PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 11062 PCT	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US05/46843	International filing date (*day/month/year*) 20 December 2005 (20.12.2005)	(Earliest) Priority Date (*day/month/year*) 20 December 2004 (20.12.2004)
Applicant PROXENSE, LLC		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 2 sheets.

☒ It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the Report**
   a. With regard to the **language**, the international search was carried out on the basis of:
      ☒ the international application in the language in which it was filed.
      ☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.
2. ☐ **Certain claims were found unsearchable** (See Box No. II)
3. ☐ **Unity of invention is lacking** (See Box No. III)
4. With regard to the **title,**
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the **drawings,**
   a. the figure of the **drawings** to be published with the abstract is Figure No. 3
      ☐ as suggested by the applicant.
      ☒ as selected by this Authority, because the applicant failed to suggest a figure.
      ☐ as selected by this Authority, because this figure better characterizes the invention.
   b. ☐ none of the figures is to be published with the abstract.

Form PCT/ISA/210 (first sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US05/46843

A. CLASSIFICATION OF SUBJECT MATTER
IPC: **H04L 9/32**(2006.01)

USPC: 713/186
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/186

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 6,041,410 (HSU et al), 21 March 2000, Column 4, lines 15-56, Column 5, line 1 to Column 6, line 24, and Column 6, line 42 to Column 7, line 34	1, 4-11, 15, 18 --- 2, 3, 12-14, 16, 17, 19-21
Y	US 2004/0129787 (SAITO et al) 8 July 2004, Paragraphs 40-56, 81-91, 91-101, and 164	2, 3, 12-14, 16, 17, 19-21

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"B" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 January 2007 (18.01.2007)	01 MAR 2007
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer Emmanuel Moise Telephone No. (571)-305-3900

Form PCT/ISA/210 (second sheet) (April 2005)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
JOHN T. MCNELIS
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing (*day/month/year*)	01 MAR 2007
Applicant's or agent's file reference 11062 PCT	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date (*day/month/year*)	Priority date (*day/month/year*)
PCT/US05/46843	20 December 2005 (20.12.2005)	20 December 2004 (20.12.2004)

International Patent Classification (IPC) or both national classification and IPC

IPC: **H04L 9/32**(2006.01)
USPC: 713/186

Applicant

PROXENSE, LLC

1. This opinion contains indications relating to the following items:

☒	Box No. I	Basis of the opinion
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☐	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☐	Box No. VII	Certain defects in the international application
☐	Box No. VIII	Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis(b)* that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/ US	Date of completion of this opinion	Authorized officer
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	18 January 2007 (18.01.2007)	Emmanuel Moise Telephone No. (571)-305-3900

Form PCT/ISA/237 (cover sheet) (April 2005)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US05/46843

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

☒ the international application in the language in which it was filed

☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

a. type of material

☐ a sequence listing

☐ table(s) related to the sequence listing

b. format of material

☐ on paper

☐ in electronic form

c. time of filing/furnishing

☐ contained in the international application as filed.

☐ filed together with the international application in electronic form.

☐ furnished subsequently to this Authority for the purposes of search.

3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US05/46843

Box No. V Reasoned statement under Rule 43 *bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims 2, 3, 12-14, 16, 17, and 19-21	YES
	Claims 1, 4-11, 15, and 18	NO
Inventive step (IS)	Claims NONE	YES
	Claims 1-21	NO
Industrial applicability (IA)	Claims 1-21	YES
	Claims NONE	NO

2. Citations and explanations:

Please See Continuation Sheet

Form PCT/ISA/237 (Box No. V) (April 2005)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US05/46843

Supplemental Box
In case **the space in any of the preceding boxes is not sufficient.**

V. 2. Citations and Explanations:
Claims 1, 4-11, 15, and 18 lack novelty under PCT Article 33(2) as being anticipated by Hsu (US 6041410 A) 21 March 2000.

Regarding Claim 1,
Hsu discloses a method for verifying a user during authentication of an integrated device, comprising the steps of:
Persistently storing biometric data for the user in a tamper-resistant format (Column 4, lines 15-25);
Responsive to receiving a request for biometric verification of the user, receiving scan data from a biometric scan (Column 4, lines 26-56);
Comparing the scan data to the biometric data to determine whether the data match (Column 4, lines 26-56); and
Wirelessly sending a code for authentication (Column 4, lines 26-56; and Column 5, line 1 to Column 6, line 9).

Regarding Claim 10,
Claim 10 is a device claim that corresponds to method claim 1 and is rejected for the same reasons.

Regarding Claim 4,
Hsu discloses that the code uniquely identifies the integrated device (Column 5, line 1 to Column 6, line 9; and Column 7, lines 17-34).

Regarding Claim 5,
Hsu discloses that the code indicates that the biometric verification was successful (Column 5, line 1 to Column 6, line 9; and Column 7, lines 17-34).

Regarding Claim 6,
Hsu discloses that persistently storing biometric data comprises permanently storing biometric data (Column 4, lines 15-25; and Column 5, lines 1-47).

Regarding Claim 11,
Claim 11 is a device claim that corresponds to method claim 6 and is rejected for the same reasons.

Regarding Claim 7,
Hsu discloses that the biometric data and the scan data are both based on a fingerprint scan by the user (Column 4, lines 15-56).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US05/46843

Supplemental Box
In case **the space in any of the preceding boxes is not sufficient.**

Regarding Claim 8,
Hsu discloses establishing a secure communication channel prior to sending the code for authentication (Column 6, line 42 to Column 7, line 34).

Regarding Claim 9,
Hsu discloses receiving a request for the code without a request for biometric verification (Column 5, line 57 to Column 6, line 24); and responsive to receiving the request for the code without a request for biometric verification, sending the code without requesting the scan data (Column 5, line 57 to Column 6, line 24).

Regarding Claim 15,
Hsu discloses a method for authenticating a verified user, comprising:
Receiving a code associated with a biometrically verified user (Column 5, line 1 to Column 6, line 9; and Column 7, lines 17-34);
Requesting authentication of the code (Column 5, line 1 to Column 6, line 9; and Column 7, lines 17-34);
Receiving an authentication result (Column 5, line 1 to Column 6, line 9; and Column 7, lines 17-34); and
In response to the authentication result being positive, providing access to an application (Column 5, line 1 to Column 6, line 9; and Column 7, lines 17-34).

Regarding Claim 18,
Hsu discloses establishing a secure communications channel with a biometric key, wherein the code associated with the biometrically verified user is received from the biometric key (Column 6, line 42 to Column 7, line 34).

Claims 2, 3, 12-14, 16, 17, and 19-21 lack an inventive step under PCT Article 33(3) as being obvious over Hsu in view of Saito (US 20040129787 A1) 8 July 2004.

Regarding Claim 2,
Hsu does not disclose that the code is registered with a trusted authority, and the code can be authenticated to a third party by the trusted authority.
Saito, however, discloses that the code is registered with a trusted authority, and the code can be authenticated to a third party by the trusted authority (Paragraphs 95-101). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the authentication procedures of Saito into the personal identification fob authentication system of Hsu in order to increase reliability and security of authentication and authorization by providing a trusted entity that can confirm that the user and device are authentic.

Regarding Claim 12,
Claim 12 is a device claim that corresponds to method claim 2 and is rejected for the same reasons.

Regarding Claim 3,
Hsu does not disclose registering an age verification for the user in association with the code.
Saito, however, discloses registering an age verification for the user in association with the code (Paragraphs 82, 83, and 164). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the authentication procedures of Saito into the personal identification fob authentication system of Hsu in order to increase reliability and security of authentication and authorization by providing a trusted entity that can confirm that the user and device are authentic.

Regarding Claim 13,
Claim 13 is a device claim that corresponds to method claim 3 and is rejected for the same reasons.

Regarding Claim 14,
Hsu does not disclose that the verification module comprises an LED to be activated for requesting the biometric scan.
Saito, however, discloses that the verification module comprises an LED to be activated for requesting the biometric scan (Paragraphs 40-56). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the authentication procedures of Saito into the personal identification fob authentication system of Hsu in order to increase reliability and security of authentication and authorization by providing a trusted entity that can confirm that the user and device are authentic.

Regarding Claim 16,
Hsu does not disclose registering the code with a trusted authority, wherein requesting authentication of the code comprises providing the code to the trusted authority and wherein receiving an authentication result comprises receiving the authentication result from the trusted authority.

Supplemental Box
In case **the space in any of the preceding boxes is not sufficient.**

Saito, however, discloses registering the code with a trusted authority, wherein requesting authentication of the code comprises providing the code to the trusted authority and wherein receiving an authentication result comprises receiving the authentication result from the trusted authority (Paragraphs 95-101). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the authentication procedures of Saito into the personal identification fob authentication system of Hsu in order to increase reliability and security of authentication and authorization by providing a trusted entity that can confirm that the user and device are authentic.

Regarding Claim 17,
Hsu as modified by Saito does discloses the method of claim 16, in addition, Saito discloses registering a date of birth or age with the trusted authority (Paragraphs 82, 83, and 164).

Regarding Claim 19,
Hsu discloses a system comprising:
A biometric key to store biometric data for a user in a tamper resistant format, and if scan data can be verified as being from the user by comparing the scan data to the biometric data, wirelessly sending a code (Column 4, lines 15-56; and Column 5, line 1 to Column 6, line 9);
An authentication module to authenticate the user for access to an application (Column 7, lines 17-34);
But does not disclose sending the code to a trusted authority for authentication.
Saito, however, discloses an authentication module to receive the code and send the code to a trusted authority for authentication, and responsive to the code being authenticated, allowing the user to access an application (Paragraphs 95-101). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the authentication procedures of Saito into the personal identification fob authentication system of Hsu in order to increase reliability and security of authentication and authorization by providing a trusted entity that can confirm that the user and device are authentic.

Regarding Claim 20,
Hsu as modified by Saito discloses the system of claim 19, in addition, Hsu discloses that the biometric key receives an authentication request from the authentication module, and in response, requests a biometric scan from the user to generate the scan data (Column 4, lines 26-56; and Column 5, line 1 to Column 6, line 9); and Saito discloses that the biometric key receives an authentication request from the authentication module, and in response, requests a biometric scan from the user to generate the scan data (Paragraphs 40-56; and 81-91

Regarding Claim 21,
Hsu as modified by Saito discloses the system of claim 19, in addition, Hsu discloses that if the biometric key cannot verify the scan data as being from the user, it does not send the code (Column 5, lines 1-47).

RECEIVED
PATENT DOCKETING

OCT 06 2008

Fenwick & West

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
GREG T. SUEOKA
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

	Date of mailing (*day/month/year*) 03 OCT 2008
Applicant's or agent's file reference 12785 PCT	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US07/11102	International filing date (*day/month/year*) 07 May 2007 (07.05.2007)
Applicant PROXENSE, LLC	

1. ☒ The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

   Filing of amendments and statement under Article 19:
   The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

   Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Facsimile No.: (41-22) 338.82.70.

   For more detailed instructions, see the notes on the accompanying sheet.

2. ☐ The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. ☐ **With regard to the protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

   ☐ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

   ☐ no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

   Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90*bis*.1 and 90*bis*.3, respectively, before the completion of the technical preparations for international publication.

   The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

   Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

   In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

   See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/ US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer Gilberto Barron Telephone No. (571) 272-1018

Form PCT/ISA/220 (January 2004) (*See notes on accompanying sheet*)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 12785 PCT	**FOR FURTHER ACTION**	see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.
International application No. PCT/US07/11102	International filing date *(day/month/year)* 07 May 2007 (07.05.2007)	(Earliest) Priority Date *(day/month/year)* 05 May 2006 (05.05.2006)
Applicant PROXENSE, LLC		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 2 sheets.

☒ It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the Report**
   a. With regard to the **language**, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.
   ☒ the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).
   b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international search was carried out on the basis of the sequence listing:
   ☐ contained in the international application in written form.
   ☐ filed together with the international application in computer readable form.
   ☐ furnished subsequently to this Authority in written form.
   ☐ furnished subsequently to this Authority in computer readable form.
   ☐ the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
   ☐ the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.
2. ☐ **Certain claims were found unsearchable** (See Box I).
3. ☐ **Unity of invention is lacking** (See Box II).
4. With regard to the **title**,
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is Figure No. ____
   ☐ as suggested by the applicant. ☒ None of the figures
   ☐ because the applicant failed to suggest a figure.
   ☐ because this figure better characterizes the invention.

Form PCT/ISA/210 (first sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US07/11102

A. CLASSIFICATION OF SUBJECT MATTER

IPC: **H04L 9/00**(2006.01),**1/00**(2006.01)

USPC: 713/168;713/170;713/182

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/168;713/170;713/182

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	U.S. 2003/0127511 A1 (KELLY et al.) 10 July 2003 (10.07.2003), paragraph 0037.	1-31
Y	U.S. 2006/0022046 A1 (IWAMURA) 02 February 2006 (2.02.2006), paragraph 0013.	1-10,12,14-31
Y	U.S. 5,416,780 A (PATEL) 16 May 1995(16.05.1995), column 7 lines 39-68.	11
Y	U.S. 2003/0139190 A1 (STEELBERG et al.) 24 July 2003 (24.07.2003), abstract and paragraph 0053.	13

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 June 2008 (11.06.2008)	03 OCT 2008
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner of Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer Gilberto Barron Telephone No. (571)270-1018

Form PCT/ISA/210 (second sheet) (July 1998)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
GREG T. SUEOKA
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	03 OCT 2008
Applicant's or agent's file reference 12785 PCT	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US07/11102	07 May 2007 (07.05.2007)	05 May 2006 (05.05.2006)

International Patent Classification (IPC) or both national classification and IPC

IPC: **H04L 9/00**(2006.01),**1/00**(2006.01)
USPC: 713/168;713/170;713/182

Applicant

PROXENSE, LLC

1. This opinion contains indications relating to the following items:

☒	Box No. I	Basis of the opinion
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☐	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☐	Box No. VII	Certain defects in the international application
☐	Box No. VIII	Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis(b)* that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/ US	Date of completion of this opinion	Authorized officer
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	01 October 2008 (01.10.2008)	Gilberto Barron Telephone No. (571)270-1018

Form PCT/ISA/237 (cover sheet) (April 2007)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US07/11102

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

☒ the international application in the language in which it was filed

☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of:

a. type of material

☐ a sequence listing

☐ table(s) related to the sequence listing

b. format of material

☐ on paper

☐ in electronic form

c. time of filing/furnishing

☐ contained in the international application as filed.

☐ filed together with the international application in electronic form.

☐ furnished subsequently to this Authority for the purposes of search.

4. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US07/11102

Box No. V Reasoned statement under Rule 43 *bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims 1-31	YES
	Claims NONE	NO
Inventive step (IS)	Claims NONE	YES
	Claims 1-31	NO
Industrial applicability (IA)	Claims 1-31	YES
	Claims NONE	NO

2. Citations and explanations:

Please See Continuation Sheet

Form PCT/ISA/237 (Box No. V) (April 2007)

Supplemental Box
In case **the space in any of the preceding boxes is not sufficient**.

V. 2. Citations and Explanations:

Claims 1-10, 12, and 14-31 lack an inventive step under PCT Article 33(3) as being obvious over Kelly et al (U.S. 7,090,126) in view of Iwamura (U.S. 2006/0022046). With respect to claim 1, a method for differentiating between a first personal digital key (PDK) and a second PDK within a proximity zone of an external device, comprising:

obtaining a first differentiation metric (see Kelly column 7 lines 32-59 i.e. set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410) associated with the first PDK (see Kelly column 7 lines 32-33 i.e. smart card) after it enters the proximity zone (see Kelly column 7 lines 32-33 i.e. a user may be required to input his/her smart card into smart card reader);

obtaining a second differentiation metric associated with the second PDK after it enters the proximity zone (see Kelly column 7 lines 32-33 the next user that comes and gets his smartcard scanned);

responsive to the first PDK being most likely associated with the transaction, executing an authentication test for the first PDK (see Kelly column 7 lines 32-59 i.e. Data read from frequent flyer smart card 400 or a smart card boarding pass 410 is then passed to processor 12 and a comparison performed. Processor 12 may, for example, compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410 with the information obtained from one or more of the biometric/image capture devices 22 and 24. The result of this comparison is the decision whether the traveler is physically the same individual as that described on frequent flyer smart card 400 or smart card boarding pass 410. If the comparison is positive, processor 12 indicates this to an access control interface (not shown), which then would open a door or a gate, for example); and

authorizing the transaction responsive to the first PDK satisfying the authentication test (see Kelly column 7 lines 32-59 i.e. If the comparison is positive, processor 12 indicates this to an access control interface (not shown), which then would open a door or a gate, for example).

Kelly does not teach determining whether the first PDK is most likely to be associated with a transaction based on the first and second differentiation metrics. Iwamura teaches that with the increase popularity in wireless smartcards devices will is more and more likely that multiple smart cards will be in communication range of a terminal. Iwamura teaches that when many smart cards exist in the communication range a specific carrier is selected by a shock absorbing mechanism so that the process can be correctly performed i.e. determining whether the first PDK is most likely to be associated with a transaction based on the first and second differentiation metrics (see paragraph 0013). It 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 to have modified Kelly with a system that allows many smartcards in communication range while still making sure the process is carried out correctly. Therefore one would have been motivated to have selected the smartcard based on first and second differentiation metrics of the smartcards

With respect to claim 2, further comprising receiving an input to initiate an authentication of an individual (see Kelly column 7

Supplemental Box
In case **the space in any of the preceding boxes is not sufficient**.

lines 32-59 i.e. a user may be required to input his/her smart card into smart card reader/writer 26 as well as have one or more of the user's immutable characteristics (fingerprint, image, etc.) recorded).

With respect to claim 3, further comprising: receiving a first profile sample from the first PDK, wherein the profile sample comprises a subset of information from a first profile in the first PDK computed according to a first function (see Kelly figure 6 and column 7 lines 32-59 i.e. the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410); computing an input sample from the received input according to the first function (see Kelly column 7 lines 32-59 i.e. compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410); and responsive to the first profile sample not matching the input sample, indicating that the first PDK does not satisfy the authentication test (see Kelly column 7 lines 32-59 i.e. Data read from frequent flyer smart card 400 or a smart card boarding pass 410 is then passed to processor 12 and a comparison performed. Processor 12 may, for example, compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410 with the information obtained from one or more of the biometric/image capture devices 22 and 24. The result of this comparison is the decision whether the traveler is physically the same individual as that described on frequent flyer smart card 400 or smart card boarding pass 410. If the comparison is positive, processor 12 indicates this to an access control interface (not shown), which then would open a door or a gate, for example).

With respect to claim 4, further comprising: receiving a second profile sample from the first PDK (see Kelly column 7 lines 32-59 (see column 7 lines 32-33 the next user that comes and gets his smartcard scanned): comparing the second profile sample to the input sample (see Kelly column 7 lines 32-59 i.e. compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410); and determining if the second profile sample matches the input sample (see column 7 lines 32-59 i.e. Data read from frequent flyer smart card 400 or a smart card boarding pass 410 is then passed to processor 12 and a comparison performed. Processor 12 may, for example, compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410 with the information obtained from one or more of the biometric/image capture devices 22 and 24. The result of this comparison is the decision whether the traveler is physically the same individual as that described on frequent flyer smart card 400 or smart card boarding pass 410. If the comparison is positive, processor 12 indicates this to an access control interface (not shown), which then would open a door or a gate, for example).

With respect to claim 5, wherein the first profile sample is received at a predetermined period of time after the first PDK enters the proximity zone (see Kelly column 7 lines 32-33 right after the card is inserted into the reader).

With respect to claim 6, Kelly teaches wherein the input is a biometric input and wherein executing the authentication test further comprises: receiving a biometric profile from the first PDK (see Kelly column 7 lines 32-59 i.e. Data read from frequent flyer smart card 400 or a smart card boarding pass 410); comparing the received biometric profile to the biometric input (see Kelly column 7 lines 32-59 i.e. compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410 with the information obtained from one or more of the biometric/image capture devices 22 and 24); and responsive to the biometric profile matching the biometric input, indicating that the authentication test is satisfied (see Kelly column 7 lines 32-59 i.e. Data read from frequent flyer smart card 400 or a smart card boarding pass 410 is then passed to processor 12 and a comparison performed. Processor 12 may, for example, compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410 with the information obtained from one or more of the biometric/image capture devices 22 and 24. The result of this comparison is the decision whether the traveler is physically the same individual as that described on frequent flyer smart card 400 or smart card boarding pass 410. If the comparison is positive, processor 12 indicates this to an access control interface (not shown), which then would open a door or a gate, for example).

Kelly does not teach wirelessly receiving data from the first PDK. Iwamura teaches wirelessly receiving data from the smart card. It 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 to have been able a use wireless smartcards to communicate with a device to increase the flexible of smart card. Therefore one would have been motivated to have used wireless smart cards (see Iwamura paragraph 0017).

With respect to claim 7, wherein the input is a personal identification number (PIN) and wherein executing the authentication test further comprises: wirelessly receiving a PIN profile from the first PDK (see column 8 lines 8-17); comparing the received PIN profile to the PIN input (see column 8 lines 8-17); and responsive to the PIN profile matching the PIN input, indicating that the authentication test is satisfied (see Kelly column 8 lines 8-17).

With respect to claim 8, wherein executing the authentication test further comprises: wirelessly receiving a picture profile from the first PDK (see Kelly column 7 lines 32-59 i.e. Data read from frequent flyer smart card 400 or a smart card boarding pass 410); comparing the received picture profile to the individual (see Kelly column 7 lines 32-59 i.e. compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410 with the information obtained from one or more of the biometric/image capture devices 22 and 24); and responsive to the picture profile matching the appearance of the individual, indicating that the authentication test is satisfied (see Kelly column 7 lines 32-59 i.e. Data read from frequent flyer smart card 400 or a smart card boarding pass 410 is then passed to processor 12 and a comparison performed. Processor 12 may, for example, compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410 with the information obtained from one or more of the biometric/image capture devices 22 and 24. The result of this comparison is the decision whether the traveler is physically the same individual as that described on frequent flyer smart card 400 or smart card boarding pass 410. If the comparison is positive, processor 12 indicates this to an access control interface (not shown), which then would open a door or a gate, for example).

With respect to claim 9, further comprising: responsive to the authentication test not being satisfied, determining whether the second PDK is next most likely to be associated with the individual based on the differentiation metrics; executing the authentication test for the second PDK; and authorizing the transaction responsive to the second PDK satisfying the authentication test (see Kelly column 7 lines 32-59 i.e. compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410); and determining if the second profile sample matches the input sample (see Kelly column 7 lines 32-59 i.e. Data read from frequent flyer smart card 400 or a smart card boarding pass 410 is then passed to processor 12 and a comparison performed. Processor 12 may, for example, compare

Supplemental Box
In case **the space in any of the preceding boxes is not sufficient.**

the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410 with the information obtained from one or more of the biometric/image capture devices 22 and 24. The result of this comparison is the decision whether the traveler is physically the same individual as that described on frequent flyer smart card 400 or smart card boarding pass 410. If the comparison is positive, processor 12 indicates this to an access control interface (not shown), which then would open a door or a gate, for example).

With respect to claim 10, wherein the first differentiation metric is based on at least one of a distance metric, a detection duration metric, and a location metric (see Kelly column 7 lines 32-33).

With respect to claim 12, wherein the detection duration metric includes a length of time the first PDK is within the proximity zone of the external device (see Kelly column 7 lines 32-33).

With respect to claim 14, an apparatus for differentiating between a first personal digital key (PDK) and a second PDK within a proximity zone, comprising:

a receiver/decoder circuit adapted to obtain a first differentiation metric associated with the first PDK when the first PDK enters the proximity zone and obtain a second differentiation metric associated with the second PDK when the second PDK enters the proximity zone (see Kelly column 7 lines 32-33 i.e. a user may be required to input his/her smart card into smart card reader); and

a processor coupled to the receiver decoder circuit, the processor for determining whether the first PDK is most likely to be associated with a transaction based on the differentiation metrics, executing an authentication test for the first PDK responsive to determining that the first PDK is most likely associated with the transaction, and authorizing the transaction responsive to the first PDK satisfying the authentication test (see Kelly column 7 lines 32-59 i.e. Data read from frequent flyer smart card 400 or a smart card boarding pass 410 is then passed to processor 12 and a comparison performed. Processor 12 may, for example, compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410 with the information obtained from one or more of the biometric/image capture devices 22 and 24. The result of this comparison is the decision whether the traveler is physically the same individual as that described on frequent flyer smart card 400 or smart card boarding pass 410. If the comparison is positive, processor 12 indicates this to an access control interface (not shown), which then would open a door or a gate, for example).

With respect to claim 15, further comprising a memory coupled to the receiver/decoder circuit, the memory adapted to buffer the first and second differentiation metrics (see Kelly column 3 lines 37-52).

With respect to claim 16, further comprising an input device adapted to receive an input from an individual to initiate the transaction (see Kelly column 7 lines 32-59 i.e. a user may be required to input his/her smart card into smart card reader/writer 26 as well as have one or more of the user's immutable characteristics (fingerprint, image, etc.) recorded).

With respect to claim 17. The apparatus of claim 16, wherein the input device comprises at least one of a keypad, a touch screen, a biometric reader and a pointing device (see Kelly column 7 lines 32-59 i.e. one or more of the user's immutable characteristics (fingerprint, image, etc.) recorded).

With respect to claim 18. The apparatus of claim 17, wherein the biometric reader is further adapted to obtain a representation of physical or behavioral characteristics derived from the individual (see Kelly column 7 lines 32-59 i.e. one or more of the user's immutable characteristics (fingerprint, image, etc.) recorded).

With respect to claim 19. The apparatus of claim 17, wherein the biometric reader comprises at least one of a fingerprint scanner, a retinal scanner, an iris scanner, a face scanner, a palm scanner, a DNA analyzer, a signature analyzer and a voice analyzer (see Kelly column 7 lines 32-59 i.e. one or more of the user's immutable characteristics (fingerprint, image, etc.) recorded).

With respect to claim 20, wherein the receiver/decoder circuit is further adapted to wirelessly receive a profile sample from the first PDK, wherein the profile sample comprises a subset of information computed by applying a first function to a profile of the first PDK (see Kelly column 7 lines 32-59 i.e. Data read from frequent flyer smart card 400 or a smart card boarding pass 410 is then passed to processor 12 and a comparison performed. Processor 12 may, for example, compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410 with the information obtained from one or more of the biometric/image capture devices 22 and 24. The result of this comparison is the decision whether the traveler is physically the same individual as that described on frequent flyer smart card 400 or smart card boarding pass 410. If the comparison is positive, processor 12 indicates this to an access control interface (not shown), which then would open a door or a gate, for example).

With respect to claim 21, wherein the processor is further configured to compute an input sample by applying the first function to the received input, and determine if the input sample matches the buffered profile sample associated with the first PDK (see Kelly column 7 lines 32-59 i.e. Data read from frequent flyer smart card 400 or a smart card boarding pass 410 is then passed to processor 12 and a comparison performed. Processor 12 may, for example, compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410 with the information obtained from one or more of the biometric/image capture devices 22 and 24. The result of this comparison is the decision whether the traveler is physically the same individual as that described on frequent flyer smart card 400 or smart card boarding pass 410. If the comparison is positive, processor 12 indicates this to an access control interface (not shown), which then would open a door or a gate, for example).

With respect to claim 22, wherein the receiver/decoder circuit automatically receives the profile sample at a fixed period of time after the first PDK enters the proximity zone (see Kelly column 7 lines 32-33 right after the card is inserted into the reader).

With respect to claim 23, wherein the processor is further adapted to determine whether the second PDK is next most likely to be associated with the individual based on the differentiation metrics responsive to the authentication test not being satisfied, execute the authentication test for the second PDK, and authorize the transaction responsive to the second PDK satisfying the authentication test (see Kelly column 7 lines 32-59 i.e. Data read from frequent flyer smart card 400 or a smart card boarding pass 410 is then passed to processor 12 and a comparison performed. Processor 12 may, for example, compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410 with the information obtained from one or more of the biometric/image capture devices 22 and 24. The result of this comparison is the decision whether the traveler is physically the same individual as that described on frequent flyer smart card 400 or smart card boarding pass 410. If the comparison is positive, processor 12 indicates this to an access control interface (not shown), which then would open a door or a gate, for example).

Supplemental Box
In case the space in any of the preceding boxes is not sufficient.

With respect to claim 24, wherein the first differentiation metric is based on at least one of a distance metric, a detection duration metric, and a location metric (see Kelly column 7 lines 32-33).

With respect to claim 25, further comprising a screen coupled to the receiver/decoder circuit, the screen adapted to display an image received from the PDK (see Kelly figure 10).

With respect to claim 26, a computer readable storage medium for differentiating between a plurality of personal digital keys (PDKs) within a proximity zone of an external device, structured to store instructions executable by a processing system, the instructions when executed cause the processing system to:

obtaining a first differentiation metric associated with the first PDK after it enters the proximity zone (see Kelly column 7 lines 32-33 i.e. a user may be required to input his/her smart card into smart card reader);

obtaining a second differentiation metric associated with the second PDK after it enters the proximity zone (see Kelly column 7 lines 32-33 the next user that comes and gets his smartcard scanned);

responsive to the first PDK being most likely associated with the transaction, executing an authentication test for the first PDK (see column 7 lines 32-59 i.e. Data read from frequent flyer smart card 400 or a smart card boarding pass 410 is then passed to processor 12 and a comparison performed. Processor 12 may, for example, compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410 with the information obtained from one or more of the biometric/image capture devices 22 and 24. The result of this comparison is the decision whether the traveler is physically the same individual as that described on frequent flyer smart card 400 or smart card boarding pass 410. If the comparison is positive, processor 12 indicates this to an access control interface (not shown), which then would open a door or a gate, for example); and

authorizing the transaction responsive to the first PDK satisfying the authentication test (see Kelly column 7 lines 32-59 i.e. Data read from frequent flyer smart card 400 or a smart card boarding pass 410 is then passed to processor 12 and a comparison performed. Processor 12 may, for example, compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410 with the information obtained from one or more of the biometric/image capture devices 22 and 24. The result of this comparison is the decision whether the traveler is physically the same individual as that described on frequent flyer smart card 400 or smart card boarding pass 410. If the comparison is positive, processor 12 indicates this to an access control interface (not shown), which then would open a door or a gate, for example).

Kelly does not teach determining whether the first PDK is most likely to be associated with a transaction based on the first and second differentiation metrics. Iwamura teaches that with the increase popularity in wireless smartcards devices will is more and more likely that multiple smart card will be in communication range of a terminal. Iwamura teaches that when many smart cards exist in the communication range a specific carrier is selected by a shock absorbing mechanism so that the process can be correctly performed i.e. determining whether the first PDK is most likely to be associated with a transaction based on the first and second differentiation metrics (see paragraph 0013). It 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 to have modified Kelly with a system that allows many smartcards in communication range while still making sure the process is carried out correctly. Therefore one would have been motivated to have selected the smartcard based on first and second differentiation metrics of the smartcards

With respect to claim 27, the instruction when executed further causing the processing system to receive an input to initiate an authentication of an individual (see Kelly column 7 lines 32-59 i.e. a user may be required to input his/her smart card into smart card reader/writer 26 as well as have one or more of the user's immutable characteristics (fingerprint, image, etc.) recorded).

With respect to claim 28, the instructions when executed further causing the processing system to: receiving a first profile sample from the first PDK, wherein the profile sample comprises a subset of information from a first profile in the first PDK computed according to a first function (see Kelly figure 6 and column 7 lines 32-59 i.e. the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410); computing an input sample from the received input according to the first function (see Kelly column 7 lines 32-59 i.e. compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410); and responsive to the first profile sample not matching the input sample, indicating that the first PDK does not satisfy the authentication test (see column 7 lines 32-59 i.e. Data read from frequent flyer smart card 400 or a smart card boarding pass 410 is then passed to processor 12 and a comparison performed. Processor 12 may, for example, compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410 with the information obtained from one or more of the biometric/image capture devices 22 and 24. The result of this comparison is the decision whether the traveler is physically the same individual as that described on frequent flyer smart card 400 or smart card boarding pass 410. If the comparison is positive, processor 12 indicates this to an access control interface (not shown), which then would open a door or a gate, for example).

With respect to claim 29, wherein the input is a biometric input and wherein the instructions when executed further cause the processing system to: wirelessly receiving a biometric profile from the first PDK (see column 7 lines 32-59 i.e. Data read from frequent flyer smart card 400 or a smart card boarding pass 410); comparing the received biometric profile to the biometric input (see Kelly column 7 lines 32-59 i.e. compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410 with the information obtained from one or more of the biometric/image capture devices ~~22~~ and 24); and responsive to the biometric profile matching the biometric input, indicating that the authentication test is satisfied (see Kelly column 7 lines 32-59 i.e. Data read from frequent flyer smart card 400 or a smart card boarding pass 410 is then passed to processor 12 and a comparison performed. Processor 12 may, for example, compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410 with the information obtained from one or more of the biometric/image capture devices 22 and 24. The result of this comparison is the decision whether the traveler is physically the same individual as that described on frequent flyer smart card 400 or smart card boarding pass 410. If the comparison is positive, processor 12 indicates this to an access control interface (not shown), which then would open a door or a gate, for example).

With respect to claim 30, the instructions when executed further causing the processing system to: responsive to the authentication test not being satisfied, determine whether the second PDK is next most likely to be associated with the individual based

Supplemental Box
In case **the space in any of the preceding boxes is not sufficient**.

on the differentiation metrics; execute the authentication test for the second PDK; and authorize the transaction responsive to the second PDK satisfying the authentication test (see Kelly column 7 lines 32-59 i.e. compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410); and determining if the second profile sample matches the input sample (see Kelly column 7 lines 32-59 i.e. Data read from frequent flyer smart card 400 or a smart card boarding pass 410 is then passed to processor 12 and a comparison performed. Processor 12 may, for example, compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410 with the information obtained from one or more of the biometric/image capture devices 22 and 24. The result of this comparison is the decision whether the traveler is physically the same individual as that described on frequent flyer smart card 400 or smart card boarding pass 410. If the comparison is positive, processor 12 indicates this to an access control interface (not shown), which then would open a door or a gate, for example).

With respect to claim 31, wherein the first differentiation metric is based on at least one of a distance metric, a detection duration metric, and a location metric (see Kelly column 7 lines 32-33).

Claims 11 lack an inventive step under PCT Article 33(3) as being obvious over Kelly et al (U.S. 7,090,126) in view of Iwamura (U.S. 2006/0022046) in further view of Patel (U.S. 5,416,780). Kelly nor Iwamura teach with respect to claim 11, wherein the distance metric is determined based on at least one of bit error rate, packet error rate, signal strength. Patel teaches wherein the distance metric is determined based on at least one of bit error rate, packet error rate, signal strength (see column 7 lines 39-68). It 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 to have chosen the base station based on the best signal strength between the smartcard and the reader to increase the chance that the message gets sent correctly (see column 7 lines 39-68). Therefore one would have been motivated to have the smartcard with the best signal strength.

Claims 13 lack an inventive step under PCT Article 33(3) as being obvious over Kelly et al (U.S. 7,090,126) in view of Iwamura (U.S. 2006/0022046) in further view of Steelberg et al (U.S. 2003/0139190).

Kelly nor Iwamura teach with respect to claim 13, wherein the location metric is determined using coordinate triangulation. Steelberg teaches the uses triangulation to help set secure radio frequency communication between smartcard and other device (see abstract and paragraph 0053). It 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 to have used triangulation to help set secure radio frequency communication between smartcard and other device. Therefore one would have been motivated to have used triangulation to help set secure radio frequency communication between smartcard and other device (see abstract and paragraph 0053).

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
GREG T. SUEOKA
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

Fenwick & West LLP
APR 25 2008
RECEIVED

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

	Date of mailing (*day/month/year*)
Applicant's or agent's file reference 12786 PCT	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US07/11103	International filing date (*day/month/year*) 07 May 2007 (07.05.2007)
Applicant PROXENSE, LLC	

25000-

1. ☒ The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

Filing of amendments and statement under Article 19:
The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):

When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Facsimile No.: (41-22) 338.82.70.

For more detailed instructions, see the notes on the accompanying sheet.

2. ☐ The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. ☐ **With regard to the protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

☐ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

☐ no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90*bis*.1 and 90*bis*.3, respectively, before the completion of the technical preparations for international publication.

The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/ US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer SUMAN DEBNATH Telephone No. 571 270 9922

Form PCT/ISA/220 (January 2004) *(See notes on accompanying sheet)*

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
GREG T. SUEOKA
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

	Date of mailing (*day/month/year*) 23 APR 2008
Applicant's or agent's file reference 12786 PCT	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US07/11103	International filing date (*day/month/year*) 07 May 2007 (07.05.2007)
Applicant PROXENSE, LLC	

1. ☒ The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

   Filing of amendments and statement under Article 19:
   The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

   Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Facsimile No.: (41-22) 338.82.70.

   For more detailed instructions, see the notes on the accompanying sheet.

2. ☐ The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. ☐ **With regard to the protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

   ☐ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

   ☐ no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

   Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90*bis*.1 and 90*bis*.3, respectively, before the completion of the technical preparations for international publication.

   The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

   Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

   In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

   See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/ US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer SUMAN DEBNATH Telephone No. 571 270 9922

Form PCT/ISA/220 (January 2004) (*See notes on accompanying sheet*)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 12786 PCT	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US07/11103	International filing date (*day/month/year*) 07 May 2007 (07.05.2007)	(Earliest) Priority Date (*day/month/year*) 05 May 2006 (05.05.2006)
Applicant PROXENSE, LLC		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 2 sheets.

☐ It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the Report**
   a. With regard to the **language**, the international search was carried out on the basis of:
      ☒ the international application in the language in which it was filed.
      ☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. ☐ This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 Rule 43.6 *bis(a)*
   c. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.
2. ☐ **Certain claims were found unsearchable** (See Box No. II)
3. ☐ **Unity of invention is lacking** (See Box No. III)
4. With regard to the **title**,
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the **drawings**,
   a. the figure of the **drawings** to be published with the abstract is Figure No. 1
      ☐ as suggested by the applicant.
      ☒ as selected by this Authority, because the applicant failed to suggest a figure.
      ☐ as selected by this Authority, because this figure better characterizes the invention.
   b. ☐ none of the figures is to be published with the abstract.

Form PCT/ISA/210 (first sheet) (April 2007)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US07/11103

A. CLASSIFICATION OF SUBJECT MATTER
IPC: **H04K 1/00**(2006.01)

USPC: 713/186
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/186

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
USPAT, US-PGPUB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2002/0104006 A1 (Boate et al.) 01 August 2002 (01.08.2002), [0011], [0012], [0014], [0027], [0035], [0043].	1-20
A,E	US 7,249,177 B1 (MILLER) 24 July 2007	1-20

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
08 April 2008 (08.04.2008)

Date of mailing of the international search report
23 APR 2008

Name and mailing address of the ISA/US
Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
Facsimile No. (571) 273-3201

Authorized officer
SUMAN DEBNATH
DEBORAH A. THOMAS
PARALEGAL SPECIALIST
Telephone No. 571 270 9922

Form PCT/ISA/210 (second sheet) (April 2007)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
GREG T. SUEOKA
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing (*day/month/year*)	23 APR 2008
Applicant's or agent's file reference 12786 PCT	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date (*day/month/year*)	Priority date (*day/month/year*)
PCT/US07/11103	07 May 2007 (07.05.2007)	05 May 2006 (05.05.2006)

International Patent Classification (IPC) or both national classification and IPC

IPC: **H04K 1/00**(2006.01)
USPC: 713/186

Applicant

PROXENSE, LLC

1. This opinion contains indications relating to the following items:

☒	Box No. I	Basis of the opinion
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☐	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☐	Box No. VII	Certain defects in the international application
☐	Box No. VIII	Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(*b*) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/ US	Date of completion of this opinion	Authorized officer
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	08 April 2008 (08.04.2008)	SUMAN DEBNATH Telephone No. 571 270 9922

Form PCT/ISA/237 (cover sheet) (April 2007)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US07/11103

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

☒ the international application in the language in which it was filed

☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of:

a. type of material

☐ a sequence listing

☐ table(s) related to the sequence listing

b. format of material

☐ on paper

☐ in electronic form

c. time of filing/furnishing

☐ contained in the international application as filed.

☐ filed together with the international application in electronic form.

☐ furnished subsequently to this Authority for the purposes of search.

4. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US07/11103

Box No. V Reasoned statement under Rule 43 *bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims NONE	YES
	Claims 1-20	NO
Inventive step (IS)	Claims NONE	YES
	Claims 1-20	NO
Industrial applicability (IA)	Claims 1-20	YES
	Claims NONE	NO

2. Citations and explanations:

Please See Continuation Sheet

Form PCT/ISA/237 (Box No. V) (April 2007)

Supplemental Box
In case **the space in any of the preceding boxes is not sufficient.**

V. 2. Citations and Explanations:

Claims 1-20 lack novelty under PCT Article 32(2) as being anticipated by Boate et al. (Pub. No.: US 2002/0104006 A1), hereinafter "Boate".

As to claim 1, Boate discloses a method for electronic transaction processing comprising: wirelessly receiving data from a personal digital key (PDK) ([0011], [0012]); receiving a biometric input ([0012], [0027]); authenticating the personal digital key ([0012], [0035]); authenticating the biometric input ([0012], [0043]); and performing a transaction responsive to the personal digital key and the biometric input being authenticated ([0012], [0027], [0035]).

As to claim 2, Boate discloses wherein receiving the biometric input comprises performing at least one of a fingerprint scan, a retinal scan, an iris scan, a facial scan, a palm scan, a DNA analysis, a signature analysis, and a voice analysis ([0027], lines 1-11).

As to claim 3, Boate discloses wherein wirelessly receiving data from a personal digital key includes receiving biometric data ([0012]), and authenticating the biometric input includes comparing the biometric data to the biometric input for match ([0012], [0043]).

As to claim 4, Boate discloses wherein the biometric data is a portion or subset of an entire biometric data set for an attribute ([0027]).

As to claim 5, Boate discloses wherein wirelessly receiving data from a personal digital key includes establishing a secure communication channel between the PDK and a reader, and wherein a profile is sent from the PDK to the reader ([0012], [0035]).

As to claim 6, Boate discloses wherein the profile includes a PDK identification number and one from the group of financial information, credit card information and personal identification information ([0027]).

As to claim 7, Boate discloses wherein authenticating the personal digital key begins before authenticating the biometric input ([0012], [0027]).

Supplemental Box
In case **the space in any of the preceding boxes is not sufficient.**

As to claim 8, Boate discloses wherein authenticating the biometric input begins before authenticating the personal digital key ([0012], [0027]).

As to claim 9, Boate discloses wherein authenticating the personal digital key includes receiving data from the personal digital key and comparing it against an external system ([0027]).

As to claim 10, Boate discloses wherein the external system is one from the group of a central registry, a validation database and a private registry ([0014]).

As to claim 11 Boate discloses further comprising authenticating a reader ([0012]).

As to claim 12, Boate discloses wherein wirelessly receiving, receiving the biometric input, authenticating the personal digital key, authenticating the biometric input are performed by a reader device ([0012]).

As to claim 13, Boate discloses wherein receiving the biometric input and authenticating the biometric input are performed by the personal digital key ([0012], [0027]).

As to claim 14, Boate discloses wherein receiving authenticating the biometric input is performed by the personal digital key and the reader ([0012], [0027], [0035]).

