see if a fingerprint has been detected 3104. If the fingerprint does match a stored one, then at 3108 the DW allows access to functions of the DW and access to a selection of codes."* ¶39:52-59).

10

Regarding claim 9: **The system of claim 7, wherein completing the transaction includes accessing an application** (In Ludtke, access would be given applications of either computer software, a file or both. Ludtke describes the transaction device as including the "digital wallet". The POSITA would
15 recognize as an application and files that allow the user to digitally store credit card and other payment information and to make transactions with that card. See Fig. 5a-b).

2/ Claims 1-9 are rendered obvious under 35 U.S.C. §103 over
20 **Ludtke in view with Scott.**

Ludtke teaches in Fig. 1 a method comprising:

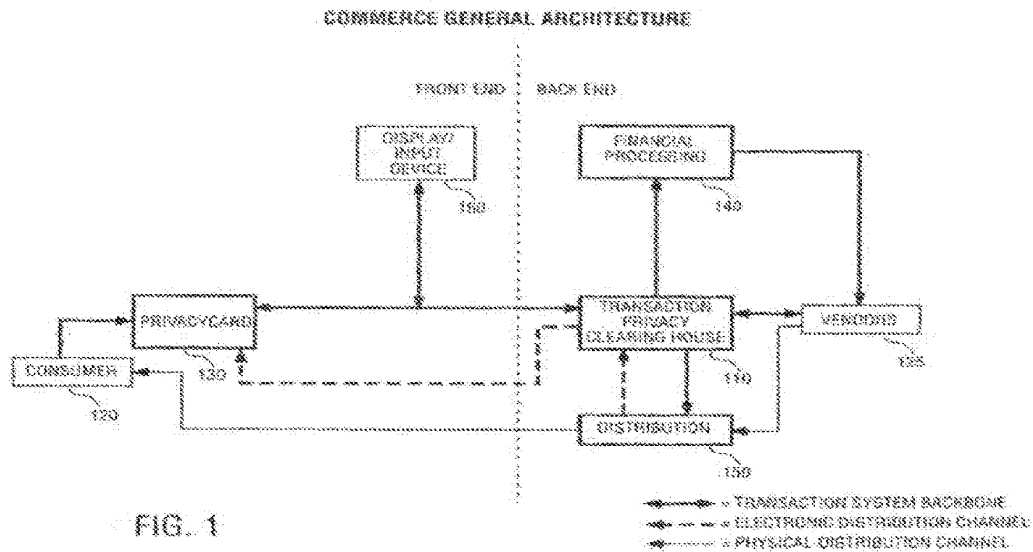


Fig. 1 of Ludtke.

receiving, at a smartphone (Ludtke discloses “the transaction device
5 may contain wireless data communication” ¶5:40-41, “cell phone functionality
built-in” ¶18:3-4, “another portable device such as a cell phone” ¶34:21. Fig. 28
discloses “consumer access device” having functions allowing the user to see
balances and credit cards, and also to “Access Dialing Codes” is inherently
seen as the smartphone), **an identification (ID) code from a third-party**
10 **trusted authority** (Ludtke discloses a transaction device (PRIVACYCARD 130)
provide information to a TRANSACTION PRIVACY CLEARING HOUSE 110 for
authorization for the transaction between a consumer 120 and vendors 125 to
be performed: “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 TPOCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed.” ¶6:36-44. The TPOCH 110 is not part of the transaction, but rather functions a third-party middleman of the transaction: “In one embodiment of electronic distribution, the TPOCH 110 functions as the middleman of the distribution channel. This allows the TPOCH 110 to retain user privacy by not exposing addressing information and possibly email addresses to third parties.” ¶7:44-48. This ensures that sensitive information is not shared with the vendor 125), **the ID code uniquely identifying the smartphone among a plurality of smartphones** (Ludtke discloses the TPOCH 110 having “transaction device information” that is maintained in a secure database by the TPOCH 110: “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 transaction.” ¶3:40-45). It would therefore be obvious that the ID code originate from the list of device information maintained by the TPOCH 110 and communicated to the smartphone. The TPOCH 110 would include the ID code in communications to the smartphone to ensure verification among the plurality of smartphone);

persistently storing biometric data and an ID code on a smartphone

(Ludtke discloses a storage location “*In one embodiment, the TPCH allows users to backup data that is generated directly on the transaction device, such as a telephone book and appointment information, into a storage location managed by the TPCH.*” ¶ 10:46-49; “*In addition, it may provide an alternative, non-PC based location from which to securely execute utility applications and to store data, thus enhancing data security and protection from danger such as PC viruses and hard disk crashes.*” ¶ 24:61-65; and the importance of maintaining the confidentiality of private information: “*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*” ¶ 3:40-47; “*For example, any type of demographic questionnaire can be created by a vendor and distributed to users of this system while retaining their individual privacy. The data can be collected and returned to the vendor along with the means of identifying the specific target transaction devices that may subsequently receive the appropriate promotional materials. However, the identity of the user is not revealed. Thus, direct marketing is available to vendors even though user identity confidentiality is maintained. Additionally, the eCommerce system may automatically collect any type of data that can be obtained through use of this system and subsequently sold to third parties.*”

However, individual privacy is always maintained.” ¶5:23-35, “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

5 *information. The TPC 110 maintains a secure database of transaction device information and user information.” ¶6:45-51. Ludtke also describes persistently storing the fingerprint data on the integrated device that cannot be afterward altered: “The fingerprint data entry process may be performed at least twice, to confirm that the user has entered the correct data (using the correct fingerprint).*

10 *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), wherein the biometric data is one selected from a group consisting of facial recognition, a finger-print scan, and a retinal scan of a legitimate user (Ludtke describes: “The identification by the biometric device

15 *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);*

receiving, at the smartphone, scan data from a biometric scan using the smartphones (Ludtke describes using biometric verification including a

20 *fingerprint to verify the user of the device. Figure 28 shows a device with a Fingerprint Identification Unit (FIU) 2806 and a touchpad 2808 for user input: “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);