As to claim 15, Boate discloses wherein performing a transaction comprises: initiating the transaction; communicating with another system to authorize and approve the transaction; and presenting the status for the transaction ([0012], [0027], [0035]).

As to claim 16, Boate discloses a method for electronic transaction authentication comprising: wirelessly receiving data from a reader ([0011], [0012]); receiving a biometric input ([0012], [0027]); authenticating the reader authenticating the biometric input ([0012], [0043]); and transmitting a signal authorizing a transaction responsive to the reader and the biometric input being authenticated ([0012], [0027], [0035]).

As to claim 17, Boate discloses wherein receiving the biometric input comprises performing at least one of a fingerprint scan, a retinal scan, an iris scan, a facial scan, a palm scan, a NA analysis, a signature analysis, and a voice analysis ([0027], lines 1-11).

As to claim 18, Boate discloses wherein receiving the biometric input comprises obtaining a representation of physical or behavioral characteristics derived from the individual ([0027]).

As to claim 19, Boate discloses a method for electronic transaction processing comprising: wirelessly receiving a biometric reference from a personal digital key ([0012], [0027], [0043]); receiving a biometric input ([0012], [0027]); authenticating the biometric input ([0012], [0043]); and performing a transaction responsive to the biometric input being authenticated ([0012], [0027], [0035]).

As to claim 20, Boate discloses wherein receiving the biometric input comprises performing at least one of a fingerprint scan, a retinal scan, an iris scan, a facial scan, a palm scan, a DNA analysis, a signature analysis, and a voice analysis ([0027]).

PATENT COOPERATION TREATY

Fenwick & West LLP

JUN 30 200

RECEIVED

From the INTERNATIONAL SEARCHING AUTHORITY

To:
GREG T. SUEOKA
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

	Date of mailing (*day/month/year*) 26 JUN 2008
Applicant's or agent's file reference 12784 PCT	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US07/11104	International filing date (*day/month/year*) 07 May 2007 (07.05.2007)
Applicant PROXENSE, LLC	

25000

1. ☒ The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

   Filing of amendments and statement under Article 19:
   The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

   Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Facsimile No.: (41-22) 338.82.70.

   For more detailed instructions, see the notes on the accompanying sheet.

2. ☐ The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. ☐ **With regard to the protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

   ☐ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

   ☐ no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

   Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90*bis*.1 and 90*bis*.3, respectively, before the completion of the technical preparations for international publication.

   The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

   Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

   In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

   See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/ US	Authorized officer
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450	/Tongoc Tran/
Facsimile No. (571) 273-3201	Telephone No. 571-272-3843

Form PCT/ISA/220 (January 2004) *(See notes on accompanying sheet)*

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 12784 PCT	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US07/11104	International filing date (*day/month/year*) 07 May 2007 (07.05.2007)	(Earliest) Priority Date (*day/month/year*) 05 May 2006 (05.05.2006)
Applicant PROXENSE, LLC		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 3 sheets.

☐ It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the Report**
   a. With regard to the **language**, the international search was carried out on the basis of:
      ☒ the international application in the language in which it was filed.
      ☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. ☐ This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 Rule 43.6 *bis(a)*
   c. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.
2. ☐ **Certain claims were found unsearchable** (See Box No. II)
3. ☐ **Unity of invention is lacking** (See Box No. III)
4. With regard to the **title**,
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,
   ☐ the text is approved as submitted by the applicant.
   ☒ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the **drawings**,
   a. the figure of the **drawings** to be published with the abstract is Figure No. 8
      ☒ as suggested by the applicant.
      ☐ as selected by this Authority, because the applicant failed to suggest a figure.
      ☐ as selected by this Authority, because this figure better characterizes the invention.
   b. ☐ none of the figures is to be published with the abstract.

Form PCT/ISA/210 (first sheet) (April 2007)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US07/11104

Box IV TEXT OF THE ABSTRACT (Continuation of Item 5 of the first sheet)

NEW ABSTRACT

A system and method provide efficient, secure, and highly reliable authentication for transaction processing and/or access control applications. A personal digital key (PDK) 802 is programmed using a trusted programming device to initialize and/or register the PDK 802 for use. In one embodiment, the initialization and registration processes are administered by a specialized trusted Notary to ensure the processes follow defined security procedures. In a biometric initialization, the programming device acquires a biometric input 804 from a user and writes the biometric data to a tamperproof memory in the PDK 802. In registration, the programmer 810 communicates to one or more remote registers to create or update entries associated with the user PDK 802. Once initialized and registered, the PDK 802 can be used for various levels of secure authentication processes.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US07/11104

A. CLASSIFICATION OF SUBJECT MATTER
IPC: **H04L 9/00**(2006.01)

USPC: 713/186
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/186

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EAST

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2003/0079133 A1 (BREITER et al.) 24 April 2003 (24.04.2003), Fig. 4 and 5, paragraphs [0082]-[0083].	1-24
Y	US 2002/0191816 A1 (MARITZEN et al.), 19 December 2002 (19.12.2002), paragraph 0056.	1-24

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 May 2008 (10.05.2008)	26 JUN 2008
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer /Tongoc Tran/ Telephone No. (571) 272-3843

Form PCT/ISA/210 (second sheet) (April 2007)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
GREG T. SUEOKA
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	26 JUN 2008
Applicant's or agent's file reference 12784 PCT	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US07/11104	07 May 2007 (07.05.2007)	05 May 2006 (05.05.2006)

International Patent Classification (IPC) or both national classification and IPC

IPC: **H04L 9/00**(2006.01)
USPC: 713/186

Applicant

PROXENSE, LLC

1. This opinion contains indications relating to the following items:

- ☒ Box No. I — Basis of the opinion
- ☐ Box No. II — Priority
- ☐ Box No. III — Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV — Lack of unity of invention
- ☒ Box No. V — Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI — Certain documents cited
- ☐ Box No. VII — Certain defects in the international application
- ☐ Box No. VIII — Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(*b*) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/ US	Date of completion of this opinion	Authorized officer
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	10 May 2008 (10.05.2008)	/Tongoc Tran/ Telephone No. 571-272-3843

Form PCT/ISA/237 (cover sheet) (April 2007)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US07/11104

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

☒ the international application in the language in which it was filed

☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of:

a. type of material

☐ a sequence listing

☐ table(s) related to the sequence listing

b. format of material

☐ on paper

☐ in electronic form

c. time of filing/furnishing

☐ contained in the international application as filed.

☐ filed together with the international application in electronic form.

☐ furnished subsequently to this Authority for the purposes of search.

4. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US07/11104

Box No. V Reasoned statement under Rule 43 *bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims NONE	YES
	Claims 1-24	NO
Inventive step (IS)	Claims NONE	YES
	Claims 1-24	NO
Industrial applicability (IA)	Claims 1-24	YES
	Claims NONE	NO

2. Citations and explanations:

Please See Continuation Sheet

Form PCT/ISA/237 (Box No. V) (April 2007)

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US07/11104

Supplemental Box
In case **the space in any of the preceding boxes is not sufficient**.

V. 2. Citations and Explanations:

Claims 1-24 lack an inventive step under PCT Article 33(3) as being obvious over Breiter et al. (U.S> Patent Application Publication No. 2003/0079133, hereinafter Breiter) in view of Maritzen et al. (U.S. Patent Application Publication No. 2002/0191816, hereinafter Marizen).

With respect to claims 1 and 16, Breiter discloses a method and an apparatus of using a programmer to initialize a personal digital key (PDK) for use in secure authentication (e.g. rights wallet, Fig. 4, 5, 7), comprising:

reading user information from a user PDK to determine if the user is authorized for initialization (e.g. paragraph]0082], user PDK- rights wallets);

reading notary information from a notary PDK to determine if the notary is authorized to administer the initialization (e.g. [0082]-0083], certificate authority).

acquiring a credential from the user, wherein the acquisition is witnessed by the notary ; and responsive to the user and notary being authorized (e.g. paragraph, [0082]),

Breiter does not explicitly disclose but the credential information is biometric information and storing a biometric profile based on the acquired biometric input to the user's PDK (e.g. Maritzen, paragraph, [0056]). It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the acquiring rights wallet taught by Breiter with acquiring biometrics information and storing as user profile taught by Martizen to ensure secure authentication of user in order to prevent unauthorized access to secure information.

With respect to claims 2 and 17. Breiter amd Maritzen disclose the method and apparatus of claims 1 and 16, wherein determining if the user is authorized for initialization comprises:

detecting the user PDK(e.g. paragraph, [0082]);

checking a status of the user PDK in a registry; and responsive to the status being in good standing, determining that the user is authorized for initialization (e.g. Breiter, paragraph, [0082]).

With respect to claims 3 and 18. Breoter and Maritzen disclose the method and apparatus of claims 2 and 17, wherein the user PDK is in good standing if the user PDK has not been reported as lost, stolen, expired, or revoked (e.g. Breiter, paragraph, [0082]).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US07/11104

Supplemental Box
In case **the space in any of the preceding boxes is not sufficient**.

With respect to claims 4 and 19, Breiter and Maritzen disclose the method and apparatus of claims 2 and 17, wherein the user PDK is in good standing if the user PDK has never been initialized (e.g. Breiter, paragraph, [0082]).

With respect to claims 5 and 20, Breiter and Maritzen disclose the method and apparatus of claims 1 and 17, wherein acquiring the biometric input comprises:
scanning the biometric input from a user associated with the user PDK; and performing a transformation on the biometric input to generate the biometric profile (e.g. Marizen, paragraph, [0056]).

With respect to claims 6 and 21, Breiter and Maritzen disclose the method and apparatus of claims 5 and 16, Breiter and Marizen disclose further comprising:
checking the quality of the scanned biometric input; and responsive to the quality not being satisfactory, re-scanning the biometric input (e.g.. Marizen, paragraph, 0056]).

With respect to claims 7 and 22, Breiter and Maritzen disclose the method and apparatus of claims 1 and 16, further comprising
storing initialization history data to the programmer, wherein initialization history data comprises at least one of a user PDK ID, a notary ID, a programmer ID, and a site ID (e.g. Breiter, paragraph, [0069], [0082]).

With respect to claim 8, Breiter and Maritzen disclose the method of claim 1, further comprising writing initialization history data to the user PDK, wherein initialization history data comprises at least one of a user PDK ID, a notary ID, a programmer ID, and a site ID (e.g. Breiter, paragraph, [0082]).

With respect to claim 9, Breiter and Maritzen disclose the method of claim 1, further comprising:
receiving a hardware authentication request from the user PDK; transmitting programmer information to the user PDK; and responsive to the user PDK determining that the programmer is a valid device, receiving authorization from the user PDK to continue initialization (e.g. Breiter, paragraph, [0082]).

With respect to claim 10, Breiter and Maritzen disclose he method of claim 1, wherein determining if the notary is authorized to administer initialization comprises: detecting the notary PDK; checking a status of the notary PDK in a registry; and responsive to the status being in good standing, determining that the notary is authorized to use the programmer for initialization of the user PDK (e.g. Breiter, paragraph, [0082]-[0083]).

With respect to claim 11, Breiter and Maritzen disclose the method of claim 10, wherein the notary PDK is in good standing if the notary PDK has not been reported as lost, stolen, expired, or revoked (e.g. Breiter, paragraph [0082]-[0083]).

With respect to claim 12, Breiter and Maritzen disclose the method of claim 1, further comprising determining if the programmer is in good standing (e.g. Breiter, paragraph, [0082], [0083]).

With respect to claim 13, Breiter and Maritzen disclose the method of claim 12, wherein the programmer is in good standing if the programmer has not been reported as lost, stolen, expired, or revoked and the programmer does not comprise altered software (e.g. Breiter, paragraph, [0082]-[0083]).

With respect to claim 14, Breiter and Maritzen disclose the method of claim 1, wherein the notary administers the initialization process from a remote location (e.g. Breiter, paragraph, [0082]).

With respect to claim 15, Breiter and Maritzen disclose the method of claim 1, further comprising transmitting registry information to a remote registry to add or update a registry entry, wherein the registry information comprises at least one of a user PDK ID, purchasing information, and personal information (e.g. Breither, paragraph, [0082]).

With respect to claim 23, Breiter and Maritzen disclose the apparatus of claim 16, wherein the biometric reader is adapted to obtain a representation of physical or behavioral characteristics derived from the individual (e.g. Maritzen, paragraph, [0056]).

With respect to claim 24, Breiter and Maritzen disclose the apparatus of claim 16, wherein the biometric reader comprises at least one of a fingerprint scanner, a retinal scanner, an iris scanner, a face scanner, a palm scanner, a DNA analyzer, a signature analyzer, and a voice analyzer (e.g. Maritzen, paragraph, [0056]).

Claims 1-24 meet the criteria set out in PCT Article 33(4), and thus have industrial applicability because the subject matter claimed can be made or used in industry.

RECEIVED
PATENT DOCKETING

OCT 23 2008

Fenwick & West

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
GREG T. SUEOKA
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

Applicant's or agent's file reference 11744 PCT	Date of mailing *(day/month/year)* 20 OCT 2008 **FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US07/11105	International filing date *(day/month/year)* 07 May 2007 (07.05.2007)
Applicant PROXENSE, LLC	

25000 -

1. ☒ The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

   Filing of amendments and statement under Article 19:
   The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

   Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Facsimile No.: (41-22) 338.82.70.

   For more detailed instructions, see the notes on the accompanying sheet.

2. ☐ The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. ☐ **With regard to the protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

   ☐ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

   ☐ no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

   Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90*bis*.1 and 90*bis*.3, respectively, before the completion of the technical preparations for international publication.

   The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

   Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

   In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

   See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/ US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer Hosuk Song Telephone No. 5712722100

Form PCT/ISA/220 (January 2004) *(See notes on accompanying sheet)*

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 11744 PCT	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US07/11105	International filing date (*day/month/year*) 07 May 2007 (07.05.2007)	(Earliest) Priority Date (*day/month/year*) 05 May 2006 (05.05.2006)
Applicant PROXENSE, LLC		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 4 sheets.

☐ It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the Report**
   a. With regard to the **language**, the international search was carried out on the basis of:
      ☒ the international application in the language in which it was filed.
      ☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. ☐ This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 Rule 43.6 *bis(a)*
   c. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.
2. ☐ **Certain claims were found unsearchable** (See Box No. II)
3. ☐ **Unity of invention is lacking** (See Box No. III)
4. With regard to the **title**,
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,
   ☐ the text is approved as submitted by the applicant.
   ☒ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the **drawings**,
   a. the figure of the **drawings** to be published with the abstract is Figure No. 1
      ☒ as suggested by the applicant.
      ☐ as selected by this Authority, because the applicant failed to suggest a figure.
      ☐ as selected by this Authority, because this figure better characterizes the invention.
   b. ☐ none of the figures is to be published with the abstract.

Form PCT/ISA/210 (first sheet) (April 2007)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US07/11105

Box IV TEXT OF THE ABSTRACT (Continuation of Item 5 of the first sheet)

NEW ABSTRACT

A system and method provide efficient, secure, and highly reliable authentication for transaction processing and/or access control applications. A Personal Digital Key stores one or more profiles(e.g., a biometric profile) in a tamper-proof memory that is acquired in a secure trusted process. Biometric profiles comprise a representation of physical or behavioral characteristics that are uniquely associated with an individual that owns and carries the PDK(102). The PDK wirelessly transmits the biometric profile over a secure wireless transaction to a Reader(108) for use in a biometric authentication process. The Reader compares the received biometric wireless transaction to a Reader(108) for use in a biometric authentication process. The Reader compares the received biometric profile to a biometric input(104) acquired at the point of transaction in order to determine if the transactionshould be authorized.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US07/11105

A. CLASSIFICATION OF SUBJECT MATTER
IPC: **H04K 1/00**(2006.01);**H04L 9/32**(2006.01)

USPC: 713/182,186;726/2;380/270
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/182,186; 726/2;380/270

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,E	US 7,249,177 B(MILLER) 24 July 2007 (24.07.2007), column 3 lines 28-42; column 4,lines 19-25; column 5,lines 1-17	1-42
A	US 6,070,796 A(SIRBU) 06 June 2000 (06.06.2000), column 7,lines 7-40; column 9,lines 25-55.	1-42
X	US 6,850,147 B(PROKOSKI et al) 01 February 2005 (01.02.2005), column 4,lines 39-62; column 6,lines 46-67; column 11,lines 1-22.	1-42

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 September 2008 (30.09.2008)	20 OCT 2008
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer Hosuk Song Telephone No. 5712722100

Form PCT/ISA/210 (second sheet) (April 2007)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US07/11105

Continuation of B. FIELDS SEARCHED Item 3:
EAST, foreign patent databse
search terms: biometric, fingerprint,iris,key, password, wireless, authentication, authorization,access,control,tamper-proof,memory,storage.

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
GREG T. SUEOKA
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing (*day/month/year*)	20 OCT 2008
Applicant's or agent's file reference 11744 PCT	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date (*day/month/year*)	Priority date (*day/month/year*)
PCT/US07/11105	07 May 2007 (07.05.2007)	05 May 2006 (05.05.2006)

International Patent Classification (IPC) or both national classification and IPC

IPC: **H04K 1/00**(2006.01);**H04L 9/32**(2006.01)
USPC: 713/182,186;726/2;380/270

Applicant

PROXENSE, LLC

1. This opinion contains indications relating to the following items:

☒	Box No. I	Basis of the opinion
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☐	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☐	Box No. VII	Certain defects in the international application
☐	Box No. VIII	Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(*b*) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/ US	Date of completion of this opinion	Authorized officer
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	29 September 2008 (29.09.2008)	Hosuk Song Telephone No. 5712722100

Form PCT/ISA/237 (cover sheet) (April 2007)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US07/11105

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

☒ the international application in the language in which it was filed

☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of:

a. type of material

☐ a sequence listing

☐ table(s) related to the sequence listing

b. format of material

☐ on paper

☐ in electronic form

c. time of filing/furnishing

☐ contained in the international application as filed.

☐ filed together with the international application in electronic form.

☐ furnished subsequently to this Authority for the purposes of search.

4. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

Form PCT/ISA/237(Box No. I) (April 2007)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US07/11105

Box No. V Reasoned statement under Rule 43 *bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims NONE	YES
	Claims 1-42	NO
Inventive step (IS)	Claims NONE	YES
	Claims 1-42	NO
Industrial applicability (IA)	Claims 1-42	YES
	Claims NONE	NO

2. Citations and explanations:

Please See Continuation Sheet

Form PCT/ISA/237 (Box No. V) (April 2007)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US07/11105

Supplemental Box
In case **the space in any of the preceding boxes is not sufficient**.

V. 2. Citations and Explanations:
Claims 1-42 lack novelty under PCT Article 33(2) as being anticipated by Prokoski et al(US 6,850,147).
Claim 1: Prokoski disclose wirelessly receiving a biometric profile from a personal digital key (PDK), wherein the biometric profile is uniquely associated with an individual in (col.5,lines 30-56). Prokoski disclose receiving a biometric input; comparing the biometric profile to the biometric input and authorizing a transaction responsive to the biometric profile matching the biometric input in (col.7,lines 35-59).
Claim 2: Prokoski disclose obtaining a representation of physical or behavioral characteristics derived from the individual in (fig.1).
Claim 3: Prokoski disclose receiving the biometric input comprises performing at least one of a fingerprint scan, a retinal scan, an iris scan, a facial scan, a palm scan, a DNA analysis, a signature analysis, and a voice analysis in (fig.6).
Claim 4: Prokoski disclose performing a device authentication to verify that the PDK is a valid device responsive to the PDK entering a proximity zone in (fig.4).
Claim 5: Prokoski disclose performing a challenge-response authentication to verify the PDK is valid wherein the PDK further verifies validity of an external device in (fig.6).
Claim 6: Prokoski disclose receiving available profile types from the PDK and comparing the available profile types to required profile types of authentication in (col.10,lines 15-29). Prokoski disclose responsive to the available profile types being sufficient indicating that the PDK is valid and responsive to the available profile types not being sufficient indicating that the PDK is not valid in (fig.4).
Claim 7: Prokoski disclose establishing a secure communication channel with a remote registry in (col.10,lines 30-41). Prokoski disclose transmitting PDK information to the remote registry wherein the PDK information is uniquely associated with the PDK receiving validity information from the remote registry and determining if a transaction should be authorized based on the validity information and the comparison between the biometric profile and biometric input in(fig.6).
Claim 8:Prokoski disclose remote registry is a Central Registry comprising a secured centrally-located database administered by a trusted third-party organization in (fig.4).
Claim 9: Prokoski disclose remote registry is a private registry comprising a database administered by a private controlling entity in (fig.5).
Claim 10: Prokoski disclose receiving purchasing information from the PDK, the purchasing information comprising at least one of bank information, credit card information,debit card information, ATM card information and coupon information in (col.2,lines 35-64).
Claim 11: Prokoski disclose determining if the purchasing information is valid by querying a remote validation database in (fig.6).
Claim 12: Prokoski disclose receiving a picture from the PDK comprising an image of the individual;displaying the image on a screen and prompting an administrator to confirm or deny the identity of the individual based on the appearance of the individual and the displayed image in (col.11,lines 1-22).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US07/11105

Supplemental Box
In case the space in any of the preceding boxes is not sufficient.

Claim 13: Prokoski disclose acquiring a personal identification number from the individual;receiving a PIN profile from the PDK and determining if the acquired personal identification number matches the received PIN profile in (fig.4).
Claim 14: Prokoski disclose computing a representation of the biometric input based on a mathematical hash of the biometric input and comparing the representation of the biometric input to the biometric profile in (fig.3).
Claim 15: Prokoski disclose a receiver/decoder circuit adapted to wirelessly receive a biometric profile from a personal digital key(PDK) wherein the biometric profile is uniquely associated with an individual in (fig.3). Prokoski disclose a biometric reader adapted to receive a biometric input and a processor coupled to the receiver/decoder circuit and the biometric reader the processor adapted to compare the biometric profile to the biometric input and indicate that a transaction should be authorized responsive to the biometric profile matching the biometric input in (fig.4).
Claim 16: Prokoski disclose a establishing a secure communication channel with a remote registry; transmit PDK information to the remote registry wherein the PDK information is uniquely associated with the PDK and receive validity information from the remote registry in (fig.6).
Claim 17: Prokoski disclose a credit card terminal input/output coupled to the receiver/decoder circuit, the credit card terminal input/output adapted to communicate with a credit card terminal in (col.2,lines 50-64).
Claim 18: Prokoski disclose biometric reader is further adapted to obtain a representation of physical or behavioral characteristics derived from the individual in (col.11,lines 7-13).
Claim 19: Prokoski disclose biometric reader comprises at least one of a fingerprint scanner, a retinal scanner, an iris scanner, a face scanner, a palm scanner, a DNA analyzer, a signature analyzer, and a voice analyzer in (col.6,lines 54-65).
Claim 20: Prokoski disclose receiver/decoder circuit is further adapted to receive the biometric profile in an encrypted format over a secure wireless channel, and decrypt the biometric profile to an unencrypted format in (fig.5).
Claim 21: Prokoski disclose receiver/decoder circuit is adapted to detect a PDK in response to the PDK entering a proximity zone of the receiver/decoder circuit and request the PDK to transmit the biometric profile in (fig.4).
Claims 22,26-28: Prokoski disclose a memory adapted to store a biometric profile in a tamper-proof format, wherein the biometric profile is uniquely associated with an individual and a transceiver coupled to the memory, the transceiver adapted to wirelessly receive a request from an external device to transmit the biometric profile to the extenal device and wirelessly transmit the biometric profile over a secure wireless channel to the extenal device in (fig.1).
Claim 23: Prokoski disclose memory further stores initialization information comprising at least one of a programmer ID, a notary ID, and a site ID associated with an initialization process in(fig.2).
Claim 24: Prokoski disclose memory is further adapted to store at least one of purchasing information, registration information and personal information in (col.11,lines 50-62).
Claim 25: Prokoski disclose a programmer interface adapted to write the biometric profile to the memory during a trusted initialization process in(fig.3).
Claim 29,32-37: Prokoski disclose storing a biometric profile in a tamper-proof memory, wherein the biometric profile is uniquely associated with an individual and wirelessly receiving a request from an external device to transmit the biometric profile to the external device in (fig.1). Prokoski disclose responsive to receiving the request wirelessly transmitting the biometric profile over a secure wireless channel to the external device wherein the external device authenticates an individual for a transaction based on a comparison between the biometric profile and a biometric input acquired from the individual in (fig.3).
Claim 30: Prokoski disclose encrypting the stored biometric profile for transmission over the secure wireless channel in (fig.2).
Claim 31: Prokoski disclose storing at least one of purchasing information, registration information and personal information in (fig.6).
Claim 38: Prokoski disclose wirelessly receiving uniquely identifying information from a personal digital key(PDK) and analyzing the uniquely identifying information to determine if the PDK is valid in (col.3,lines 28-42,57-63). Miller disclose receiving profile information from the PDK indicating types of profiles stored in the PDK and determining if the types of profiles are compatible with allowable authentication types in (col.5,lines 45-57). Prokoski disclose performing one or more authentication tests to determine if a profile is valid and authorizing a transaction responsive to determining that the PDK is valid, determining that the types of profiles are compatible and determining that the profile is valid in (col.10,lines 15-29).
Claim 39: Prokoski disclose wirelessly receiving a biometric profile from the PDK, wherein the biometric profile is uniquely associated with an individual in (fig.3). Prokoski disclose acquiring a biometric input and determining that the profile is valid responsive to the acquired biometric input matching the received biometric profile in (fig.4).
Claim 40: Prokoski disclose wirelessly receiving a Personal Identification Number(PIN) profile forn the PDK, wherein the PIN profile is uniquely associated with an individual;acquiring a PIN input and determining that the profile is valid responsive to the acquired PIN matching the received PIN profile in (fig.6).
Claim 41: Prokoski disclose wirelessly receiving a picture profile from the PDK, wherein the picture profile is uniquely associated with an image of an individual;acquiring an image and determining that the profile is valid responsive to the acquired image matching the received picture profile in (col.11,lines 2-13).
Claim 42: Prokoski disclose receiving a registry profile from the PDK wherein the registry profile is uniquely associated with an individual and establishing a secure communication channel with a remote registry in (fig.1). Prokoski disclose transmitting the registry profile to the remote registry;receiving status information from the remote registry and determining that the profile is valid responsive to the status information indicating a valid registry entry in (fig.4).
Claims 1-42 meet the criteria set out in PCT Article 33(4), and thus meet industrial applicability because the subject matter claimed can be made or used in industry.

Electronic Acknowledgement Receipt

EFS ID:	21487689
Application Number:	14521982
International Application Number:	
Confirmation Number:	8239
Title of Invention:	Biometric Personal Data Key (PDK) Authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Paige McDede Alsbury
Filer Authorized By:	
Attorney Docket Number:	10001-04540 US
Receipt Date:	12-FEB-2015
Filing Date:	23-OCT-2014
Time Stamp:	16:49:05
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	04540US_IDS.pdf	619218 955604c99c923eab699611fc502c78d5c6ce89bc	no	22

Warnings:	
Information:	

2	Foreign Reference	01_WO0062505.pdf	939694 5ce5cb0dd11bbc758e1d30a5d1fa00979eba2784	no	27
Warnings:					
Information:					
3	Foreign Reference	02_WO0122724.pdf	1257552 2397b42fa8bf41be284186526a9ec6992979c976	no	32
Warnings:					
Information:					
4	Foreign Reference	03_WO0175876.pdf	1238267 68efaf81bd7f3ffd88395b255bbae522b85fd252	no	28
Warnings:					
Information:					
5	Foreign Reference	04_WO0177790.pdf	818043 c7e3a024ce24e36efcf80cfa54c59b8ac6f44b4c	no	20
Warnings:					
Information:					
6	Foreign Reference	05_WO2005050450.pdf	1758377 84ec9eca7924e958684bf6046532d2a980bcd6e2	no	49
Warnings:					
Information:					
7	Foreign Reference	06_WO2005086802.pdf	2017652 b79310d08b09d4211693aa74154e6a726f13895c	no	58
Warnings:					
Information:					
8	Non Patent Literature	01_AllianceActivities.pdf	226093 3a149c485022af159b17b0edd455d458d0173ac4	no	3
Warnings:					
Information:					
9	Non Patent Literature	02_AmrFarouk_AuthenticationMechanismsInGrid.pdf	1786086 f9bd310f701ec58b2788f8a851986f1080f7ef72	no	6
Warnings:					
Information:					
10	Non Patent Literature	03_Antonoff_VisitingVideoValley.pdf	1001904 8fa85f3153915fcbae89a24e5c2f9590a3bbd561	no	3
Warnings:					
Information:					

11	Non Patent Literature	04_ApplyingBiometricstoDoorAccess.pdf	346855 f9af7321aecb4b2def71495ba661f4e5167a4c36	no	5
Warnings:					
Information:					
12	Non Patent Literature	05_BioPayLLC_FrequentlyAskedQuestions.pdf	231993 96c8f4b9366666f073abd42470936e6450a9496e	no	5
Warnings:					
Information:					
13	Non Patent Literature	06_Blum_DigitalRightsManagementMaySolveTheNapster.pdf	349236 e1452e8c2f986cc194a4ada5edda2c522b186cb9	no	4
Warnings:					
Information:					
14	Non Patent Literature	07_DeBow_CreditDebitDebutsinMidwestSmartCardTest.pdf	657848 1773ef3ad9b896b2eb6aa53b63512d2bc935c3e3	no	4
Warnings:					
Information:					
15	Non Patent Literature	08_Dennis_DigitalPassportsNeedNotInfringeCivil.pdf	81856 4324c84fef98a5fb0f69735768bdf12b6f612522	no	2
Warnings:					
Information:					
16	Non Patent Literature	09_Fasca_TheCircuit.pdf	139107 c385ac718b7f0d2a6be3d6a9166377412cc5162a	no	2
Warnings:					
Information:					
17	Non Patent Literature	10_FirecrestShowsHowTrulyCommerciallyMindedCompanies.pdf	173133 f542234fb4a64551aea511b133ab47ad9f91bc46	no	2
Warnings:					
Information:					
18	Non Patent Literature	11_Kontzer_ThomsonBetsOnSmartCardsForVideo.pdf	67757 8e125353da0d334992e578d9d9890a1c8a950a70	no	1
Warnings:					
Information:					
19	Non Patent Literature	12_Lake_DownloadingforDollars.pdf	290663 ad7ef08e8937515910ef783ce7b9adec1e6a7e6f	no	2
Warnings:					
Information:					

20	Non Patent Literature	13_Lewis_SonyAndVisaInOnLineEntertainmentVenture.pdf	56440 e183f812be16d563399278260deffed202fadc35	no	1
Warnings:					
Information:					
21	Non Patent Literature	14_McIver_IdentificationandVerificationWorkingTogether.pdf	347011 7d958fbf0dfeba680cb6fb033aeaa0d90c8f45f7	no	5
Warnings:					
Information:					
22	Non Patent Literature	15_MicronasAndThomsonMultimediaShowcaseaNewCopy.pdf	169904 f021567ffe10585d21577b16178ebd3caadeb44e	no	3
Warnings:					
Information:					
23	Non Patent Literature	16_Nilsson_MatchOnCardForJavaCards.pdf	1011494 e50233adfa1bb35486bc68af3ceec3fab74903b5	no	5
Warnings:					
Information:					
24	Non Patent Literature	17_Nordin_MatchOnCardTechnology.pdf	1530705 504809efc706248c6b00b2ed6932d630deaaa0dc	no	7
Warnings:					
Information:					
25	Non Patent Literature	18_Paget_TheSecurityBehindSecureExtranets.pdf	324885 09fdc48f283744598ffdbd7c23e56d80294e149d	no	4
Warnings:					
Information:					
26	Non Patent Literature	19_PCTUS0438124.pdf	431799 b9d8cee6f85b9a37c4a265baf9ab46b08ae0a82e	no	10
Warnings:					
Information:					
27	Non Patent Literature	20_PCTUS0543447.pdf	341979 e06a0bc860468257522f92cbb0888a0b29911987	no	7
Warnings:					
Information:					
28	Non Patent Literature	21_PCTUS0546843.pdf	538413 0ebb0ba9323405efb1c8b3abbe0f9ac8b7462b6b	no	10
Warnings:					
Information:					

29	Non Patent Literature	22_PCTUS0711102.pdf	779621 bc08b8e1785656880d0c1b5ad988bf8c06146bd2	no	11
Warnings:					
Information:					
30	Non Patent Literature	23_PCTUS0711103.pdf	478058 4913218c747373b0b4ffa13151f026946d921db0	no	9
Warnings:					
Information:					
31	Non Patent Literature	24_PCTUS0711104.pdf	415819 8eaa9fea7d2fddf128f023eab6bd0a5cdeac7bc6	no	9
Warnings:					
Information:					
32	Non Patent Literature	25_PCTUS0711105.pdf	463359 10ca7e6029cc9e7dd891da26293de857acd025f5	no	10
Warnings:					
Information:					
33	Non Patent Literature	26_Pope_OasisDigitalSignatureServices.pdf	500950 96b3b3bf7bb7dd24d1fa936136f3b429a033b648	no	4
Warnings:					
Information:					
34	Non Patent Literature	27_SAFModuleTMALookIntoStrongAuthentication.pdf	404905 174befaccf905371360dc459482830f14f516f9d	no	8
Warnings:					
Information:					
35	Non Patent Literature	28_Sapsford_EBusinessSoundWavesCouldHelp.pdf	175123 242dee98e1ff7afed5dd004f8a66b0095eacdc91	no	2
Warnings:					
Information:					
36	Non Patent Literature	29_SayHelloToBluetooth.pdf	1126006 3a79860984b0abd13548a7704847a2462fb5f587	no	5
Warnings:					
Information:					
37	Non Patent Literature	30_SmartCardsAndBiometricsWhitePaper.pdf	310708 ffb7e11a22feacf7fd0bfac41ca78587156b6f61	no	7
Warnings:					
Information:					

38	Non Patent Literature	31_ThomsonMultimediaUnveilsCopyProtectionProposalDesigned.pdf	161763 595b77a62fa25ae58ac89df597cc16b6659f645e	no	2
Warnings:					
Information:					
39	Non Patent Literature	32_VanWinkle_BluetooththeKingofConnectivity.pdf	557066 b9829d8fc03ba8bc082d22b494ceca99b802de70	no	6
Warnings:					
Information:					
40	Non Patent Literature	33_Wade_UsingFingerprintsToMakePaymentsAtPOS.pdf	330268 991ab43f676f3ba58851acbdee21daf42148391a	no	3
Warnings:					
Information:					
41	Non Patent Literature	34_Wallace_TheInternetUnplugged.pdf	311563 82efeea8e7a8de75a3077741d26e9b75a2837d99	no	3
Warnings:					
Information:					
42	Non Patent Literature	35_Weber_InTheAgeOfNapster.pdf	162882 593bc896376b21ca23a73ade41fd5f6c024b6e68	no	3
Warnings:					
Information:					
43	Non Patent Literature	36_WhatIsAFile.pdf	42536 143edf491eb43706355e5ed7eec7e34aaa84b5d6	no	1
Warnings:					
Information:					
44	Non Patent Literature	37_Yoshida_ContentProtectionPlanTargetsWirelessHome.pdf	132557 e0702c3d6f06c7b588e5e523bb54dc715e92bf26	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	25107148		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

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 NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/521,982	10/23/2014	John J. Giobbi	10001-04540 US

CONFIRMATION NO. 8239

89194
Patent Law Works/Proxense
Greg Sueoka
201 South Main Street, Suite 250
Salt Lake City, UT 84111

POA ACCEPTANCE LETTER

OC000000073211543

Date Mailed: 02/05/2015

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 01/29/2015.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/ltaba/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

Doc Code: PA..

Document Description: Power of Attorney

PTO/AIA/82B(07-12)
Approved for use through 11/30/2014. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in the attached transmittal letter.

☒ I hereby appoint Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A or equivalent):

89194

OR

☐ I hereby appoint Practitioner(s) named below as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A or equivalent):

Name	Registration Number	Name	Registration Number

Please recognize or change the correspondence address for the application identified in the attached transmittal letter to:

☒ The address associated with the above-mentioned Customer Number.

OR

☐ The address associated with Customer Number:

OR

☐ Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the Applicant:

☐ Inventor or Joint Inventor

☐ Legal Representative of a Deceased or Legally Incapacitated Inventor

☒ Assignee or Person to Whom the Inventor is Under an Obligation to Assign

☐ Person Who Otherwise Shows Sufficient Proprietary Interest (*e.g.*, a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document)

SIGNATURE of Applicant for Patent

Signature		Date	02/20/14
Name	John J. Gibbi	Telephone	
Title and Company	Chief Executive Officer Proxense, LLC		

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms for more than one signature, see below *.

☒ *Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	21344445
Application Number:	14521982
International Application Number:	
Confirmation Number:	8239
Title of Invention:	Biometric Personal Data Key (PDK) Authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Paige McDede Alsbury
Filer Authorized By:	
Attorney Docket Number:	10001-04540 US
Receipt Date:	29-JAN-2015
Filing Date:	23-OCT-2014
Time Stamp:	14:35:30
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Power of Attorney	04540US_20150129_POA_Transmittal.pdf	162114 375339c90d320dad76e348a2e2e21de098c6394b	no	2
Warnings:					
Information:					

2	Power of Attorney	04540US_20150129_POA.pdf	2293497 4f7c72ed2550548de95fc950d085d0a6243dbe8a	no	2

Warnings:	
Information:	
Total Files Size (in bytes):	2455611

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82A (07-13)
Approved for use through 11/30/2014. OMB 0651-0051
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	14/521,982
Filing Date	October 23, 2014
First Named Inventor	John J. Giobbi
Title	Biometric Personal Data Key (PDK) Authentication
Art Unit	2437
Examiner Name	Not Yet Known
Attorney Docket Number	10001-04540 US

SIGNATURE of Applicant or Patent Practitioner

Signature	/Paige Alsbury/	Date (Optional)	January 29, 2015
Name	Paige M. Alsbury	Registration Number	72,965
Title (if Applicant is a juristic entity)	Agent for Applicant		
Applicant Name (if Applicant is a juristic entity)	Proxense, LLC		

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.

☑ *Total of One (1) forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

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 NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
14/521,982	10/23/2014	2431	800	10001-04540 US	20	3

CONFIRMATION NO. 8239

UPDATED FILING RECEIPT

89194
Patent Law Works/Proxense
Greg Sueoka
201 South Main Street, Suite 250
Salt Lake City, UT 84111

OC000000072630197

Date Mailed: 01/05/2015

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

John J. Giobbi, Bend, OR;

Applicant(s)

Proxense, LLC, Bend, OR

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CON of 13/710,109 12/10/2012 PAT 8886954
which is a CON of 11/314,199 12/20/2005 PAT 8352730
which claims benefit of 60/652,765 02/14/2005
and claims benefit of 60/637,538 12/20/2004

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

If Required, Foreign Filing License Granted: 10/31/2014

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/521,982**

Projected Publication Date: Request for Non-Publication Acknowledged

Non-Publication Request: Yes

Early Publication Request: No
**** SMALL ENTITY ****

Title

Biometric Personal Data Key (PDK) Authentication

Preliminary Class

713

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

APPLICANT:	John J. Giobbi
APPLICATION NO:	14/521,982
FILING DATE:	October 23, 2014
TITLE:	Biometric Personal Data Key (PDK) Authentication
EXAMINER:	Not Yet Known
GROUP ART UNIT:	2431
ATTY. DKT. NO:	10001-04540 US
CONFIRMATION NO:	8239

CERTIFICATE OF EFS-WEB TRANSMISSION

Pursuant to 240 OG 45 and the Legal Framework For EFS-Web, I hereby certify that this follow-on correspondence is being officially submitted through the USPTO EFS-Web system from the Mountain Time Zone of the United States on the local date shown below:

Dated: December 23, 2014 By: /Paige Alsbury/

Paige M. Alsbury, Reg. No. 72,965

COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

RESPONSE TO NOTICE TO FILE MISSING PARTS OF AN APPLICATION

Sir/Madam:

Responsive to the Notice of Missing Parts dated November 3, 2014, received in the above-identified application,

☒ Enclosed is:

☒ payment in the amount of $800 for the:

☒ $70 basic filing fee;

(continued)

RESPONSE TO NOTICE TO FILE MISSING PARTS OF APPLICATION

☒ $300 search fee;

☒ $360 examination fee; and

☒ $70 late fee surcharge.

☒ Applicant claims small entity status under 37 C.F.R. § 1.27.

Respectfully submitted,
JOHN J. GIOBBI

Dated: December 23, 2014 By: /Paige Alsbury/

Paige M. Alsbury, Reg. No. 72965
Attorney for Applicant
PATENT LAW WORKS LLP
201 South Main Street, Suite 250
Salt Lake City, UT 84111
Tel.: (801) 258-9837
Fax: (801) 355-0160
Email: palsbury@patentlawworks.net

Electronic Patent Application Fee Transmittal

Application Number:	14521982
Filing Date:	23-Oct-2014
Title of Invention:	Biometric Personal Data Key (PDK) Authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Filer:	Paige McDede Alsbury/Esther Kim
Attorney Docket Number:	10001-04540 US

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility filing Fee (Electronic filing)	4011	1	70	70
Utility Search Fee	2111	1	300	300
Utility Examination Fee	2311	1	360	360
Pages:				
Claims:				
Miscellaneous-Filing:				
Late Filing Fee for Oath or Declaration	2051	1	70	70
Petition:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**800**

Electronic Acknowledgement Receipt	
EFS ID:	21057231
Application Number:	14521982
International Application Number:	
Confirmation Number:	8239
Title of Invention:	Biometric Personal Data Key (PDK) Authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Paige McDede Alsbury
Filer Authorized By:	
Attorney Docket Number:	10001-04540 US
Receipt Date:	23-DEC-2014
Filing Date:	23-OCT-2014
Time Stamp:	18:55:08
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$800
RAM confirmation Number	19396
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Applicant Response to Pre-Exam Formalities Notice	04540US_ResponseToMissingParts.pdf	60014 8633c37ee47dcb615dbbc1a3979218e1e2186813	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	37036 ac4d81ad91e577171018c00d14360338d7bf2590	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	97050		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

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 NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/521,982	10/23/2014	John J. Giobbi	10001-04540 US

CONFIRMATION NO. 8239

89194
Patent Law Works/Proxense
Greg Sueoka
201 South Main Street, Suite 250
Salt Lake City, UT 84111

FORMALITIES LETTER

OC000000072479254

Date Mailed: 12/22/2014

NOTICE OF INCOMPLETE REPLY (NONPROVISIONAL)

Filing Date Granted

The U.S. Patent and Trademark Office has received your reply on to the Notice to File Missing Parts (Notice) mailed 11/03/2014 and it has been entered into the nonprovisional application. The reply, however, does not include the following items required in the Notice. A complete reply must be timely filed to prevent ABANDONMENT of the above-identified application. Replies should be mailed to: Mail Stop Missing Parts, Commissioner for Patents, P.O. Box 1450, Alexandria VA 22313-1450.

Applicant is given **TWO MONTHS** from the date of the Notice to File Missing Parts (Notice) mailed 11/03/2014 within which to file all required items and pay any fees required below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The statutory basic filing fee is missing.
- The application search fee was not received.
- The application examination fee was not received.
- Surcharge as set forth in 37 CFR 1.16(f) was not received.
  The surcharge is due for any one of:
  - late submission of the basic filing fee, search fee, or examination fee,
  - late submission of inventor's oath or declaration,
  - filing an application that does not contain at least one claim on filing, or
  - submission of an application filed by reference to a previously filed application.

SUMMARY OF FEES DUE:

The fee(s) required within **TWO MONTHS** from the date of the Notice to avoid abandonment is/are itemized below. Small entity discount is in effect. If applicant is qualified for micro entity status, an acceptable Certification of Micro Entity Status must be submitted to establish micro entity status. (See 37 CFR 1.29 and forms PTO/SB/15A and 15B.)

- $ **70** basic filing fee.
- $ **70** surcharge.
- $ **300** search fee.
- $ **360** examination fee.
- $(**0**) previous unapplied payment amount.
- $ **800** TOTAL FEE BALANCE DUE.

Replies must be received in the USPTO within the set time period or must include a proper Certificate of Mailing or Transmission under 37 CFR 1.8 with a mailing or transmission date within the set time period. For more information and a suggested format, see Form PTO/SB/92 and MPEP 512.

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web, including a copy of this Notice and selecting the document description "Applicant response to Pre-Exam Formalities Notice". https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html

For more information about EFS-Web please call the USPTO Electronic Business Center at **1-866-217-9197** or visit our website at http://www.uspto.gov/ebc.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

/ltaba/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 14/521,982

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	70		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	300		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	360		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	20 minus 20 =	*	x 40 =	0.00	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*	x 210 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	730		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)	OR	RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

APPLICANT:	John J. Giobbi
APPLICATION NO:	14/521,982
FILING DATE:	October 23, 2014
TITLE:	Biometric Personal Data Key (PDK) Authentication
EXAMINER:	Not Yet Known
GROUP ART UNIT:	2431
ATTY. DKT. NO:	10001-04540 US
CONFIRMATION NO:	8239

CERTIFICATE OF EFS-WEB TRANSMISSION

Pursuant to 240 OG 45 and the Legal Framework For EFS-Web, I hereby certify that this follow-on correspondence is being officially submitted through the USPTO EFS-Web system from the Mountain Time Zone of the United States on the local date shown below:

Dated: December 12, 2014 By: /Matthew M. Holmes/

Matthew M. Holmes, Reg. No. 65,160

COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

PRELIMINARY AMENDMENT

Prior to examination of the above-identified patent application, please enter the following amendment and consider the following remarks.

IN THE CLAIMS

All pending claims are reproduced below.

1. (Canceled)

2. (New) A method comprising:

persistently storing biometric data of a legitimate user and an ID code on the integrated device;

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

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

responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for authentication by an agent that is a third-party trusted authority; and

responsive to receiving an access message from the agent indicating that the agent successfully authenticated the user as the legitimate user based on the ID code, allowing the user to perform an action.

3. (New) The method of claim 1, further comprising:

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

4. (New) The method of claim 1, wherein an indication that the biometric verification was successful is sent with the ID code.

5. (New) The method of claim 1, wherein the biometric data includes data from one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;

6. (New) The method of claim 1, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.

7. (New) The method of claim 1, wherein the action includes accessing an application.

8. (New) The method of claim 1, wherein the action includes completing a transaction.

9. (New) The method of claim 1, wherein the action includes accessing one or more of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file and a financial account.

10. (New) The method of claim 1, further comprising:

responsive to determining the action does not require biometric verification, receiving a request for the ID code without a request for biometric verification; and

responsive to receiving the request for the ID code without a request for biometric verification, sending the ID code for authentication without requesting the scan data.

11. (New) An integrated device comprising:

a persistent storage media that stores biometric data of a user and an ID code;

a validation module, coupled to communicate with the persistent storage media, that receives scan data from a biometric scan for comparison against the biometric data, and that sends the ID code for authentication by a third party that operates a trusted authority; and

a radio frequency communication module that receives an access message from the trusted authority indicating that the trusted authority successfully authenticated the ID code sent to the third party and allowing the user to perform an action.

12. (New) The integrated device of claim 11, wherein the ID code is transmitted to the trusted authority over a network.

13. (New) The integrated device of claim 11, wherein an age verification is registered in association with the device ID code.

14. (New) The integrated device of claim 11, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.

15. (New) A system, comprising:

an integrated hardware device that stores biometric data of a legitimate user and an ID code in the integrated hardware device, and that wirelessly sends the device ID code; and

an authentication circuit that receives the one or more codes and other data values and sends the one or more codes and other data values to a third party that operates a trusted authority for authentication, and that receives an access message from the trusted authority indicating that the trusted authority successfully authenticated the ID code and allows the user to perform an action; and

the trusted authority operated by a third party, the trusted authority storing a list of legitimate codes and determining the authentication of a user based on a comparison of the device ID received and the list.

16. (New) The system of claim 15, wherein the integrated hardware device receives an authentication request from the authentication circuit, and in response, requests a biometric scan from a user to generate scan data and, when the integrated hardware device cannot verify scan data as being from the legitimate user, the integrated hardware device does not send the ID code.

17. (New) The system of claim 15, wherein the integrated hardware device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.

18. (New) The system of claim 15, wherein the biometric data includes data based on one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;

19. (New) The system of claim 15, wherein the action includes accessing one or more of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file and a financial account.

20. (New) The system of claim 15, wherein the action includes completing a financial transaction.

21. (New) The system of claim 15, wherein the action includes accessing an application.

REMARKS

Allowance of all claims is requested. If the Examiner believes that direct contact with Applicant's attorney will advance the prosecution of this case, the Examiner is encouraged to contact the undersigned as indicated below.

Respectfully submitted,
JOHN J. GIOBBI

Dated: December 12, 2014 By: /Matthew M. Holmes/

Matthew M. Holmes, Reg. No. 65,160
Attorney for Applicant
PATENT LAW WORKS LLP
201 South Main Street, Suite 250
Salt Lake City, UT 84111
Tel.: (385) 232-7853
Fax: (801) 355-0160
Email: mholmes@patentlawworks.net

MMH:jam

Electronic Acknowledgement Receipt

EFS ID:	20946020
Application Number:	14521982
International Application Number:	
Confirmation Number:	8239
Title of Invention:	Biometric Personal Data Key (PDK) Authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Matthew M. Holmes
Filer Authorized By:	
Attorney Docket Number:	10001-04540 US
Receipt Date:	12-DEC-2014
Filing Date:	23-OCT-2014
Time Stamp:	16:10:53
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		04540US_PreliminaryAmendment.pdf	74644 7b4874bad12e698fb2f30b744749091de014f3b0	yes	6

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Preliminary Amendment	1	1
	Claims	2	6
Warnings:			
Information:			
	Total Files Size (in bytes):	74644	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/521,982	Filing Date 10/23/2014	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)		
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

		(Column 1)		(Column 2)	(Column 3)		
	12/12/2014	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
AMENDMENT	Total (37 CFR 1.16(i))	* 17	Minus	** 20	= 0	X $40 =	0
	Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $210 =	0
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	0

		(Column 1)		(Column 2)	(Column 3)		
		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
AMENDMENT	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LDRC
/ADRIANE WINSTON/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

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 NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
14/521,982	10/23/2014	2431	0.00	10001-04540 US	1	1

CONFIRMATION NO. 8239

CORRECTED FILING RECEIPT

89194
Patent Law Works/Proxense
Greg Sueoka
201 South Main Street, Suite 250
Salt Lake City, UT 84111

OC000000072075728

Date Mailed: 12/01/2014

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

John J. Giobbi, Bend, OR;

Applicant(s)

Proxense, LLC, Bend, OR

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CON of 13/710,109 12/10/2012 PAT 8886954
which is a CON of 11/314,199 12/20/2005 PAT 8352730
which claims benefit of 60/652,765 02/14/2005
and claims benefit of 60/637,538 12/20/2004

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

If Required, Foreign Filing License Granted: 10/31/2014

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/521,982**

Projected Publication Date: Request for Non-Publication Acknowledged

Non-Publication Request: Yes

Early Publication Request: No

** **SMALL ENTITY** **

Title

Biometric Personal Data Key (PDK) Authentication

Preliminary Class

713

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

APPLICANT:	John J. Giobbi
APPLICATION NO:	14/521,982
FILING DATE:	October 23, 2014
TITLE:	Biometric Personal Data Key (PDK) Authentication
EXAMINER:	Not Yet Known
GROUP ART UNIT:	2431
ATTY. DKT. NO:	10001-04540 US
CONFIRMATION NO:	8239

CERTIFICATE OF EFS-WEB TRANSMISSION

Pursuant to 240 OG 45 and the Legal Framework For EFS-Web, I hereby certify that this follow-on correspondence is being officially submitted through the USPTO EFS-Web system from the Mountain Time Zone of the United States on the local date shown below:

Dated: November 25, 2014 By: /Paige Alsbury/

Paige M. Alsbury, Reg. No. 72,965

COMMISSIONER FOR PATENTS
OFFICE OF INITIAL PATENT EXAMINATION
CUSTOMER SERVICE CENTER
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

REQUEST FOR CORRECTED FILING RECEIPT

Sir/Madam:

Enclosed is a copy of the Official Filing Receipt. It contains the following errors:

1. The Domestic Priority data as claimed by applicant is missing a priority claim.

This application is a CON of 13/710,109, filed on December 10, 2012, which is a CON of 11/314,199, filed on December 20, 2005, which claims benefit of 60/652,765, filed on February 14, 2006 and claims the benefit of 60/637,538, filed on December 20, 2004. The Official Filing

Receipt is currently missing the last priority claim of 60/652,765. This priority claim was listed in the Application Data Sheet as-filed, however the prior Application Number was inadvertently omitted.

Attached is a Marked-Up Application Data Sheet indicating the required changes as well as the first page of the specification as-filed, which properly indicates the priority claim in question.

Please issue a corrected Filing Receipt rectifying this error.

Respectfully submitted,
JOHN J. GIOBBI

Dated: November 25, 2014 By: /Paige Alsbury/

Paige M. Alsbury, Reg. No. 72965
Attorney for Applicant
PATENT LAW WORKS LLP
201 South Main Street, Suite 250
Salt Lake City, UT 84111
Tel.: (801) 258-9837
Fax: (801) 355-0160
Email: palsbury@patentlawworks.net

MARKED UP APPLICATION DATA SHEET

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	10001-04540 US
	Application Number	
Title of Invention	Biometric Personal Data Key (PDK) Authentication	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	John	J.	Giobbi	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Bend	State/Province	OR	Country of Residence	US

Mailing Address of Inventor:

Address 1	689 NW Stonepine Drive		
Address 2			
City	Bend	State/Province	OR
Postal Code	97701	Country	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	89194		
Email Address	docketing@patentlawworks.net	Add Email	Remove Email

Application Information:

Title of the Invention	Biometric Personal Data Key (PDK) Authentication		
Attorney Docket Number	10001-04540 US	Small Entity Status Claimed	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)		Suggested Figure for Publication (if any)	

Filing By Reference :

MARKED UP APPLICATION DATA SHEET

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	10001-04540 US
	Application Number	
Title of Invention	Biometric Personal Data Key (PDK) Authentication	

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☒ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	89194		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the application number blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation of	13710109	2012-12-10
Prior Application Status	Patented		Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13710109	Continuation of	11314199	2005-12-20	8352730	2013-01-08

Prior Application Status	Expired	Remove

MARKED UP APPLICATION DATA SHEET

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	10001-04540 US
	Application Number	
Title of Invention	Biometric Personal Data Key (PDK) Authentication	

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
11314199	Claims benefit of provisional	60652765	2005-02-14
Prior Application Status	Expired	Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
* 11314199	Claims benefit of provisional	60637538	2004-12-20

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button.

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(d). When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)[i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(h)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Remove

Application Number	Country[i]	Filing Date (YYYY-MM-DD)	Access Code[i] (if applicable)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button.

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Authorization to Permit Access:

☐ Authorization to Permit Access to the Instant Application by the Participating Offices

MARKED UP APPLICATION DATA SHEET

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	10001-04540 US
	Application Number	
Title of Invention	Biometric Personal Data Key (PDK) Authentication	

If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date o f filing this Authorization.

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

○ Assignee	○ Legal Representative under 35 U.S.C. 117	○ Joint Inventor
○ Person to whom the inventor is obligated to assign.	○ Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor :

If the Applicant is an Organization check here. ☒

Organization Name	Proxense, LLC		
Mailing Address Information For Applicant:			
Address 1	689 NW Stonepine Drive		
Address 2			
City	Bend	**State/Province**	OR
Country	US	Postal Code	97701
Phone Number		Fax Number	

MARKED UP APPLICATION DATA SHEET

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	10001-04540 US
	Application Number	
Title of Invention	Biometric Personal Data Key (PDK) Authentication	

Email Address	

Additional Applicant Data may be generated within this form by selecting the Add button.

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not subsitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication . An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

If the Assignee or Non-Applicant Assignee is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1			
Address 2			
City		**State/Province**	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button.

Signature:

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Signature	/Paige Alsbury/			Date (YYYY-MM-DD)	2014-11-25
First Name	Paige	Last Name	Alsbury	Registration Number	72965

Additional Signature may be generated within this form by selecting the Add button.

MARKED UP APPLICATION DATA SHEET

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	10001-04540 US
	Application Number	
Title of Invention	Biometric Personal Data Key (PDK) Authentication	

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent C o o p eration Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	20803702
Application Number:	14521982
International Application Number:	
Confirmation Number:	8239
Title of Invention:	Biometric Personal Data Key (PDK) Authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Paige McDede Alsbury
Filer Authorized By:	
Attorney Docket Number:	10001-04540 US
Receipt Date:	25-NOV-2014
Filing Date:	23-OCT-2014
Time Stamp:	20:01:11
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Corrected Filing Receipt	04540US_RequestForCorrected.pdf	57472 0d8ebe438d500df348a30ed1991fab52b2f3dbf4	no	2

Warnings:	
Information:	

2	Application Data Sheet	04540US_MarkedUpADS.pdf	87446 1d1473e4f014063c31681e560d97bf915ea5f19c	no	7

Warnings:	
Information:	
This is not an USPTO supplied ADS fillable form	
Total Files Size (in bytes):	144918

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

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 NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
14/521,982	10/23/2014	2431	0.00	10001-04540 US	1	1

CONFIRMATION NO. 8239

89194
Patent Law Works/Proxense
Greg Sueoka
201 South Main Street, Suite 250
Salt Lake City, UT 84111

FILING RECEIPT

OC000000071643421

Date Mailed: 11/03/2014

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

John J. Giobbi, Bend, OR;

Applicant(s)

Proxense, LLC, Bend, OR

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CON of 13/710,109 12/10/2012 PAT 8886954
which is a CON of 11/314,199 12/20/2005 PAT 8352730
which claims benefit of 60/652,765 02/14/2005

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

If Required, Foreign Filing License Granted: 10/31/2014

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/521,982**

Projected Publication Date: Request for Non-Publication Acknowledged

Non-Publication Request: Yes

Early Publication Request: No
** **SMALL ENTITY** **

Title

Biometric Personal Data Key (PDK) Authentication

Preliminary Class

713

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 14/521,982

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	70		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	300		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	360		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	1 minus 20 =	*	x 40 =	0.00	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	1 minus 3 =	*	x 210 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	730		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)	OR	RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

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 NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/521,982	10/23/2014	John J. Giobbi	10001-04540 US

CONFIRMATION NO. 8239

89194
Patent Law Works/Proxense
Greg Sueoka
201 South Main Street, Suite 250
Salt Lake City, UT 84111

FORMALITIES LETTER

OC000000071643422

Date Mailed: 11/03/2014

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The statutory basic filing fee is missing.
- The application search fee must be submitted.
- The application examination fee must be submitted.
- Surcharge as set forth in 37 CFR 1.16(f) must be submitted.
  The surcharge is due for any one of:
  - late submission of the basic filing fee, search fee, or examination fee,
  - late submission of inventor's oath or declaration,
  - filing an application that does not contain at least one claim on filing, or
  - submission of an application filed by reference to a previously filed application.

SUMMARY OF FEES DUE:

The fee(s) required within **TWO MONTHS** from the date of this Notice to avoid abandonment is/are itemized below. Small entity discount is in effect. If applicant is qualified for micro entity status, an acceptable Certification of Micro Entity Status must be submitted to establish micro entity status. (See 37 CFR 1.29 and forms PTO/SB/15A and 15B.)

- $ **70** basic filing fee.
- $ **70** surcharge.
- $ **300** search fee.
- $ **360** examination fee.
- $(**0**) previous unapplied payment amount.
- $ **800** TOTAL FEE BALANCE DUE.

Replies must be received in the USPTO within the set time period or must include a proper Certificate of Mailing or Transmission under 37 CFR 1.8 with a mailing or transmission date within the set time period. For more information and a suggested format, see Form PTO/SB/92 and MPEP 512.

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web, including a copy of this Notice and selecting the document description "Applicant response to Pre-Exam Formalities Notice". https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html

For more information about EFS-Web please call the USPTO Electronic Business Center at **1-866-217-9197** or visit our website at http://www.uspto.gov/ebc.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

/zretta/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

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 NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/521,982	10/23/2014	John J. Giobbi	10001-04540 US

CONFIRMATION NO. 8239

89194
Patent Law Works/Proxense
Greg Sueoka
201 South Main Street, Suite 250
Salt Lake City, UT 84111

IMPROPER CFR REQUEST

OC000000071655436

Date Mailed: 11/03/2014

RESPONSE TO REQUEST FOR CORRECTED FILING RECEIPT

Continuity, Priority Claims, Petitions, and Non-Publication Requests

In response to your request for a corrected Filing Receipt, the Office is unable to comply with your request because:

- One or more of the benefit claims under 35 U.S.C. § 120 cannot be included on the Filing Receipt since applicant did not specify whether the application is a continuation, divisional or continuation-in-part of the prior application. Applicant must submit a new application data sheet (ADS) that sets forth the relationship, and the ADS must be accompanied by a petition under 37 CFR 1.78 if filed after the time period set forth in 37 CFR 1.78.

Improper Benefit Claim(s) to Prior-Filed Provisional Application(s)

The benefit claim(s) to prior-filed provisional application(s) is improper because the instant application was not filed within twelve (12) months from the filing date of the provisional application, and there is no indication of an intermediate nonprovisional or international application designationg the United States that is directly claiming the benefit of the provisional application and filed within 12 months of the filing date of the provisional application. Applicant should review each benefit claim submitted and, if appropriate, provide the proper reference to the prior-filed applications (including an indication of any intermediate application that is directly claiming the benefit of the provisional application and filed with 12 months of the filing date of the provisional application) as required by 37 CFR 1.78.

Alternatively, if the instant application (or intermediate application) was filed within 14 months of the prior provisional application, applicant may file a petition (in the instant application or the intermediate application, as appropriate) to restore the benefit of the provisional application if the delay in filing the instant application (or intermediate application) within the 12 month time period was unintentional. See 37 CFR 1.78 for the requirements of a petition to restore the benefit of the provisional application.

For applications filed on or after September 16, 2012, applicant must submit a corrected application data sheet (ADS) to include a specific reference.

Timeliness: The required reference for each benefit claim must be filed during the pendency of the instant application and within the later of: (1) four months from the actual filing date of the instant application, or the national stage commencement date if the instant application is a national stage application under 35 U.S.C. 371; or (2) sixteen months from the filing date of the prior-filed application. Failure to timely file the required reference is considered a waiver of any benefit claim, unless a grantable petition to accept an unintentionally

delayed claim under 37 CFR 1.78, the petition fee set forth in 37 CFR 1.17(m), and the required reference are filed.

/tnguyen/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	10001-04540 US
	Application Number	
Title of Invention	Biometric Personal Data Key (PDK) Authentication	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	John	J.	Giobbi	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Bend	State/Province	OR	Country of Residence i	US

Mailing Address of Inventor:

Address 1	689 NW Stonepine Drive		
Address 2			
City	Bend	State/Province	OR
Postal Code	97701	Country i	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	89194		
Email Address	docketing@patentlawworks.net	Add Email	Remove Email

Application Information:

Title of the Invention	Biometric Personal Data Key (PDK) Authentication		
Attorney Docket Number	10001-04540 US	Small Entity Status Claimed	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)		Suggested Figure for Publication (if any)	

Filing By Reference :

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	10001-04540 US
	Application Number	
Title of Invention	Biometric Personal Data Key (PDK) Authentication	

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☒ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	89194		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the application number blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation of	13710109	2012-12-10

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13710109	Continuation of	11314199	2005-12-20	8352730	2013-01-08

Prior Application Status	Expired	Remove

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	10001-04540 US
	Application Number	
Title of Invention	Biometric Personal Data Key (PDK) Authentication	

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
11314199	Claims benefit of provisional	60652765	2005-02-14
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Claims benefit of provisional	60637538	2004-12-20

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button. Add

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(d). When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) [i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(h)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Remove

Application Number	Country [i]	Filing Date (YYYY-MM-DD)	Access Code [i] (if applicable)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Authorization to Permit Access:

☐ Authorization to Permit Access to the Instant Application by the Participating Offices

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	10001-04540 US
	Application Number	
Title of Invention	Biometric Personal Data Key (PDK) Authentication	

If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing this Authorization.

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1 Remove

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

◯ Assignee	◯ Legal Representative under 35 U.S.C. 117	◯ Joint Inventor
◯ Person to whom the inventor is obligated to assign.	◯ Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor :

If the Applicant is an Organization check here. ☒

Organization Name	Proxense, LLC

Mailing Address Information:

Address 1	689 NW Stonepine Drive		
Address 2			
City	Bend	**State/Province**	OR
Country [i]	US	Postal Code	97701
Phone Number		Fax Number	

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	10001-04540 US
	Application Number	
Title of Invention	Biometric Personal Data Key (PDK) Authentication	

Email Address	

Additional Applicant Data may be generated within this form by selecting the Add button. Add

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not subsitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication . An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

Remove

If the Assignee or Non-Applicant Assignee is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1			
Address 2			
City		**State/Province**	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. Add

Signature:

Remove

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications

Signature	/Matthew Holmes/			Date (YYYY-MM-DD)	2014-10-23
First Name	Matthew	Last Name	Holmes	Registration Number	65160

Additional Signature may be generated within this form by selecting the Add button. Add

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	10001-04540 US
	Application Number	
Title of Invention	Biometric Personal Data Key (PDK) Authentication	

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION

INVENTOR: JOHN J. GIOBBI

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] The present application claims priority, under 35 U.S.C. § 120, to U.S. Patent Application No. 13/710,109 filed December 10, 2012 and entitled "Biometric Personal Data Key (PDK) Authentication" which claims priority to U.S. Patent Application No. 11/314,199, filed December 20, 2005 and entitled "Biometric Personal Data Key (PDK) Authentication," which claims the benefit of U.S. Provisional Application No. 60/637,538, filed on December 20, 2004, and of U.S. Provisional Application No. 60/652,765, filed on February 14, 2005, the entire contents of which are hereby incorporated by reference.

FIELD OF THE INVENTION

[0002] The present invention relates generally to computerized authentication, and more specifically, to an authentication responsive to biometric verification of a user being authenticated.

BACKGROUND

[0003] Conventional user authentication techniques are designed to prevent access by unauthorized users. One technique is to require a user being authenticated to provide secret credentials, such as a password, before allowing access. Similarly, a PIN number can be required by an ATM machine before allow-

ing a person to perform automated bank transactions. A difficulty with this technique is that it requires the user to memorize or otherwise keep track of the credentials. A uses often has multiple sets of credentials (e.g., passwords and PINs) and it can be quite difficult to keep track of them all.

[0004] Another technique that does not require the user to memorize credentials is to provide the user with an access object such as a key (e.g., an electronic key) that the user can present to obtain access. For example, a user can be provided with a small electronic key fob that allows access to a building or other secured location. A difficulty with using access objects is that authentication merely proves that the access object itself is valid; it does not verify that the legitimate user is using the access object. That is, illegitimate user can use a stolen access object to enter a secured location because the user's identity is never checked.

[0005] Some hybrid authentication techniques require the user to provide both an access object and credentials. The user is authenticated only upon providing both items. Of course, this solution does not resolve the problem of making the user memorize credentials.

[0006] Therefore, there is a need for systems and methods for verifying a user that is being authenticated that does not suffer from the limitations described above. Moreover, the solution should ease authentications by wirelessly providing an identification of the user.

SUMMARY

[0007] The present invention addresses the above needs by providing systems and methods for authentication responsive to biometric verification of a user being authenticated. In one embodiment, an integrated device includes a persistent storage to persistently stores a code such as a device identifier (ID) and biometric data for a user in a tamper-resistant format, and a verification module, in communication with the persistent storage, to receive scan data from a biometric scan for comparison against the biometric data, and if the scan data matches the biometric data, wirelessly sending a code for authentication.

[0008] In one embodiment, a method for verifying a user during authentication of an integrated device, includes persistently storing biometric data for the user in a tamper-resistant format; responsive to receiving a request for biometric verification of the user, receiving scan data from a biometric scan; comparing the scan data to the biometric data to determine whether the data match; and responsive to a determination that the scan data matches the biometric data, wirelessly sending a code for authentication.

[0009] Other embodiments include corresponding systems, apparatus, and computer programming products, configured to perform the actions of the methods, encoded on computer storage devices. These and other embodiments may each optionally include one or more of the following features. For instance the operations further include registering an age verification for the user in association with the code. For instance the operations further include establishing a

secure communication channel prior to sending the code for authentication. For instance the operations further include receiving a request for the code without a request for biometric verification, and responsive to receiving the request for the code without a request for biometric verification, sending the code without requesting the scan data. For instance, the features include: the code is registered with a trusted authority, and the code can be authenticated to a third party by the trusted authority; the code uniquely identifies the integrated device; the code indicates that the biometric verification was successful; persistently storing biometric data includes permanently storing biometric data; the biometric data and the scan data are both based on a fingerprint scan by the user, an LED to be activated for requesting the biometric scan.

[0010] In one embodiment, a method for authenticating a verified user, includes receiving a code associated with a biometrically verified user; requesting authentication of the code; receiving an authentication result; and in response to the authentication result being positive, providing access to an application.

[0011] In one embodiment, a system includes an integrated device (e.g. a biometric key) to store biometric data for a user in a tamper resistant format, and if scan data can be verified as being from the user by comparing the scan data to the biometric data, wirelessly sending a code; and an authentication module to receive the code and send the code to a trusted authority for authentication, and responsive to the code being authenticated, allowing the user to access an application.

[0012] Other embodiments include corresponding systems, apparatus, and computer programming products, configured to perform the actions of the methods, encoded on computer storage devices. These and other embodiments may each optionally include one or more of the following features. For instance, the operations further include registering the code with a trusted authority, wherein requesting authentication of the code includes providing the code to the trusted authority and wherein receiving an authentication result comprises receiving the authentication result from the trusted authority. For instance the operations further include registering a date of birth or age with the trusted authority. For instance the operations further include establishing a secure communications channel with an integrated device, wherein the code associated with the biometrically verified user is received from the integrated device. For instance the features include: the integrated device receives an authentication request from the authentication module, and in response, requests a biometric scan from the user to generate the scan data; when the integrated device cannot verify the scan data as being from the user, it does not send the code.

[0013] Advantageously, user authentication is bolstered with highly reliable biometric verification of the user in an integrated device. Furthermore, a keyless environment relieves authorized users from having to memorize credentials, and of having to physically enter credentials or keys. In addition, the integrated device can be authenticated for an application that is open to the public (i.e., in an open loop system).

[0014] The features and advantages described in the specification are not all inclusive and, in particular, many additional features and advantages will be apparent to one of ordinary skill in the art in view of the drawings, specifications, and claims. Moreover, it should be noted that the language used in the specification has been principally selected for readability and instructional purposes and may not have been selected to delineate or circumscribe the inventive matter.

BRIEF DESCRIPTION OF THE DRAWINGS

[0015] The teachings of the present invention can be readily understood by considering the following detailed description in conjunction with the accompanying drawings.

[0016] FIG. 1 is a schematic diagram illustrating a biometric key for providing authentication information for a biometrically verified user according to one embodiment of the present invention.

[0017] FIG. 2 is a block diagram illustrating functional modules within the biometric key according to one embodiment of the present invention.

[0018] FIG. 3 is a block diagram illustrating a system for providing authentication information for a biometrically verified user.

[0019] FIG. 4 is a flow chart illustrating a method for providing authentication information for a biometrically verified user.

[0020] FIG. 5 is a flow chart illustrating a method for enrolling biometric data of the user with the biometric key.

[0021] FIG. 6 is a flow chart illustrating a method for verifying a subject presenting the biometric key according to one embodiment of the present invention.

[0022] FIG. 7 is a flow chart illustrating a method for authenticating a verified user of the biometric key according to one embodiment of the present invention.

DETAILED DESCRIPTION

[0023] Systems and methods for authentication responsive to biometric verification of a user being authenticated are described. Generally, biometric verification uses biometric data to ensure that the user of, for example, a biometric key, is the person registered as an owner. Biometric data is a digital or analog representation of characteristics unique to the user's body. For example, a fingerprint of a subject can be compared against previously-recorded biometric data for verification that the subject is the registered owner of the biometric key. Then, the biometric key itself can be authenticated.

[0024] Although the embodiments below are described using the example of biometric verification using a fingerprint, other embodiments within the spirit of the present invention can perform biometric verification using other types of biometric data. For example, the biometric data can include a palm print, a retinal scan, an iris scan, hand geometry recognition, facial recognition, signature recognition, or voice recognition.

[0025] FIG. 1 is a schematic diagram illustrating an example of a biometric key 100 for providing authentication information for a biometrically verified user according to one embodiment of the present invention. In one embodiment, the biometric key 100 comprises a frame 110, a scan pad 120, and an LED 130. In one embodiment, biometric key 100 has a small form factor (e.g., the size of an automobile remote control) such that it can be unobtrusively carried by a user. In one embodiment, the biometric key 100 is integrated into another object or device. A

device having an integrated biometric key 100 is occasionally referred to herein as an "integrated device." For example, in one embodiment, the biometric key 100 is integrated into a mobile phone (e.g. a cellular phone or smartphone), tablet, laptop, mp3 player, mobile gaming device, watch, key fob or other mobile device, thereby making the biometric key 100 unobtrusive to carry.

[0026] Frame 110 can be formed by plastic, metal or another suitable material. Frame 110 is shaped to secure scan pad 120, and includes a perforation for attachment to, for example a key chain or clip. In one embodiment, frame 110 is formed from a unitary molding to protect biometric data. Accordingly, frame 110 cannot be opened to expose the underlying components unless it is broken.

[0027] Scan pad 120 can be, for example, an optical scanner using a charge coupled device, or a capacitive scanner. Scan pad 120 can be sized to fit a thumb or other finger. Biometric key 100 of the present embodiment includes LED 130 that lights up to request a fingerprint scan from a user. In one embodiment, LED 130 can also confirm that user verification and/or authentication has completed.

[0028] Biometric key 100 can authenticate a user for various purposes. For example, biometric key 100 can allow keyless entry into homes and autos. In another example, biometric key 100 can log a user onto a computer system or point of sale register without typing in credentials. In still another example, biometric key 100 can verify that an enrolled user is above a certain age (e.g., before allowing access to a slot machine in a casino). In some embodiments, biometric key

100 operates without biometric verification, and request a fingerprint scan from a user only when biometric verification is needed for the particular use.

[0029] FIG. 2 is a block diagram illustrating biometric key 100 according to one embodiment of the present invention. Biometric key 100 comprises control module 210, biometric portion 220, RF communication module 230, persistent storage 240, and battery 250. Biometric key 100 can be formed from a combination of hardware and software components as described above. In one embodiment, biometric key 100 comprises a modified key fob.

[0030] Control module 210 coordinates between several functions of biometric key 100. In one embodiment, control module 210 provides a verification code upon successful verification of the user. More specifically, once biometric portion 220 indicates that a fingerprint scan matches biometric data that was collected during enrollment, control module 210 can trigger RF communication module 230 for sending a code indicating that the user was verified. In another embodiment, control module 210 can work in the opposite direction by detecting a request for verification from RF communication module 230, and then requesting verification of the user from biometric portion 210. Note that control module 210 of FIG. 2 is merely a grouping of control functions in a central architecture, and in other embodiments, the control functions can be distributed between several modules around biometric key 100.

[0031] Biometric portion 220 comprises enrollment module 222, validation module 224, and biometric data base 226. In one embodiment, enrollment mod-

ule 222 registers a user with biometric key 100 by persistently storing biometric data associated with the user. Further, enrollment module 222 registers biometric key 100 with a trusted authority by providing the code (e.g., device ID) to the trusted authority. Or conversely, the trusted authority can provide the code to biometric key 100 to be stored therein.

[0032] 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 214 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.

[0033] 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.

[0034] 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.

[0035] In one embodiment, persistent storage 226 also stores the code that is provided by the key 100 responsive to successful verification of the user. 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.

[0036] Radio frequency (RF) communication module 230 is, for example, a transceiver or other mechanism for wireless communication. RF communication module 230 can send and receive data (e.g., the code) as modulated electromagnetic signals. In one embodiment, RF communication 220 can be optimized for low-power usage by, for example, using short-range transceivers. RF communi-

cation module 230 can actively send out connection requests, or passively detect connection requests.

[0037] Battery 260 can be a conventional power source suitable for the components of biometric key 100. Battery 260 can be either replaceable or rechargeable. Alternatively, battery 260 can be embedded within key 100 such that the key must be discarded or recycled upon expiration of the battery.

[0038] FIG. 3 is a block diagram illustrating a system 300 for providing authentication information for a biometrically verified user. System 300 comprises an authentication module 310 in communication with biometric key 100, a trusted key authority 320, and an application 330.

[0039] Authentication module 310 is coupled in communication with biometric key via line 311 (i.e., a wireless medium such as EM signals), and with trusted key authority 320 via line 312 (e.g., a secure data network such as the Internet, or a cell network). Authentication module 310 can include one or more of, for example, a computerized device, software executing on a computerized device, and/or a reader/decoder circuit. In one embodiment, authentication module 310 servers as a gatekeeper to application 330 by requiring the code indicating successful biometric verification of the user prior to allowing access to the application. Further, in one embodiment, authentication module 310 provides the code to trusted key authority 320 in order to verify that it belongs to a legitimate key (e.g., when application 330 is security-critical). Authentication module

310 can send a message to application 330, or otherwise allow access to the application, responsive to a successful authentication by trusted key authority 320.

[0040] Application 330 is a resource that can be accessed by a verified and authenticated user. Application 330 can be, for example, a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file, a financial account (e.g. a savings account, checking account, brokerage account, credit card account, credit line, etc.) and the like. In one embodiment, a file includes medical information such as a medical record, insurance information or other healthcare information. Application 330 can execute on the same system as authentication module 310 or on another system in communication with the system of the authentication module. In one embodiment, application module 330 allows access by a user after receiving a message from authentication module 310. At that point, application 330 can allow direct use by the user, or require that communications continue to pass through authentication module 310 for continued authentication.

[0041] 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, 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.

[0042] In an open system, where unknown users can attempt authentication (e.g., in a public grocery store), trusted key authority 320 provides verification that a key presenting a certain code is legitimate. By contrast, in a closed system, only known users are legitimate (e.g., owners of a home), the trusted key authority 320 can be maintained locally and serves to verify that the key belongs to one of the limited number of users that can use the system.

[0043] FIG. 4 is a flow chart illustrating a method 400 for authenticating a biometrically verified user using a trusted key authority (e.g., authority 320). A biometric key (e.g., biometric key 100) is registered 410 with the trusted key authority. The code (e.g., device ID) of the key is stored by the trusted key authority. Additionally, a user is enrolled 420 with the biometric key as described below with reference to FIG. 5.

[0044] In various situations, authentication of the key is needed 430 (e.g., by authentication module 310). In one embodiment, authentication can be required prior to allowing access to an application (e.g., application 330). For example, a user can be standing proximate to a slot machine in a casino which requires that a user be over the age of 21. The slot machine can detect the biometric key in the user's pocket, and, in response, spawn a conspicuous pop-up window on the slot machine requesting age verification. Alternatively, the bio-

metric key can blink an LED. In other embodiments, biometric verification is not necessary and only the key itself is authenticated.

[0045] The biometric key establishes communication with the authentication module using various techniques. In one embodiment, the key and authentication module engage in preliminary data exchanges to determine who and/or what they are (e.g., to ascertain that they belong to the same system). These data exchanges can include challenge-response dialogs, hashing algorithms, and the like in order to ensure that the biometric key and authentication module are themselves legitimate. Further, in one embodiment the key and authentication module establish a secure communications channel. The key performs the biometric verification of the user 440 as described below with reference to FIG. 6. If the biometric verification of the user is successful, the key provides its code over the secure communications channel.

[0046] The code is utilized to authenticate the biometric key itself 450, 460 as described below with reference to FIG. 7 and profile information is received. Responsive to successful authentication of the key, access is allowed 470 to the application. In the slot machine example, a new pop-up window can be spawned to indicate a successful age verification.

[0047] FIG. 5 is a flow chart illustrating a method 500 for enrolling biometric data of the user with the biometric key according to one embodiment of the present invention. An agent checks 510 an identification of the user and establishes a profile. The agent can be, for example, a government official, a nota-

ry, and/or an employee of a third party which operates the trusted key authority, or another form of witness. The agent can follow standardized procedures such as requiring identification based on a state issued driver license, or a federally issued passport in order to establish a true identity of the user.

[0048] The profile describes the user and can include, for example, the user's name, date of birth, age, passwords, account numbers, preferences etc. In some embodiments, the profile stores no or only limited information about the user. For example, the agent might store the date of birth of the user in the profile, but not store any other information about the user. In addition, the profile describes the biometric key and/or key authority. For the biometric key, the profile can store a value indicating the status of the key, such as whether the key is in-service, out-of-service, abandoned, lost, stolen etc. For the key authority, the profile can store a value identifying the key authority.

[0049] The agent also collects and persistently stores 520 biometric data from the user. To do so, a fingerprint or eye retina can be scanned and converted to data which is then persistently stored in the biometric key. In one embodiment, the agent does not retain the biometric data. Since this step occurs under control of the agent, the agent can be certain that the biometric data stored within the key matches the user who presented the identification. The agent also obtains the code (e.g., device ID) from the biometric key in which the biometric data was stored. The agent associates the code and the profile using a table and/or other data structure.

[0050] FIG. 6 is a flow chart illustrating a method 600 for verifying a subject presenting the biometric key according to one embodiment of the present invention. In response to an authentication request, a user scan is requested 610 (e.g., by a blinking LED). Once the subject provides a fingerprint, scan data is received 620. Scan data is compared for a match 630 to previously-stored biometric data. If there is no match, then verification fails 650.

[0051] If there is a match, the subject is verified 640 as the user. The code indicating a successful verification is wirelessly sent 650 from the biometric key (e.g., by RF communication module 230).

[0052] 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 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.

[0053] In some embodiments, the biometric key provides multiple codes and/or other data values. For example, the key can provide a device ID code that the authentication module can provide to the trusted key authority in order

to authenticate the key, and the key can provide a secret decryption value that can be used to communicate with the biometric key. As used herein, the term "code" is intended to include one or more of these values, depending upon the specific embodiment.

[0054] The order in which the steps of the methods of the present invention are performed is purely illustrative in nature. The steps can be performed in any order or in parallel, unless otherwise indicated by the present disclosure. The methods of the present invention may be performed in hardware, firmware, software, or any combination thereof operating on a single computer or multiple computers of any type. Software embodying the present invention may comprise computer instructions in any form (e.g., source code, object code, interpreted code, etc.) stored in any computer-readable storage medium (e.g., a ROM, a RAM, a magnetic media, a compact disc, a DVD, etc.). Such software may also be in the form of an electrical data signal embodied in a carrier wave propagating on a conductive medium or in the form of light pulses that propagate through an optical fiber.

[0055] While particular embodiments of the present invention have been shown and described, it will be apparent to those skilled in the art that changes and modifications may be made without departing from this invention in its broader aspect and, therefore, the appended claims are to encompass within their scope all such changes and modifications, as fall within the true spirit of this invention.

[0056] In the above description, for purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the invention. It will be apparent, however, to one skilled in the art that the invention can be practiced without these specific details. In other instances, structures and devices are shown in block diagram form in order to avoid obscuring the invention.

[0057] Reference in the specification to "one embodiment" or "an embodiment" means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment of the invention. The appearances of the phrase "in one embodiment" in various places in the specification are not necessarily all referring to the same embodiment.

[0058] Some portions of the detailed description are presented in terms of algorithms and symbolic representations of operations on data bits within a computer memory. These algorithmic descriptions and representations are the means used by those skilled in the data processing arts to most effectively convey the substance of their work to others skilled in the art. An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. The steps are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated. It has proven convenient at times, prin-

cipally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like.

[0059] It should be borne in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities. Unless specifically stated otherwise as apparent from the discussion, it is appreciated that throughout the description, discussions utilizing terms such as "processing" or "computing" or "calculating" or "determining" or "displaying" or the like, refer to the action and processes of a computer system, or similar electronic computing device, that manipulates and transforms data represented as physical (electronic) quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission or display devices.

[0060] The present invention also relates to an apparatus for performing the operations herein. This apparatus can be specially constructed for the required purposes, or it can comprise a general-purpose computer selectively activated or reconfigured by a computer program stored in the computer. Such a computer program can be stored in a computer readable storage medium, such as, but is not limited to, any type of disk including floppy disks, optical disks, CD-ROMs, and magnetic-optical disks, read-only memories (ROMs), random access memories (RAMs), EPROMs, EEPROMs, magnetic or optical cards, or any

type of media suitable for storing electronic instructions, and each coupled to a computer system bus.

[0061] The algorithms and modules presented herein are not inherently related to any particular computer or other apparatus. Various general-purpose systems can be used with programs in accordance with the teachings herein, or it may prove convenient to construct more specialized apparatuses to perform the method steps. The required structure for a variety of these systems will appear from the description below. In addition, the present invention is not described with reference to any particular programming language. It will be appreciated that a variety of programming languages can be used to implement the teachings of the invention as described herein. Furthermore, as will be apparent to one of ordinary skill in the relevant art, the modules, features, attributes, methodologies, and other aspects of the invention can be implemented as software, hardware, firmware or any combination of the three. Of course, wherever a component of the present invention is implemented as software, the component can be implemented as a standalone program, as part of a larger program, as a plurality of separate programs, as a statically or dynamically linked library, as a kernel loadable module, as a device driver, and/or in every and any other way known now or in the future to those of skill in the art of computer programming. Additionally, the present invention is in no way limited to implementation in any specific operating system or environment.

[0062] It will be understood by those skilled in the relevant art that the above-described implementations are merely exemplary, and many changes can be made without departing from the true spirit and scope of the present invention. Therefore, it is intended by the appended claims to cover all such changes and modifications that come within the true spirit and scope of this invention.

CLAIMS

What is claimed is:

1. A method comprising:

persistently storing biometric data of the user and a plurality of codes and other data values comprising a device ID code uniquely identifying an integrated device and a secret decryption value in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered;

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

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

responsive to a determination that the scan data matches the biometric data, wirelessly sending one or more codes and other values from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority, wherein the one or more codes and other data values includes the device ID code; and

receiving an access message from the agent indicating that the agent successfully authenticated the one or more codes and other data values and allowing the user access to an application.

ABSTRACT

Systems and methods verifying a user during authentication of an integrated device. In one embodiment, the system includes an integrated device and an authentication unit. The integrated device stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format, and when scan data is verified by comparing the scan data to the biometric data, wirelessly sends one or more codes and other data values including the device ID code. The authentication unit receives and sends the one or more codes and the other data values to an agent for authentication, and receives an access message from the agent indicating that the agent successfully authenticated the one or more codes and other data values and allows the user to access an application.