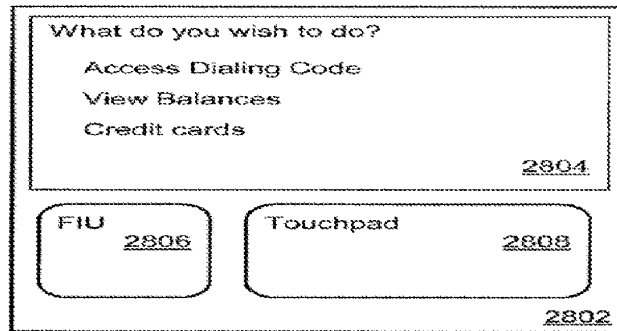


FIG. 28

Fig. 28 of Ludtke.

comparing, using the smartphone, the scan data to the biometric data (Fig. 31 of Ludtke describes the process to verify the user of the device.

10 As can be seen in the flow chart, the device is continuously looking for a request for verification (“Detect fingerprint 3104”). In response to that request, it will receive scan data from the touchpad so it can determine whether the fingerprint matches (3106): “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
15 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. If a match does not occur, then at 3110 an error message is output and the DW returns to checking to see if a fingerprint has been detected

3104. If the fingerprint does match a stored one, then at 3108 the DW allows access to functions of the DW and access to a selection of codes.” ¶39:49-59).

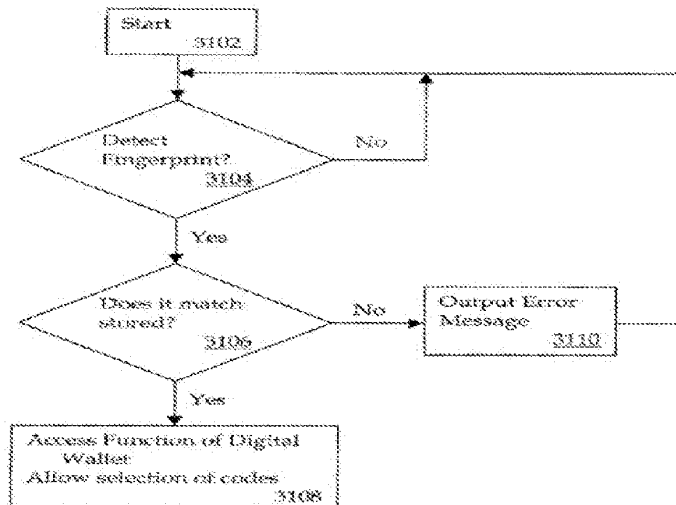


Fig. 31 of Ludtke

5

responsive to a determination that a scan data matches the biometric data (Ludtke describes: “If a fingerprint has been detected, then at 3106 a check is made to see if it matches a stored authorized fingerprint. If a match does not occur, then at 3110 an error message is output and the DW returns to checking to see if a fingerprint has been detected 3104. If the fingerprint does match a stored one, then at 3108 the DW allows access to functions of the DW and access to a selection of codes.” ¶39:52-59), **wirelessly sending from the smartphone** (Ludtke discloses “In one embodiment, the transaction device may be configured to closely resemble a standard credit card. More particularly, the card may have a magnetic stripe or a smart card chip that

10

15

functions similarly to standard credit cards. In addition, the transaction device may contain wireless data communication, data storage and communication protocols for selectively communicating with outside devices such as a digital wallet described herein, point of sale (POS) terminal or personal computer (PC) and digital televisions (DTV)." ¶5:36-44, and "A variety of communication devices may be used, such as the Internet, direct dial-up modem connections, wireless or cellular signals, etc." ¶9:39-42), **the ID code for comparison by the third-party trusted authority against one or more previously registered ID codes** (Ludtke discloses the TPC 110 includes information that can be compared with information from the consumer 120 and the consumer's device so the TPC 110 can determine whether the consumer 120 is authorized to complete a transaction with the vendor 125: "The *transaction device information is provided to the TPC 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed.*" ¶6:41-44) **maintained by the third-party trusted authority** (Ludtke describes: "The TPC 110 maintains a secure database of transaction device information and user information. In one embodiment, the TPC 110 interfaces to at least one financial processing system 140 to perform associated financial transactions, such as confirming sufficient funds to perform the transaction, and transfers to the vendor 125 the fees required to complete the transaction" ¶6:49-55), **a transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code** (Ludtke teaches once the TPC 110 authenticates the ID code, it provides notice to the parties and the transaction can be

performed and completed: “The *transaction device information is provided to the TPCCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed*” ¶6:41-44), **wherein the transaction being completed includes accessing one or more from a group consisting of a**

5 **casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account** (Ludtke teaches: “A *variety of user interfaces may be used. In one embodiment, an input device may be incorporated on the transaction device. Alternately or supplementally an input device may be coupled to the transaction device. In one embodiment, an input device may be provided on a*

10 *digital wallet coupled to a privacy card. User inputs may be provided on the POS terminals including a personal POS terminal.*” ¶5:65- ¶6:4. Since Ludtke describes the transaction device as including “a digital wallet”, a POSITA would recognize as files that allow the user to digitally store credit card and other payment information and to make transactions with that card. Moreover, the

15 POSITA would recognize that giving access to the digital wallet is providing access to a financial account) as called for in claim 1.

Although Ludtke discloses “transaction device information” that is communicated from the consumer’s transaction device (PRIVACYCARD 130) to the TPCCH 110 for authorization, the storage location for this information and

20 the importance of maintaining the confidentiality of private information. However, Ludtke does not specifically indicate that this “transaction device information” is unique (“ID code” that is unique) to the consumer’s transaction device, and storage of secret information in the user’s device.