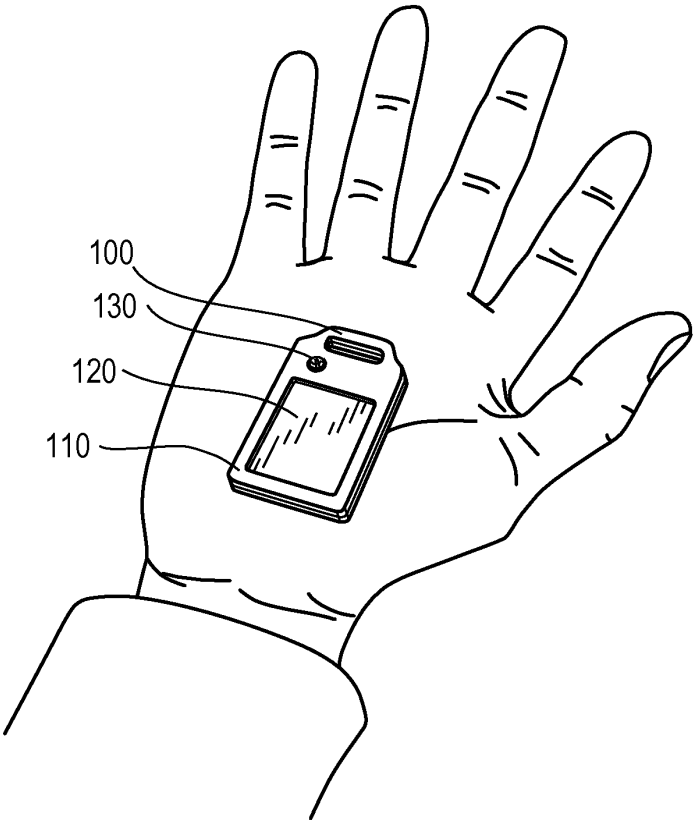

100
130
120
110

FIG. 1

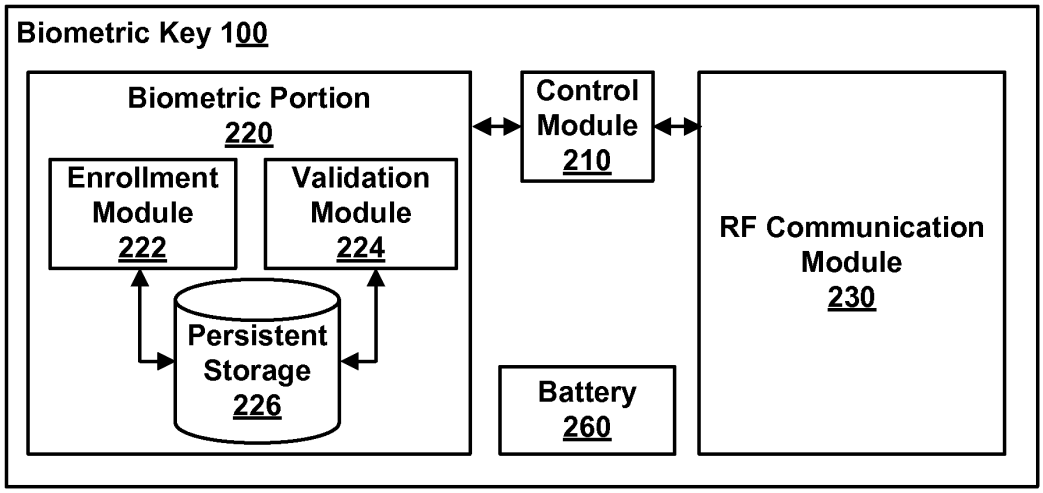

Biometric Key 100
Biometric Portion
220
Enrollment
Module
222
Validation
Module
224
Persistent
Storage
226
Control
Module
210
Battery
260
RF Communication
Module
230

FIG. 2

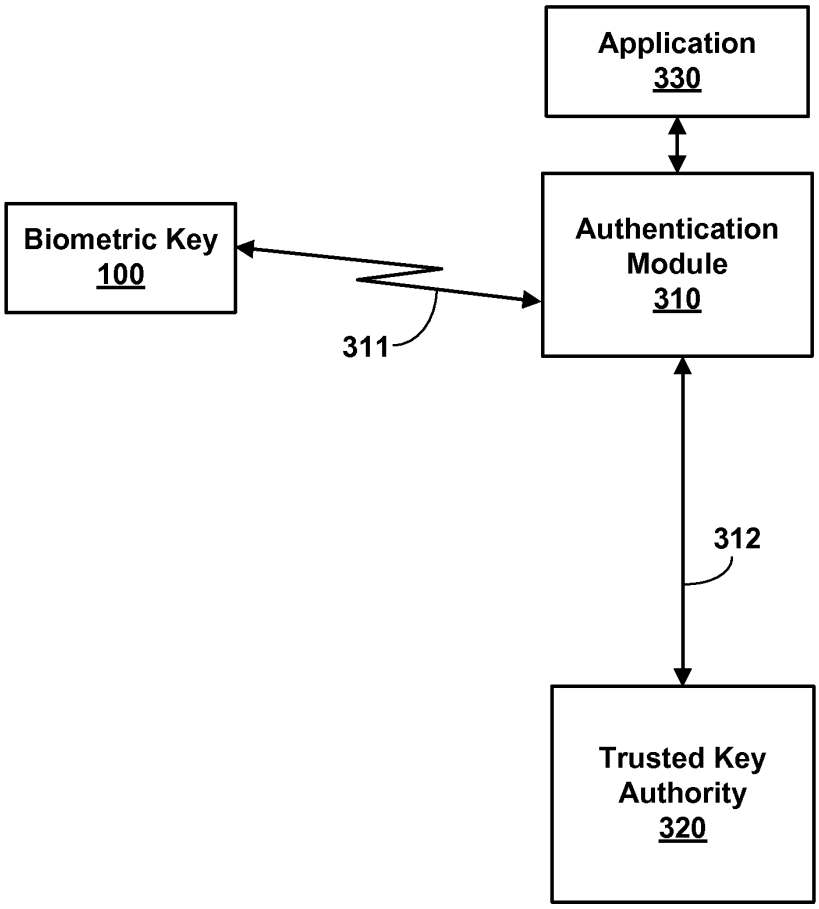

Application
330
Authentication
Module
310
Biometric Key
100
311
312
Trusted Key
Authority
320

FIG. 3

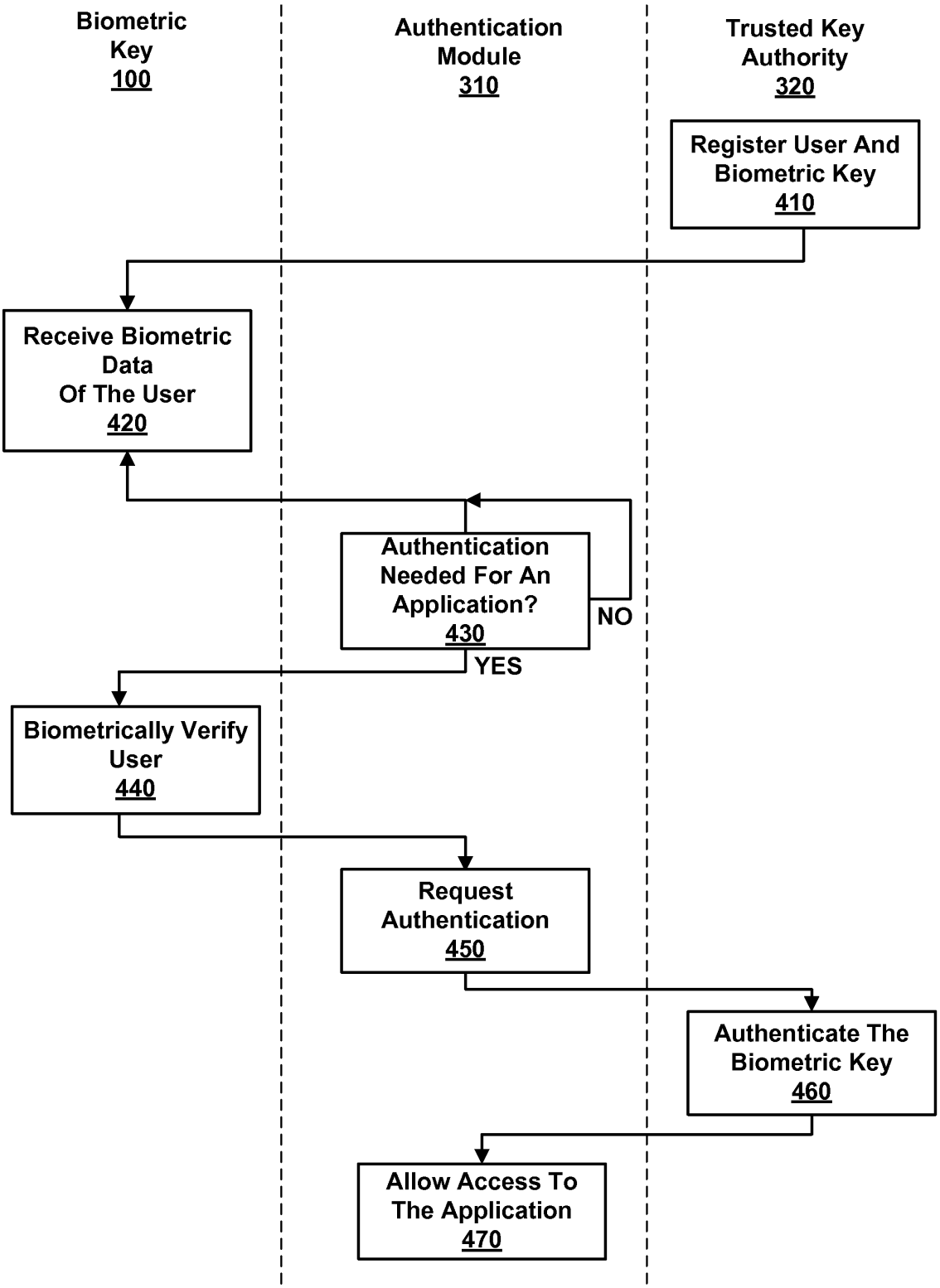

Biometric Key 100
Authentication Module 310
Trusted Key Authority 320
Register User And Biometric Key 410
Receive Biometric Data Of The User 420
Authentication Needed For An Application? 430
NO
YES
Biometrically Verify User 440
Request Authentication 450
Authenticate The Biometric Key 460
Allow Access To The Application 470

FIG. 4

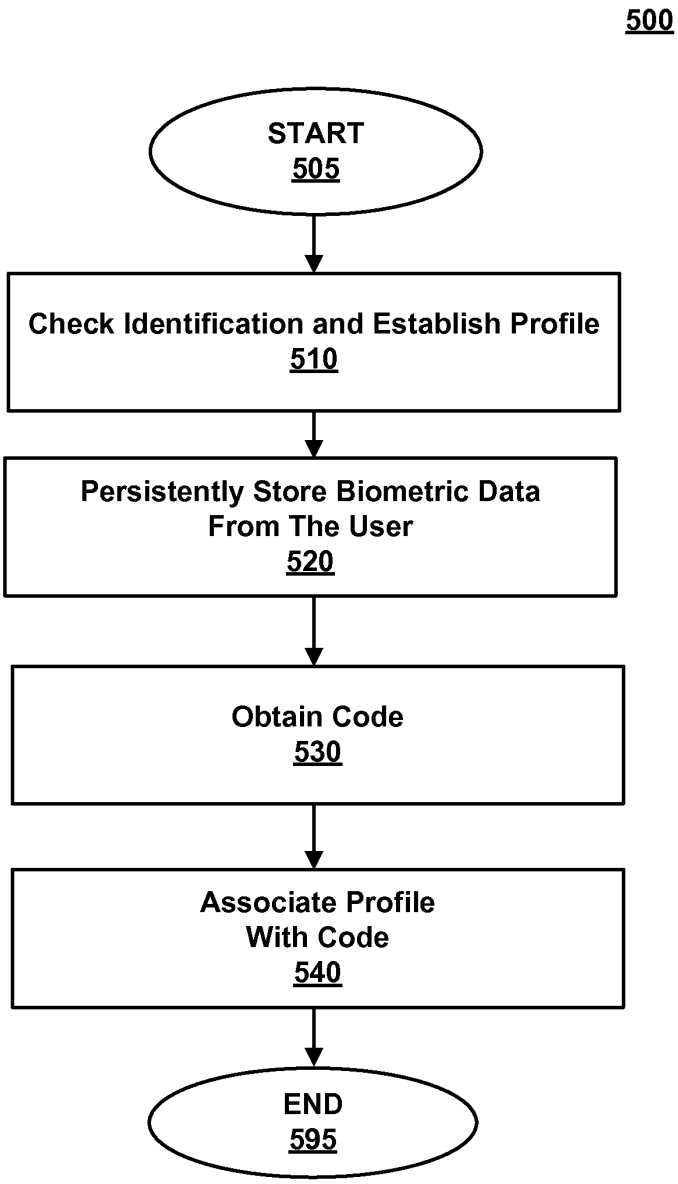

500
START
505
Check Identification and Establish Profile
510
Persistently Store Biometric Data From The User
520
Obtain Code
530
Associate Profile With Code
540
END
595

FIG. 5

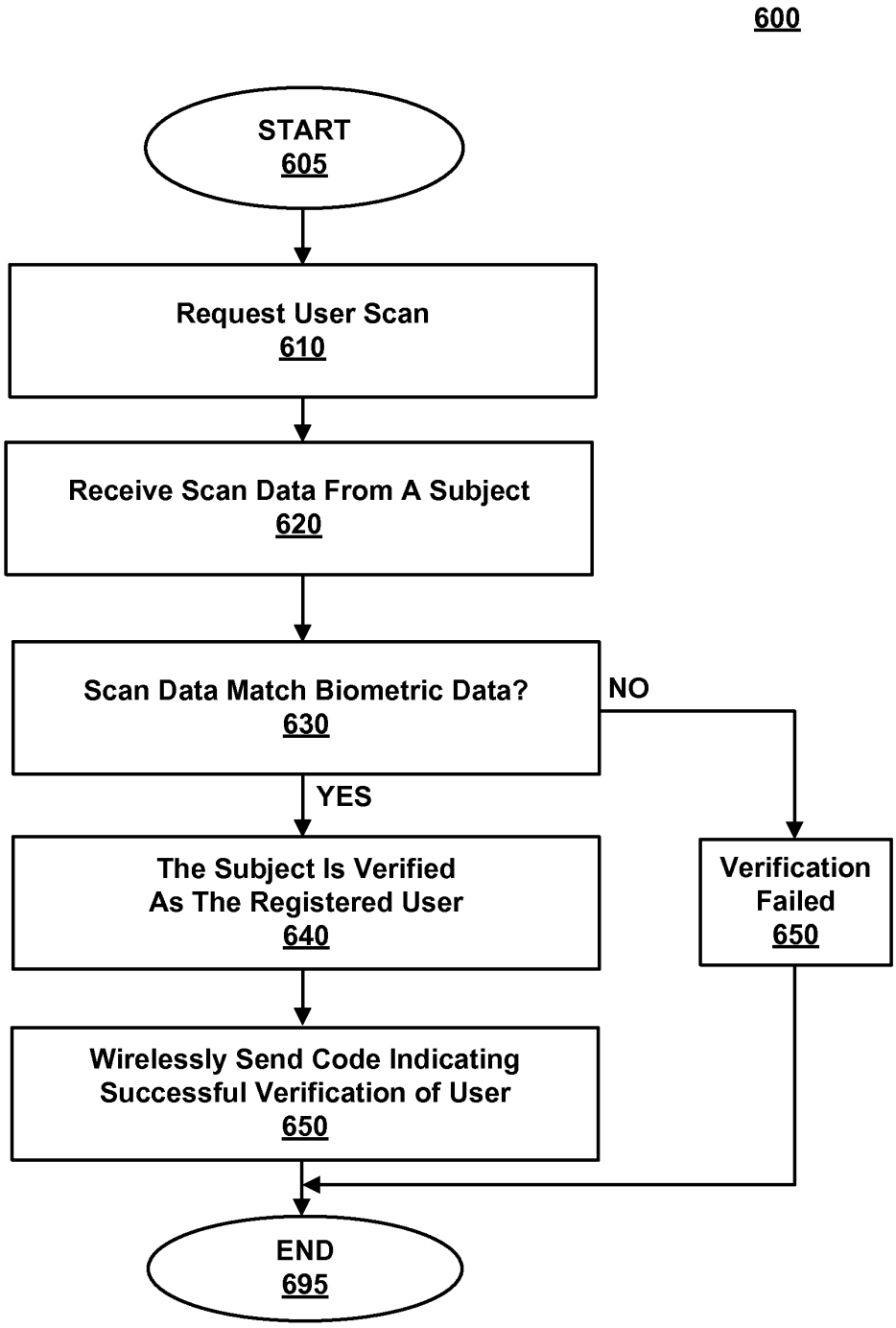

600
START
605
Request User Scan
610
Receive Scan Data From A Subject
620
Scan Data Match Biometric Data?
630
NO
YES
The Subject Is Verified
As The Registered User
640
Verification
Failed
650
Wirelessly Send Code Indicating
Successful Verification of User
650
END
695

FIG. 6

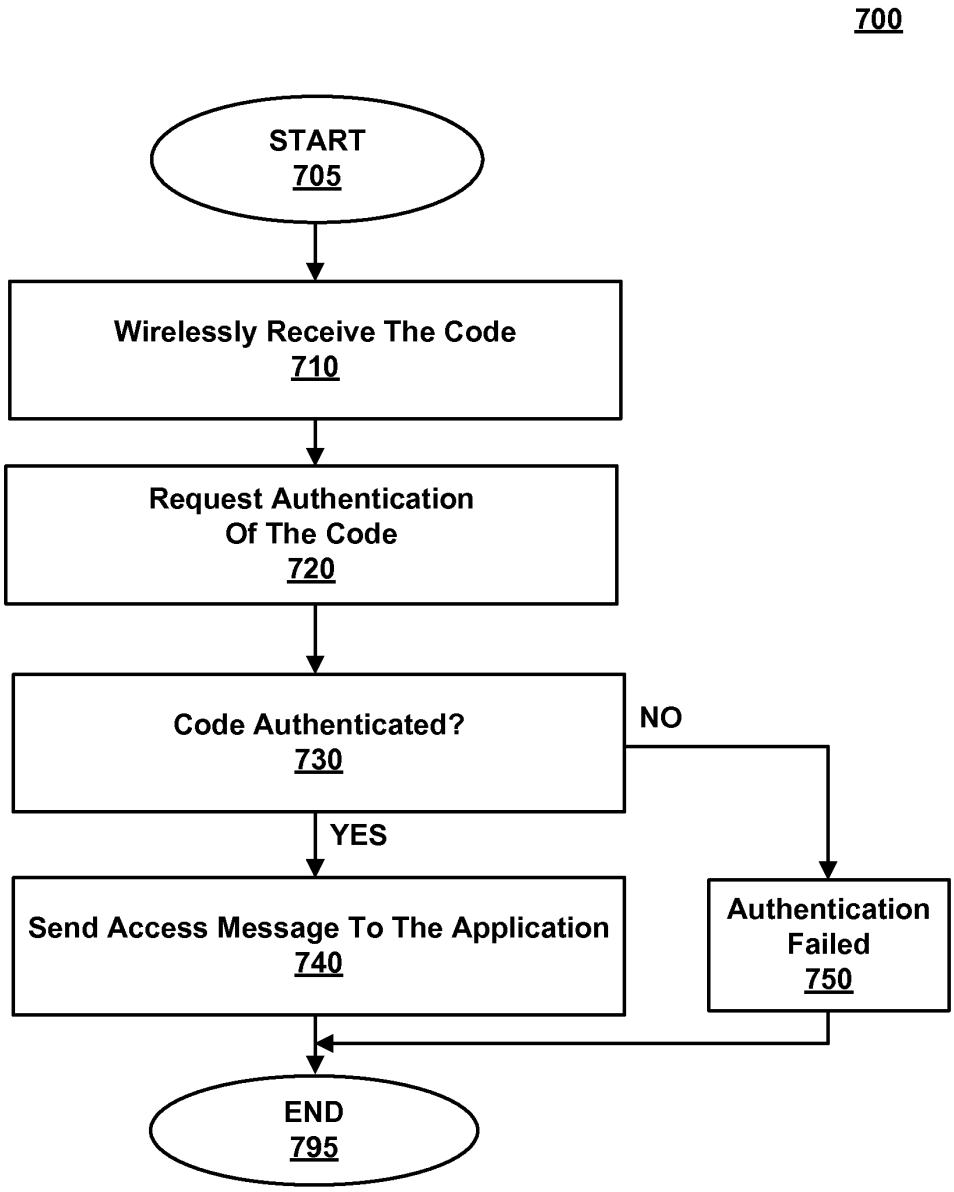

700
START
705
Wirelessly Receive The Code
710
Request Authentication
Of The Code
720
Code Authenticated?
730
NO
YES
Send Access Message To The Application
740
Authentication
Failed
750
END
795

FIG. 7

PTO/AIA/01 (08-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	Biometric Personal Data Key (PDK) Authentication

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [x] The attached application, or
- [ ] United States application or PCT international application number _____ filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: John J. Giobbi Date (Optional): 12/10/12

Signature: _____

Note: An application data sheet (PTO/AIA/14 or equivalent), including naming the entire inventive entity, must accompany this form. Use an additional PTO/SB/AIA01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	20499600
Application Number:	14521982
International Application Number:	
Confirmation Number:	8239
Title of Invention:	Biometric Personal Data Key (PDK) Authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Matthew M. Holmes
Filer Authorized By:	
Attorney Docket Number:	10001-04540 US
Receipt Date:	23-OCT-2014
Filing Date:	
Time Stamp:	15:28:43
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet	04540US_ApplicationDataSheet.pdf	1561392 d439ba5a9030e9ff705e0bfaf6242f5753b1ae46	no	7

Warnings:	
Information:	

2		04540US_Specification.pdf	131764 d4416d847baa9c200f12c875894a94f73c821025	yes	25

Multipart Description/PDF files in .zip description		
Document Description	**Start**	**End**
Specification	1	23
Claims	24	24
Abstract	25	25

Warnings:

Information:

3	Drawings-only black and white line drawings	04540US_Drawings.pdf	82588 4e3c63c77aaff8bdc0ea838506ae2995153b1cff	no	6

Warnings:

Information:

4	Oath or Declaration filed	04540US_Declaration.pdf	446969 6c2442ad680b2b87db1c56f131567ba1b49df78a	no	2

Warnings:

Information:

Total Files Size (in bytes):	2222713

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Giobbi	
U.S. Patent No.: 8,352,730; 9,298,905; 10,698,989	Examiner: To Be Assigned
Issued: January 8, 2013; March 29, 2016; June 30, 2020	Art Unit: To Be Assigned
Application No.: 11/314,199; 14/521,982; 15/049,060	
Filed: December 20, 2005, October 23, 2014, February 20, 2016	
Title: BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION	

Mail Stop *Ex Parte* Reexam
Attn: Central Reexamination Unit
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

DECLARATION OF BENJAMIN F. GOLDBERG, PH.D. IN SUPPORT OF SAMSUNG'S REQUESTS FOR *EX PARTE* REEXAMINATION OF U.S. PATENT NOS. 8,352,730; 9,298,905; and 10,698,989

TABLE OF CONTENTS

Page

I. INTRODUCTION 12

II. QUALIFICATIONS 13

III. LEGAL UNDERSTANDING 15

A. The Person of Ordinary Skill in the Art 15

B. My Understanding of Patent Invalidity Law (Anticipation & Obviousness) 16

C. My Understanding of Claim Construction 18

IV. BACKGROUND OF THE TECHNOLOGY DISCLOSED IN THE CHALLENGED PATENTS 19

A. Public Key Cryptography 19

B. Developments in the Industry 23

V. OVERVIEW OF THE PRIOR ART 27

A. Ludtke (Ex. 1005) 27

B. Okereke (Ex. 1006) 30

C. Robinson (Ex. 1007) 31

D. Scott (WO1999056429) (Ex. 1008) 31

VI. DISCUSSION 32

A. SNQ 1: Ludtke in combination with Okereke Renders Claims 1-2, 4-9, 11-12, and 14-17 of the '730 Patent Obvious 32

1. The Proposed Combination 32

2. Claim 1 of the '730 Patent 39

3. Claim 2: "The method of claim 1, wherein the one or more codes and the other data values are transmitted to the agent over a network." 54

4. Claim 4: "The method of claim 1, wherein the one or more codes and the other data values indicate that the biometric verification was successful." 54

5. Claim 5: "The method of claim 1, wherein the biometric data and the scan data are both based on a fingerprint scan by the user." 56

6. Claim 6: "The method of claim 1, further comprising: establishing a secure connection channel prior to

sending the one or more codes and other data values for authentication" *56*

7. *Claim 7: "The method of claim 1, further comprising: receiving a request for the one or more codes and the other data values without a request for biometric information; and responsive to receiving the request for the one or more codes and the other data values without a request for biometric information, sending the one or more codes and the other data values without requesting the scan data."* *58*

8. *Claim 8:* *58*

9. *Claim 11: "The integrated device of claim 8, wherein the verifier comprises: an LED to be activated for requesting the biometric scan."* *60*

10. *Claim 12* *60*

11. *Claim 14: "The method of claim 12, further comprising: establishing a secure communications channel with a biometric key, wherein the one or mode codes and the other data values associated with the biometrically verified user is received from the biometric key."* *62*

12. *Claim 15* *63*

13. *Claim 16: "The system of claim 15, wherein the biometric key receives an authentication request from the authentication unit, and in response, requests a biometric scan from the user to generate the scan data."* *65*

14. *Claim 17: "The system of claim 15, wherein if the biometric key cannot verify the scan data as being from the user, it does not send the one or more codes and the other data values."* *65*

B. SNQ 2: Ludtke in combination with Okereke and Robinson Renders Claims 3, 10, and 13 of the '730 Patent Obvious 67

1. *The Proposed Combination* *67*

2. *Claim 3: "The method of claim 1, further comprising: registering an age verification for the user in association with the device ID code.* *69*

3. *Claim 10: "The integrated device of claim 9, wherein an age verification is registered in association with the device ID code.* *69*

4. *Claim 13: "The method of claim 12, further comprising: registering a date of birth or age with the agent."* 70

C. SNQ 3: Ludtke in combination with Scott Renders Claims 1-2, 4-9, 11-12, and 14-17 of the '730 Patent Obvious 70

1. *The proposed combination* 70

2. *Claim 1 of the '730 Patent* 77

3. *Claim 2: "The method of claim 1, wherein the one or more codes and the other data values are transmitted to the agent over a network."* 81

4. *Claim 4: "The method of claim 1, wherein the one or more codes and the other data values indicate that the biometric verification was successful."* 82

5. *Claim 5: "The method of claim 1, wherein the biometric data and the scan data are both based on a fingerprint scan by the user."* 82

6. *Claim 6: "The method of claim 1, further comprising: establishing a secure connection channel prior to sending the one or more codes and other data values for authentication"* 82

7. *Claim 7: "The method of claim 1, further comprising: receiving a request for the one or more codes and the other data values without a request for biometric information; and responsive to receiving the request for the one or more codes and the other data values without a request for biometric information, sending the one or more codes and the other data values without requesting the scan data."* 82

8. *Claim 8:* 82

9. *Claim 9: "The integrated device of claim 8, wherein the one or more codes and the other data values are transmitted to the agent over a network."* 84

10. *Claim 11: "The integrated device of claim 8, wherein the verifier comprises: an LED to be activated for requesting the biometric scan."* 84

11. *Claim 12* 84

12. *Claim 14: "The method of claim 12, further comprising: establishing a secure communications channel with a*

biometric key, wherein the one or mode codes and the other data values associated with the biometrically verified user is received from the biometric key." 86

13. Claim 15 86

14. Claim 16: "The system of claim 15, wherein the biometric key receives an authentication request from the authentication unit, and in response, requests a biometric scan from the user to generate the scan data." 88

15. Claim 17: "The system of claim 15, wherein if the biometric key cannot verify the scan data as being from the user, it does not send the one or more codes and the other data values." 88

D. SNQ 4: Ludtke in combination with Scott and Robinson Renders Claims 3, 10, and 13 of the '730 Patent Obvious 88

1. The Proposed Combination 88

2. Claim 3: "The method of claim 1, further comprising: registering an age verification for the user in association with the device ID code. 90

3. Claim 10: "The integrated device of claim 9, wherein an age verification is registered in association with the device ID code. 91

4. Claim 13: "The method of claim 12, further comprising: registering a date of birth or age with the agent." 91

VII. '905 PATENT 92

A. SNQ 1: Ludtke in combination with Okereke Renders Claims 1, 3-10, and 12-18 of the '905 Patent Obvious 92

1. The Proposed Combination 92

2. Claim 1 of the '905 Patent 98

3. Claim 3: "The method of claim 1, wherein an indication that the biometric verification was successful is sent with the ID code." 111

4. Claim 4: "The method of claim 1, wherein the biometric data includes data from one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition." 111

5. *Claim 5: "The method of claim 1, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob."* *111*

6. *Claim 6: "The method of claim 1, wherein completing the financial transaction includes accessing an application."* *112*

7. *Claim 7: "The method of claim 1, wherein completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account."* *112*

8. *Claim 8: "The method of claim 1, further comprising: responsive to determining the action does not require biometric verification, receiving a request for the ID code without a request for biometric verification, and responsive to receiving the request for the ID code without a request for biometric verification, sending the ID code for authentication without requesting the scan data."* *112*

9. *Claim 9:* *113*

10. *Claim 10: "The integrated device of claim 7, wherein the ID code is transmitted to the third-party trusted authority over a network."* *114*

11. *Claim 12: "The integrated device of claim 7, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch, and a key fob."* *115*

12. *Claim 13:* *115*

13. *Claim 14: "The system of claim 11 wherein the integrated hardware device receives an authentication request from the authentication circuit, and in response, requests a biometric scan from a user to generate scan data and, when the integrated hardware device cannot verify the scan data as being from the legitimate user, the integrated hardware device does not send the ID code."* *116*

14. *Claim 15: "The system of claim 11, wherein the integrated hardware device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob."* *117*

15. *Claim 16: "The system of claim 11, wherein the biometric data includes data based on one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition, and a voice recognition."* *118*

16. *Claim 17: "The system of claim 11, wherein completing the financial transaction includes accessing one or more of a casino machine, keyless lock, an ATM machine, a web site, a file and a financial account."* *118*

17. *Claim 18: "The system of claim 11, wherein completing the financial transaction includes accessing an application."* *118*

B. SNQ 2: Ludtke in combination with Okereke and Robinson Renders Claims 2 and 11 of the '905 Patent Obvious 118

1. *The Proposed Combination* *118*

2. *Claim 2: "The method of claim 1, further comprising: registering an age verification for the user in association with the ID code."* *120*

3. *Claim 11: "The integrated device of claim 7 [sic – 9], wherein an age verification is registered in association with the ID code.* *121*

C. SNQ 3: Ludtke in combination with Scott Renders Claims 1, 3-10, and 12-18 of the '905 Patent Obvious 121

1. *The proposed combination* *121*

2. *Claim 1 of the '905 Patent* *128*

3. *Claim 3: "The method of claim 1, wherein an indication that the biometric verification was successful is sent with the ID code."* *131*

4. *Claim 4: "The method of claim 1, wherein the biometric data includes data from one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition."* *132*

5. *Claim 5: "The method of claim 1, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob."* *132*

6. *Claim 6: "The method of claim 1, wherein completing the financial transaction includes accessing an application."* *132*

7. *Claim 7: "The method of claim 1, wherein completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account."* *132*

8. *Claim 8: "The method of claim 1, further comprising: responsive to determining the action does not require biometric verification, receiving a request for the ID code without a request for biometric verification, and responsive to receiving the request for the ID code without a request for biometric verification, sending the ID code for authentication without requesting the scan data."* *132*

9. *Claim 9:* *133*

10. *Claim 10: "The integrated device of claim 7, wherein the ID code is transmitted to the third-party trusted authority over a network."* *134*

11. *Claim 12: "The integrated device of claim 7, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch, and a key fob."* *134*

12. *Claim 13:* *134*

13. *Claim 14: "The system of claim 11 wherein the integrated hardware device receives an authentication request from the authentication circuit, and in response, requests a biometric scan from a user to generate scan data and, when the integrated hardware device cannot verify the scan data as being from the legitimate user, the integrated hardware device does not send the ID code."* *135*

14. *Claim 15: "The system of claim 11, wherein the integrated hardware device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob."* *135*

15. *Claim 16: "The system of claim 11, wherein the biometric data includes data based on one or more of a fingerprint, palm print, a retinal scan, an iris scan, a*

hand geometry, a facial recognition, a signature recognition, and a voice recognition." *136*

16. *Claim 17: "The system of claim 11, wherein completing the financial transaction includes accessing one or more of a casino machine, keyless lock, an ATM machine, a web site, a file and a financial account."* *136*

17. *Claim 18: "The system of claim 11, wherein completing the financial transaction includes accessing an application."* *136*

D. SNQ 4: Ludtke in combination with Scott and Robinson Renders Claims 2 and 11 Obvious 136

1. *The Proposed Combination* *136*

2. *Claim 2: "The method of claim 1, further comprising: registering an age verification for the user in association with the device ID code."* *139*

3. *Claim 11: "The integrated device of claim 7 [sic – 9], wherein an age verification is registered in association with the device ID code."* *139*

VIII. '989 PATENT 139

A. SNQ 1: Ludtke in combination with Okereke Renders Claims 1-9 of the '989 Patent Obvious 139

1. *The proposed combination* *139*

2. *Claim 1* *146*

3. *Claim 2: "The method of claim 1, further comprising: Receiving a request for biometric verification, 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."* *159*

4. *Claim 3: "The method of claim 1, wherein completing the transaction includes accessing an application."* *163*

5. *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 authority sending an indication that the third party trusted authority authenticated the ID code to another party."* *163*

6. *Claim 5:* *163*

7. *Claim 6: "The smartphone of claim 5, wherein the ID code is transmitted to the third-party trusted authority over a network."* *165*

8. *Claim 7* *165*

9. *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 smartphone does not send the ID code."* *167*

10. *Claim 9: "The system of claim 7, wherein completing the transaction includes accessing an application."* *167*

B. SNQ 2: Ludtke in combination with Scott Renders Claims 1-9 of the '989 Patent Obvious 167

1. *The proposed combination* *167*

2. *Claim 1* *174*

3. *Claim 2: "The method of claim 1, further comprising: Receiving a request for biometric verification, 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."* *177*

4. *Claim 3: "The method of claim 1, wherein completing the transaction includes accessing an application."* *178*

5. *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 authority sending an indication that the third party trusted authority authenticated the ID code to another party."* *178*

6. *Claim 5:* *178*

7. *Claim 6: "The smartphone of claim 5, wherein the ID code is transmitted to the third-party trusted authority over a network."* *180*

8. *Claim 7* *180*

9. *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 smartphone does not send the ID code."* *181*

10. *Claim 9: "The system of claim 7, wherein completing the transaction includes accessing an application."* *182*

IX. SECONDARY CONSIDERATIONS 182

X. CONCLUSION 182

I, Benjamin F. Goldberg, hereby declare as follows:

I. INTRODUCTION

1. My name is Benjamin F. Goldberg. I have been retained on behalf of Samsung Electronics America, Inc. ("Samsung") to provide this Declaration in support of Samsung's requests for *ex parte* reexamination ("Requests") of U.S. Patent No. 8,352,730 ("the '730 Patent"), U.S. Patent No. 9,298,905 ("the '905 Patent"), and U.S. Patent No. 10,698,989 ("the '989 Patent")—each entitled "Biometric Personal Data Key (PDK) Authentication" (collectively, the "Challenged Patents," whose claims are referred to as the "Challenged Claims").

2. I am being compensated for my time at the rate of $475 per hour. My compensation is not based on the resolution of this matter. My findings are based on my education, experience, and background in the fields discussed below.

3. In preparing this declaration, I have reviewed and am familiar with all the prior art references referenced herein including at least the following:

> ***Ludtke*** (Ex. 1005) is U.S. Patent No. 7,188,110 ("Ludtke").
>
> ***Okereke*** (Ex. 1006) is U.S. Patent Publication No. 2003/0196084 ("Okereke")
>
> ***Robinson*** (Ex. 1007) is U.S. Patent Publication No. 2003/0177102 ("Robinson")
>
> ***Scott*** (Ex. 1008) is International Publication Number WO 99/56429 ("Scott")

4. I have also considered all other materials cited and discussed herein. I have reviewed the Challenged Patents and their file histories. At a general level, the

Challenged Patents describe various techniques for preventing unauthorized use of a wireless device by verifying both biometric data and the device itself. The Challenged Patents describe biometric authentication of a user of a wireless device using a generic "computerized authentication" system that provides secure access to resources such as ATMs and locked areas. Ex. 1001 ('730 Patent[1]), 1:15-18.

5. It is my opinion that the prior art cited in this Declaration raises substantial new questions of patentability (SNQs) as to each of the Challenged Claims.

6. The statements made herein are based on my own knowledge and opinion. This Declaration represents only the opinions I have formed to date. I may consider additional documents as they become available or other documents that are necessary to form my opinions. I reserve the right to revise, supplement, or amend my opinions based on new information and on my continuing analysis.

II. QUALIFICATIONS

7. My qualifications can be found in my Curriculum Vitae, which is submitted with this Declaration as **Exhibit 1004** and includes a complete list of my publications.

---

[1] While some of the Challenged patents include slightly different disclosure, the claims on the Challenged Patents are all substantially similar. For simplicity, I therefore sometimes use the disclosure of the '730 Patent as representative of all the Challenged patents herein. I note any relevant distinctions between each of the respective Challenged patents where applicable to my analysis below.

8. I am a tenured Associate Professor in the Department of Computer Science of the Courant Institute of Mathematical Sciences, New York University ("NYU"), in New York, New York. I have held this position since September 1994. From 1987 to 1994, I was an Assistant Professor in the Department of Computer Science at NYU. Since September 2014, I have been the Director of Graduate Studies for the MS programs in the Department of Computer Science, having previously served in that role from September 2009 through August 2012. I served as the Director of Undergraduate Studies for the Department of Computer Science from September 1995 through August 1998 and from September 2003 through August 2006. In addition, I have held a one year visiting professorship at the Institut National de Recherche en Informatique et en Automatique (INRIA), a national laboratory in France, and was twice appointed to a month-long position as an invited professor at the Ecole Normale Supérieure, a university in Paris.

9. I received my Doctoral degree in Computer Science from Yale University, New Haven, Connecticut in 1988, having previously received Master of Science and Master of Philosophy degrees in Computer Science from Yale in 1984. My undergraduate degree from Williams College in 1982 was a Bachelor of Arts degree with highest honors in Mathematical Sciences.

10. I have taught courses at the undergraduate and graduate level in programming languages, hardware design, embedded systems, operating systems, and other areas related to the technology at issue in this matter.

11. Additional information concerning the computer science courses that I have taught, my professional publications and presentations in the field of computer science, and cases in which I have testified as an expert at trial or deposition in the past five years are set forth in my current Curriculum Vitae (Ex.1004).

III. LEGAL UNDERSTANDING

A. The Person of Ordinary Skill in the Art

12. I understand that a person of ordinary skill in the relevant art (also referred to herein as "POSITA") is presumed to be aware of all pertinent art, thinks along conventional wisdom in the art, and is a person of ordinary creativity—not an automaton. I have been asked to consider the level of ordinary skill in the field that someone would have had at the time the claimed invention was made. In deciding the level of ordinary skill, I considered the following:

- the levels of education and experience of persons working in the field;
- the types of problems encountered in the field; and
- the sophistication of the technology.

13. In my opinion a Person of Ordinary Skill in the Art would have had a bachelor's degree in computer science or electrical engineering (or an equivalent degree) with at least three years of experience in the field of encryption and security (or equivalent experience). This level of skill is approximate, and more education would compensate for less experience and vice versa.

B. My Understanding of Patent Invalidity Law (Anticipation & Obviousness)

14. I am not a lawyer and will not provide any legal opinions. Though I am not a lawyer, I have been advised that certain legal standards are to be applied by technical experts in forming opinions regarding the meaning and validity of patent claims.

15. I understand that a patent claim is invalid if each and every element of the claim is disclosed by a single prior art reference. This is known as anticipation, and the claim is said to be "anticipated" by the prior art reference.

16. I understand that disclosure of a limitation of a patent claim can be "express" or "inherent." Express disclosure means the limitation is actually disclosed in the words or figures of the reference, while inherent disclosure means that the limitation is necessarily present or the natural, inevitable result of the elements explicitly disclosed.

17. I understand that a patent claim is invalid if the claimed invention would have been obvious to a person of ordinary skill in the field at the time the application was filed. This means that even if all of the limitations or requirements of the patent claim cannot be found in a single prior art reference that would anticipate the claim, the claim can still be invalid as obvious in view of that reference or in view of multiple prior art references.

18. To obtain a patent, a claimed invention must have been, as of the invention date, nonobvious in view of the prior art in the field. I understand that an invention is obvious when 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.

19. I understand that to prove that prior art, or a combination of prior art, renders a patent obvious, it is necessary to: (1) identify the particular references that singly, or in combination, make the patent obvious; (2) specifically identify which elements of the patent claim appear in each of the asserted references; and (3) explain how the prior art references would have been combined to create the inventions claimed in the asserted claim. I understand that the combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results. I also understand that when there are a finite number of identified, predictable solutions, a POSITA has good reason to pursue the known options within his or her technical grasp. I further understand that design incentives or market forces can motivate a POSITA to modify or combine teachings in the same field or in different fields. When considering obviousness of a combination of known elements, the operative question is thus whether the improvement is merely the predictable use of prior art elements according to their established functions.

20. I understand that certain objective indicia or "secondary considerations" can be important evidence regarding whether a patent is obvious or nonobvious. Such indicia include: (1) commercial success of products covered by the patent claims; (2) a long-felt need for the invention; (3) failed attempts by others to make the invention; (4) copying of the invention by others in the field; (5) unexpected results achieved by the invention as compared to the closest prior art; (6) praise of the invention by the infringer or others in the field; (7) the taking of licenses under the patent by others; (8) expressions of surprise by

experts and those skilled in the art at the making of the invention; and (9) the patentee proceeded contrary to the accepted wisdom of the prior art.

21. For the reasons I set out below, in my opinion, the prior art references demonstrate a strong case of obviousness against the Challenged Claims of the Challenged Patents. The prior art references therefore raise substantial new questions of patentability (SNQs) of the Challenged Claims.

22. I understand that in evaluating the invalidity of the Challenged Claims, the content of a prior art patent or printed publication should be interpreted the way a POSITA would have interpreted the prior art as of the effective filing date of the Challenged Patent (December 2004 for all Challenged Patents).

23. My analysis below is based upon this understanding.

C. My Understanding of Claim Construction

24. I have been instructed by counsel on the law regarding claim construction and patent claims, and understand that a patent may include two types of claims—independent claims and dependent claims. An independent claim stands alone and includes only the features it recites. A dependent claim depends from an independent claim or another dependent claim. I understand that a dependent claim includes all the features that it recites in addition to all of the features recited in the claim(s) from which it depends.

25. I have been informed that in an *ex parte* reexamination, patent claims are to be given their broadest reasonable interpretation consistent with the specification.

26. I reserve my right to amend or alter my analysis and opinions in view of the Patent Owner's proposed claim constructions, if any.

IV. BACKGROUND OF THE TECHNOLOGY DISCLOSED IN THE CHALLENGED PATENTS

27. As explained herein, in my opinion the Challenged Patents relate to generic "computerized authentication" systems used to gain access to devices, applications, or accounts through a biometric validation procedure. Ex. 1001 ('730 Patent) at 1:15-18, 1:51-53.[2] The device validates a user's biometric scan against biometric data stored on the device. *Id.* at 1:59-64. After validation, a code stored on the device is transmitted to indicate that the user's identity has been verified. *Id.* at 1:64-67. The device transmits the code to a third-party trusted authority that determines if the code is authentic by checking it against a list of legitimate integrated device codes. *Id.* at 2:1-4. If the code is authentic, the user is allowed access to the device, application, or account they seek access to. *Id.* at 2:4-5. The '730 Patent purports to solve for users the problem of having to "memorize or otherwise keep track of the[ir] credentials." *Id.* at 1:28-30. The patents also purport to solve the problem of illegitimate users "us[ing] a stolen access object to enter a secured location because the user's identity is never checked." *Id.* at 1:41-43.

A. Public Key Cryptography

28. Fundamental to the "computerized authentication" the Challenged Patents relate to is the use of public key cryptography. Indeed, the Challenged Patents themselves

[2] The Challenged Patents share a common specification. I will cite to the '730 Patent in this Background section, but the discussion is equally applicable to the '905 and '989 Patents.

describe one particular aspect of the public key infrastructure, the Certificate Authority.[3] *See* Ex. 1001 at 5:40-52. A POSITA would have been familiar with such technologies at least years, if not decades, before the Challenged Patents.

29. By 2004, public key cryptography had been in existence for over 30 years, starting in 1970 in classified work and in 1977 in the public literature. Several international standards for an extensive infrastructure to support public key cryptography, known as public key infrastructure (PKI), for use in industry and in the public sector were developed by 2000. A helpful summary of the public key cryptography and PKI is found in a February 2001 publication from the National Institute of Standards and Technology entitled "Introduction to Public Key Technology and the Federal PKI Infrastructure" by Kuhn et al.[4] ("Kuhn"), which I will quote from in this background section.

30. In its simplest form, public key cryptography supports confidential, authenticated, and robust communication between two entities, often represented in the cryptography literature as "Alice" and "Bob". In public key cryptography, Alice generates

---

[3] While the implementation of Public Key Cryptography described in Hsu, did not itself render the '730 Claims obvious or anticipated, (*see* Ex. 1002 at 10/5/11 Final Rejection; 8/21/12 Notice of Allowance), Hsu did not disclose a certificate authority, and this request does not rely on Public Key Cryptography to render the claims obvious. Rather, this discussion of Public Key Cryptography is intended to demonstrate the breadth of knowledge available to a POSITA, in particular that a POSITA would understand the use of keys, ID codes, and trusted authorities.

[4] Ex. 1012 *Introduction to Public Key Technology and the Federal PKI Infrastructure*, D.R. Kuhn et al, NIST Special Publication 800-32, Feb. 26, 2001. Available from the NIST website at https://www.nist.gov/publications/introduction-public-key-technology-and-federal-pki-infrastructure. I am familiar with this publication and NIST is generally respected in the field.

a pair of keys and makes one of the keys public – and is thus called the "public key" – and keeps the other key to herself, i.e., the "private key". Bob similarly generates a public key and a private key. To encrypt a message to send to Bob, for example, only Bob's public key is required. Only Bob, using his private key, is able to decrypt a message encrypted using Bob's public key. *See* Kuhn at 13.

31. Conversely, a message can be decrypted using, for example, Alice's public key, but only for messages encrypted using Alice's private key. Thus, if Alice encrypts her name (or some other value that Bob knows to expect) using her private key to form a digital signature, and then encrypts some text along with her digital signature using Bob's public key, sending the encrypted data in a message to Bob, only Bob can decrypt the message using his public key to read the text. Bob can then verify Alice as the sender by decrypting her digital signature using Alice's public key and comparing it to her name (or other known value). Robust communication, ensuring that any corruption to or tampering with Alice's message can be detected, is supported by having Alice's digital signature be a digest (cryptographic hash) of the original text in Alice's message to Bob. *Id.*

32. Without more, public key cryptography has significant difficulty scaling or handling otherwise unfamiliar parties. As such, a more developed infrastructure is needed. In particular, the widespread use of public key cryptography in commerce, including the use of smart cards as described here, relies on trusted, authenticated distribution of public keys. That is, if Alice wants to send an encrypted message to Bob to purchase an item – where Alice's financial information is included in the message – then Alice must find a

way to reliably retrieve Bob's public key and be sure that no attacker is presenting a false public key for Bob in an attempt to steal Alice's financial information. Similarly, Bob must be able to reliably retrieve Alice's public key in order to verify her digital signature. A public key infrastructure (PKI) provides the mechanism for safely distributing public keys through the use of digital certificates issued by a trusted third party known as a "certification authority" (or "certificate authority"), commonly referred to as a "CA". Kuhn explains:

> **3 PUBLIC KEY INFRASTRUCTURES**
>
> A public key infrastructure (PKI) binds public keys to entities, enables other entities to verify public key bindings, and provides the services needed for ongoing management of keys in a distributed system.

Id. at 17.

> The overall goals of modern security architectures are to protect and distribute information that is needed in a widely distributed environment, where the users, resources and stake-holders may all be in different places at different times. The emerging approach to address these security needs makes use of the scalable and distributed characteristics of public key infrastructure ("PKI"). PKI allows you to conduct business electronically with the confidence that:
>
> - The person or process identified as sending the transaction is actually the originator.
> - The person or process receiving the transaction is the intended recipient.
> - Data integrity has not been compromised.

(*id.*)

> Public key infrastructure is the combination of software, encryption technologies, and services that enables enterprises to protect the security of their communications and business transactions on networks. PKI integrates digital certificates, public key cryptography, and certification authorities into a complete enterprise-wide network security architecture. A typical enterprise's PKI encompasses the issuance of digital certificates to individual users and servers; end-user enrollment software; integration with certificate directories; tools for managing, renewing, and revoking certificates; and related services and support.

(*id.* at 17-18)

33. Although a PKI encompasses numerous components, including certificate authorities (CAs), registration authorities (RA) who are trusted by the CAs to register new uses, a repository of active certificates, and an archive of past data to settle disputes, of particular relevance here are the CAs. It is the CAs that issue digital certificates, each of which associates an entity (e.g., Alice or Bob) with its public key. Again, Kuhn explains:

> The CA issues a public key certificate for each identity, confirming that the identity has the appropriate credentials. A digital certificate typically includes the public key, information about the identity of the party holding the corresponding private key, the operational period for the certificate, and the CA's own digital signature. In addition, the certificate may contain other information about the signing party or information about the recommended uses for the public key. A subscriber is an individual or business entity that has contracted with a CA to receive a digital certificate verifying an identity for digitally signing electronic messages.

(*Id.* at 18)

> A CA may issue certificates to users, to other CAs, or both. When a CA issues a certificate, it is asserting that the subject (the entity named in the certificate) has the private key that corresponds to the public key contained in the certificate. If the CA includes additional information in the certificate, the CA is asserting that information corresponds to the subject as well. This additional information might be contact information (e.g., an electronic mail address), or policy information (e.g., the types of applications that can be performed with this public key.) When the subject of the certificate is another CA, the issuer is asserting that the certificates issued by the other CA are trustworthy.

(*Id.* at 19).

B. Developments in the Industry

34. The market for "computerized authentication" in "keyless environment[s]" (*see* Ex. 1001 at 1:15-2:30) as described in the Challenged Patents was already saturated by the time these patents were filed. In particular, by the late 1990s, many companies were

working on technology for contactless payments using mobile devices and smart cards. A focus of this work was developing encryption schemes that provided security but also would allow decryption and authentication to occur very quickly – e.g. within 100 milliseconds – to allow their use in public transportation systems where users quickly wave their device or card over a sensor before proceeding on. In an article from 1998 entitled "Security Issues for Contactless Smart Cards"[5] by M.W. David and K. Sakurai ("David"), the authors (one of whom was an engineer for a company working on contactless smart cards for the Chicago and Washington, DC transit systems) listed some of the companies who had developed contactless smart card (CSC) technology for this purpose:

> **2.2 Products (Single frequency)**
>
> MIFARE, a registered trademark, was developed by Mikron GmbH. Mikron is now owned by Phillips Semiconductors, and has a major share of the installed contactless smart card base. For example, the Korean firm INTEC, has used the MIFARE card for large scale applications in Korea bus fare collection system. It is also being tested for applications in Korean subways. MIFARE will also be adopted (Single frequency) by the light rail system in Kuala Lumpur and the subway in Shanghai.
>
> Japan's NTT Corporation will be using a CSC for its new telephone card system.
>
> FELICA, a registered trademark, was developed by the Sony Corporation. It is the basis for Hong Kong's "Octopus' card, being used by the Creative Star Limited consortium. Creative Star uses the cards to integrate fare collection on the subway, bus and ferry systems in Hong Kong.
>
> GO CARD, a registered trademark, was developed by the Cubic Corporation. It will be in use in the Chicago and Washington D.C. transit systems. As in Hong Kong, this will apply to multiple modes of transportation to include subway, bus and parking lots.

(Ex. 1013 (David) at 248)

[5] Ex. 1013 Security Issues for Contactless Smart Cards, by M. W. David and K. Sakurai, International Workshop on Public Key Cryptography, Springer 1998.

35. By 2001, this market was so developed that a smart card industry-wide association, the Smart Card Alliance was created (resulting from the merger of two existing industry groups) comprising "over 225 member organizations [to]serve as a single voice for the smart card industry in the United States."[6] A 2003 report of the Smart Card Alliance, entitled "Contactless Payment and the Retail Point of Sale: Applications, Technologies and Transaction Models"[7] ("SCA") describes the state of the industry and says the following about the technology governed by the ISO/IEC 14443 standard for contactless smart cards:

> **ISO/IEC 14443-Compliant High-Frequency 13.56 MHz Contactless Smart Cards**
>
> ISO/IEC 14443 is a contactless technology standard for "proximity" smart cards operating at 13.56 MHz. This standard specifies the characteristics of cards with an operational range of up to 4 inches (10 centimeters). The technology was originally designed for electronic ticketing and electronic cash applications. For these applications, short operational ranges and fast transaction speeds are critical. These same market requirements led ISO/IEC 14443 to be adopted for transit, off-line purchase, vending, and physical access control applications.
>
> **Advantages and Disadvantages**
>
> ISO/IEC 14443 was initiated in 1994 to standardize contactless proximity cards and finalized in 2001. To date, approximately 250 to 300 million contactless smart cards have been shipped based on the ISO/IEC 14443 standard.32 The majority of these cards are used in transportation applications for automatic fare collection, with the largest installations in Asia. ISO/IEC 14443 cards are supplied by the largest base of semiconductor suppliers and card manufacturers.

---

[6] Ex. 1014 https://web.archive.org/web/20010401152456/http://www.smartcardalliance.org/, captured on April 1, 2001.

[7] Ex. 1015 Smart Card Alliance, Publication Number PT-03002. See https://web.archive.org/web/20040227032450/http://smartcardalliance.org/alliance_activities/contactless_payment_report.cfm (captured February 27, 2004). Available at https://www.it.iitb.ac.in/~tijo/seminar/Contactless_Pmt_Report.pdf

A number of different ISO/IEC 14443-compliant card products are available, offering a range of characteristics at a number of price points. These characteristics include compliance to different levels of the standards, differing encryption and authentication schemes, and differences in processing power and card resources. Readers are available that can interoperate with the range of available card products, allowing an issuer to provide a choice of solutions and a migration path to more powerful devices if required.

ISO/IEC 14443 does not specify a standard for contactless link encryption or card-to-reader authentication. However, virtually every semiconductor vendor provides options to provide these security services. A common encryption/authentication protocol used with ISO/IEC 14443 Type A is the MIFARE protocol. An independent certification institute offers MIFARE compliance testing, ensuring that certified products from multiple vendors will work together.

Ex. 1015 at 18-19.

36. In particular, the SCA report also listed transit systems that used Sony's FeliCa technology, including the Hong Kong Octopus card, and provided a detailed description of the Hong Kong Octopus card:

FeliCa Card

The FeliCa card is used by the Hong Kong Octopus card transit system, the New Delhi Metro, the Singapore Land Transit Authority, and by the majority of Japanese transit agencies. The FeliCa card uses the same frequency and form factor as ISO/IEC 14443-compliant cards but differs in some technical specifications. In Hong Kong, the FeliCa card is also increasingly being used for non-transit payment applications (for example, quick service retail and vending applications). Sony is promoting FeliCa with an electronic purse in Japan and other countries.

(*Id.* at 21)

Hong Kong Octopus Card

The Hong Kong Octopus card, launched in 1997 as an electronic purse for public transportation, is the most successful and mature implementation of contactless smart cards used for mass transit payment. The card's acceptance and popularity have since extended its use to nearby retailers. Its success highlights two critical components of

> any payment strategy: strong self-service habits and the ability to leverage these habits to launch payment technologies for the general retail environment.4 The Octopus card is a good example of a contactless transit payment application that is evolving into a general retail payment mechanism.
>
> Octopus cards were developed as an automatic fare collection (AFC) scheme for Hong Kong's transit system. Over 9 million Octopus cards and 150,000 smart watches have been issued, and over 7 million transactions are recorded on a daily basis, for a daily transaction value of over HK$50 million (about US$6.5 million).5 This contactless smart card ticketing system currently includes over 100 service providers, including all of the major transport operators (bus, taxi, subway, train, tram, and ferry services). Because Hong Kong's main transport operators are all partners in the Octopus card, kiosks are widely available, making it easy for customers to check the balance on a card and recharge it with cash or electronic payments. The use of the card has shortened queues at ticket barriers, because the card doesn't have to be taken out of a bag or wallet — customers can just wave it past a scanner at a distance of several centimeters.

(*Id.* at 7-8)

> The contactless Octopus card is based on Sony's FeliCa™ technology, a proprietary 13.56 MHz technology similar to but not compliant with the ISO/IEC 14443 standard technology. This technology has widespread acceptance in the Asia Pacific region, with over 25 million cards issued worldwide. 8 Terminals read the cards instantly, processing transactions in less than one-third of a second. On the MTR, a scanner at the ticket barrier loads data on the card that is then used by scanners at the exit gates to deduct the correct fare and show the remaining credit.

(*Id.* at 8)

V. OVERVIEW OF THE PRIOR ART

A. Ludtke (Ex. 1005)

37. U.S. Patent No. 7,188,110 ("Ludtke") was filed on December 11, 2000. It issued on March 6, 2007. I understand that it is therefore prior art under 35 U.S.C. § 102(e) (pre-AIA).

38. Titled "Secure and Convenient Method and Apparatus for Storing and Transmitting Telephony-Based Data," Ludtke discloses a method of identifying an

authorized user with a biometric device and enabling the authorized user to access private information. Ex. 1005 at Abstract. In particular, Ludtke discloses "[o]ne embodiment may be visualized in a form similar to Sony Corporation's (Japan) FeliCa Card. The FeliCa is a contactless (wireless) card execution platform." *Id.* at 11:2-5. Ludtke recognizes both the need to ensure the integrity of financial information and the privacy of the user. *Id.* at 1:11-21.

39. The system disclosed in Ludtke is very much like the system disclosed in the Challenged Patents. Indeed, the Ludtke system allows transactions with an eCommerce system through a "transaction device" that has a unique identifier (ID). *Id.* at 3:34-35. The transaction device can be a privacy card or a digital wallet or both. *Id.* at 35-39. This transaction device is a wireless device that is carried and maintained by a user. *Id.* The transaction device includes a highly secured memory that can provide a transaction processing clearing house (TPCH) the necessary information to authorize a transaction. *Id.* at 40-45. The Ludtke system is depicted in Figure 1:

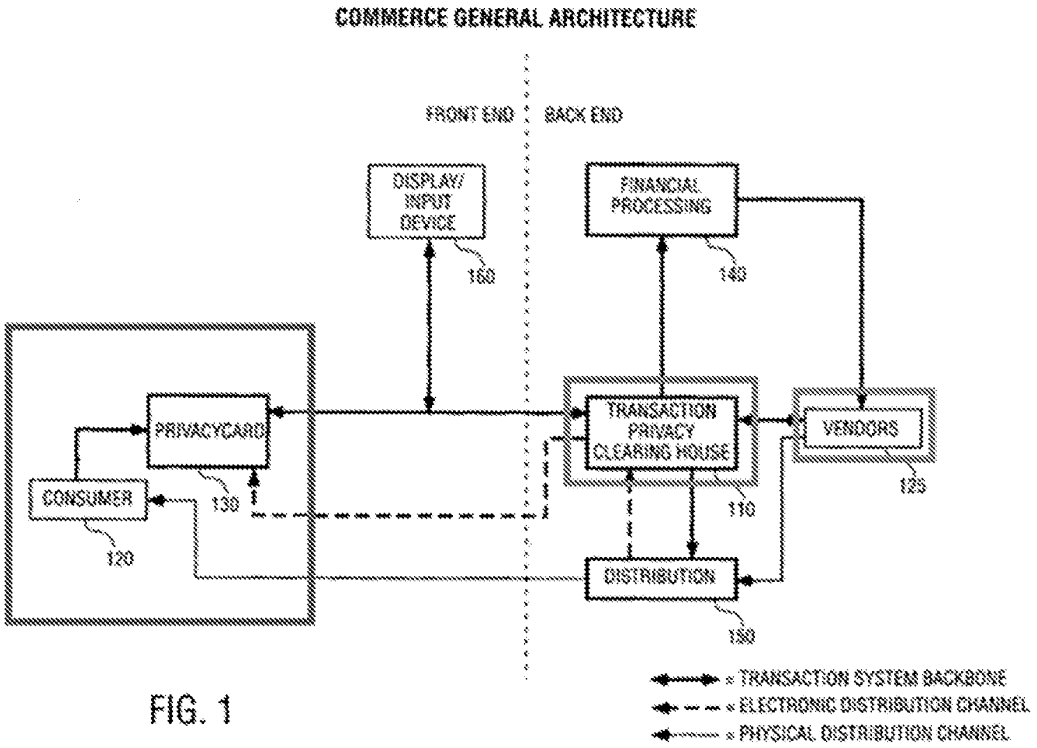


FIG. 1

40. As demonstrated in this Figure, the Consumer uses a transaction device 130 (in this Figure, shown as a privacy card). The consumer wishes to purchase something from a vendor 125. The transaction device provides information to the TPCH for authorization for the transaction between the consumer and vendor to be performed. *Id.* at 6:36-44. The TPCH is not part of the transaction, but rather functions as a third-party middleman of the transaction. *Id.* at 7:44-46. This ensures that sensitive information is not shared with the vendor. *Id.*

41. Recognizing the need to authorize a user, Ludtke also discloses the use of fingerprint recognition as part of the digital wallet. *Id.* at 18:16-17. This biometric

verification occurs before any transaction can take place, and therefore authorizes the user before the transaction device authorizes the device with the TPCH. *Id.* at 25:65-26:9.

B. Okereke (Ex. 1006)

42. U.S. Publication No. 2003/0196084 ("Okereke") was filed on April 11, 2003. It published on October 16, 2003. I understand that it is therefore prior art under 35 U.S.C. § 102(a) (pre-AIA).

43. Okereke describes a "system and method for allowing users of wireless and mobile devices to participate in Public Key Infrastructure [PKI]" and also indicates that it "facilitates secure remote communications." Ex. 1006 at Abstract. Okereke states that "systems that perform electronic financial transactions or electronic commerce must protect against unauthorized access to confidential records and unauthorized modification of data." *Id.* at ¶3.

44. In setting up communications for a mobile device, Okereke teaches that "a unique identifier for the wireless product to be employed is passed at 210 to the proxy server 125 program for authorization. The wireless product 165 can be a personal digital assistant (PDA), laptop, cellular telephone or any other device capable of remote wireless communication. The unique identifier can be a serial number or SIM." *Id.* at ¶ 25.

45. Okereke describes the PKI: "With PKI, a public and private key are created simultaneously using the same algorithm by a certificate authority. Information encrypted by the private key can only be decrypted with the corresponding public key. The private key is given only to the requesting party, and the public key is made publicly available as

part of a digital certificate in a directory that all parties can access. The private key is never shared with anyone or sent across the network." *Id.* at ¶ 7. Therefore, the private key is secret information.

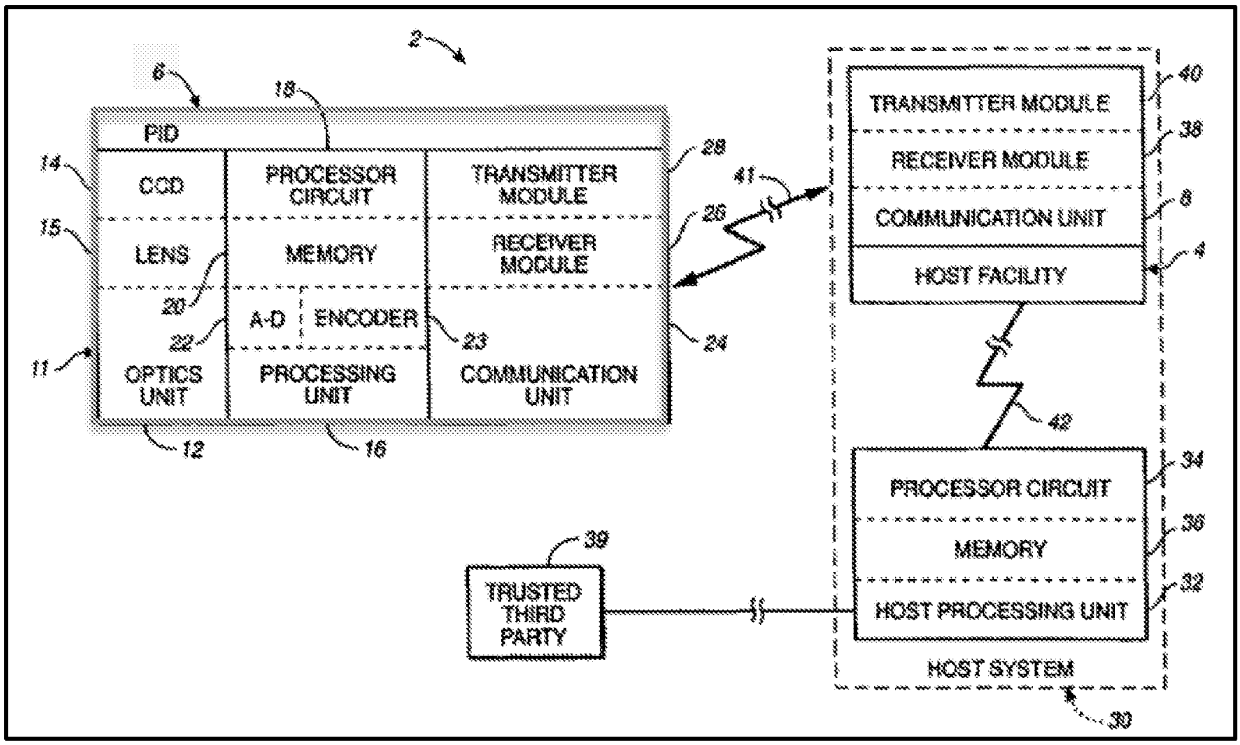
C. Robinson (Ex. 1007)

46. U.S. Publication No. 2003/00177102 ("Robinson") was filed on February 19, 2003. It published on September 18, 2003. I understand that it is therefore prior art under 35 U.S.C. § 102(a) (pre-AIA).

47. Robinson discloses that a central database 102 holds information related to users to authenticate a user's age to access an age restricted area, for example. Ex. 1007 at ¶¶27-28, 32, 66-67, & Fig. 1. The central database 102 stores age verification records related to individuals seeking age verification (called "presenters"), including information such as a user's age, date of birth, government ID number, biometric template, and at least one ID number that identifies the presenter within the system. *Id.* Prior to using the age-verification system, an individual presents biometric and age-verifying information. *Id.* at ¶¶13-15. Robinson further discloses that age-verifying information is associated with at least one ID number (SID) identifying the user. *Id.* at ¶28.

D. Scott (WO1999056429) (Ex. 1008)

48. Scott discloses a method for verifying a user during authentication of an integrated device (e.g., personal identification device ("PID") 6), in order to, for example, provide secure access to protected resources such as a hotel room or a point-of-sale transaction. Ex. 1008 at Abstract, 2:5-23, 4:22-5:9, 7:24-8:12.



Ex. 1008 at Fig. 1.

VI. DISCUSSION

A. SNQ 1: Ludtke in combination with Okereke Renders Claims 1-2, 4-9, 11-12, and 14-17 of the '730 Patent Obvious

1. The Proposed Combination

(a) The Prior Art Discloses the Claim Limitations

49. I believe the combination of Ludtke and Okereke renders obvious the above claims. SNQ 1 relies on Ludtke as the base reference, which discloses a mobile device used for performing financial transactions. Ludtke discloses all of the limitations in claims 1-2, 4-9, 11-12, and 14-17 except the "unique Device ID" and storage of "secret information." Specifically, Ludtke discloses the system as shown below in figure 1:

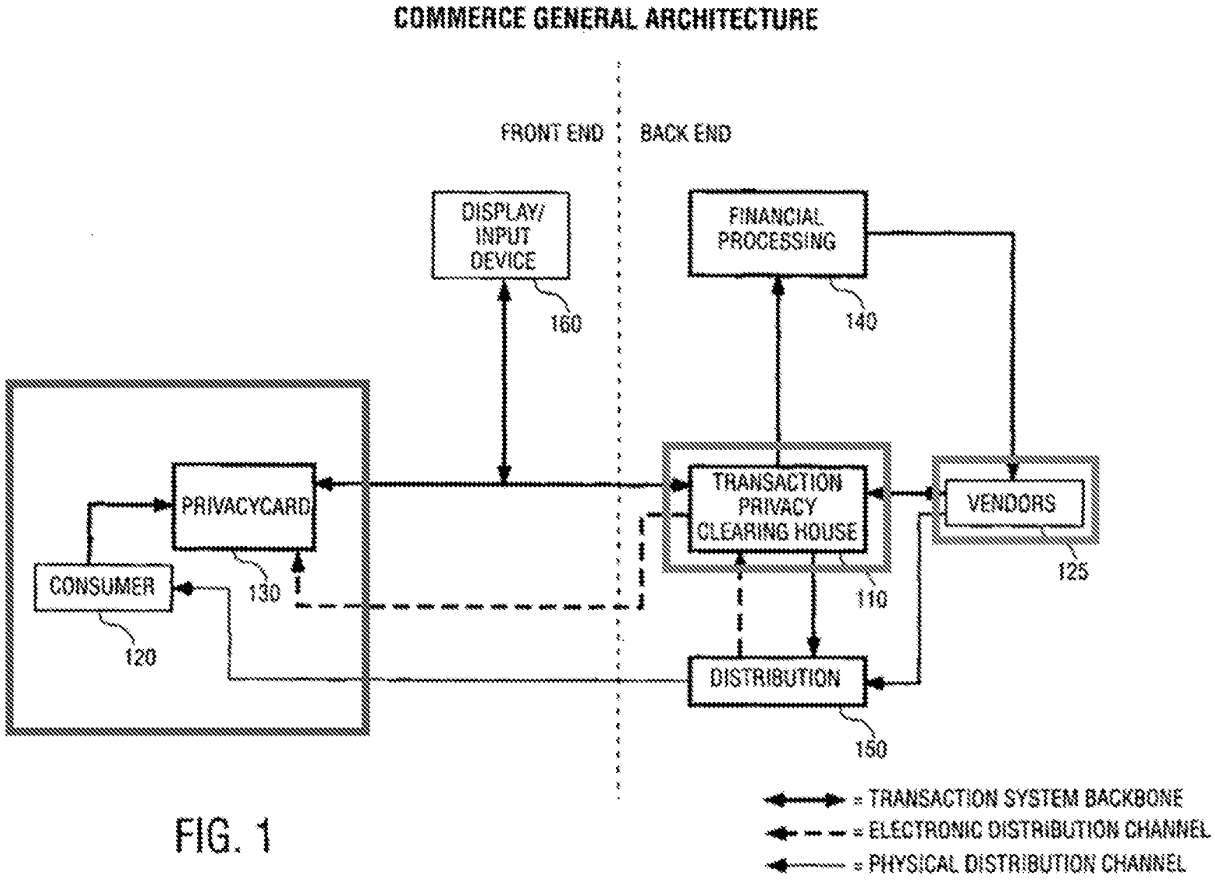


FIG. 1

Figure 1 shows one embodiment of the system in Ludtke. Ludtke discloses a "transaction device," which is seen above as the Privacy Card 130. Ex. 1005 at 6:36-44, Fig. 1. The transaction device is a device that the consumer 120 uses and includes a number of embodiments, including a privacy card, and digital wallet. *Id.* at 5:1-5, 11-14, 6:36-44. The transaction device also authorizes the consumer 120 using biometric data, including a fingerprint and other biometric information. Ludtke's transaction device includes and discloses a persistent, tamper proof storage. Ludtke also discloses the process to authenticate a financial transaction between the consumer 120 and a vendor 125. The financial transaction is authorized through the transaction privacy clearing house 110,

which is a third party, independent of the consumer 120 and the vendor 125. Ludtke emphasizes the third-party aspect of the transaction privacy clearing house 110 because the third party ensures that private information is not exchanged between the consumer 120 and the vendor 125. *Id.* at 6:45-49, 29:43-53.

50. The claims require storage of "secret information" in the user's device. Although Ludtke does not explicitly disclose this "secret information," it does disclose (1) a storage location for this information, (*id.* at 10:46-49, 24:61-65), as well as (2) the importance of maintaining the confidentiality of private information (*id.* at 3:45-47; 5:30-31, 6:45-49). Okereke discloses this "secret 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. Ex. 1006 at ¶25.

51. The claims also require an "ID code" that is unique and identifies the user's device ("a unique code identifying a device") that is communicated to the third party trusted authority for authorization of the device. Ludtke discloses "transaction device information" that is communicated from the consumer's transaction device 130 to the transaction privacy clearing house 110 for authorization, but Ludtke does not explicitly indicate that this "transaction device information" is a unique code identifying the consumer's transaction device. Okereke, however, does disclose this unique device ID code information, in the form of a unique serial number or SIM number for the user device. *Id.*

(b) A POSITA Would be Motivated to Combine Ludtke and Okereke

52. In my opinion, not only would a POSITA have been motivated to combine Ludtke and Okereke, a POSITA implementing Ludtke would have most likely done so according to Okereke. Such an implementation would have resulted in a product that meets all the limitations I discuss below. As I note above, the Ludtke reference meets most of the limitations of the claims of the '730 Patent with the exception of the "unique Device ID" and storage of "secret information" limitations. Instead Ludtke discusses using "transaction device information" as part of the described encrypted transaction without explaining how to implement such information. A POSITA would naturally have used public key cryptography to fill in this gap. As I describe above, public key cryptography is the standard for encrypted transactions and as such it would have been natural for a POSITA to implement it where a reference in this field does not provide detailed instructions. Okereke would have been a natural choice as it is an implementation of public key cryptography itself. *See* Ex. 1006 at Abstract.

53. In my opinion, the scope and content of the prior art would have motivated a POSITA to combine Ludtke and Okereke. As I explain above, Ludtke discloses almost all of the limitations of the claims except for "secret information" and the "unique" nature of a device ID.

54. Ludtke discloses a persistent, tamper-proof memory, and, in my opinion, a POSITA would have been motivated to combine the secret key disclosed in Okereke with the system disclosed in Ludtke. As I note above, *supra* § IV.A, a POSITA would have

already known, as of the priority date of the '730 patent, that encryption using a secret key such as Okereke's as part of a PKI would have been obvious when communicating confidential information. In my opinion, a POSITA would have specifically recognized the importance of encrypted communication when engaging in communications regarding financial information and especially when authenticating financial transactions. The use of secret information to perform this type of encryption was well-known ***decades*** before the filing date of the '730 patent, and was a well-established, well-known method for implementing encryption. Public key encryption was developed in the 1970s, and serves as a well-known way to encrypt and authenticate secret or confidential information. A POSITA would have recognized that such encryption is important to many applications, including financial information where it is particularly important to keep the information secret. In my opinion, a POSITA would therefore recognize that the use of PKI encryption (*i.e.,* public key encryption in the context of a PKI), which is disclosed in Okereke, would make the system of Ludtke even more secure. Okereke simply demonstrates this knowledge prior to the '730 patent's priority date.

55. Ludtke discloses transaction device information communicated between the transaction device and the transaction privacy clearing house for authorization of a financial transaction. In my opinion, a POSITA would have combined the teachings of Okereke's unique Device ID with Ludtke's system. As discussed above, Ludtke explicitly teaches communication of "transaction device information" with the TPCH. Ex. 1005 at 6:38-51. In my opinion, a POSITA would have recognized that such transaction device

information necessarily includes unique device identifiers such as a serial number or a SIM. Okereke explicitly discloses this fundamental information. Ex. 1006 at ¶25.

56. I understand the legal examination of motivation to combine is often performed by examining particular factors. I analyze some of these factors separately here, but these factors are important in my analysis above. In my opinion, a POSITA would have been motivated to combine Ludtke and Okereke because they are both in the same field of endeavor. Indeed, both references are in the same field of endeavor as the '730 patent, *i.e.*, authentication of a user and device, including use of biometric information, for the purpose of exchanging sensitive information over a network. *See* Ex. 1001 at 1:15-18 ("The present invention relates generally to computerized authentication, and more specifically, to an authentication responsive to biometric verification of a user being authenticated"); Ex. 1005 at Abstract ("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"); Ex. 1006 at Title ("System and method for secure wireless communication using PKI"); *id.* ¶31 ("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 password or biometric signature.").

57. Likewise, in my opinion, a POSITA would also have reasonably expected the combination of Ludtke and Okereke to succeed and yield predictable results. Ludtke's system already discloses a persistent and tamper-proof memory and discusses the use of sensitive information. Ludtke also discloses transaction device information. Ex. 1005 at

6:38-51. Given this disclosure in Ludtke, a POSITA would have expected the combination to result in Ludtke's financial system storing the secret information in Ludtke's memory and using the unique device ID disclosed in Okereke as the transaction device information. In my opinion, a 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 authorized device using unique device identifying information, such as a serial number or SIM, and would have expected this combination to succeed.

58. For example, Ludtke describes a protected memory to keep the type of important and sensitive information described in Okereke. Ex. 1005 at 19:37-40. Moreover, a POSITA would be familiar with the PKI-compliant encryption system because it had long been used as a way to encrypt and decrypt information and share such information only for authorized users. §IV.A *supra*. In my opinion, implementing such a system with Ludtke would have been logical and obvious to a POSITA. Finally, both systems have similar types of mobile devices, and have similar goals. It would make sense to a POSITA to use the type of information identified in Okereke in the Ludtke system to further complement Ludtke's features.

2. Claim 1 of the '730 Patent

(a) [1a] "A method for verifying a user during authentication of an integrated device, comprising the steps of:"

59. In my opinion, Ludtke discloses a method for verifying a user during authentication of an integrated device. It is also my opinion that Ludtke discloses an integrated device, *e.g.*, Ludtke's "transaction device." Ex. 1005 at 3:34-35.

60. Ludtke's transaction device provides a number of different "integrated" functions, including maintaining bills and bill paying on the device (*id.* at 4:4-6), online shopping (*id.* at 4:7-35), and downloading and accessing electronic catalogs (*id.* at 4:36-39). The transaction device includes a number of hardware options such as a magnetic stripe generator (*id.* at 3:49-51), a screen (*id.* at 55-57), and a bar code reader (*id.* at 3:61-63).

61. Ludtke explains that the "transaction device enhances security by ***authenticating the user of the card prior to usage***…" *Id.* at 4:62-65. This authentication can be performed by PIN code entry, or by other technologies such as a biometric solution. *Id.* at 4:65-5:1.

62. Ludtke also specifically discloses authentication of a device through the use of "transaction device information." *Id.* at 6:36-44. In my opinion, a POSITA would recognize that this transaction device information necessarily includes unique device IDs, such as serial numbers and SIMs. But this knowledge of a POSITA is further embedded within Okereke. Ex. 1006 at ¶30. As I explain above in detail, a POSITA would have been motivated to combine the disclosure of Ludtke with the disclosure in Okereke.

63. Okereke also discloses a method for verifying a user during authentication of an integrated device. Okereke discloses wireless and mobile devices which are integrated devices. *Id.* at Abstract. "The wireless product 165 can be a personal digital assistant (PDA), laptop, cellular telephone or any other device capable of remote wireless communication". *Id.* at ¶25.

64. Okereke specifically discloses authenticating the wireless device. Okereke describes a proxy server program awaiting initiation to establish secure wireless access capabilities. *Id.* When authentication is requested "a unique identifier for the wireless product to be employed is passed as at 210 to the proxy server 125 program for authorization." *Id.* "The unique identifier can be a serial number or SIM number, for example." *Id.* In my opinion, a POSITA would recognize that a serial number or SIM number is a unique identifier of a mobile device. Once the proxy server confirms the unique identifier, it authorizes the device by sending approval to a desktop computer to make a key exchange to allow communication. *Id.*

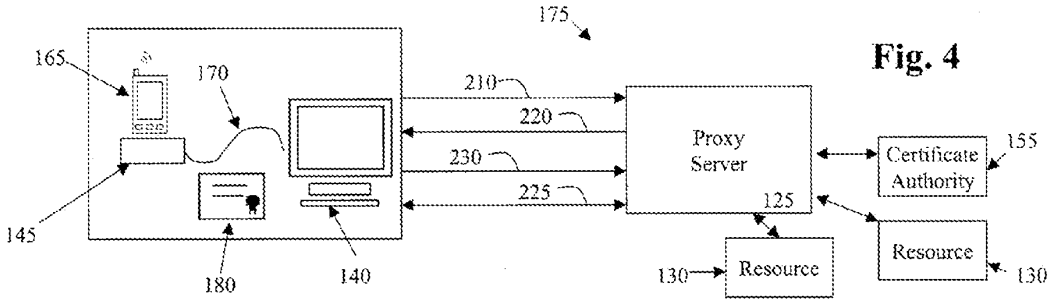


Fig. 4

(b) [1b] persistently storing biometric data of the user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to a

storage element on the integrated device that is unable to be subsequently altered wherein the biometric data is selected from a group consisting of a palm print a retinal scan, an iris scan, a hand geometry, a facial recognition and a voice recognition;

65. ***Persistently storing biometric data of the user . . . in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered***: In my opinion, Ludtke discloses a tamper-proof format on the integrated device. Specifically, the transaction device disclosed in Ludtke includes a process to use fingerprint data (biometric data of the user) to secure the device. Ludtke describes persistently storing the fingerprint data on the integrated device in a tamper-proof format that cannot be subsequently 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.

Ex. 1005 at 19:35-40. This fingerprint data is persistently stored in a tamper-proof format that is unable to be subsequently altered (write-once memory or other memory that is protected from accidental modification). Indeed, a write-once memory will only allow writing once, therefore, the information cannot be tampered with, and cannot be modified. Memory that is protected from accidental modification is also tamper-proof, since it will prevent unauthorized modification – whether by accident, or by someone who might have malicious intent. In each case, this tamper-proof memory is persistent storage, because the information stored is not easily re-writable.

66. ***Persistently storing . . . a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered***: As I explain above, Okereke discloses a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value. Specifically, Okereke discloses a device ID code in the form of a serial number or SIM number. Ex. 1006 at ¶25. In my opinion, both serial numbers and SIM numbers are unique codes that identify the devices they are attached to. Okereke also discloses a "secret decryption value." Specifically, Okereke describes a private/public key process. Okereke, for example, describes a Diffie Hellman Key Exchange, which uses AES (Advanced Encryption Standard). "AES is an encryption algorithm used by U.S. government agencies for securing sensitive but unclassified communications." *Id.* Specifically, the system uses a secret "private key" which can be used to encrypt and decrypt data that is exchanged between the wireless device and other system devices. *Id.* at ¶24.

67. As I discuss above, in my opinion, a POSITA would have been motivated to modify the system of Ludtke to incorporate the public/private key structure of Okereke and the unique serial numbers and SIMs; *see* §IV.A *supra.* Specifically, the Okereke device did not include a tamper-proof format that could not be altered, but Ludtke does include such an area of the integrated device. In my opinion, a POSITA would have been motivated to store permanent information, such as the secret key (private key) and unique

device identifiers (serial number and/or SIM). Moreover, a POSITA would have recognized that the "transaction device information" disclosed within Ludtke could further include the unique device information in Okereke, which would ensure that the information used to authenticate the device only identifies the authorized device. A POSITA would also store the unique device identifiers and the secret key in the persistent tamper-proof memory, because this is important information that allows authorization and sensitive communications to take place, and a POSITA would have recognized the need to take care to ensure it is not easy to tamper with and modify the information.

68. In particular, it is my opinion that a POSITA would not have found the lack of such disclosures in Ludtke to be material. Rather, because, as I note above, the use of public key encryption was known for decades and had become a standard, the author of Ludtke would not have felt it necessary to explain. In my opinion, a POSITA would have naturally implemented public key encryption as described in Okereke to fill in such a gap. A POSITA would have recognized the importance of secret keys and tamper proof environments for storing them. As I note in my Background section, such a key is needed for secure communications and keeping such a key secure is essential for the overall security of the system. *See* §IV.A, *supra*.

69. ***Wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition and a voice recognition***: Ludtke describes a number of different types of biometric information that may be used: "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." Ex. 1005 at 36:60-64.

(c) [1c] responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan

70. Further, it is my opinion that Ludtke describes receiving scan data from a biometric scan responsive to receiving a request for a biometric verification of the user. As I explain above, Ludtke describes using biometric verification – including a fingerprint[8] – 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:

[8] I understand Samsung contends that a fingerprint is not within the scope of claim 1. However, in my opinion, Ludtke still discloses the elements of claim 1 in that it discloses different types of biometric information, including those covered by claim 1. *Id.*

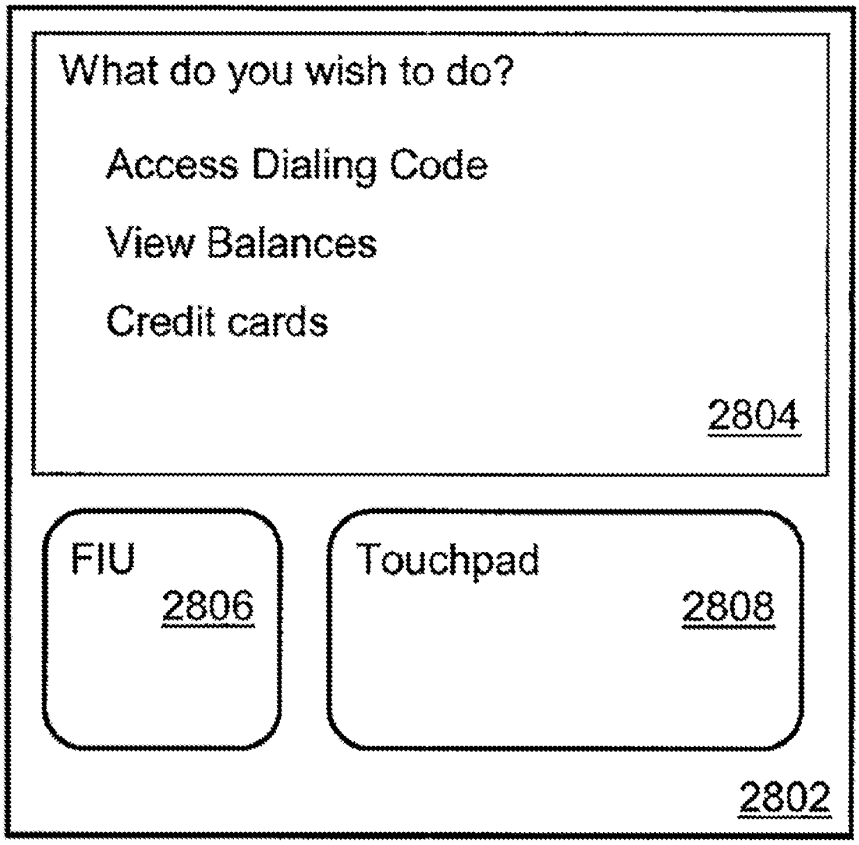


FIG. 28

Ex. 1005 at Fig. 28. "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." *Id.* at 39:24-27.