Nevertheless, Scott teaches authenticating a user using a “personal identification device” (PID) for protected application: “*The personal identification device and system of the invention has several advantages ... The private key used by the device is never disclosed.*” ¶8:13-22. Scott also teaches a unique

5 ID code identifying each device, which may be set by the device manufacturer and can be the device serial number. “*Memory 20 stores information that is specific to processing unit 16. Memory 20 stores an ID code that is set in PID 6 by the manufacturer. The ID code of a device, which may be the device serial number, is unique to each device...*” ¶11:11-13. Scott further discloses the

10 device’s memory 20 stores a private key unique to each device and used for encryption: “*The processor unit employs the encryption algorithm and the private key to encrypt the host response signal to create the verification signal, and causes the transmitter circuit to transmit the verification signal to the host system only if the biometric signal corresponds sufficiently to the biometric data*

15 *to verify that the user is the enrolled person.*” ¶4:14-18, “*Processing unit 16 also includes an encryption algorithm incorporated into an encoder 23. In the embodiment illustrated in FIG. 1, the encryption algorithm is programmed into processor circuit 18. A private key that is stored in memory 20 is used with the encryption algorithm for encryption. The private key can be set into memory by*

20 *the manufacture, and is specific to each PID 6. Different PIDs 6, which have different processing units 16, will typically have different private keys...*”

¶11:24-29, “*encrypting the random number signal with the transmitting device,*

the random number signal being encrypted according to an encryption algorithm employing a private key associated only with the transmitting device” ¶28:13-15.

It would have been obvious to a person of ordinary skill in the art (POSITA) at the time the invention was filed to modify the system of Ludtke to
5 incorporate the private key structure, specifically the unique serial numbers and store permanent information such as the private key and unique serial numbers as taught by Scott for the purpose of providing secure wireless communication. The POSITA would have recognized that the “transaction device information” of Ludtke would necessarily include the unique device
10 information, which would ensure that the information used to authenticate the device only identifies the authorized device. Since Ludtke includes the persistent storage area of the device where the ID code can be stored. The POSITA would have stored the unique device identifiers and the secret key in the persistent memory of Ludtke with the teachings of Scott’s unique Device ID
15 since this is important information that allows authorization and sensitive communication to take place. Examiners find this combination is merely the use of a known technique to improve similar devices in a similar way. See MPEP §2143(I)(C). The combination is not seen to create a greater expenditure of time, effort or other resources nor do the references even vaguely include a
20 teaching away of the proposed modification.

In addition, the POSITA would have been motivated to combine Ludtke and Scott because they are both in the same field of endeavor: authentication of a device, including use of biometric information, for the purpose of

exchanging sensitive information over a network. (Ludtke discloses “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). Scott discloses “A *portable, hand-held personal identification device*
5 *(6) and method for providing secure access to a host facility (4) includes a biometric sensory system capable of sensing a biometric trait of a user that is unique to the user and providing a biometric signal indicative of the sensed biometric trait...*” (Abstract)). .

10 Regarding claim 2: **The method of claim 1, further comprising:**

Receiving a request for biometric verification (Ludtke describes using biometric verification including the fingerprint to verify the user of the device. Figure 28 shows the device with the Fingerprint Identification Unit (FIU) 2806 and the touchpad 2808 for user input: “*The user of the consumer access device*
15 *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.*” ¶39:24-27),
 and responsive to a determination that the scan data does not match the biometric data, indicating the smartphone cannot verify the scan data as being from the legitimate user, the smartphone does not send the ID code
20 (As can be seen in the flow chart shown in Fig. 31 of Ludtke, the device is continuously looking for a request for verification (“Detect fingerprint”). In response to that request, it will receive scan data from the touchpad so it can determine whether the fingerprint matches (3106). If the scan data does not

match the stored data (i.e., the device cannot authenticate the user), it will output an error message, and not allow access to the digital wallet or selection of codes: *“If a fingerprint has been detected, then at 3106 a check is made to see if it matches a stored authorized fingerprint. If a match does not occur, then at*
5 *3110 an error message is output and the DW returns to checking to see if a fingerprint has been detected 3104. If the fingerprint does match a stored one, then at 3108 the DW allows access to functions of the DW and access to a selection of codes.” ¶39:52-59).*

10 Regarding claim 3: **The method of claim 1, wherein completing the transaction includes accessing an application** (In Ludtke, access would be given applications of either computer software, a file or both. Ludtke describes the transaction device as including the “digital wallet”. The POSITA would recognize as an application and files that allow the user to digitally store credit
15 card and other payment information and to make transactions with that card. Figs. 5A-5B).

Regarding claim 4: **The method of claim 1, wherein the transaction being completed responsive to the third-party trusted authority**
20 **successfully authenticating the ID code includes the third party trusted authority sending an indication that the third party trusted authority authenticated the ID code to another party** (Ludtke teaches once the TPCB 110 notifies both the user 120 and the vendor 125 (another party) that the

TPCH 110 authenticated the ID code, the transaction can be completed: “*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.*” ¶6:41-44).

5

Regarding claim 5: A smartphone (Ludtke discloses “*the transaction device may contain wireless data communication*” ¶5:40-41, “*cell phone functionality built-in*” ¶18:3-4, “*another portable device such as a cell phone*” ¶34:21. Fig. 28 discloses “consumer access device” having functions allowing the user to see balances and credit cards, and also to “Access Dialing Codes” is inherently seen as the smartphone), **comprising:**

a persistent storage having an input that receives an identification (ID) code (Ludtke discloses the storage “*In one embodiment, the TPCH allows users to backup data that is generated directly on the transaction device, such as a telephone book and appointment information, into a storage location managed by the TPCH.*” ¶10:46-49; “*In addition, it may provide an alternative, non-PC based location from which to securely execute utility applications and to store data, thus enhancing data security and protection from danger such as PC viruses and hard disk crashes.*” ¶24:61-65; and the importance of maintaining the confidentiality of private information: “*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 ¶3:40-47; *“For example, any type of demographic questionnaire can be created by a vendor and distributed to users of this system while retaining their individual privacy. The data can be collected and returned to the vendor along with the means of identifying the specific target transaction devices that may subsequently receive the appropriate promotional materials. However, the identity of the user is not revealed. Thus, direct marketing is available to vendors even though user identity confidentiality is maintained.*