71. Figure 31 describes the process to verify a user of the integrated device (described in this embodiment as a digital wallet):

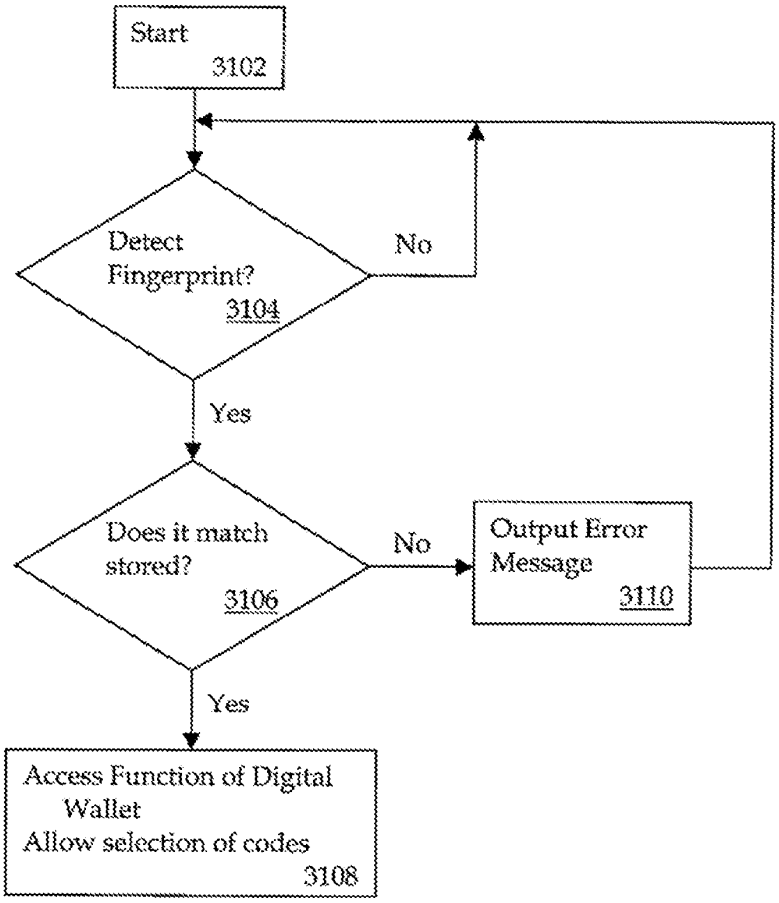


FIG. 31

Id. at Fig. 31. As can be seen in the flow chart, 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). *Id.* at 39:47-59.

(d) [1d] comparing the scan data to the biometric data to determine whether the scan data matches the biometric data

72. Ludtke also shows this limitation in Figure 31:

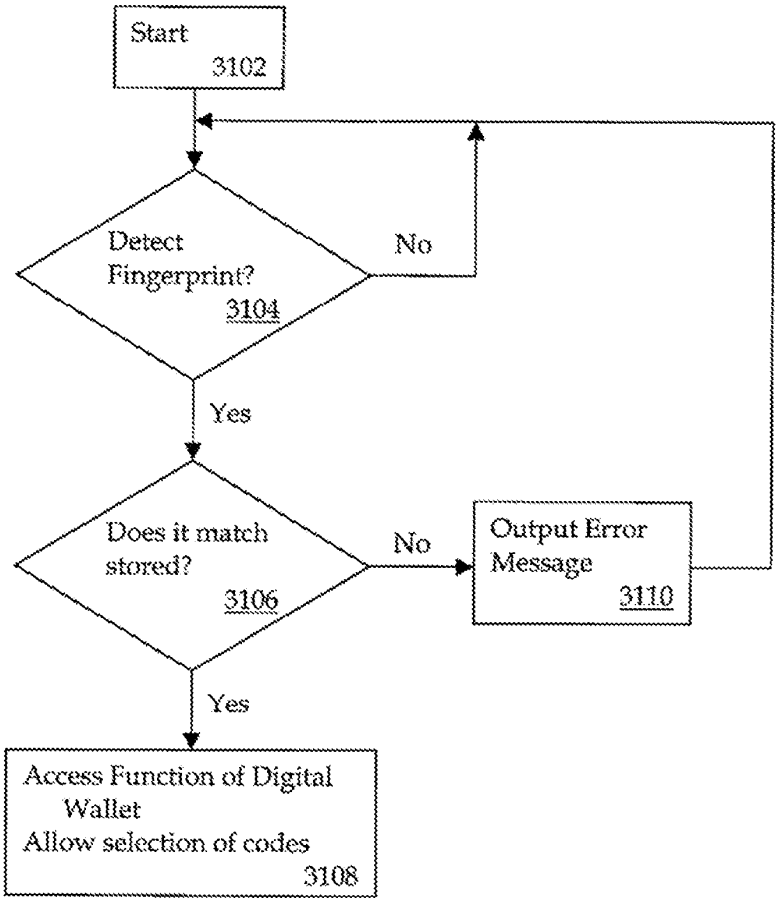


FIG. 31

Id. at Fig. 31. Ludtke explains that 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 [Digital Wallet/Integrated Device] 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." *Id.* at 39:47-54.

(e) [1e] responsive to a determination that the scan data matches the biometric data, wirelessly sending one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, wherein the one or more codes and other data values includes the device ID code; and

73. In my opinion Ludtke discloses this limitation. Although this limitation includes citations to "one or more codes from the plurality of codes and the other data values," that refers back to the storage of that category of information as described in element [1b]. The "wherein" clause in this limitation shows that only the device ID code is wirelessly sent. Therefore, of the information required to be stored in the persistent memory, only the Device ID code needs to be sent (although additional information is not precluded from being sent). Taking this into consideration, I interpret this limitation to mean: "responsive to a determination that the scan data matches the biometric data, wirelessly sending [the device ID code] for authentication by an agent that is a third party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices."

74. ***Responsive to a determination that the scan data matches the biometric data***: As I explain in conjunction with limitation [1d], if the scanned fingerprint data matches the stored fingerprint, then access to functions of the integrated device, such as the digital wallet, is permitted. *Id.* at 39:47-54.

75. ***Third party trusted authority***: In my opinion, Ludtke describes a transaction processing [or privacy] clearing house (TCPH) which is a third party trusted authority. The

TPCH "may access relevant account information to authorize transactions." *Id.* at 3:40-45. Figure 1 of Ludtke shows how the TPCH is a third party:

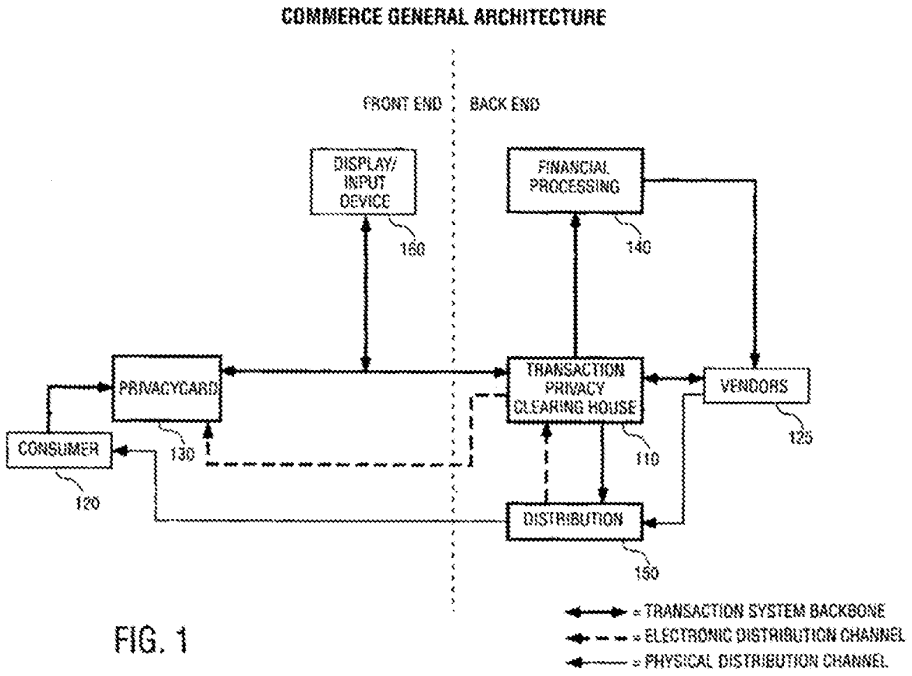


FIG. 1

Id. at Figure 1. Figure 1 shows the "commerce general architecture." *Id.* at 6:36-8:24. Figure 1 shows a consumer 120 who is the user wishes to complete a purchase, *id.* at 6:36-64, and a vendor 125, who is selling something to the user 120. *Id.* "In this embodiment, a transaction privacy clearing house (TPCH) 110 interfaces a user 120 and a vendor 125." *Id.* at 6:36-39.

76. In my opinion, the TPCH is a third party to the transaction between the user/consumer 120 and the vendor 125. Ludtke explains that in "one embodiment of electronic distribution, the TPCH 110 functions as the middleman of the distribution

channel. This allows TPCH 110 to retain user privacy by not exposing addressing information and possibly email addresses to third parties." *Id.* at 42-46. This demonstrates that the TPCH acts as a middleman to ensure that only necessary information is exchanged between the consumer 120 and the vendor 125, but is not associated with either of them.

77. Further, it is my opinion that the TPCH is also a "trusted authority." Ludtke explains that 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." *Id.* at 6:41-44. The consumer 120 and vendor 125 therefore trust the TPCH to indicate whether the transaction may be complete.

78. ***The third party trusted authority possesses a list of codes***: Ludtke also explains that the "TPCH 110 maintains a secure database of transaction device information and user information. In one embodiment, the TPCH 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." *Id.* at 6:49-55. And as I explain above, Ludtke explains that 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." *Id.* at 6:41-44. Therefore, the TPCH includes information that can be compared with information from the consumer and the consumer's device so the TPCH can determine whether the consumer 120 is authorized to complete a transaction with vendor 125. Indeed, the transaction device information that the TPCH compares to the received transaction

device information must be stored within the TPCH as a list of codes (and specifically, a list of Device ID codes), in order to perform the comparison function that is disclosed. *Id.* at 30:19-27.

79. ***Wirelessly sending a code to the third party trusted authority for authorization***: Ludtke explains that "[t]he 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." *Id.* at 6:41-44. Ludtke also explains that "the transaction device may contain wireless data communication," and may also "closely resemble a standard credit card." *Id.* at 5:36-41. In describing the TPCH specifically, Ludtke indicates that a "variety of communication devices may be used, such as the Internet, direct dial-up modem connections, wireless or cellular signals, etc." *Id.* at 9:35-42.

80. ***Device ID Code***: Ludtke does not describe the specific "transaction device information" that is provided to the TPCH 110 and that is maintained in a secure database by the TPCH 110. *Id.* at 6:41-125. However, as I discuss above, in my opinion, a POSITA would be motivated to combine Ludtke with the teachings of Okereke, and would recognize that the "transaction device information" would include a unique device serial code or SIM code, both of which identify the integrated device.

(f) [1f] responsive to authentication of the one or more codes and the other data values by the agent, receiving an access message from the agent allowing user access to an application, where the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.

81. In my opinion, Ludtke teaches this limitation. As I explain above, the terms "the one or more code and other data values" can be synthesized into the "Device ID code."

82. ***Responsive to authentication of the device ID code by the agent, receiving an access message from the agent allowing user access to an application***: In this case, the "agent" is the third party trusted authority. As I indicate above, Ludtke explains that 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." Ex. 1005 at 6:41-44. In my opinion, a POSITA would recognize that when the TPCH 110 "indicates to . . . the user 120," that indication is in the form of an access message allowing the user access to an application. *Id.* In this case, the TPCH is allowing access to the application on the transaction device that will permit the transaction to be completed. Ludtke further discloses this limitation at Fig. 15, Step 1520:

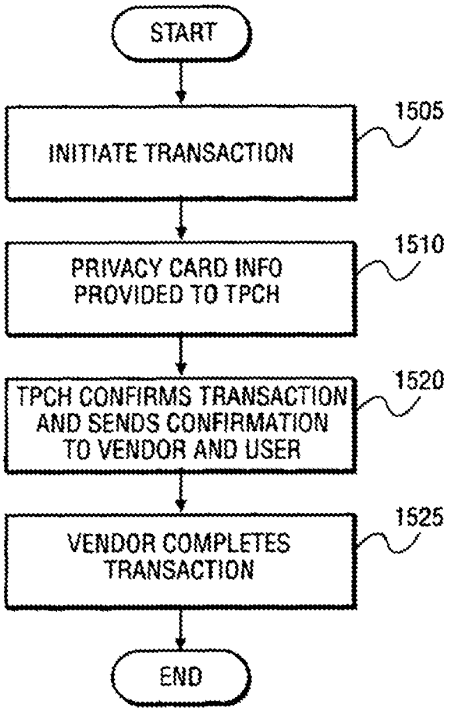


FIG. 15

Id. at Fig. 15, *see also* Figs. 16-17, steps 8 and 9-1. With regard to step 1520, Ludtke teaches that the "TPCH, at step 1520, confirms the transaction and provides the confirmation to the vendor and the user. At step 1525, the vendor completes the transaction without the knowledge of the user." *Id.* at 27:13-16.

83. ***Where the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file***: In my opinion, in Ludtke, access would be given applications of either computer software, a file (or both). In a number of embodiments,

Ludtke describes the transaction device as including a "digital wallet" which a POSITA would recognize as computer software and files that allow a user to digitally store credit card and other payment information and to make transactions with that card. *Id.* at Fig. 5a-b, 9:7-25.

3. Claim 2: "The method of claim 1, wherein the one or more codes and the other data values are transmitted to the agent over a network."

84. As I explain above, Ludtke explains that "[t]he 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." *Id.* at 6:41-44. Ludtke also explains that "the transaction device may contain wireless data communication," and may also "closely resemble a standard credit card." *Id.* at 5:36-41. In describing the TPCH specifically, Ludtke indicates that a "variety of communication devices may be used, such as the Internet, direct dial-up modem connections, wireless or cellular signals, etc." *Id.* at 9:35-42. Therefore, in my opinion, the communications described above in conjunction with claim 1 (by both Ludtke and Okereke) to the agent are transmitted over a network.

4. Claim 4: "The method of claim 1, wherein the one or more codes and the other data values indicate that the biometric verification was successful."

85. As I explain above, Ludtke includes a disclosure where the biometric information is checked to verify the user before they can access the financial application. Ludtke describes this in Figure 31:

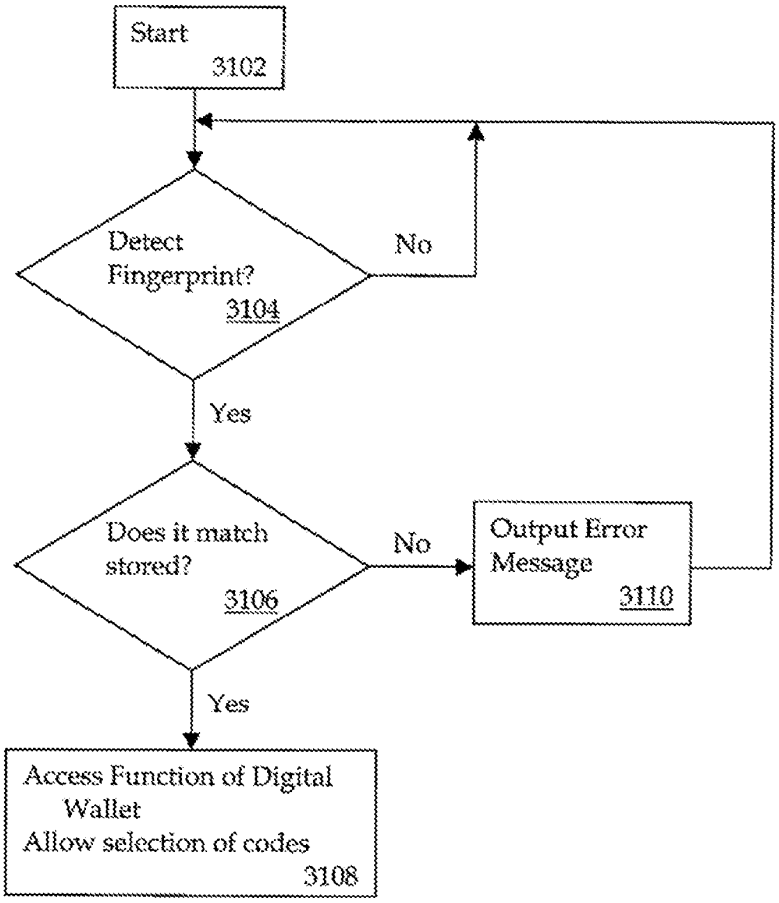


FIG. 31

86. *Id.* at Fig. 31. Ludtke explains that 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 [Digital Wallet/Integrated Device] 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." *Id.* at 39:47-54.

87. Claim 4 requires only that the verification is part of the "one or more codes or other data values." In claim 1, these codes are stored in the persistent tamper-proof memory. In my opinion, one of ordinary skill in the art would find it obvious to store the verification as part of the codes and other data values in this memory as it relates to the biometric information which is important information that one would not want to be tampered with. Moreover, the storage as part of the "one or more codes or other data values" ensures that the verification information is available to be used for other purposes by the device.

5. Claim 5: "The method of claim 1, wherein the biometric data and the scan data are both based on a fingerprint scan by the user."

88. In my opinion, Ludtke discloses this limitation. Ludtke describes a number of different types of biometric information that may be used, including a fingerprint: "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." *Id.* at 36:60-64.

6. Claim 6: "The method of claim 1, further comprising: establishing a secure connection channel prior to sending the one or more codes and other data values for authentication"

89. In my opinion, Ludtke discloses this limitation. This limitation refers to the transaction device establishing a connection for communicating with the TPCH, or third party trusted authority. The TPCH includes a security management function 620 responsible for secure communications:

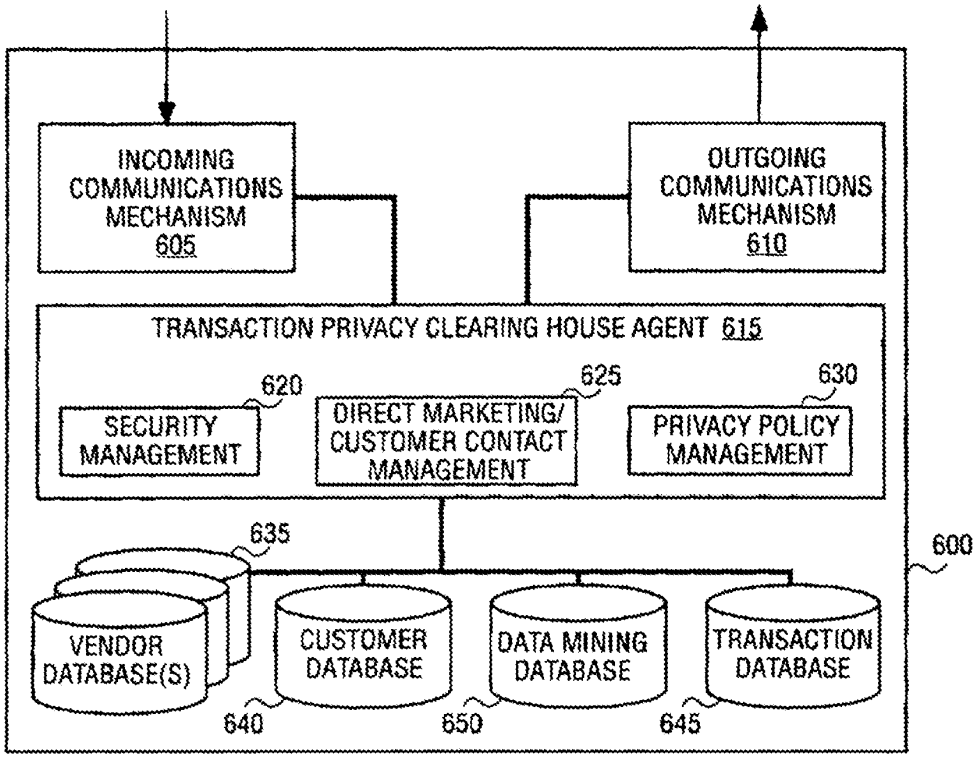


FIG. 6

Id. at Fig. 6. "The security management function 620 ensures secure communications among the components internal to the TPCH 600 and the external entities external to the TPCH 600. This ensures that only authorized entities are allowed access to data and that only authorized transaction devices can execute transactions against a user's account." *Id.* at 9:52-59. Therefore, with the security management 620, the transaction devices communicate with the TPCH 600 via a secure communication channel.

7. Claim 7: "The method of claim 1, further comprising: receiving a request for the one or more codes and the other data values without a request for biometric information; and responsive to receiving the request for the one or more codes and the other data values without a request for biometric information, sending the one or more codes and the other data values without requesting the scan data."

90. In my opinion, Ludtke discloses this limitation. Ludtke envisions using different forms of authentication other than biometric information. Ludtke states: "One means of authentication is some kind of PIN code entry. Alternately, authentication may be achieved by using more sophisticated technologies such as a biometric solution (*e.g.*, fingerprint recognition)." *Id.* at 4:65-5:1. In the situation where a PIN was used, there would be no need for a request for biometric information.

8. Claim 8:

(a) [8a] "An integrated device for verifying a user during authentication of the integrated device, comprising]"

91. In my opinion, Ludtke and Okereke disclose an integrated device for verifying a user during authentication of the integrated device. *See* Element [1a], Section VII.A.2.a, *supra*.

(b) [8b] "a memory stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to the memory that is unable to be subsequently altered; wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;"

92. In my opinion, Ludtke and Okereke disclose this element. *See* Element [1b], Section VII.A.2.b, *supra*.

(c) [8c] "a verification unit, in communication with the memory, receives scan data from a biometric scan for comparison against the biometric data, and if the scan data matches the biometric data, wirelessly sends one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, wherein the one or more codes and other data values includes the device ID code; and"

93. In my opinion, Ludtke discloses this limitation. *See* Elements [1c-1e], Sections VII.A.2.c-e, *supra*.

94. The "verification unit" will be the portion of memory and instructions that verify the biometric information. In my opinion, a POSITA would recognize that the verification unit would be in communication with the memory, since the biometric information that the verification unit compares with received biometric information is stored in the memory for comparison.

(d) [8d] "responsive to the agent authenticating the one or more codes and the other data values, a radio frequency communicator, receives an access message from the agent allowing the user access to an application, wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file."

95. In my opinion, Ludtke discloses this limitation. *See* Element [1f], Section VII.A.2.f, *supra*."

(e) Claim 9: "The integrated device of claim 8, wherein the one or more codes and the other data values are transmitted to the agent over a network."

96. *See* Claim 2. Section VII.A.3, *supra*.

9. Claim 11: "The integrated device of claim 8, wherein the verifier comprises: an LED to be activated for requesting the biometric scan."

97. In my opinion, Ludtke discloses notifications to request a biometric scan and it would be obvious to use an LED. In describing the fingerprint scanner, Ludtke indicates that at "various times during interaction, the user is prompted to supply a fingerprint recognition sample." Ex. 1005 at 14:40-42. In my opinion, a POSITA would recognize that the prompt can be in a number of ways that would be consistent with alerts on a mobile device. One of the common alert mechanisms in a mobile device is an LED.

10. Claim 12

(a) [12a]. "A method for authenticating a verified user using a computer processor configured to execute method steps, including:"

98. In my opinion, Ludtke and Okereke disclose this limitation. *See* Element [1a]. Section VII.A.2.a, *supra*.

99. In my opinion, it is inherent that any steps needed to authenticate the verified user would be executed using a computer processor.

(b) [12b]. "receiving one or more codes from a plurality of codes and other data values including a device ID code, wherein the plurality of codes and the other data values comprises the device ID code uniquely identifying the integrated device and a secret decryption value associated with a biometrically verified user, the device ID code being registered with an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices"

100. In my opinion, Ludtke and Okereke disclose this limitation. See Elements [1b], [1e], Sections VII.A.2.b, VII.A.2.e, *supra*.

101. The claim does not specifically indicate what "receives" the one or more codes, and therefore the receiver can be the device itself, a memory or processor on the device, or another device receiving the codes. Specifically, the transaction device disclosed in Ludtke includes a process to use fingerprint data (biometric data of the user) to secure the device. In my opinion, this means Ludtke discloses "biometrically verified users."

102. In my opinion, a POSITA would recognize that in order for the transaction device's information to be present in the TPCH, the information would need to be registered with the TPCH. The registration process ensures that the information is stored on the TPCH when it authenticates the device.

(c) [12c] "requesting authentication of the one or more codes and the other data values by the agent, wherein the authentication determines whether the one or more codes and the other data values are-legitimate;"

103. In my opinion, Ludtke discloses this limitation. *See* element [1e], section VII.A.2.e, *supra*. Ludtke explains that "[t]he 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." Ex. 1005 at 6:41-44. Ludtke also explains that "the transaction device may contain wireless data communication," and may also "closely resemble a standard credit card." *Id.* at 5:36-41. In describing the TPCH specifically, Ludtke indicates that a "variety of communication devices may be used, such as the Internet, direct dial-up modem connections, wireless or cellular signals, etc." *Id.* at 9:35-42. In my opinion, a POSITA would recognize that when the transaction device information is sent to the agent, it is a request for authentication. When the TPCH approves the

transaction, it is indicating that the codes and other data [transaction device information] is legitimate.

(d) [12d] "receiving an access message from the agent; and"

104. In my opinion, Ludtke discloses this limitation. *See* element [1f], section VII.A.2.f, *supra*.

(e) [12e] "in response to a positive access message, allowing the biometrically verified user access to an application, wherein the application is selected from a group consisting of a casino machine , a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a website and a file."

105. In my opinion, Ludtke discloses this limitation. *See* element [1f], section VII.A.2.f, *supra*.

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

106. In my opinion, Ludtke discloses this limitation. *See* Claim 6, section VII.A.6, *supra*. This claim indicates that the "one or more codes and the other data values associated with the biometrically verified user" are stored on a "biometric key" before being transferred to the third party trusted authority. The memory where these values are stored on the Ludtke user device is a "biometric key" because it is accessed when the user is verified with biometric information, giving access to the data on the device, and eventually allowing authentication by the TPCH. Ex. 1005 at 4:62-5:1.

12. Claim 15

(a) [15a] "a system, comprising:"

107. In my opinion, Ludtke discloses this limitation. Specifically, Ludtke discloses a system for transactions between a transaction device 130 being used by a consumer 120, and a vendor 125, with authorization performed by the transaction privacy clearing house 110, as shown in Figure 1:

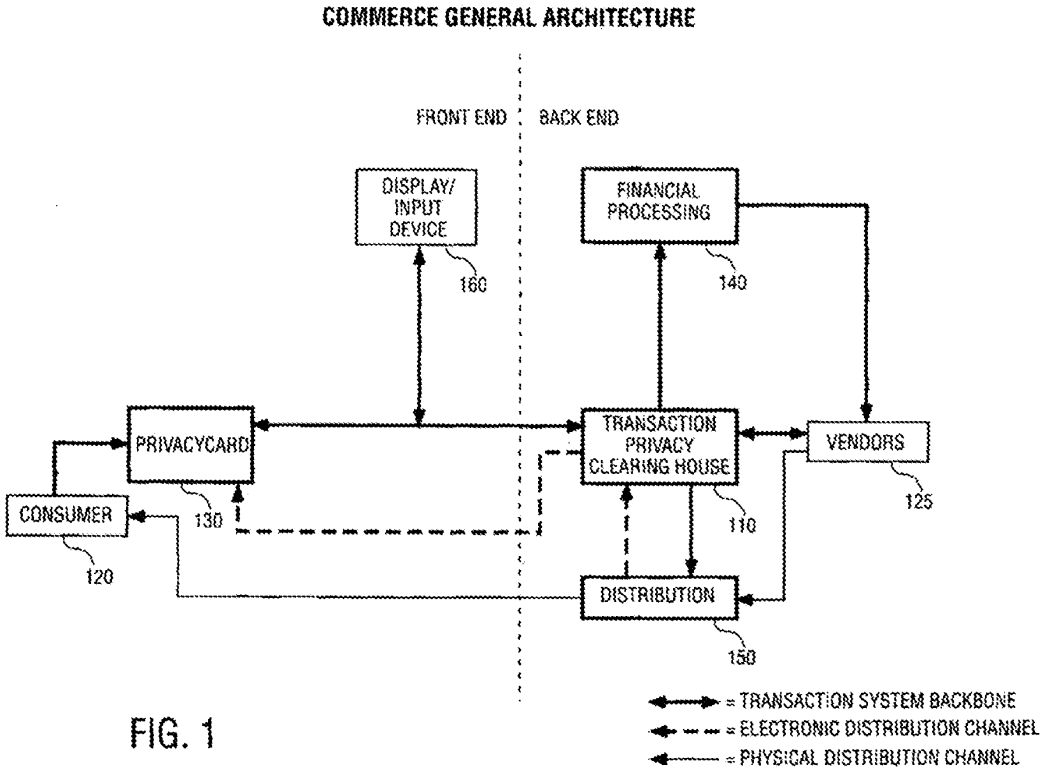


FIG. 1

(b) [15b] "a biometric key stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the biometric key and a secret decryption value in a tamper proof format written to a storage element on the biometric key that is unable to be subsequently altered,"

108. In my opinion, Ludtke and Okereke disclose this limitation. *See* element [1b], section VII.A.2.b, *supra*. This claim uses the term "biometric key" to refer to the device the user uses (known in other claims as an "integrated device.")

(c) [15c]: "and if scan data can be verified as being from the user by comparing the scan data to the biometric data, wirelessly sending, one or more codes from the plurality of codes and other data values wherein the one or more codes and other data values include the device ID code, and the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition, and a voice recognition; and"

109. In my opinion, Ludtke and Okereke disclose this limitation. *See* claim elements [1b], [1d], and [1e], sections VII.A.2.b, d, and e, *supra*.

(d) [15d]: "an authentication unit receives the plurality of codes and the other data values and send[] the plurality of codes and the other data values to agent for authentication to determine whether the one or more codes and the other data values are legitimate, wherein the agent is a third party trusted authority possessing a list of device ID codes uniquely identifying integrated devices,"

110. In my opinion, Ludtke and Okereke disclose this limitation. *See* claim element [1e], section VII.A.2.e, *supra*. Here, the "authentication unit" is code on a processor on the integrated device that is responsible for sending the Device ID code or additional codes to the third party trusted authority to authenticate the user and device.

(e) [15e]: "and responsive to the device ID code being authenticated, the authentication unit receiving an access message from the agent allowing the user to access an application, wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, and a file."

111. In my opinion, Ludtke discloses this limitation. *See* claim element [1f], section VII.A.2.f, *supra*.

13. Claim 16: "The system of claim 15, wherein the biometric key receives an authentication request from the authentication unit, and in response, requests a biometric scan from the user to generate the scan data."

112. In my opinion, Ludtke discloses this limitation. *See* claim element [1c], section VII.A.2.c, *supra*.

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

113. In my opinion, Ludtke discloses this limitation. Figure 31 describes the process to verify a user of the integrated device (described in this embodiment as a digital wallet):

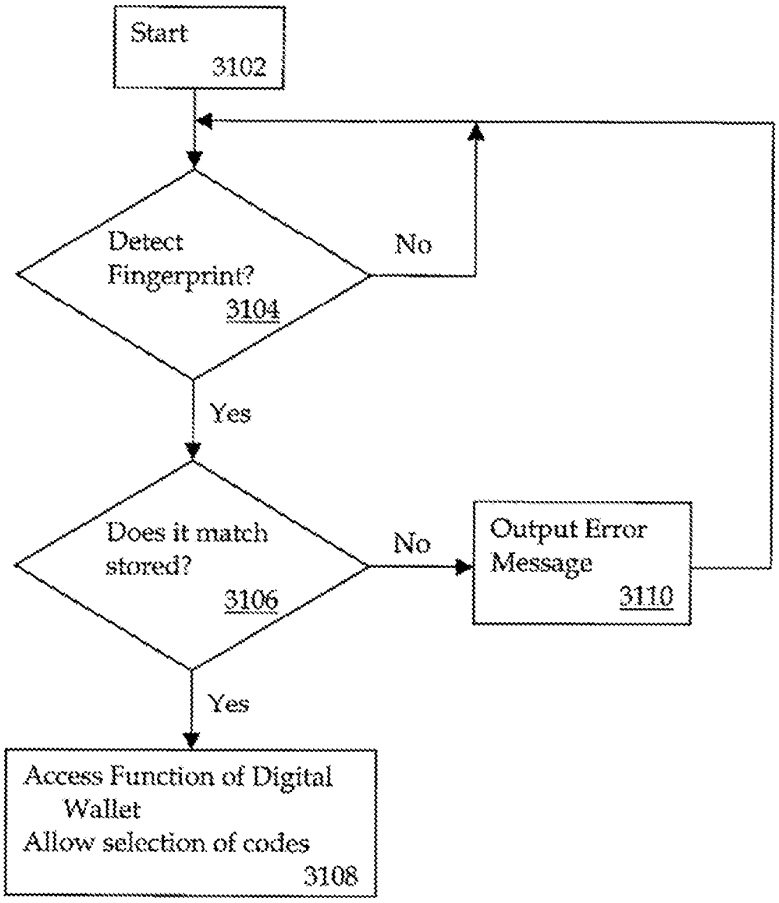


FIG. 31

Ex. 1005 at Fig. 31. As can be seen in the flow chart, 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. *Id.* at 39:47-59.

B. SNQ 2: Ludtke in combination with Okereke and Robinson Renders Claims 3, 10, and 13 of the '730 Patent Obvious

1. The Proposed Combination

(a) The Prior Art Discloses the Claim Limitations

114. I believe the combination of Ludtke, Okereke, and Robinson renders obvious the above claims. SNQ 2 relies entirely on Ludtke and Okereke for the same reasons as I outline in SNQ 1, but also relies on Robinson for the limitations in dependent claims 3, 10, and 13. All three of these dependent claims involve registering an age verification. Where Ludtke and Okereke do not explicitly disclose registering an age verification, Robinson discloses the age verification in claims 3, 10, and 13. As I explain below, a POSITA would be motivated to combine the age verification disclosed in Robinson with the system disclosed in Ludtke with the secret information and unique device ID disclosed in Okereke.

(b) POSITA Would have been Motivated to Combine Robinson with Ludtke and Okereke

115. In my opinion, age verification would have been a feature a POSITA would have readily considered. Indeed, the age of a user is important in various transactions relevant to Ludtke. For example, Ludtke is expressly directed to the FeliCa Card, *see e.g.*, Ex. 1005 at 11:1-6, which, as I note above, was implemented in Hong Kong's Octopus transit card. In my opinion, a POSITA would have recognized a need for age authentication to allow preferred pricing for minors, student, and/or seniors as is often done in public transit. As such a POSITA would have been motivated to combine Robinson with Ludtke and Okereke.

116. Again, as I noted above, I also provide explanation of the specific factors that I understand are considered. For example, the scope and content of the prior art would have motivated a POSITA to combine Robinson with Ludtke and Okereke. Like both Ludtke and Okereke, Robinson discloses a way to improve security and to authenticate a user and device. Ex. 1007 at ¶¶27-29, 32, 66-67 Fig. 1.

117. Further, in my opinion, all three of the references are therefore in the same field of endeavor, with Robinson specifically teaching improving security with an additional age-based authorization factor and to authenticate a user for age-restricted access or transactions initiated by a wireless device like Ludtke's transaction device. *Id.* at ¶9-10. In my opinion, a POSITA would have recognized that the disclosure of Ludtke welcomes this modification with its stated aim to provide, for example, secure access to restricted areas. Ex. 1005 at 2:5-8, 10:24-28. Indeed, it is also my opinion that a POSITA would have recognized that the age verification disclosed in Robinson would, for example, allow a way for the Ludtke system to ensure that the user is old enough to conduct a transaction, access a specific financial system or application, or to enter a restricted area.

118. In my opinion, a POSITA would also have had a reasonable expectation of success because age verification as disclosed in Robinson is a logical extension of the type of information that is exchanged. Robinson, like Ludtke and Okereke, also discloses the use of biometric information to verify a user. Ex. 1007 at ¶39. It would be logical to modify the system of Ludtke and Okereke to also include the age of the user who was verified with biometric information. In my opinion, the age would logically be registered

at Ludtke's TPCH, where the age can also be kept confidential from third parties, consistent with Ludtke's goals.

2. Claim 3: "The method of claim 1, further comprising: registering an age verification for the user in association with the device ID code.

119. In my opinion, Ludtke in combination with Okereke disclose all of the limitations of claim 1. *See* SNQ 1, Claim 1. Section VII.A.2, *supra*.

120. However, neither Ludtke nor Okereke expressly discloses "registering an age verification for the user" as recited in this limitation. Robinson discloses that a central database 102 holds information related to users to authenticate a user's age to access an age restricted area, for example. Ex. 1007 at ¶¶27-28, 32, 66-67 Fig. 1. The central database 102 stores age verification records related to individuals seeking age verification (called "presenters"), including information such as a user's age, date of birth, government ID number, biometric template, and at least one ID number that identifies the presenter within the system. *Id.* Prior to using the age-verification system, an individual presents biometric and age-verifying information. *Id.* at ¶¶13-15. Robinson further discloses that age-verifying information is associated with at least one ID number (SID) identifying the user. *Id.* at ¶28.

3. Claim 10: "The integrated device of claim 9, wherein an age verification is registered in association with the device ID code.

121. In my opinion, Ludtke in combination with Okereke disclose all of the limitations of claim 9. *See* SNQ 1, Claim 9. Section VII.A.9, *supra*.

122. In my opinion, Robinson in combination with Ludtke and Okereke disclose all of the limitations of claim 10 for the same reasons as described in conjunction with claim 3. Section VII.B.2, *supra*.

4. Claim 13: "The method of claim 12, further comprising: registering a date of birth or age with the agent."

123. In my opinion, Ludtke in combination with Okereke disclose all of the limitations of claim 12. *See* SNQ 1, Claim 12. Section VII.A.11, *supra*.

124. In my opinion, Robinson in combination with Ludtke and Okereke disclose all of the limitations of claim 13 for the same reasons as described in conjunction with claim 3. Section VII.B.2, *supra*.

C. SNQ 3: Ludtke in combination with Scott Renders Claims 1-2, 4-9, 11-12, and 14-17 of the '730 Patent Obvious

1. The proposed combination

(a) The Prior Art Discloses the Claim Limitations

125. I believe the combination of Ludtke and Scott renders obvious the above claims. SNQ 3 relies on Ludtke as the base reference, which discloses a mobile device used for performing financial transactions. In my opinion, Ludtke discloses all of the limitations in claims 1-2, 4-9, 11-12, and 14-17 except the "unique Device ID" and storage of "secret information." Specifically, Ludtke discloses the system as shown below in figure 1:

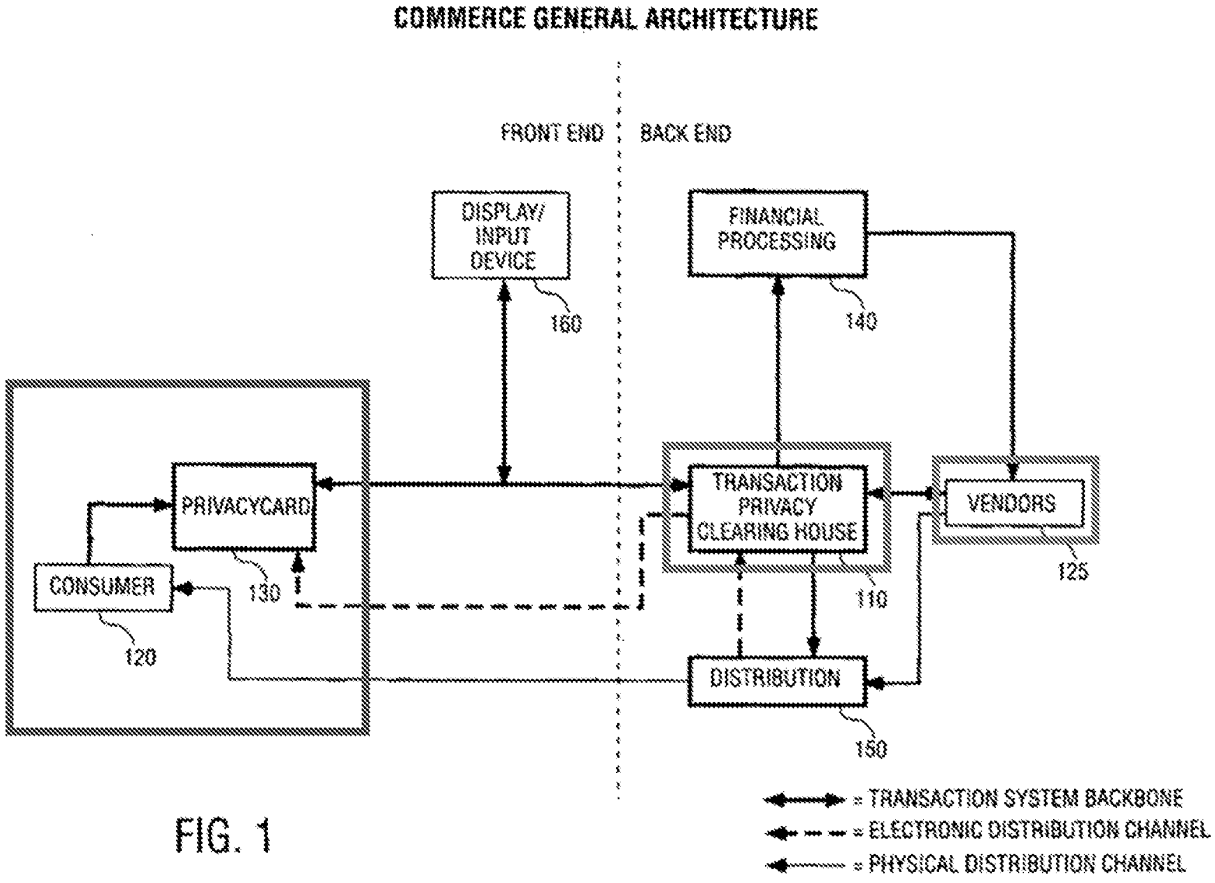


FIG. 1

Figure 1 shows one embodiment of the system in Ludtke. Ludtke discloses a "transaction device," which is seen above as the Privacy Card 130. Ex. 1005 at 6:36-44, Fig. 1. The transaction device is a device that the consumer 120 uses and includes a number of embodiments, including a privacy card, and digital wallet. *Id.* at 5:1-5, 11-14, 6:36-44. The transaction device also authorizes the consumer 120 using biometric data, including a fingerprint and other biometric information. Ludtke's transaction device includes and discloses a persistent, tamper proof storage. Ludtke also discloses the process to authenticate a financial transaction between the consumer 120 and a vendor 125. The financial transaction is authorized through the transaction privacy clearing house 110,

which is a third party, independent of the consumer 120 and the vendor 125. Ludtke emphasizes the third-party aspect of the transaction privacy clearing house 110 because the third party ensures that private information is not exchanged between the consumer 120 and the vendor 125. *Id.* at 6:45-49, 29:43-53.

126. The claims require storage of "secret information" in the user's device. Although Ludtke does not explicitly disclose this "secret information," it does disclose (1) a storage location for this information, (*id.* at 10:46-49, 24:61-65), as well as (2) the importance of maintaining the confidentiality of private information (*id.* at 3:45-47; 5:30-31, 6:45-49). In my opinion, Scott discloses this "secret information." Specifically, Scott includes an extensive discussion regarding a secret key infrastructure. Scott discloses that the device's memory 20 also stores a private key unique to each device and used for encryption, which can be "set into memory by the manufacturer." Ex. 1008 at 11:24-30, 28:13-15, 4:14-18. Scott discloses that this "private key" used by the PID 6 is never disclosed. *Id.* at 8:21-22.

127. The claims also require an "ID code" that is unique and identifies the user's device that is communicated to the third party trusted authority for authorization of the device. Ludtke discloses "transaction device information" that is communicated from the consumer's transaction device 130 to the transaction privacy clearing house 110 for authorization, but Ludtke does not explicitly indicate that this "transaction device information" is a unique code identifying the consumer's transaction device. Scott, however, does disclose an ID code that uniquely identifies the PID 6. *Id.* at 4:9-10 ("The

memory can further 10 store an ID code indicative of the enrolled person or the device."), 8:13-22, 11:14-20. Specifically, memory 20 stores information "specific to processing unit 16," including an ID code unique to the device, which may be set by the device manufacturer and can be the device serial number. *Id.* at 11:11-13. In my opinion, a serial number is a unique code that identifies the device it is attached to. Scott also discloses wherein the PID 6 stores other data values such as "a synchronization counter associated with the user device." *Id.* at 6:28-7:23, 13:10-15, 19:30-32.

(a) POSITA Would be Motivated to Combine Ludtke and Scott

128. In my opinion, a POSITA would have been motivated to combine Ludtke and Scott. As I note above, the Ludtke reference meets most of the limitations of the claims of the '730 Patent with the exception of the "unique Device ID" and storage of "secret information" limitations. Instead Ludtke discusses using "transaction device information" as part of the described encrypted transaction without explaining how to implement such information. In my opinion, a POSITA would naturally have turned to a similar implementation which provides detailed instructions, particularly one implementing a well-known solution, such as public key cryptography. As I describe below, Scott describes a similar implementation in detail and describes public key cryptography, *see* Ex. 1008 at 4:6-8.

129. Again, as I noted above, I also provide explanation of the specific factors that I understand are considered. The scope and content of the prior art would have motivated a POSITA to combine Ludtke and Okereke. As I note above, Ludtke discloses almost all of

the limitations of the claims except for "secret information" and the "unique" nature of a device ID code. Similar to Ludtke, Scott discloses authenticating a user using a "personal identification device" (PID) for protected applications such as opening a hotel room door or a conducting a point-of-sale transaction. *Id.* at 8:5-12. Scott specifically describes a system for authentication of a mobile device to protect information for financial transactions. *Id.* at 2:5-16.

130. In my opinion, Ludtke discloses a persistent, tamper proof memory, and a POSITA would have been motivated to combine the secret key disclosed in Scott with the system disclosed in Ludtke. The secret key infrastructure disclosed in Scott is similar to that disclosed in Okereke, as discussed above. As I note above, a POSITA would have already known, as of the priority date of the '730 patent, that encryption using a secret key such as that disclosed in Scott would have been obvious when communicating confidential information. In my opinion, a POSITA would have specifically recognized the importance of encrypted communication when engaging in communications regarding financial information and especially when authenticating financial transactions. The use of secret information (such as that in PKI encryption) to perform this type of encryption was well-known ***long*** before the filing date of the '730 patent, and was a well-established, well-known method for implementing encryption. *Id.* For example, public key encryption was developed in the 1970s, and serves as a well-known way to encrypt and authenticate secret or confidential information. In my opinion, a POSITA would have recognized that such encryption is important to many applications, including financial information where it is

particularly important to keep the information secret. A POSITA would therefore recognize that the use of secret information, which is disclosed in Scott, would make the system of Ludtke even more secure. In my opinion, Scott demonstrates this knowledge prior to the '730 patent's priority date.

131. Ludtke discloses transaction device information communicated between the transaction device and the transaction privacy clearing house for authorization of a financial transaction. A POSITA would have combined the teachings of Scott's unique Device ID with Ludtke's system. As discussed above, Ludtke explicitly teaches communication of "transaction device information" with the TPCH. Ex. 1005 at 6:38-51. In my opinion, a POSITA would have recognized that such transaction device information necessarily includes unique device identifiers such as a serial number or other number that is specific to the processing unit. Scott explicitly discloses this fundamental information. Ex. 1008 at 8:20-23.

132. In my opinion, a POSITA would have been motivated to combine Ludtke and Scott because they are both in the same field of endeavor. Indeed, both references are in the same field of endeavor as the '730 patent, *i.e.*, authentication of a device, including use of biometric information, for the purpose of exchanging sensitive information over a network. *See* Ex. 1001 at 1:15-18 ("The present invention relates generally to computerized authentication, and more specifically, to an authentication responsive to biometric verification of a user being authenticated"); Ex. 1005 at Abstract ("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"); Ex. 1008 at Abstract ("A portable, hand-held personal identification device (6) and method for providing secure access to a host facility…"); *id.* at 1:16-18 ("Where absolute security is essential, some host facilities employ a biometric sensor to measure a biometric trait of a person requesting access to the host facility").

133. In my opinion, a POSITA would have reasonably expected the combination of Ludtke and Scott to succeed and yield predictable results. Ludtke's system already discloses a persistent and tamper-proof memory and discusses the use of sensitive information. Ludtke also discloses transaction device information. Ex. 1005 at 6:38-51. Scott similarly discloses a persistent, tamper-proof memory. Scott teaches that data is stored in a memory where, after biometric enrollment, "there is no going back or editing." Ex. 1008 at 16:11-12. Given these disclosures, a POSITA would have expected the combination to result in Ludtke's financial system storing the secret information in Ludtke's memory and using the unique device ID disclosed in Scott as the transaction device information. In my opinion, a POSITA would have expected this to yield the predictable result of the option to use secret key encryption and decryption with a private key (secret information), as well as the ability to ensure authentication of an authorized device using unique device identifying information such as a serial number, and would have expected this combination to succeed.

134. For example, Ludtke describes a protected memory to keep the type of important and sensitive information described in Okereke. Ex. 1005 at 19:37-40.

Moreover, in my opinion, a POSITA would be familiar with the secret key encryption system because it had long been used as a way to encrypt and decrypt information and share such information only for authorized users. §IV.A *supra*. Implementing such a system with Ludtke would have been logical and obvious to a POSITA. Finally, both systems have similar types of mobile devices, and have similar goals. In my opinion, it would make sense to a POSITA to use the type of information identified in Scott in the Ludtke system to further complement Ludtke's features.

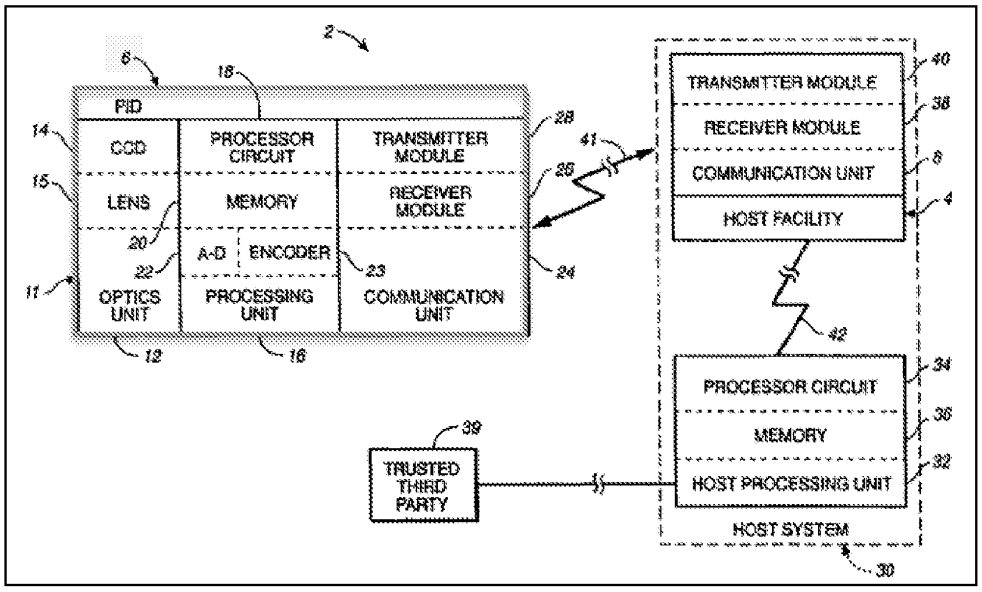
2. Claim 1 of the '730 Patent

(a) [1a] "A method for verifying a user during authentication of an integrated device, comprising the steps of:"

135. In my opinion, the disclosure of Ludtke for this limitation is described above in SNQ 1. Section VII.A.2.a, *supra*.

136. As I explain above in detail, a POSITA would be motivated to combine the disclosure of Ludtke with the disclosure in Scott.

137. Scott also discloses a method for verifying a user during authentication of an integrated device (*e.g.*, personal identification device ("PID") 6), in order to, for example, provide secure access to protected resources such as a hotel room or a point-of-sale transaction. Ex. 1008 at Abstract, 2:5-23, 4:22-5:9, 7:24-8:12; *see* claims [1A]-[1H] *infra*.



Ex. 1008 at Fig. 1.

(b) [1b] "persistently storing biometric data of the user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered wherein the biometric data is selected from a group consisting of a palm print a retinal scan, an iris scan, a hand geometry, a facial recognition and a voice recognition;"

138. In my opinion, the disclosure of Ludtke for this limitation is described above in SNQ 1. Section VII.A.2.b, *supra*.

139. ***Persistently storing . . . a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered***: As explained above, Scott discloses that the memory 20 of the PID 6 persistently stores a plurality of codes and other data values including an

ID code that uniquely identifies the PID 6. Ex. 1008 at 4:9-10 ("The memory can further store an ID code indicative of the enrolled person or the device."), 8:13-22, 11:14-20. Specifically, memory 20 stores information "specific to processing unit 16," including an ID code unique to the device, which may be set by the device manufacturer and can be the device serial number. *Id.* at 11:11-13. In my opinion, a serial number is a unique code that identifies the device it is attached to. Scott also discloses wherein the PID 6 stores other data values such as "a synchronization counter associated with the user device." *Id.* at 6:28-7:23, 13:10-15, 19:30-32

140. In my opinion, Scott also discloses a "secret decryption value." Specifically, Scott discloses that the device's memory 20 also stores a private key unique to each device and used for encryption, which can be "set into memory by the manufacturer." *Id.* at 11:24-30, 28:13-15, 4:14-18. Scott also discloses that the private key used by the PID 6 is never disclosed. *Id.* at 8:21-22. The PID 6 uses its private key to encrypt a transmission to a host system. *Id.* at 17:9-12. The host system uses a corresponding public key to decrypt the transmission. *Id.* Thus, in my opinion, a POSITA would recognize the benefits of increased security and privacy by using the private/public key pair to protect all transmissions between PID 6 and host facility 4. Scott's PID 6 would thus use its private key to decrypt messages such as, for example, a random number signal for verification (*id.* at 17:32-18:2, 27:4-17), that were encrypted with the corresponding public key at the host system.

141. As I discuss above, a POSITA would have been motivated to modify the system of Ludtke to incorporate the public/private key structure of Scott and the unique serial numbers also disclosed in Scott. In my opinion, a POSITA would have been motivated to store permanent information, such as the secret key (private key) and unique device identifiers (serial number). Moreover, a POSITA would have recognized that the "transaction device information" disclosed within Ludtke could further include the unique device information in Scott, which would ensure that the information used to authenticate the device only identifies the authorized device. In my opinion, a POSITA would also store the unique device identifiers and the secret key in the persistent tamper-proof memory, because this is important information that allows authorization and sensitive communications to take place, and a POSITA would recognize the need to take care to ensure it is not easy to tamper with and modify the information.

(c) [1c] responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan

142. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VII.A.2.c, *supra*.

(d) [1d] comparing the scan data to the biometric data to determine whether the scan data matches the biometric data

143. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VII.A.2.d, *supra*.

(e) [1e] responsive to a determination that the scan data matches the biometric data, wirelessly sending one or more codes from the plurality of codes and the other data values for

authentication by an agent that is a third party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, wherein the one or more codes and other data values includes the device ID code; and

144. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VII.A.2.e, *supra*.

145. ***Device ID Code***: Ludtke does not describe the specific "transaction device information" that is provided to the TPCH 110 and that is maintained in a secure database by the TPCH 110. Ex. 1005 at 6:41-125. However, as I discuss above, a POSITA would be motivated to combine Ludtke with the teachings of Scott, and would recognize that the "transaction device information" would include a device serial code which uniquely identify the integrated device. Ex. 1008 at 4:1-14, 5:10-21.

(f) [1f] responsive to authentication of the one or more codes and the other data values by the agent, receiving an access message from the agent allowing user access to an application, where the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.

146. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VII.A.2.f, *supra*.

3. Claim 2: "The method of claim 1, wherein the one or more codes and the other data values are transmitted to the agent over a network."

147. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VII.A.3, *supra*.

4. Claim 4: "The method of claim 1, wherein the one or more codes and the other data values indicate that the biometric verification was successful."

148. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VII.A.4, *supra*.

5. Claim 5: "The method of claim 1, wherein the biometric data and the scan data are both based on a fingerprint scan by the user."

149. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VII.A.5, *supra*.

6. Claim 6: "The method of claim 1, further comprising: establishing a secure connection channel prior to sending the one or more codes and other data values for authentication"

150. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VII.A.6, *supra*.

7. Claim 7: "The method of claim 1, further comprising: receiving a request for the one or more codes and the other data values without a request for biometric information; and responsive to receiving the request for the one or more codes and the other data values without a request for biometric information, sending the one or more codes and the other data values without requesting the scan data."

151. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VII.A.7, *supra*.

8. Claim 8:

(a) [8a] "An integrated device for verifying a user during authentication of the integrated device, comprising."

152. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VII.A.8.a, *supra*.

153. In my opinion, Ludtke and Scott disclose this limitation. *See* Claim Element [1a], Section VII.C.2.a, *supra*

(b) [8b] "a memory stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to the memory that is unable to be subsequently altered; wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;"

154. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VII.A.8.b, *supra*.

155. In my opinion, Ludtke and Scott disclose this limitation. *See* Claim Element [1b], Section VII.C.2.b, *supra*

(c) [8c] "a verification unit, in communication with the memory, receives scan data from a biometric scan for comparison against the biometric data, and if the scan data matches the biometric data, wirelessly sends one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, wherein the one or more codes and other data values includes the device ID code; and

156. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VII.A.8.c, *supra*.

157. In my opinion, Ludtke and Scott disclose this limitation. *See* Claim Elements [1c-1e], Sections VII.C.2.c-e, *supra*

(d) [8d] responsive to the agent authenticating the one or more codes and the other data values, a radio frequency

communicator, receives an access message from the agent allowing the user access to an application, wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.

158. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VII.A.8.d, *supra*.

159. In my opinion, Ludtke and Scott disclose this limitation. *See* Claim Element [1f], Section VII.C.2.f, *supra.*

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

160. *See* Claim 2. Section VII.C.3, *supra.*

10. Claim 11: "The integrated device of claim 8, wherein the verifier comprises: an LED to be activated for requesting the biometric scan."

161. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VII.A.8.10, *supra*.

11. Claim 12

(a) [12a]. "A method for authenticating a verified user using a computer processor configured to execute method steps, including:"

162. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VII.A.11.a, *supra*.

163. In my opinion, Ludtke and Scott disclose this limitation. *See* Claim Element [1a], Section VII.C.2.a, *supra*

(b) [12b]. "receiving one or more codes from a plurality of codes and other data values including a device ID code, wherein the plurality of codes and the other data values comprises the device ID code uniquely identifying the integrated device and a secret decryption value associated with a biometrically verified user, the device ID code being registered with an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices"

164. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VII.A.11.b, *supra*.

165. In my opinion, Ludtke and Scott disclose this limitation. *See* Claim Elements [1b], [1e], Section VII.C.2.b, VII.A.2.e, *supra*

(c) [12c] "requesting authentication of the one or more codes and the other data values by the agent, wherein the authentication determines whether the one or more codes and the other data values are-legitimate;"

166. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VII.A.11.c, *supra*.

167. In my opinion, Ludtke and Scott disclose this limitation. *See* Claim Element [1e], Section VII.C.2.e, *supra*

(d) [12d] "receiving an access message from the agent; and"

168. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VII.A.11.d, *supra*.

169. In my opinion, Ludtke and Scott disclose this limitation. *See* Claim Element [1f], Section VII.C.2.f, *supra*

(e) [12e] "in response to a positive access message, allowing the biometrically verified user access to an application, wherein

the application is selected from a group consisting of a casino machine , a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a website and a file."

170. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VII.A.11.e, *supra*.

171. In my opinion, Ludtke and Scott disclose this limitation. *See* Claim Element [1f], Section VII.C.2.f, *supra.*

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

172. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VII.A.12, *supra*.

13. Claim 15

(a) [15a] "a system, comprising:"

173. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VII.A.13.a, *supra*.

(b) [15b] "a biometric key stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the biometric key and a secret decryption value in a tamper proof format written to a storage element on the biometric key that is unable to be subsequently altered,"

174. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VII.A.13.b, *supra*.

175. In my opinion, Ludtke and Scott disclose this limitation. *See* Claim Element [1b], Section VII.C.2.b, *supra*.

(c) [15c]: "and if scan data can be verified as being from the user by comparing the scan data to the biometric data, wirelessly sending, one or more codes from the plurality of codes and other data values wherein the one or more codes and other data values include the device ID code, and the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition, and a voice recognition; and"

176. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VII.A.13.c, *supra*.

177. In my opinion, Ludtke and Scott disclose this limitation. *See* Claim Elements [1b], [1d], and [1e], Section VII.C.2.b, d, e, *supra*.

(d) [15d]: "an authentication unit receives the plurality of codes and the other data values and send[] the plurality of codes and the other data values to agent for authentication to determine whether the one or more codes and the other data values are legitimate, wherein the agent is a third party trusted authority possessing a list of device ID codes uniquely identifying integrated devices,"

178. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VII.A.13.d, *supra*.

179. In my opinion, Ludtke and Scott disclose this limitation. *See* Claim Element [1e], Section VII.C.2.e, *supra.*

(e) [15e]: "and responsive to the device ID code being authenticated, the authentication unit receiving an access message from the agent allowing the user to access an application, wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door

opener, an ATM machine, a hard drive, computer software, a web site, and a file."

180. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VII.A.13.e, *supra*.

181. In my opinion, Ludtke and Scott disclose this limitation. *See* Claim Element [1f], Section VII.C.2.f, *supra.*

14. Claim 16: "The system of claim 15, wherein the biometric key receives an authentication request from the authentication unit, and in response, requests a biometric scan from the user to generate the scan data."

182. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VII.A.14, *supra*.

183. In my opinion, Ludtke and Scott disclose this limitation. *See* Claim element [1c], Section VII.C.2.c, *supra.*

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

184. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VII.A.15, *supra*.

D. SNQ 4: Ludtke in combination with Scott and Robinson Renders Claims 3, 10, and 13 of the '730 Patent Obvious

1. The Proposed Combination

(a) The Prior Art Discloses the Claim Limitations

185. I believe the combination of Ludtke, Scott, and Robinson renders obvious the above claims. SNQ 4 relies entirely on Ludtke and Scott for the same reasons as outlined

in SNQ 3, but also relies on Robinson for the limitations in dependent claims 3, 10, and 13. All three of these dependent claims involve registering an age verification. Where Ludtke and Scott do not explicitly disclose registering an age verification, Robinson discloses the age verification in claims 3, 10, and 13. As I note below, a POSITA would be motivated to combine the age verification disclosed in Robinson with the system disclosed in Ludtke with the secret information and unique device ID disclosed in Scott.

(b) POSITA Would have been Motivated to Combine Robinson with Ludtke and Scott

186. In my opinion, age verification would have been a feature a POSITA would have readily considered. Indeed, the age of a user is important in various transactions relevant to Ludtke. For example, Ludtke is expressly directed to the FeliCa Card, *see e.g.*, Ex. 1005 at 11:1-6, which, as I note above, was implemented in Hong Kong's Octopus transit card. In my opinion, a POSITA would have recognized a need for age authentication to allow preferred pricing for minors, students, and/or seniors as is often done in public transit. As such a POSITA would have been motivated to combine Robinson with Ludtke and Scott.

187. Again, as I noted above, I also provide explanations of the specific factors that I understand are considered. The scope and content of the prior art would have motivated POSITA to combine Robinson with Ludtke and Scott. Like both Ludtke and Scott, Robinson discloses a way to improve security and to authenticate a user and device. Ex. 1007 at ¶¶27-29, 32, 66-67 Fig. 1.

188. All three of the references are therefore in the same field of endeavor, with Robinson specifically teaching improving security with an additional age-based authorization factor and to authenticate a user for age-restricted access or transactions initiated by a wireless device like Ludtke's transaction device. *Id.* at ¶9-10. In my opinion, a POSITA would have recognized that the disclosure of Ludtke welcomes this modification with its stated aim to provide, for example, secure access to restricted areas. Ex. 1005 at 2:5-8, 10:24-28. Indeed, in my opinion, a POSITA would have recognized that the age verification disclosed in Robinson would, for example, allow a way for the Ludtke system to ensure that the user is old enough to conduct a transaction, access a specific financial system or application, or to enter a restricted area.

189. In my opinion, a POSITA would also have had a reasonable expectation of success because age verification as disclosed in Robinson is a logical extension of the type of information that is exchanged. Robinson, like Ludtke and Scott, also discloses the use of biometric information to verify a user. Ex. 1007 at ¶39. It would be logical to modify the system of Ludtke and Scott to also include the age of the user who was verified with biometric information. The age would logically be registered at Ludtke's TPCH, where the age can also be kept confidential from third parties, consistent with Ludtke's goals.

2. Claim 3: "The method of claim 1, further comprising: registering an age verification for the user in association with the device ID code.

190. Ludtke in combination with Scott disclose all of the limitations of claim 1. *See* SNQ 3, Claim 1. Section VII.C.2, *supra*.

191. However, neither Ludtke nor Scott expressly disclose "registering an age verification for the user" as recited in this limitation. Robinson discloses this limitation as described in SNQ 2. *See* Section VII.B.2, *supra*.

3. Claim 10: "The integrated device of claim 9, wherein an age verification is registered in association with the device ID code.

192. Ludtke in combination with Scott disclose all of the limitations of claim 9. *See* SNQ 3, Claim 9. Section VII.C.9, *supra*.

193. In my opinion, Robinson in combination with Ludtke and Okereke disclose all of the limitations of claim 10 for the same reasons as described in conjunction with claim 3. Section VII.D.2, *supra*.

4. Claim 13: "The method of claim 12, further comprising: registering a date of birth or age with the agent."

194. Ludtke in combination with Scott disclose all of the limitations of claim 9. *See* SNQ 3, Claim 12. Section VII.C.11, *supra*.

195. In my opinion, Robinson in combination with Ludtke and Okereke disclose all of the limitations of claim 13 for the same reasons as described in conjunction with claim 3. Section VII.D.2, *supra*.

VII. '905 PATENT

A. SNQ 1: Ludtke in combination with Okereke Renders Claims 1, 3-10, and 12-18 of the '905 Patent Obvious

1. The Proposed Combination

(a) The Prior Art Discloses the Claim Limitations

196. I believe the combination of Ludtke and Okereke renders obvious the above claims. SNQ 1 relies on Ludtke as the base reference, which discloses a mobile device used for performing financial transactions. Ludtke discloses all of the limitations in claims 1, 3-10, and 12-18 except the "unique Device ID" and storage of "secret information." Specifically, Ludtke discloses the system as shown below in figure 1:

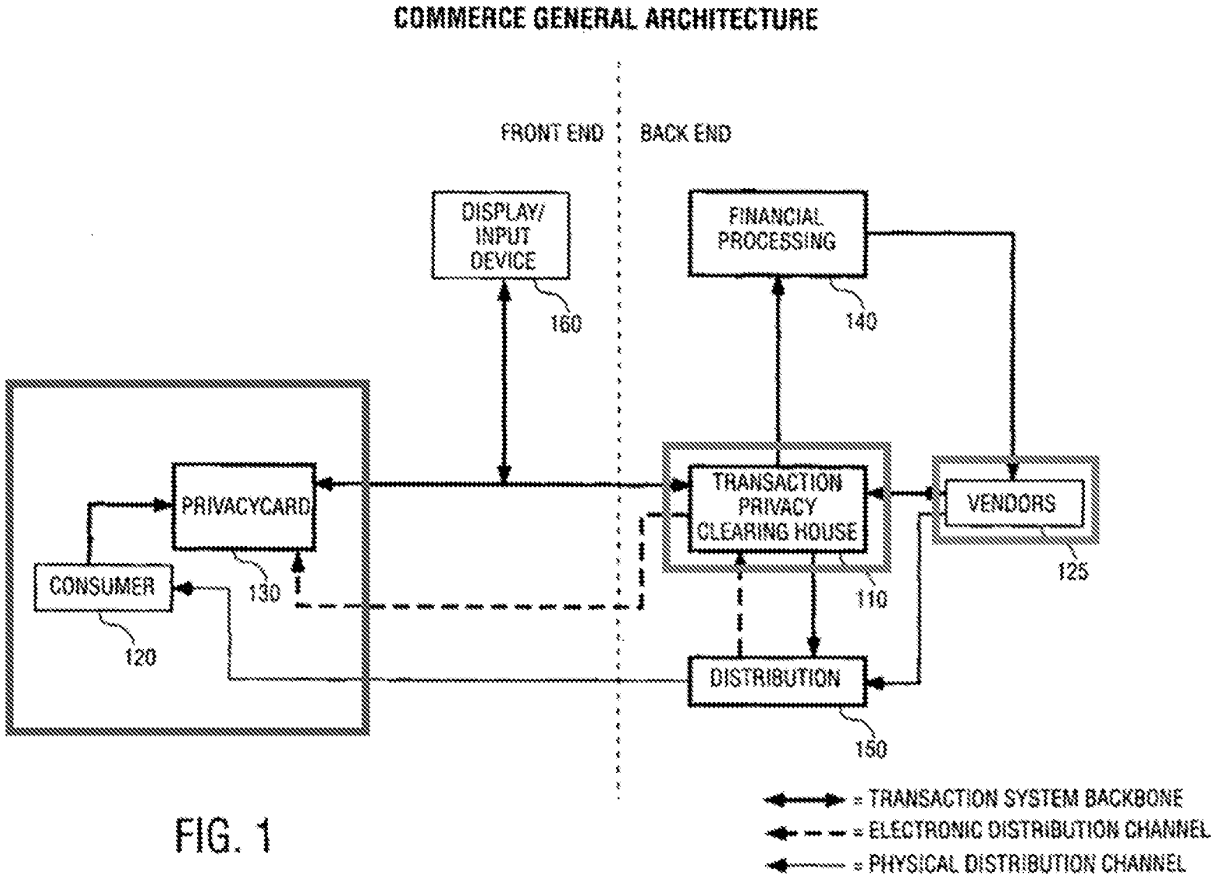


FIG. 1

Figure 1 shows one embodiment of the system in Ludtke. Ludtke discloses a "transaction device," which is seen above as the Privacy Card 130. Ex. 1005 at 6:36-44, Fig. 1. The transaction device is a device that the consumer 120 uses and includes a number of embodiments, including a privacy card, and digital wallet. *Id.* at 5:1-5, 11-14, 6:36-44. The transaction device also authorizes the consumer 120 using biometric data, including a fingerprint and other biometric information. Ludtke's transaction device includes and discloses a persistent, tamper proof storage. Ludtke also discloses the process to authenticate a financial transaction between the consumer 120 and a vendor 125. The financial transaction is authorized through the transaction privacy clearing house 110,

which is a third party, independent of the consumer 120 and the vendor 125. Ludtke emphasizes the third-party aspect of the transaction privacy clearing house 110 because the third party ensures that private information is not exchanged between the consumer 120 and the vendor 125. *Id.* at 6:45-49, 29:43-53.

197. The claims require storage of "secret information" in the user's device. Although Ludtke does not explicitly disclose this "secret information," it does disclose (1) a storage location for this information, (*id.* at 10:46-49, 24:61-65), as well as (2) the importance of maintaining the confidentiality of private information (*id.* at 3:45-47; 5:30-31, 6:45-49). Okereke discloses this "secret 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. Ex. 1006 at ¶25.

198. The claims also require an "ID code" that is unique and identifies the user's device ("a unique code identifying a device") that is communicated to the third party trusted authority for authorization of the device. Ludtke discloses "transaction device information" that is communicated from the consumer's transaction device 130 to the transaction privacy clearing house 110 for authorization, but Ludtke does not explicitly indicate that this "transaction device information" is a unique code identifying the consumer's transaction device. Okereke, however, does disclose this unique device ID code information, in the form of a unique serial number or SIM number for the user device. *Id.*

(b) A POSITA Would Have Been Motivated to Combine Ludtke and Okereke

199. In my opinion, not only would a POSITA have been motivated to combine Ludtke and Okereke, a POSITA implementing Ludtke would have most likely done so according to Okereke. Such an implementation would have resulted in a product that meets all the limitations I discuss below. As I note above, the Ludtke reference meets most of the limitations of the claims of the '905 Patent with the exception of the "unique Device ID" limitations. Instead Ludtke discusses using "transaction device information" as part of the described encrypted transaction without explaining how to implement such information. In my opinion, a POSITA would naturally have used public key cryptography to fill in this gap. As I describe above, public key cryptography is the standard for encrypted transactions and as such it would have been natural for a POSITA to implement it were a reference in this field not to provide detailed instructions. Okereke would have been a natural choice as it is an implementation of public key cryptography itself. *See* Ex. 1006 at Abstract.

200. In my opinion, the scope and content of the prior art would have motivated POSITA to combine Ludtke and Okereke. As explained above, in my opinion, Ludtke discloses almost all of the limitations of the claims except for "secret information" and the "unique" nature of a device ID.

201. In my opinion, Ludtke discloses a persistent, tamper-proof memory, and a POSITA would have been motivated to combine the secret key disclosed in Okereke with the system disclosed in Ludtke. In my opinion, a POSITA would have already known, as

of the priority date of the '905 patent, that encryption using a secret key such as that as part of a PKI would have been obvious when communicating confidential information.

202. In my opinion, a POSITA would have specifically recognized the importance of encrypted communication when engaging in communications regarding financial information and especially when authenticating financial transactions. The use of secret information to perform this type of encryption was well-known ***decades*** before the filing date of the '905 patent, and was a well-established, well-known method for implementing encryption. Public key encryption was developed in the 1970s, and serves as a well-known way to encrypt and authenticate secret or confidential information. In my opinion, a POSITA would have recognized that such encryption is important to many applications, including financial information where it is particularly important to keep the information secret. A POSITA would therefore recognize that the use of PKI encryption, which is disclosed in Okereke, would make the system of Ludtke even more secure. Okereke simply demonstrates this knowledge prior to the '905 patent's priority date.

203. Ludtke discloses transaction device information communicated between the transaction device and the transaction privacy clearing house for authorization of a financial transaction. POSITA would have combined the teachings of Okereke's unique Device ID with Ludtke's system. As discussed above, Ludtke explicitly teaches communication of "transaction device information" with the TPCH. Ex. 1005 at 6:38-51. A POSITA would have recognized that such transaction device information necessarily

includes unique device identifiers such as a serial number or a SIM. Okereke explicitly discloses this fundamental information. Ex. 1006 at ¶25.

204. In my opinion, a POSITA would have been motivated to combine Ludtke and Okereke because they are both in the same field of endeavor. Indeed, both references are in the same field of endeavor as the '905 patent, *i.e.*, authentication of a user and device, including use of biometric information, for the purpose of exchanging sensitive information over a network. *See* Ex. 1001 at 1:21-24 ("The present invention relates generally to computerized authentication, and more specifically, to an authentication responsive to biometric verification of a user being authenticated"); Ex. 1005 at Abstract ("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"); Ex. 1006 at Title ("System and method for secure wireless communication using PKI"); *id.* ¶31 ("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 password or biometric signature.").

205. In my opinion, a POSITA would also have reasonably expected the combination of Ludtke and Okereke to succeed and yield predictable results. Ludtke's system already discloses a persistent and tamper-proof memory and discusses the use of sensitive information. Ludtke also discloses transaction device information. Ex. 1005 at 6:38-51. Given this disclosure in Ludtke, a POSITA would have expected the combination to result in Ludtke's financial system storing the secret information in Ludtke's memory and using the unique device ID disclosed in Okereke as the transaction device information.

In my opinion, a 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 authorized device using unique device identifying information such as a serial number or SIM, and would have expected this combination to succeed.

206. For example, in my opinion, Ludtke describes a protected memory to keep the type of important and sensitive information described in Okereke. Ex. 1005 at 19:37-40. Moreover, a POSITA would be familiar with the PKI-compliant encryption system because it had long been used as a way to encrypt and decrypt information and share such information only for authorized users. §IV.A *supra*. In my opinion, implementing such a system with Ludtke would have been logical and obvious to a POSITA. Finally, both systems have similar types of mobile devices, and have similar goals. It would make sense to a POSITA to use the type of information identified in Okereke in the Ludtke system to further complement Ludtke's features.

2. Claim 1 of the '905 Patent

(a) [1a] "A method comprising: persistently storing biometric data of a legitimate user and an ID code on an integrated device"

207. In my opinion, Ludtke and Okereke disclose this limitation.

208. ***An integrated device, biometric data, and an ID code***: In my opinion, Ludtke discloses an integrated device, *e.g.*, Ludtke's "transaction device. Ex. 1005 at 3:34-5. Ludtke's transaction device provides a number of different "integrated" functions,

including maintaining bills and bill paying on the device (*id.* at 4:4-6), online shopping (*id.* at 4:7-35), and downloading and accessing electronic catalogs (*id.* at 4:36-39). The transaction device includes a number of hardware options such as a magnetic stripe generator (*id.* at 3:49-51), a screen (*id.* at 55-57), and a bar code reader (*id.* at 3:61-63).

209. For example, in my opinion, Ludtke explains that the "transaction device enhances security by ***authenticating the user of the card prior to usage***…" *Id.* at 4:62-65. This authentication can be performed by PIN code entry, or by other technologies such as a biometric solution. *Id.* at 4:65-5:1.

210. Further, in my opinion, Ludtke also specifically discloses authentication of a device through the use of "transaction device information." *Id.* at 6:36-44. A POSITA would recognize that this transaction device information necessarily includes unique device IDs, such as serial numbers and SIMs. But this knowledge of a POSITA is further embedded within Okereke. *See* Ex. 1005 at 6:36-44, *see also* Ex. 1006 at ¶30. As explained above in detail, a POSITA would have been motivated to combine the disclosure of Ludtke with the disclosure in Okereke.

211. In my opinion, Okereke also discloses a method for verifying a user during authentication of an integrated device. Okereke discloses wireless and mobile devices which are integrated devices. Ex. 1006 at Abstract. "The wireless product 165 can be a personal digital assistant (PDA), laptop, cellular telephone or any other device capable of remote wireless communication". *Id.* at ¶25.

212. In my opinion, Okereke also specifically discloses authenticating the wireless device. Okereke describes a proxy server program awaiting initiation to establish secure wireless access capabilities. *Id.* at ¶25. When authentication is requested, "a unique identifier for the wireless product to be employed is passed as at 210 to the proxy server 125 program for authorization." *Id.* "The unique identifier can be a serial number or SIM number, for example." *Id.* In my opinion, a POSITA would recognize that a serial number or SIM number is a unique identifier of a mobile device. Indeed, it is my opinion, that once the proxy server confirms the unique identifier, it authorizes the device by sending approval to a desktop computer to make a key exchange to allow communication.

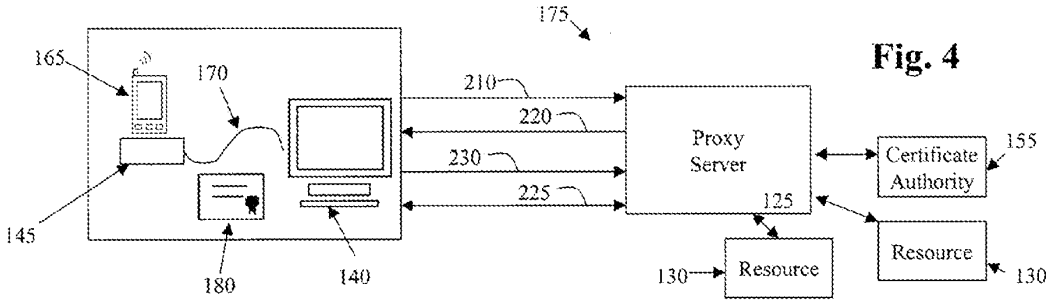


Fig. 4

213. ***Persistently storing biometric information and an ID code***: In my opinion, Ludtke discloses a persistent storage on the integrated device. Specifically, the transaction device disclosed in Ludtke includes a process to use fingerprint data (biometric data of the user) to secure the device. Indeed, it is my opinion that Ludtke describes persistently storing the fingerprint data on the integrated device:

> 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.
>
> Exhibit 1003, Page 100

Id. at 19:35-40. This fingerprint data is persistently stored in a tamper-proof format that is unable to be subsequently altered (write-once memory or other memory that is protected from accidental modification). In fact, a write-once memory will only allow writing once, therefore, the information cannot be tampered with, and cannot be modified. In each case, this memory is persistent storage, because the information stored is not easily re-writable.

(b) [1b] "responsive to receiving a request for biometric verification of a user, receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor;"

214. In my opinion, Ludtke describes receiving scan data from a biometric scan responsive to receiving a request for a biometric verification of the user. As explained above, Ludtke describes using biometric verification – including a 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:

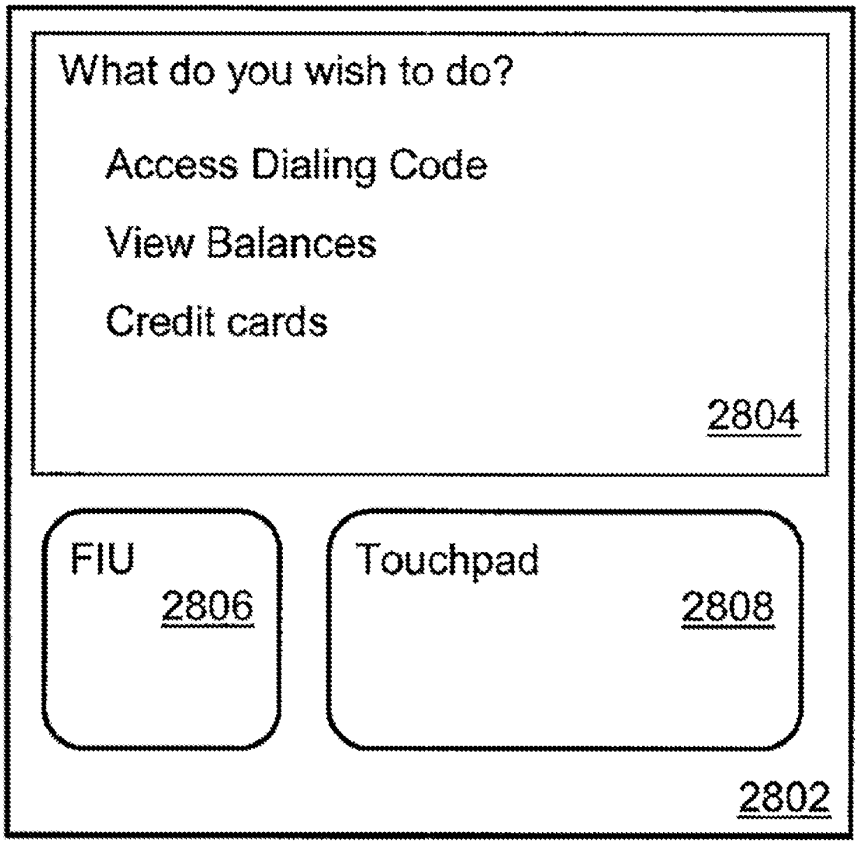


FIG. 28

Ex. 1005 at Fig. 28. "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." *Id.* at 39:24-27.

215. In my opinion, a POSITA would recognize that FIU 2806 is a "biometric sensor." Indeed, the only way the FIU would be able to detect the fingerprint – and determine the data present in the fingerprint – is if it was a fingerprint (or biometric) sensor.

216. In my opinion, Figure 31 describes the process to verify a user of the integrated device (described in this embodiment as a digital wallet):

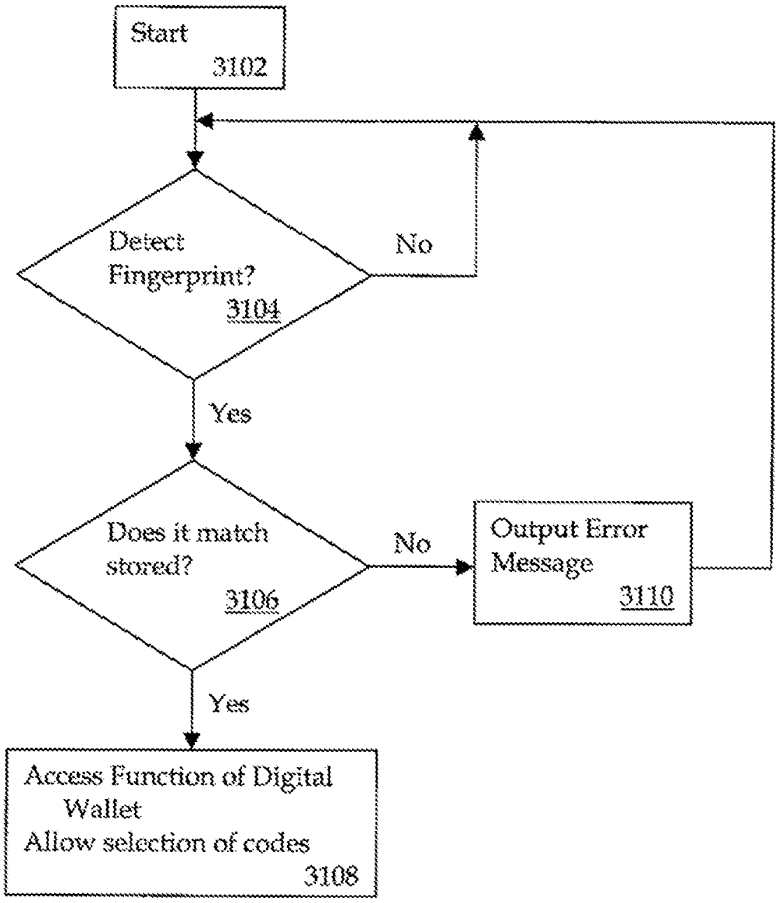


FIG. 31

Id. at Fig. 31. As can be seen in the flow chart, it is my opinion that the device is continuously looking for a request for verification ("Detect fingerprint"). In response to that request, I believe it will receive scan data from the touchpad so it can determine whether the fingerprint matches (3106). *Id.* at 39:47-59.