10 *Additionally, the eCommerce system may automatically collect any type of data that can be obtained through use of this system and subsequently sold to third parties. However, individual privacy is always maintained.”* ¶5:23-35, *“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*

15 *other entities do not have user information but rather transaction device information. The TPC 110 maintains a secure database of transaction device information and user information.”* ¶6:45-51. Ludtke also describes persistently storing the fingerprint data on the integrated device that cannot be afterward altered: *“The fingerprint data entry process may be performed at least twice, to*

20 *confirm that the user has entered the correct data (using the correct fingerprint). 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. It is noted that the storage described in Ludtke would necessarily

include an input (through which it receives the data that is stored there), **from a third-party trusted authority** (the transaction device (PRIVACYCARD 130) provide information to the TRANSACTION PRIVACY CLEARING HOUSE 110 for authorization for the transaction between the consumer 120 and vendor 125 to

5 be performed: “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

10 the TPCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed.”¶6:36-44. The TPCH 110 is not part of the transaction, but rather functions the third-party middleman of the transaction: “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

15 privacy by not exposing addressing information and possibly email addresses to third parties.” ¶7:44-48. This ensures that sensitive information is not shared with the vendor 125), **and biometric data** (Ludtke discloses “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)

20 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), **where the biometric data is one selected from a group**

consisting of facial recognition, a fingerprint scan, and a retinal scan, of a legitimate user (Ludtke describes: “*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* 5 *profile, face recognition, etc.*” ¶35:61-64), **the ID code uniquely identifying the smartphone among a plurality of smartphones** (Ludtke discloses the TPOCH 110 having “transaction device information” that is maintained in the secure database by the TPOCH 110: “*The highly secured location, accessible through or part of a transaction processing clearing house (TPCH), provides the* 10 *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 transaction.*” ¶3:40-45. It would therefore be obvious that the ID code originate from the list of device information maintained by the TPOCH 110 and communicated to the 15 smartphone. The TPOCH 110 would include the ID code in communications to the smartphone to ensure verification);

the persistent storage storing the biometric data and the ID code, the persistent storage having an output (the storage described in Ludtke would necessarily include an output: where the data can be retrieved from the 20 memory for use) **configured to provide a first set of biometric data and the ID code for use on the smartphone** (Examiners interpreting this under 112(6th ¶) as above and this limitation is limited to the ROM, flash memory or other non-volatile memory, etc. and the related programming. Ludtke discloses

the storage: *"In one embodiment, the TPCCH allows users to backup data that is generated directly on the transaction device, such as a telephone book and appointment information, into a storage location managed by the TPCCH."* ¶10:46-49; *"In addition, it may provide an alternative, non-PC based location from which to securely execute utility applications and to store data, thus enhancing data security and protection from danger such as PC viruses and hard disk crashes."* ¶24:61-65; and the importance of maintaining the confidentiality of private information: *"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"* ¶3:40-47; *"For example, any type of demographic questionnaire can be created by a vendor and distributed to users of this system while retaining their individual privacy. The data can be collected and returned to the vendor along with the means of identifying the specific target transaction devices that may subsequently receive the appropriate promotional materials. However, the identity of the user is not revealed. Thus, direct marketing is available to vendors even though user identity confidentiality is maintained. Additionally, the eCommerce system may automatically collect any type of data that can be obtained through use of this system and subsequently sold to third parties. However, individual privacy is always maintained."* ¶5:23-35, *"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 TPC 110 maintains a secure database of transaction device information and user information.” ¶6:45-51. Ludtke also describes persistently storing the fingerprint data on the integrated device that cannot be afterward altered: “The fingerprint data entry process may be performed at least twice, to confirm that the user has entered the correct data (using the correct fingerprint). 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);

a validation module (portion of the device that receives the scan and verifies the biometric information), **coupled to communicate with the persistent storage to receive the biometric data from the persistent storage, the validation module having a scan pad to capture scan data from a biometric scan** (Examiners interpreting this under 112, 6th as above and this limitation is limited to the scan pad and the related programming. Ludtke describes using biometric verification including the fingerprint to verify the user of the device. Figure 28 shows the device with the Fingerprint Identification Unit (FIU) 2806 and the touchpad 2808 for user input: “*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), **the validation module comparing the scan data to the biometric data to determine whether the scan data matches the biometric**

5 **data** (Fig. 31 of Ludtke describes the process to verify the user of the integrated device. As can be seen in the flow chart, the device is continuously looking for a request for verification (“Detect fingerprint 3104”). In response to that request, it will receive scan data from the touchpad so it can determine whether the fingerprint matches (3106): “At 3102 the user may start a device,
10 *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. If a match does not occur, then at 3110 an error message is output and the DW returns to checking to see if a fingerprint has been*
15 *detected 3104. If the fingerprint does match a stored one, then at 3108 the DW allows access to functions of the DW and access to a selection of codes.” ¶39:49-59); and*

a wireless transceiver (Ludtke discloses “In one embodiment, the
20 *transaction device may be configured to closely resemble a standard credit card. More particularly, the card may have a magnetic stripe or a smart card chip that functions similarly to standard credit cards. In addition, the transaction device may contain wireless data communication, data storage and communication*

protocols for selectively communicating with outside devices such as a digital wallet described herein, point of sale (POS) terminal or personal computer (PC) and digital televisions (DTV). ¶5:36-44; and “A variety of communication devices may be used, such as the Internet, direct dial-up modem connections, wireless or

5 *cellular signals, etc.” ¶9:39-42), **that, responsive to a determination that the scan data matches the biometric data, sends the ID code for comparison by the third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority***

(Ludtke describes: “If a fingerprint has been detected, then at 3106 a check is

10 *made to see if it matches a stored authorized fingerprint. If a match does not occur, then at 3110 an error message is output and the DW returns to checking to see if a fingerprint has been detected 3104. If the fingerprint does match a stored one, then at 3108 the DW allows access to functions of the DW and access to a selection of codes.” ¶39:52-59), **a transaction being completed responsive to***

15 ***the third-party trusted authority successfully authenticating the ID code***

(Ludtke teaches once the TPC 110 authenticates the ID code, it provides notice to the parties and the transaction can be completed: “The transaction device information is provided to the TPC 110 that then indicates to the vendor

125 *and the user 120 approval of the transaction to be performed” ¶6:41-44),*

20 ***wherein the transaction being completed includes accessing one or more from a group consisting of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account*** (Ludtke teaches: “A variety of user interfaces may be used. In one embodiment, an input device may

be incorporated on the transaction device. Alternately or supplementally an input device may be coupled to the transaction device. In one embodiment, an input device may be provided on a digital wallet coupled to a privacy card. User inputs may be provided on the POS terminals including a personal POS terminal."

5 ¶5:65- ¶6:4. Since Ludtke describes the transaction device as including "a digital wallet", the POSITA would recognize as files that allow the user to digitally store credit card and other payment information and to make transactions with that card. Moreover, the POSITA would recognize that giving access to the digital wallet is providing access to the financial account) as
10 called for in claim 5.

Although Ludtke discloses "transaction device information" that is communicated from the consumer's transaction device (PRIVACYCARD 130) to the TPC 110 for authorization, the storage location for this information and the importance of maintaining the confidentiality of private information.
15 However, Ludtke does not specifically indicate that this "transaction device information" is unique ("ID code" that is unique) to the consumer's transaction device, and storage of secret information in the user's device.

Nevertheless, Scott teaches authenticating the user using a "personal identification device" (PID) for protected application: *"The personal identification device and system of the invention has several advantages ... The private key used by the device is never disclosed."* ¶8:13-22. Scott also teaches the unique ID code identifying each device, which may be set by the device manufacturer and can be the device serial number. *"Memory 20 stores information that is*
20

specific to processing unit 16. Memory 20 stores an ID code that is set in PID 6 by the manufacturer. The ID code of a device, which may be the device serial number, is unique to each device... ¶11:11-13. Scott further discloses the device's memory 20 stores the private key unique to each device and used for encryption: *"The processor unit employs the encryption algorithm and the private key to encrypt the host response signal to create the verification signal, and causes the transmitter circuit to transmit the verification signal to the host system only if the biometric signal corresponds sufficiently to the biometric data to verify that the user is the enrolled person."* ¶4:14-18, "Processing unit 16 also includes an encryption algorithm incorporated into an encoder 23. In the embodiment illustrated in FIG. 1, the encryption algorithm is programmed into processor circuit 18. A private key that is stored in memory 20 is used with the encryption algorithm for encryption. The private key can be set into memory by the manufacture, and is specific to each PID 6. Different PIDs 6, which have different processing units 16, will typically have different private keys..."

¶11:24-29, *"encrypting the random number signal with the transmitting device, the random number signal being encrypted according to an encryption algorithm employing a private key associated only with the transmitting device"* ¶28:13-15.

It would have been obvious to a person of ordinary skill in the art (POSITA) at the time the invention was filed to modify the system of Ludtke to incorporate the private key structure, specifically the unique serial numbers and store permanent information such as the private key and unique serial numbers as taught by Scott for the purpose of providing secure wireless

communication. The POSITA would have recognized that the “transaction device information” of Ludtke would necessarily include the unique device information, which would ensure that the information used to authenticate the device only identifies the authorized device. Since Ludtke includes the

5 persistent storage area of the device where the ID code can be stored. The POSITA would have stored the unique device identifiers and the secret key in the persistent memory of Ludtke with the teachings of Scott’s unique Device ID since this is important information that allows authorization and sensitive communication to take place. Examiners find this combination is merely the

10 use of a known technique to improve similar devices in a similar way. See MPEP §2143(I)(C). The combination is not seen to create a greater expenditure of time, effort or other resources nor do the references even vaguely include a teaching away of the proposed modification.

In addition, the POSITA would have been motivated to combine Ludtke

15 and Scott because they are both in the same field of endeavor: authentication of a device, including use of biometric information, for the purpose of exchanging sensitive information over a network. (Ludtke discloses “*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*”.

20 (Abstract). Scott discloses “*A portable, hand-held personal identification device (6) and method for providing secure access to a host facility (4) includes a biometric sensory system capable of sensing a biometric trait of a user that is*

unique to the user and providing a biometric signal indicative of the sensed biometric trail...” (Abstract)).

Regarding claim 6: **The smartphone of claim 5, wherein the ID code is**
5 **transmitted to the third-party trusted authority over a network** (Ludtke
discloses “The *transaction device information is provided to the TPC 110 that*
then indicates to the vendor 125 and the user 120 approval of the transaction to
be performed” ¶6:41-44, and “The *incoming communication mechanism 605 and*
outgoing communications mechanism 610 are the means of communicating with
10 *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.”
¶9:36-42).

15 Regarding claim 7: **A system, comprising:**
a smartphone (Examiners interpreting this under 112, 6th as above and
this limitation is limited to the smartphone and the related programming.
Ludtke discloses “*the transaction device may contain wireless data*
communication” ¶5:40-41, “*cell phone functionality built-in*” ¶18:3-4, “*another*
20 *portable device such as a cell phone*” ¶34:21. Fig. 28 discloses “consumer
access device” having functions allowing the user to see balances and credit
cards, and also to “Access Dialing Codes” is inherently seen as the smartphone)
that persistently stores biometric data and an ID code (Ludtke discloses the

storage “In one embodiment, the TPCCH allows users to backup data that is generated directly on the transaction device, such as a telephone book and appointment information, into a storage location managed by the TPCCH.” ¶10:46-49; “In addition, it may provide an alternative, non-PC based location from which

5 to securely execute utility applications and to store data, thus enhancing data security and protection from danger such as PC viruses and hard disk crashes.” ¶24:61-65; and the importance of maintaining the confidentiality of private information: “The highly secured location, accessible through or part of a transaction processing clearing house (TPCH), provides the transaction

10 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” ¶3:40-47; “For example, any type of demographic questionnaire can

15 be created by a vendor and distributed to users of this system while retaining their individual privacy. The data can be collected and returned to the vendor along with the means of identifying the specific target transaction devices that may subsequently receive the appropriate promotional materials. However, the identity of the user is not revealed. Thus, direct marketing is available to vendors

20 even though user identity confidentiality is maintained. Additionally, the eCommerce system may automatically collect any type of data that can be obtained through use of this system and subsequently sold to third parties. However, individual privacy is always maintained.” ¶5:23-35, “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 TPC 110 maintains a secure database of transaction device information and user information.” ¶6:45-51. Ludtke also describes persistently storing the fingerprint data on the integrated device that cannot be afterward altered: “The fingerprint data entry process may be performed at least twice, to confirm that the user has entered the correct data (using the correct fingerprint). 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), **wherein the biometric data is one selected from a group consisting of facial recognition, a finger-print scan, and a retinal scan data of a legitimate user** (Ludtke describes: “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.” ¶35:60-64), **and the ID code is received from a third-party trusted authority** (Ludtke discloses the transaction device (PRIVACYCARD 130) provide information to the TRANSACTION PRIVACY CLEARING HOUSE 110 for authorization for the transaction between the consumer 120 and vendor 125 to be performed: “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. The TPCH 110 is not part of the transaction, but rather

5 functions a third-party middleman of the transaction: *"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."* ¶7:44-48. This ensures that sensitive information is not shared with the vendor

10 125), **the ID code uniquely identifying the smartphone among a plurality of smartphones** (Ludtke discloses the TPCH 110 having "transaction device information" that is maintained in a secure database by the TPCH 110: *"The highly secured location, accessible through or part of a transaction processing clearing house (TPCH), provides the transaction processing clearing house the*

15 *information necessary to authorize a transaction. For example, the transaction processing clearing house may access relevant account information to authorize transaction."* ¶3:40-45. It would therefore be obvious that the ID code originate from the list of device information maintained by the TPCH 110 and communicated to the smartphone. The TPCH 110 would include the ID code in

20 communications to the smartphone to ensure verification), **the smartphone configured to indicate that a biometric authentication is requested** (Ludtke describes using biometric verification including the fingerprint to verify the user of the device. Figure 28 shows the device with the Fingerprint

Identification Unit (FIU) 2806 and the touchpad 2808 for user input: “*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*

5 *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), **the smartphone configured to wirelessly send the ID code to the third-party trusted authority** (Examiners interpreting this under 112, 6th as above and this limitation is limited to the server or other computerized

10 device. Ludtke discloses “*In one embodiment, the transaction device may be configured to closely resemble a standard credit card. More particularly, the card may have a magnetic stripe or a smart card chip that functions similarly to standard credit cards. In addition, the transaction device may contain wireless data communication, data storage and communication protocols for selectively*

15 *communicating with outside devices such as a digital wallet described herein, point of sale (POS) terminal or personal computer (PC) and digital televisions (DTV).*” ¶5:36-44, and “*A variety of communication devices may be used, such as the Internet, direct dial-up modem connections, wireless or cellular signals, etc.*”

¶9:39-42) **for authentication responsive to determining that scan data**

20 **from a biometric scan performed using the smartphone matches the biometric data of the legitimate user** (Fig. 31 of Ludtke describes the process to verify the user of the integrated device. As can be seen in the flow chart, the device is continuously looking for a request for verification (“Detect fingerprint

3104”). In response to that request, it will receive scan data from the touchpad so it can determine whether the fingerprint matches (3106): “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
5 fingerprint. If a fingerprint has been detected, then at 3106 a check is made to see if it matches a stored authorized fingerprint. If a match does not occur, then at 3110 an error message is output and the DW returns to checking to see if a fingerprint has been detected 3104. If the fingerprint does match a stored one, then at 3108 the DW allows access to functions of the DW and access to a
10 selection of codes.” ¶39:49-59), **wherein a transaction is completed responsive to successful authentication of the ID code by the third-party trusted authority** (Ludtke teaches once the TPC 110 authenticates the ID code, it provides notice to the parties and the transaction can be completed: “The transaction device information is provided to the TPC 110 that then
15 indicates to the vendor 125 and the user 120 approval of the transaction to be performed” ¶6:41-44), **wherein the transaction being completed includes accessing one or more from a group consisting of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account** (Ludtke teaches: “A variety of user interfaces may be used. In one embodiment,
20 an input device may be incorporated on the transaction device. Alternately or supplementally an input device may be coupled to the transaction device. In one embodiment, an input device may be provided on a digital wallet coupled to a privacy card. User inputs may be provided on the POS terminals including a

personal POS terminal.” ¶5:65- ¶6:4. Since Ludtke describes the transaction device as including “a digital wallet”, the POSITA would recognize as files that allow the user to digitally store credit card and other payment information and to make transactions with that card. Moreover, the POSITA would recognize
5 *that giving access to the digital wallet is providing access to the financial account); and*

the third-party trusted authority operated by a third party (Ludtke discloses the transaction device (PRIVACYCARD 130) provides information to the TRANSACTION PRIVACY CLEARING HOUSE 110 for authorization for the
10 *transaction between the consumer 120 and vendor 125 to be performed: “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*
15 *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. The TPCH 110 is not part of the transaction, but rather functions a third-party middleman of the transaction:*
“In one embodiment of electronic distribution, the TPCH 110 functions as the
20 *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.” ¶7:44-48. This ensures that sensitive information is not shared with the vendor 125), the third-party trusted authority storing a plurality of*

legitimate ID codes and authenticating the ID code received based on a comparison of the ID code received and the legitimate ID codes included in the plurality of the legitimate ID codes (Ludtke discloses the TPOCH 110

includes information that can be compared with information from the

5 consumer 120 and the consumer's device so the TPOCH 110 can determine whether the consumer 120 is authorized to complete a transaction with the vendor 125: *"The transaction device information is provided to the TPOCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed."* ¶6:41-44, and *"At 3102 the user may start a*
10 *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. If a match does not occur, then at 3110 an error message is output and the DW returns to checking to see if a*
15 *fingerprint has been detected 3104. If the fingerprint does match a stored one, then at 3108 the DW allows access to functions of the DW and access to a selection of codes."* ¶39:49-59) as called for in claim 7.

Although Ludtke discloses "transaction device information" that is communicated from the consumer's transaction device (PRIVACYCARD 130) to
20 the TPOCH 110 for authorization, the storage location for this information and the importance of maintaining the confidentiality of private information. However, Ludtke does not specifically indicate that this "transaction device

information” is unique (“ID code” that is unique) to the consumer’s transaction device, and storage of secret information in the user’s device.

Nevertheless, Scott teaches authenticating the user using a “personal identification device” (PID) for protected application: “*The personal identification device and system of the invention has several advantages ... The private key used by the device is never disclosed.*” ¶8:13-22. Scott also teaches the unique ID code identifying each device, which may be set by the device manufacturer and can be the device serial number. “*Memory 20 stores information that is specific to processing unit 16. Memory 20 stores an ID code that is set in PID 6*
5 *by the manufacturer. The ID code of a device, which may be the device serial number, is unique to each device...*” ¶11:11-13. Scott further discloses the device’s memory 20 stores the private key unique to each device and used for encryption: “*The processor unit employs the encryption algorithm and the private key to encrypt the host response signal to create the verification signal,*
10 *and causes the transmitter circuit to transmit the verification signal to the host system only if the biometric signal corresponds sufficiently to the biometric data to verify that the user is the enrolled person.*” ¶4:14-18, “*Processing unit 16 also includes an encryption algorithm incorporated into an encoder 23. In the embodiment illustrated in FIG. 1, the encryption algorithm is programmed into*
15 *processor circuit 18. A private key that is stored in memory 20 is used with the encryption algorithm for encryption. The private key can be set into memory by the manufacture, and is specific to each PID 6. Different PIDs 6, which have different processing units 16, will typically have different private keys...*”
20

¶11:24-29, “*encrypting the random number signal with the transmitting device, the random number signal being encrypted according to an encryption algorithm employing a private key associated only with the transmitting device*” ¶28:13-15.

It would have been obvious to a person of ordinary skill in the art
5 (POSITA) at the time the invention was filed to modify the system of Ludtke to incorporate the private key structure, specifically the unique serial numbers and store permanent information such as the private key and unique serial numbers as taught by Scott for the purpose of providing secure wireless communication. The POSITA would have recognized that the “transaction
10 device information” of Ludtke would necessarily include the unique device information, which would ensure that the information used to authenticate the device only identifies the authorized device. Since Ludtke includes the persistent storage area of the device where the ID code can be stored. The POSITA would have stored the unique device identifiers and the secret key in
15 the persistent memory of Ludtke with the teachings of Scott’s unique Device ID since this is important information that allows authorization and sensitive communication to take place. Examiners find this combination is merely the use of a known technique to improve similar devices in a similar way. See MPEP §2143(I)(C). The combination is not seen to create a greater expenditure
20 of time, effort or other resources nor do the references even vaguely include a teaching away of the proposed modification.

In addition, the POSITA would have been motivated to combine Ludtke and Scott because they are both in the same field of endeavor: authentication

of a device, including use of biometric information, for the purpose of exchanging sensitive information over a network (Ludtke discloses “*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*”).

- 5 (Abstract). Scott discloses “*A portable, hand-held personal identification device (6) and method for providing secure access to a host facility (4) includes a biometric sensory system capable of sensing a biometric trait of a user that is unique to the user and providing a biometric signal indicative of the sensed biometric trait...*” (Abstract)). .

10

- Regarding claim 8: **The system of claim 7, wherein the smartphone receives an authentication request, and in response, requests biometric scan from a user to generate the scan data and, when the smartphone cannot verify the scan data as being from the legitimate user, the**
- 15 **smartphone does not send the ID code** (As can be seen in the flow chart shown in Fig. 31 of Ludtke, the device is continuously looking for a request for verification (“Detect fingerprint”). In response to that request, it will receive scan data from the touchpad so it can determine whether the fingerprint matches (3106). If the scan data does not match the stored data (i.e., the device
- 20 cannot authenticate the user), it will output an error message, and not allow access to the digital wallet or selection of codes: “*If a fingerprint has been detected, then at 3106 a check is made to see if it matches a stored authorized fingerprint. If a match does not occur, then at 3110 an error message is output*”

and the DW returns to checking to see if a fingerprint has been detected 3104. If the fingerprint does match a stored one, then at 3108 the DW allows access to functions of the DW and access to a selection of codes.” ¶39:52-59).

5 Regarding claim 9: **The system of claim 7, wherein completing the transaction includes accessing an application** (In Ludtke, access would be given applications of either computer software, a file or both. Ludtke describes the transaction device as including the “digital wallet”. The POSITA would recognize as an application and files that allow the user to digitally store credit
10 card and other payment information and to make transactions with that card. See Fig. 5A-5B).

Claims chart, pages 38-85 of the request for reexamination is hereby incorporated by reference for the requester’s explanation of the proposed
15 rejection.

RESPONSE TO PATENT OWNER’S STATEMENT

Patent Owner's response filed 11/02/2022 has been fully considered but it is not persuasive. Examiners have thoroughly reviewed Patent Owner’s
20 arguments but firmly believes that the cited references reasonably and properly meet the claimed limitations as rejected.

Patent Owner’s argument – Ludtke does not disclose a “Third-Party Trusted Authority” (pages 4-9).

Examiners' response – As pointed out above, Ludtke discloses in Fig. 1 a transaction privacy clearing house (TCPH) 110 may access relevant account information to authorize transactions, which can be seen as the Third-Party trusted authority limitation: *“The highly secured location, accessible through or*
5 *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*
10 *maintained.”* ¶3:40-47. Specifically, a transaction device (PRIVACYCARD130) provides information to the TCPH 110 for authorization for the transaction between the consumer 120 and vendor 125 to be performed. The financial transaction is authorized through the TCPH 110, independent of the consumer 120 and the vendor 125. Ludtke explains that the *“transaction device*
15 *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. The consumer 120 and vendor 125 therefore trust the TPCH 110 to indicate whether the transaction may be complete. Ludtke emphasizes the third-party aspect of the TPCH 110 because the third party ensures that private
20 information is not exchanged between the consumer 120 and the vendor 125: *“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 TPOCH 110 maintains a secure database of transaction device information and user information.” ¶6:45-51. The PTAB constructed the “third party trusted authority” as the “trusted authority that is an entity or party separate from the principal parties to a transaction” (IPR2021-01448
5 *Decision, page 11). In this case, since the TPOCH 110 is not part of the transaction, but rather functions a third-party middleman that grants access of the transaction to the financial processing system service, and the TPOCH 110 is an entity separate from the parties to the transaction (i.e. the user 130 and the vendor 125). This ensures that sensitive information is not shared with the*
10 *vendor: “In one embodiment of electronic distribution, the TPOCH 110 functions as the middleman of the distribution channel. This allows the TPOCH 110 to retain user privacy by not exposing addressing information and possibly email addresses to third parties.” ¶7:44-48. Thus, the Third Party trusted authority limitation is met under PTAB’s construction. Moreover, limitation name*
15 *irrelevant once the claim invokes 112(6th ¶).*

Patent Owner’s argument – Ludtke’s Figs. 16 and 17 discloses the TPOCH itself settles funds and performs other financial processes, TPOCH is the system being accessed and thus cannot be the third party trusted authority (pages 4-
20 8).

Examiners’ response - It is noted that Examiners do not relied on Figs. 16 and 17 for the third party trusted authority limitation, instead Examiners relied on Fig. 1 which teaches TPOCH 110 functions as a third-party middleman

of the transaction and interfaces with a separate financial processing system.

Ludtke clearly states “In one embodiment, the TPC 110 interfaces to at least one financial processing system 140 to perform associated financial transactions, such as confirming sufficient funds to perform the transaction, ... In
5 an alternate embodiment, the financial processing system need not be a separate entity but may be incorporated with other functionality. For example, in one embodiment, the financial processing system 140 may be combined with the TPC 110 functionality.” ¶6:51-64. (Emphasis added)

Since Ludtke teaches two different circumstances, Examiners agree with
10 the Requester that Ludtke teaches alternative embodiments that combine the TPC 110 with the financial processing system does not negate its express disclosure of other embodiments where the TPC 110 acts as a separate, third-party middleman, and interfaces with the financial processing system.

15 Patent Owner’s argument – Okereke does not disclose a “Third-Party Trusted Authority” (page 9).

Examiners’ response – Examiners do not relied on Okereke to teach the third party trusted authority limitation. Instead, Okereke is relied on as a secondary reference to teach unique device ID and storage of secret
20 information. Specifically, Okereke discloses “a secret key” that is maintained by the user, and can be used to encrypt and decrypt information communicated to the user.

Patent Owner's argument – Scott does not disclose components for or actions of communicating with a third party trusted authority (page 9).

Examiners' response – Examiners do not relied on Scott to teach the third party trusted authority limitation. Instead, Scott is relied on as a
5 secondary reference to teach unique device ID and storage of secret information. Specifically, Scott discloses a secret key set-up and the device's memory 20 stores a private key unique to each device and used for encryption.

RESPONSE TO THE REQUESTER'S REPLY

10 The Requester's reply filed 12/08/2022 has been fully considered.

Examiners generally agree with the Requester's reply regarding the "third party trusted authority" limitation, and it is incorporated by reference herein.

REEXAMINATION PROCEDURES

Extensions of time

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

Duty to Disclose

The Patent Owner is reminded of the continuing responsibility under 37 C.F.R. §1.565(a) to apprise the Office of any litigation activity, or other prior or concurrent proceeding, throughout the course of this reexamination proceeding involving the 989 Patent. The Third-Party Requester is also reminded of the ability to similarly apprise the Office of any such activity or proceeding throughout the course of this reexamination proceeding. See MPEP §§2207, 2282 and 2286.

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 C.F.R. 1.530(d)-(j), must be formally presented pursuant to 37 C.F.R. 1.52(a) and (b), and must contain any fees required by 37 C.F.R. 1.20(c). See MPEP § 2250(IV) for examples to assist in the preparation of proper proposed amendments in reexamination proceedings.

Submissions

In order to insure full consideration of any amendments, affidavits or declarations or other documents as evidence of patentability, such documents must be submitted in response to the first Office action on the merits (which does not result in a close of prosecution). Submissions after the second Office action on the merits, which is intended to be a final action, will be governed by

the requirements of 37 CFR 1.116, after final rejection and by 37 CFR 41.33 after appeal, which will be strictly enforced.

Service Of Papers

5 After the filing of a request for reexamination by a Third Party Requester, any document filed by either the Patent Owner or the Third Party Requester must be served on the other party (or parties where two or more third party requester proceedings are merged) in the reexamination proceeding in the manner provided in 37 CFR §1.248. See 37 C.F.R. §1.550(f).

10

CONCLUSION

Claims 1-9 are rejected.

All correspondence relating to this ex parte reexamination proceeding should be directed:

15

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

20

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

25

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

30

By hand: Customer Service Window
Knox Building

501 Dulany Street
Alexandria, VA 22314

For electronic 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 USPTO patent 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.

Any inquiry concerning this communication should be directed to MY TRANG TON at telephone number 571-272-1754.

Signed:

/MY TRANG TON/
Primary Examiner, Art Unit 3992

Conferees:

/KENNETH WHITTINGTON/
Primary Examiner, Art Unit 3992

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