(c) [1c] "comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;"

217. Ludtke also shows this limitation in Figure 31:

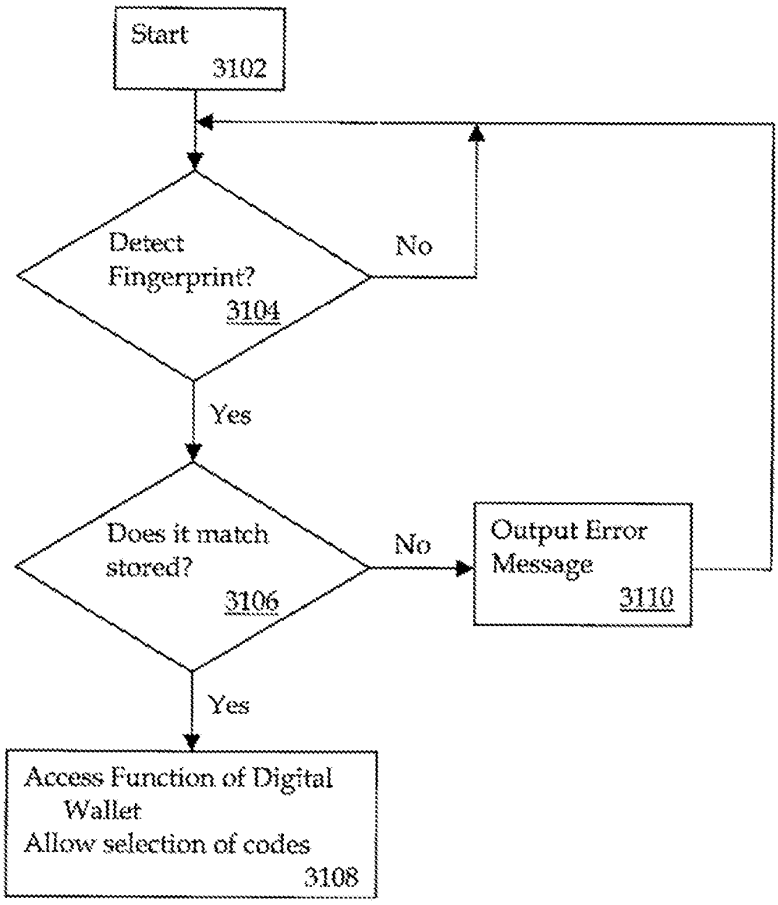


FIG. 31

Ex. 1005 at Fig. 31. In my opinion, Ludtke explains that 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 [Digital

Wallet/Integrated Device] 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." *Id.* at 39:47-54.

(d) [1d] "responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and"

218. ***Responsive to a determination that the scan data matches the biometric data***: As explained in conjunction with limitation [1c], it is my opinion that if the scanned fingerprint data matches the stored fingerprint, then access to functions of the integrated device, such as the digital wallet, is permitted. *Id.*

219. ***Third party trusted authority***: In my opinion, Ludtke describes a transaction processing [or privacy] clearing house (TCPH) which is a third party trusted authority. The TPCH "may access relevant account information to authorize transactions." *Id.* at 3:40-45. Indeed, I believe that Figure 1 of Ludtke shows how the TPCH is a third party:

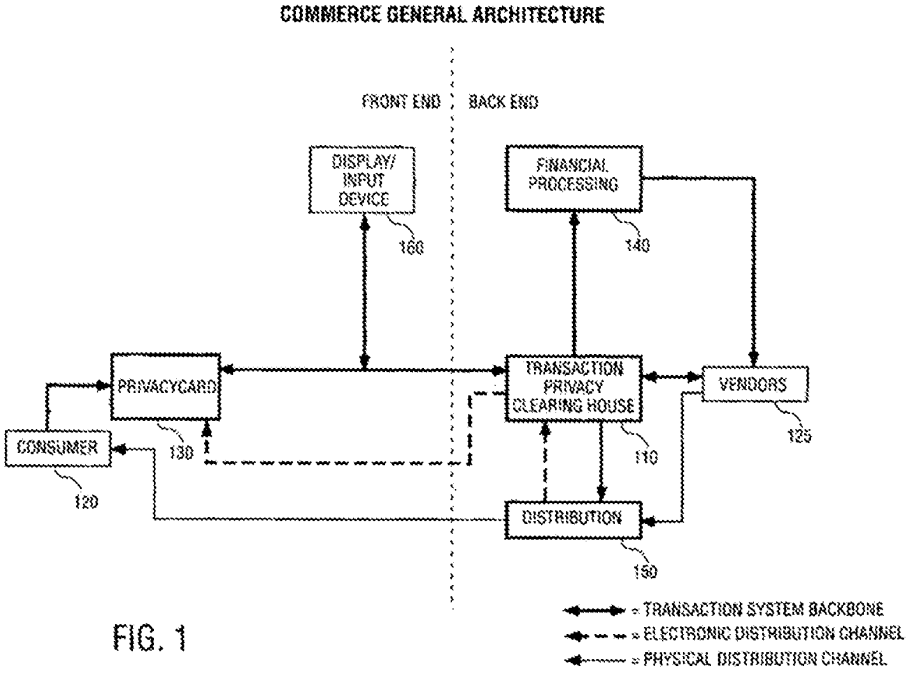


FIG. 1

Ex. 1005 at Figure 1. Figure 1 shows the commerce general architecture. *Id.* at 6:36-8:24. Figure 1 shows a consumer 120 who wishes to complete a purchase, *id.* at 6:36-64, and a vendor 125, who is selling something to the user 120. *Id.* "In this embodiment, a transaction privacy clearing house (TPCH) 110 interfaces a user 120 and a vendor 125." *Id.* at 6:36-39.

220. In my opinion, the TPCH is a third party to the transaction between the user/consumer 120 and the vendor 125. Beyond that, it is my opinion that Ludtke explains that in "one embodiment of electronic distribution, the TPCH 110 functions as the middleman of the distribution channel. This allows TPCH 110 to retain user privacy by not exposing addressing information and possibly email addresses to third parties." *Id.* at 7:44-

48. This demonstrates that the TPCH acts as a middleman to ensure that only necessary information is exchanged between the consumer 120 and the vendor 125, but is not associated with either of them.

221. In my opinion, the TPCH is also a "trusted authority." For example, in my opinion, Ludtke explains that 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." *Id.* at 6:41-44. As such, I believe that the consumer 120 and vendor 125 therefore trust the TPCH to indicate whether the transaction may be complete.

222. ***Wirelessly sending the ID code***: In my opinion, Ludtke explains that "[t]he 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." *Id.* at 6:41-44. For example, in my opinion, Ludtke also explains that "the transaction device may contain wireless data communication," and may also "closely resemble a standard credit card." *Id.* at 5:36-41. In describing the TPCH specifically, Ludtke, in my opinion indicates that a "variety of communication devices may be used, such as the Internet, direct dial-up modem connections, wireless or cellular signals, etc." *Id.* at 9:35-42.

223. ***One or more previously registered ID codes maintained by the third-party trusted authority***: In my opinion, Ludtke also explains that the "TPCH 110 maintains a secure database of transaction device information and user information. In one embodiment, the TPCH 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." *Id.* at 6:49-55. And as explained above, in my opinion, Ludtke explains that 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." *Id.* at 6:41-44. Therefore, I believe that the TPCH includes previously registered information that can be compared with information from the consumer and the consumer's device so the TPCH can determine whether the consumer 120 is authorized to complete a transaction with vendor 125. Indeed, in my opinion, the transaction device information that the TPCH compares to the received transaction device information must be stored within the TPCH as a list of codes (and specifically, a list of ID codes), in order to perform the comparison function that is disclosed. *Id.* at 30:19-27.

224. ***ID Code***: In my opinion, Ludtke does not describe the specific "transaction device information" that is provided to the TPCH 110 and that is maintained in a secure database by the TPCH 110. *Id.* at 6:41-44. However, as discussed above, I believe that a POSITA would have been motivated to combine Ludtke with the teachings of Okereke, and would have recognized that the "transaction device information" would include a unique device serial number or SIM code, both of which identify the integrated device. Ex. 1006 at ¶25.

(e) [1e] "responsive to receiving an access message from the third-party trusted authority-indicating that the third-party trusted authority successfully authenticated the ID code, allowing the user to complete a financial transaction."

225. As indicated above, in my opinion, Ludtke explains that 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." Ex. 1005 at 6:41-44. In my opinion, a POSITA would recognize that when the TPCH 110 "indicates to . . . the user 120," that indication is in the form of an access message allowing the user access to an application. In this case, in my opinion, the TPCH is allowing access to the application on the transaction device that will permit the transaction to be completed. I also believe that Ludtke further discloses this limitation at Fig. 15, Step 1520:

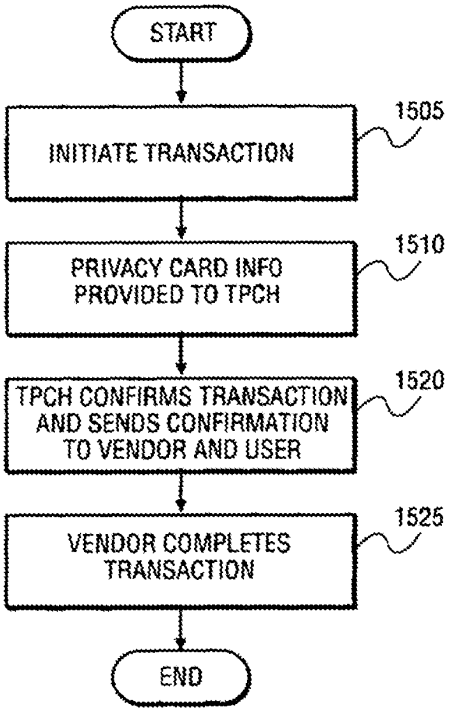


FIG. 15

Ex. 1005 at Fig. 15, *see also* Fig. 17, steps 8 and 9-1. With regard to step 1520, in my opinion, Ludtke teaches that the "TPCH, at step 1520, confirms the transaction and provides the confirmation to the vendor and the user. At step 1525, the vendor completes the transaction without the knowledge of the user." *Id.* at 27:13-16. The transaction, in my opinion, and as described in Ludtke, is a financial transaction because it is a purchase from a vendor by the user.

3. Claim 3: "The method of claim 1, wherein an indication that the biometric verification was successful is sent with the ID code."

226. In my opinion, Ludtke and Okereke disclose this limitation. As explained above, Ludtke discloses the transaction device receiving biometric information allowing access to the device and then subsequently communicates the ID code to the TPCH. It is also my opinion that it is inherent that, when the ID code is sent to the TPCH, that is an indication that the biometric verification has been successful. Indeed, as the ID code will not be sent at all if biometric verification fails (Ex. 1005 at 19:35-45), the sending of the ID code itself is an "indication that the biometric verification was successful."

4. Claim 4: "The method of claim 1, wherein the biometric data includes data from one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition."

227. In my opinion, Ludtke describes a number of different types of biometric information that may be used: "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." Ex. 1005 at 35:60-64.

5. Claim 5: "The method of claim 1, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob."

228. In my opinion, Ludtke and Okereke disclose this limitation. POSITA would recognize that the transaction device disclosed in Ludtke, which includes a number of different embodiments, including a privacy card (Ex. 1005 at 20:43-50), and a cellular telephone mechanism (*id.* at 17:3-10), would meet many of these limitations including

"mobile phone," "tablet," and "key fob." Okereke explicitly states that its device may be a mobile phone. Ex. 1006 at Abstract.

6. Claim 6: "The method of claim 1, wherein completing the financial transaction includes accessing an application."

229. In my opinion, Ludtke discloses this limitation. In Ludtke, access would be given applications of either computer software, a file (or both). It is also my opinion that in a number of embodiments, Ludtke describes the transaction device as including a "digital wallet" which a POSITA would recognize as an application and files that allow a user to digitally store credit card and other payment information and to make transactions with that card. Ex. 1005 at 5:1-5.

7. Claim 7: "The method of claim 1, wherein completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account."

230. In my opinion, Ludtke discloses this limitation. It is my opinion that in Ludtke, access would be given applications of either computer software, a file (or both). In a number of embodiments, Ludtke describes the transaction device as including a "digital wallet" which POSITA would recognize as files that allow a user to digitally store credit card and other payment information and to make transactions with that card. *Id.* Moreover, as a POSITA I recognize that giving access to the digital wallet is providing access to a financial account.

8. Claim 8: "The method of claim 1, further comprising: responsive to determining the action does not require biometric verification, receiving a request for the ID code without a request for biometric verification, and responsive to receiving the request for the ID code

without a request for biometric verification, sending the ID code for authentication without requesting the scan data."

231. In my opinion, Ludtke and Okereke disclose this limitation. For example, in my opinion, Ludtke discusses the process of requesting and receiving biometric information. *Id.* at 39:19-35. Ludtke then describes an embodiment where the biometric information is not needed: "Alternatively, the consumer access device, once the user has been identified may not require re-identification until the consumer access device is, for example, turned off." *Id.* at 39:35-38. In my opinion, a POSITA would recognize that in this embodiment, a request to authenticate the device for a financial transaction after biometric verification had occurred, but before the device was turned off, is a request to send the ID code without an additional biometric verification. In my opinion, a POSITA would recognize that in this case, the ID code would be sent without biometric verification.

9. Claim 9:

(a) [9a] "An integrated device comprising: a persistent storage media that persistently stores biometric data of a user and an ID code;"

232. *See* Claim 1, element [1a]. Section VIII.A.2.a, *supra*.

(b) [9b] "a validation module, coupled to communicate with the persistent storage media, that receives scan data from a biometric scan for comparison against the biometric data, and that sends the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and"

233. *See* Claim 1, elements [1c], [1d]. Section VIII.A.2.c, d, *supra*.

234. Further, in my opinion, the "validation module" will be the portion of the smartphone, including processors and instructions that receives the scan and verifies the biometric information. I also recognize that the validation module would be in coupled with the memory, since the biometric information that the validation module compares with received biometric information is stored in the memory for comparison.

(c) [9c] "a radio frequency communication module that receives an access message from the third-party trusted authority indicating that the third -party trusted authority successfully authenticated the ID code sent to the third-party trusted authority based on the comparison of the ID code and allowing the user to—complete a financial transaction."

235. *See* Claim 1, elements [1d], [1e]. Section VIII.A.2.d, e, *supra*. In my opinion, a POSITA would recognize that because the transaction device has wireless access, it necessarily has a "radio frequency communication module," as all wireless communications occur through an RF module.

10. Claim 10: "The integrated device of claim 7, wherein the ID code is transmitted to the third-party trusted authority over a network."

236. In my opinion, Ludtke and Okereke disclose this limitation. As explained above, it is my opinion that Ludtke explains that "[t]he 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." Ex.1005 at 6:41-44. To me, Ludtke also explains that "the transaction device may contain wireless data communication," and may also "closely resemble a standard credit card." *Id.* at 5:36-41. In describing the TPCH specifically, Ludtke indicates that a "variety of communication devices may be used, such as the

Internet, direct dial-up modem connections, wireless or cellular signals, etc." *Id.* at 9:35-42. Therefore, in my opinion, the communications described above in conjunction with claim 1 (by both Ludtke and Okereke) to the agent are transmitted over a network.

11. Claim 12: "The integrated device of claim 7, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch, and a key fob."

237. *See* Claim 5. Section VIII.A.5, *supra*.

12. Claim 13:

(a) [13a]. "A system, comprising: an integrated hardware device that persistently stores biometric data of a legitimate user and an ID code in the integrated hardware device, and that wirelessly sends the—ID code; an authentication circuit that receives the ED [sic- ID] code and sends the ID code to a third-party trusted authority for authentication, and that receives an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code and allows the user to complete a financial transaction; and"

238. *See* Claim 1, elements [1a], [1d-1e]. Section VIII.A.2.a, d-e, *supra*. More specifically, in my opinion, the integrated devices described above are hardware devices because they are held by the user. The "authentication circuit" is the portion of the hardware device, including processors executing instructions, that receives the scan and verifies the biometric information.

(b) [13b]. "the third-party trusted authority operated by a third party, the third-party trusted authority storing a list of legitimate codes and determining the authentication of the ID code received based on a comparison of the ID code received and the legitimate codes included in the list of the legitimate codes."

239. *See* Claim 1, elements [1d-1e]. Section VIII.A.2.d-e, *supra*.

13. Claim 14: "The system of claim 11 wherein the integrated hardware device receives an authentication request from the authentication circuit, and in response, requests a biometric scan from a user to generate scan data and, when the integrated hardware device cannot verify the scan data as being from the legitimate user, the integrated hardware device does not send the ID code."

240. *See* Claim 1, elements [1b-1c]. Section VIII.A.2.b-c, *supra*. In my opinion, Figure 31 describes the process to verify a user of the integrated device (described in this embodiment as a digital wallet):

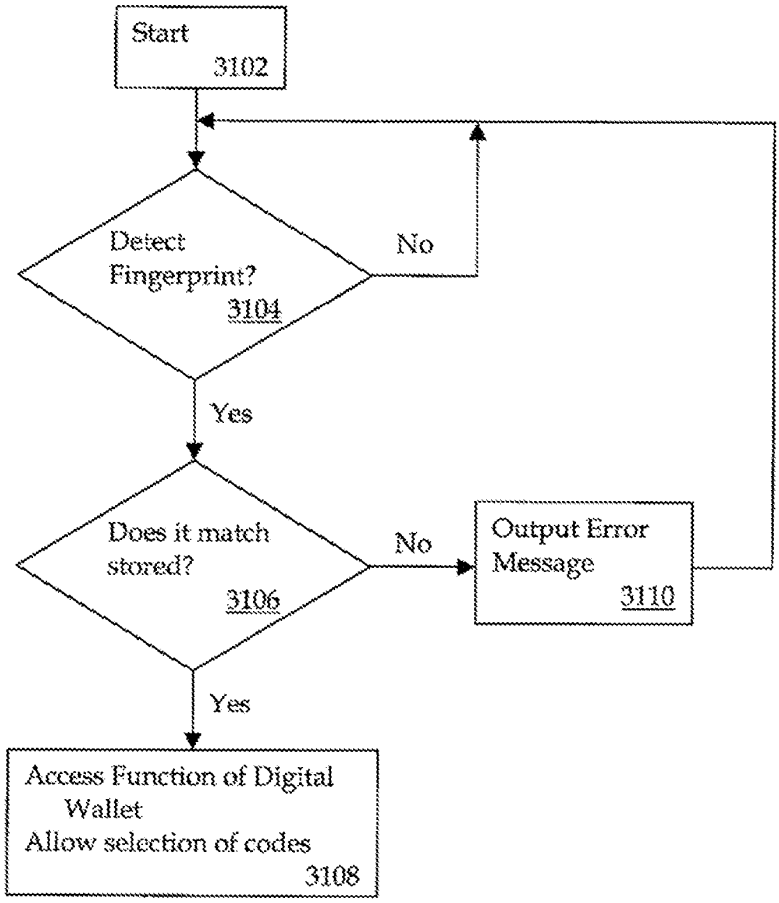


FIG. 31

241. *Id.* at Fig. 31. As can be seen in the flow chart, 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. *Id.* at 39:47-59.

14. Claim 15: "The system of claim 11, wherein the integrated hardware device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob."

242. *See* claim 5, Section VIII.A.5, *supra*.

15. Claim 16: "The system of claim 11, wherein the biometric data includes data based on one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition, and a voice recognition."

243. *See* claim 4, Section VIII.A.4, *supra*.

16. Claim 17: "The system of claim 11, wherein completing the financial transaction includes accessing one or more of a casino machine, keyless lock, an ATM machine, a web site, a file and a financial account."

244. *See* claim 7, Section VIII.A.7, *supra*.

17. Claim 18: "The system of claim 11, wherein completing the financial transaction includes accessing an application."

245. *See* claim 6, Section VIII.A.6, *supra*.

B. SNQ 2: Ludtke in combination with Okereke and Robinson Renders Claims 2 and 11 of the '905 Patent Obvious

1. The Proposed Combination

(a) The Prior Art Discloses the Claim Limitations

246. I believe the combination of Ludtke, Okereke, and Robinson renders obvious the above claims. SNQ 2 relies entirely on Ludtke and Okereke for the same reasons as outlined in SNQ 1, but also relies on Robinson for the limitations in dependent claims 2 and 11. In my opinion, all these dependent claims involve registering an age verification. It is also my opinion that where Ludtke and Okereke do not explicitly disclose registering an age verification, Robinson discloses the age verification in claims 2 and 11. As I note above, a POSITA would be motivated to combine the age verification disclosed in Robinson with the system disclosed in Ludtke with the secret information and unique device ID disclosed in Okereke.

(b) POSITA Would have been Motivated to Combine Robinson with Ludtke and Okereke

247. In my opinion, age verification would have been a feature a POSITA would have readily considered. Indeed, the age of a user is important in various transactions relevant to Ludtke. For example, Ludtke is expressly directed to the FeliCa Card, *see e.g.,* Ex. 1005 at 11:1-6, which, as I note above, was implemented in Hong Kong's Octopus transit card. In my opinion, a POSITA would have recognized a need for age authentication to allow preferred pricing for minors, student, and/or seniors as is often done in public transit. As such a POSITA would have been motivated to combine Robinson with Ludtke and Okereke.

248. Again, as I noted above, I also provide explanation of the specific factors that I understand are considered. For example, the scope and content of the prior art would have motivated a POSITA to combine Robinson with Ludtke and Okereke. Like both Ludtke and Okereke, Robinson discloses a way to improve security and to authenticate a user and device. Ex. 1007 at ¶¶27-29, 32, 66-67 Fig. 1.

249. Further, in my opinion, all three of the references are therefore in the same field of endeavor, with Robinson specifically teaching improving security with an additional age-based authorization factor and to authenticate a user for age-restricted access or transactions initiated by a wireless device like Ludtke's transaction device. *Id.* at ¶9-10. A POSITA would have recognized that the disclosure of Ludtke welcomes this modification with its stated aim to provide, for example, secure access to restricted areas. Ex. 1005 at 2:5-8, 10:24-28. Indeed, a POSITA would have recognized that the age

verification disclosed in Robinson would, for example, allow a way for the Ludtke system to ensure that the user is old enough to conduct a transaction, access a specific financial system or application, or to enter a restricted area.

250. In my opinion, a POSITA would also have had a reasonable expectation of success because age verification as disclosed in Robinson is a logical extension of the type of information that is exchanged. Robinson, like Ludtke and Okereke, also discloses the use of biometric information to verify a user. Ex. 1007 at ¶39. It would be logical to modify the system of Ludtke and Okereke to also include the age of the user who was verified with biometric information. In my opinion, the age would logically be registered at Ludtke's TPCH, where the age can also be kept confidential from third parties, consistent with Ludtke's goals.

2. Claim 2: "The method of claim 1, further comprising: registering an age verification for the user in association with the ID code."

251. In my opinion, Ludtke in combination with Okereke disclose all of the limitations of claim 1. *See* SNQ 1, Claim 1. Section VIII.A.2, *supra*.

252. However, it is also my opinion that neither Ludtke nor Okereke expressly disclose "registering an age verification for the user" as recited in this limitation. For example, in my opinion, Robinson discloses that a central database 102 holds information related to users to authenticate a user's age to access an age restricted area, for example. Ex. 1007 at ¶¶27-28, 32, 66-67, Fig. 1. It is my opinion that the central database 102 stores age verification records related to individuals seeking age verification (called "presenters"), including information such as a user's age, date of birth, government ID number, biometric

template, and at least one ID number that identifies the presenter within the system. *Id.* Prior to using the age-verification system, an individual presents biometric and age-verifying information. *Id.* at ¶13-15. I also believe that Robinson further discloses that age-verifying information is associated with at least one ID number (SID) identifying the user.

3. Claim 11: "The integrated device of claim 7 [sic – 9], wherein an age verification is registered in association with the ID code.

253. It is my opinion that Ludtke in combination with Okereke disclose all of the limitations of claim 9. *See* SNQ 1, Claim 9. Section VIII.A.9, *supra*.

254. Indeed, in my opinion, Robinson in combination with Ludtke and Okereke disclose all of the limitations of claim 11 for the same reasons as described in conjunction with claim 2. Section VIII.B.2, *supra*.

C. SNQ 3: Ludtke in combination with Scott Renders Claims 1, 3-10, and 12-18 of the '905 Patent Obvious

1. The proposed combination

(a) The Prior Art Discloses the Claim Limitations

255. I believe the combination of Ludtke and Scott renders obvious the above claims. SNQ 3 relies on Ludtke as the base reference, which discloses a mobile device used for performing financial transactions. In my opinion, Ludtke discloses all of the limitations in claims 1, 3-10, and 12-18 except the "unique Device ID" and storage of "secret information." Specifically, to me, Ludtke discloses the system as shown below in figure 1:

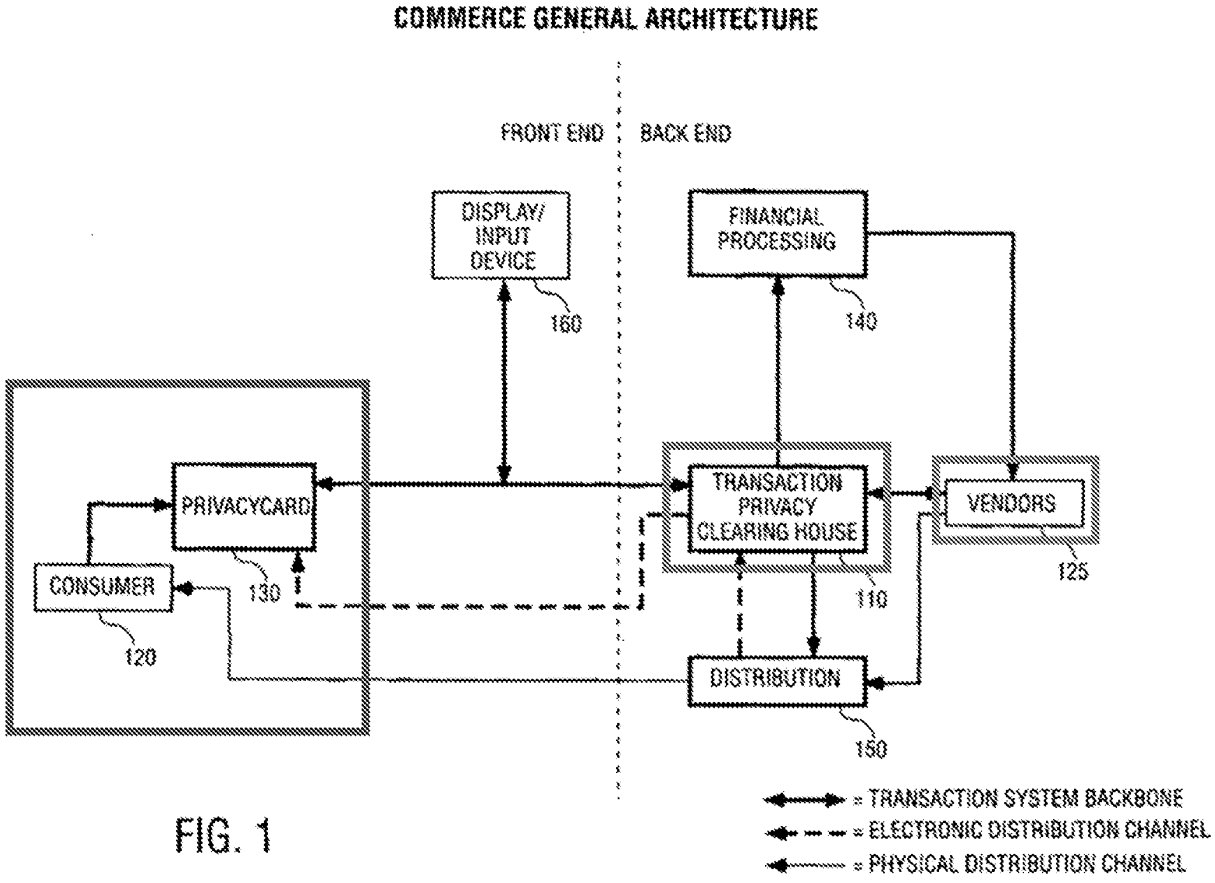


FIG. 1

256. Figure 1 shows one embodiment of the system in Ludtke. In my opinion, Ludtke discloses a "transaction device," which is seen above as the Privacy Card 130. Ex. 1005 at 6:36-44, Fig. 1. It is also my opinion that the transaction device is a device that the consumer 120 uses and includes a number of embodiments, including a privacy card, and digital wallet. *Id.* at 5:1-5, 11-14, 6:36-44. The transaction device also authorizes the consumer 120 using biometric data, including a fingerprint and other biometric information. Ludtke's transaction device includes and discloses a persistent, tamper proof storage. It is my opinion that Ludtke also discloses the process to authenticate a financial transaction

between the consumer 120 and a vendor 125. The financial transaction is authorized through the transaction privacy clearing house 110, which is a third party, independent of the consumer 120 and the vendor 125. I also believe that Ludtke emphasizes the third-party aspect of the transaction privacy clearing house 110 because the third party ensures that private information is not exchanged between the consumer 120 and the vendor 125. *Id.* at 6:45-49, 29:43-53.

257. The claims require storage of "secret information" in the user's device. In my opinion, although Ludtke does not explicitly disclose this "secret information," it does disclose (1) a storage location for this information, (id. at 10:46-49, 24:61-65), as well as (2) the importance of maintaining the confidentiality of private information (id. at 3:45-47; 5:30-31, 6:45-49). In my opinion, Scott discloses this "secret information." Specifically, to me, Scott includes an extensive discussion regarding a secret key infrastructure. Scott discloses that the device's memory 20 also stores a private key unique to each device and used for encryption, which can be "set into memory by the manufacturer." Ex. 1008 at 11:24-30, 28:13-15, 4:14-18. Scott discloses that this "private key" used by the PID 6 is never disclosed. Id. at 8:21-22.

258. The claims also require an "ID code" that is unique and identifies the user's device that is communicated to the third party trusted authority for authorization of the device. In my opinion, Ludtke discloses "transaction device information" that is communicated from the consumer's transaction device 130 to the transaction privacy clearing house 110 for authorization, but Ludtke does not explicitly indicate that this

"transaction device information" is a unique code identifying the consumer's transaction device. Scott, however, to me, does disclose an ID code that uniquely identifies the PID 6. Ex. 1008 at 4:9-10 ("The memory can further 10 store an ID code indicative of the enrolled person or the device."), 8:13-22, 11:14-20. Specifically, memory 20 stores information "specific to processing unit 16," including an ID code unique to the device, which may be set by the device manufacturer and can be the device serial number. *Id.* at 11:11-13. In my opinion, a serial number is a unique code that identifies the device it is attached to. Scott also discloses wherein the PID 6 stores other data values such as "a synchronization counter associated with the user device." Id. at 6:28-7:23, 13:10-15, 19:30-32.

(b) A POSITA would have been motivated to combine Ludtke and Scott

259. In my opinion, a POSITA would have been motivated to combine Ludtke and Scott. As I note above, the Ludtke reference meets most of the limitations of the claims of the '905 Patent with the exception of the "Device ID" limitations. Instead Ludtke discusses using "transaction device information" as part of the described encrypted transaction without explaining how to implement such information. A POSITA would naturally have turned to a similar implementation which provides detailed instructions, particularly one implementing a well-known solution, such as public key cryptography. As I describe below, Scott describes a similar implementation in detail and describes public key cryptography, *see* Ex. 1008 at 4:6-8.

260. Again, as I noted above, I also provide explanations of the specific factors that I understand are considered. In my opinion, the scope and content of the prior art would

have motivated POSITA to combine Ludtke and Okereke. As explained above, it is my opinion that Ludtke discloses almost all of the limitations of the claims except for "secret information" and the "unique" nature of a device ID code. Similar to Ludtke, to me, Scott discloses authenticating a user using a "personal identification device" (PID) for protected applications such as opening a hotel room door or a conducting a point-of-sale transaction. *Id.* at 8:5-12. Scott specifically describes a system for authentication of a mobile device to protect information for financial transactions. *Id.* at 2:5-16

261. In my opinion, Ludtke discloses a persistent, tamper proof memory, and a POSITA would have been motivated to combine the secret key disclosed in Scott with the system disclosed in Ludtke. In my opinion, the secret key infrastructure disclosed in Scott is similar to that disclosed in Okereke, as discussed above. As I note above, a POSITA would have already known, as of the priority date of the '905 patent, that encryption using a secret key such as that disclosed in Scott would have been obvious when communicating confidential information. Specifically, a POSITA would have recognized the importance of encrypted communication when engaging in communications regarding financial information and especially when authenticating financial transactions. In my opinion, the use of secret information (such as that in PKI encryption) to perform this type of encryption was well-known ***decades*** before the filing date of the '905 patent, and was a well-established, well-known method for implementing encryption. *Id.* For example, in my opinion, public key encryption was developed in the 1970s, and serves as a well-known way to encrypt and authenticate secret or confidential information. *Id.* at ¶29. As such, I

recognized that such encryption is important to many applications, including financial information where it is particularly important to keep the information secret. *Id.* at ¶143. I thus recognized that the use of secret information, which is disclosed in Scott, would make the system of Ludtke even more secure. *Id.* at ¶144. In my opinion, Scott simply demonstrates this knowledge prior to the '905 patent's priority date.

262. In my opinion, Ludtke discloses transaction device information communicated between the transaction device and the transaction privacy clearing house for authorization of a financial transaction. In my opinion, a POSITA would have combined the teachings of Scott's unique Device ID with Ludtke's system. As discussed above, in my opinion, Ludtke explicitly teaches communication of "transaction device information" with the TPCH. Ex. 1005 at 6:38-51. In my opinion, a POSITA would also have recognized that such transaction device information necessarily includes unique device identifiers such as a serial number or other number that is specific to the processing unit. In my opinion, Scott explicitly discloses this fundamental information. Ex. 1008 at 8:20-23.

263. In my opinion, a POSITA would have combined Ludtke and Scott because they are both in the same field of endeavor. Indeed, to me, both references are in the same field of endeavor as the '905 patent, *i.e.*, authentication of a device, including use of biometric information, for the purpose of exchanging sensitive information over a network. *See* Ex. 1001 at 1:21:24 ("The present invention relates generally to computerized authentication, and more specifically, to an authentication responsive to biometric verification of a user being authenticated"); Ex. 1005 at Abstract ("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"); Ex. 1008 at Abstract ("A portable, hand-held personal identification device (6) and method for providing secure access to a host facility…"); *id.* ¶31 ("Where absolute security is essential, some host facilities employ a biometric sensor to measure a biometric trait of a person requesting access to the host facility").

264. In my opinion, a POSITA would have reasonably expected the combination of Ludtke and Scott to succeed and yield predictable results. In my opinion, Ludtke's system already discloses a persistent and tamper-proof memory and discusses the use of sensitive information. Ludtke also discloses transaction device information. Ex. 1005 at 6:38-51. In my opinion, Scott similarly discloses a persistent, tamper-proof memory. It is my opinion that Scott teaches that data is stored in a memory where, after biometric enrollment, "there is no going back or editing." Ex. 1008 at 16:11-12. Given these disclosures, a POSITA would have expected the combination to result in Ludtke's financial system storing the secret information in Ludtke's memory and using the unique device ID disclosed in Scott as the transaction device information. In my opinion, a POSITA would have expected this to yield the predictable result of the option to use secret key encryption and decryption with a private key (secret information), as well as the ability to ensure authentication of an authorized device using unique device identifying information such as a serial number, and would have expected this combination to succeed.

265. For example, in my opinion, Ludtke describes a protected memory to keep the type of important and sensitive information described in Okereke. Ex. 1005 at 19:37-40. Moreover, in my opinion, a POSITA would be familiar with the secret key encryption system because it had long been used as a way to encrypt and decrypt information and share such information only for authorized users. §IV.A *supra*. Implementing such a system with Ludtke would have been logical and obvious to a POSITA. Finally, both systems have similar types of mobile devices, and have similar goals. As such, it would make sense to a POSITA to use the type of information identified in Scott in the Ludtke system to further complement Ludtke's features.

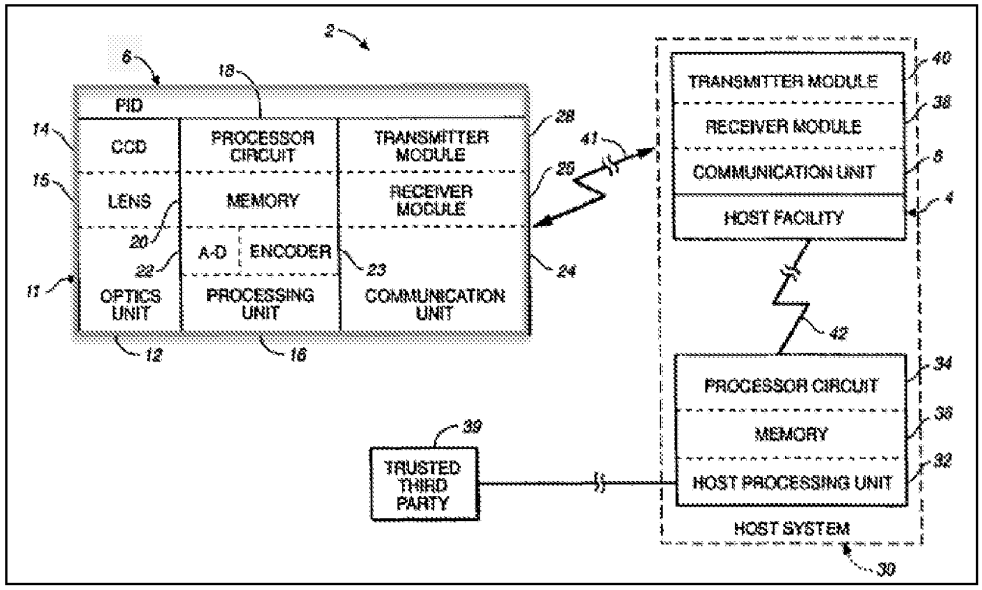
2. Claim 1 of the '905 Patent

(a) [1a] "A method comprising: persistently storing biometric data of a legitimate user and an ID code on an integrated device"

266. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VIII.A.2.a, *supra*.

267. As I explain above in detail, a POSITA would have been motivated to combine the disclosure of Ludtke with the disclosure in Scott.

268. In my opinion, Scott also discloses a method for verifying a user during authentication of an integrated device (*e.g.*, personal identification device ("PID") 6), in order to, for example, provide secure access to protected resources such as a hotel room or a point-of-sale transaction. Ex. 1008 at Abstract, 2:5-23, 4:22-5:9, 7:24-8:12; *see* claims [1A]-[1H] *infra*.



Ex. 1008 at Fig. 1.

269. As explained above, in my opinion, Scott discloses that the memory 20 of the PID 6 persistently stores a plurality of codes and other data values including an ID code that uniquely identifies the PID 6. Ex. 1008 at 4:9-10 ("The memory can further 10 store an ID code indicative of the enrolled person or the device."), 8:13-22, 11:14-20. Specifically, to me, memory 20 stores information "specific to processing unit 16," including an ID code unique to the device, which may be set by the device manufacturer and can be the device serial number. Ex. 1008 at 11:11-13. In my opinion, a serial number is a unique code that identifies the device it is attached to. Scott also discloses wherein the PID 6 stores other data values such as "a synchronization counter associated with the user device." *Id.* at 6:28-7:23, 13:10-15, 19:30-32

270. As discussed above, in my opinion, a POSITA would have been motivated to modify the system of Ludtke to incorporate the unique serial numbers also disclosed in

Scott. In my opinion, a POSITA would have been motivated to store permanent information, such as the unique device identifiers (serial number). Moreover, in my opinion, a POSITA would have recognized that the "transaction device information" disclosed within Ludtke could further include the unique device information in Scott, which would ensure that the information used to authenticate the device only identifies the authorized device. In my opinion, a POSITA would also have stored the unique device identifiers in the persistent tamper-proof memory, because this is important information that allows authorization and sensitive communications to take place, and in my opinion, a POSITA would have recognized the need to take care to ensure it is not easy to tamper with and modify the information.

(b) [1b] "responsive to receiving a request for biometric verification of a user, receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor;"

271. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VIII.A.2.b, *supra*.

(c) [1c] "comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;"

272. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VIII.A.2.c, *supra*.

(d) [1d] responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and

273. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VIII.A.2.d, *supra*.

274. ***ID Code***: In my opinion, Ludtke does not describe the specific "transaction device information" that is provided to the TPCH 110 and that is maintained in a secure database by the TPCH 110. *Id*. at 6:36-64. However, as discussed above, in my opinion, a POSITA would have been motivated to combine Ludtke with the teachings of Scott, and would have recognized that the "transaction device information" would include a unique serial number, which identifies the integrated device.

(e) [1e] "responsive to receiving an access message from the third-party trusted authority-indicating that the third-party trusted authority successfully authenticated the ID code, allowing the user to complete a financial transaction."

275. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VIII.A.2.e, *supra*.

3. Claim 3: "The method of claim 1, wherein an indication that the biometric verification was successful is sent with the ID code."

276. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VIII.A.3, *supra*.

4. Claim 4: "The method of claim 1, wherein the biometric data includes data from one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition."

277. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VIII.A.4, *supra*.

5. Claim 5: "The method of claim 1, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob."

278. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VIII.A.5, *supra*.

6. Claim 6: "The method of claim 1, wherein completing the financial transaction includes accessing an application."

279. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VIII.A.6, *supra*.

7. Claim 7: "The method of claim 1, wherein completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account."

280. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VIII.A.7, *supra*.

8. Claim 8: "The method of claim 1, further comprising: responsive to determining the action does not require biometric verification, receiving a request for the ID code without a request for biometric verification, and responsive to receiving the request for the ID code without a request for biometric verification, sending the ID code for authentication without requesting the scan data."

281. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VIII.A.8, *supra*.

9. Claim 9:

(a) [9a] "An integrated device comprising: a persistent storage media that persistently stores biometric data of a user and an ID code;"

282. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VIII.A.9.a, *supra*.

283. *See also* Claim 1, element [1a]. Section VIII.C.1.a, *supra*.

(b) [9b] "a validation module, coupled to communicate with the persistent storage media, that receives scan data from a biometric scan for comparison against the biometric data, and that sends the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and"

284. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VIII.A.9.b, *supra*.

285. *See also* Claim 1, elements [1c], [1d]. Section VIII.C.1.c, d, *supra*.

(c) [9c] "a radio frequency communication module that receives an access message from the third-party trusted authority indicating that the third -party trusted authority successfully authenticated the ID code sent to the third-party trusted authority based on the comparison of the ID code and allowing the user to—complete a financial transaction."

286. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VIII.A.9.c, *supra*.

287. *See also* Claim 1, elements [1d], [1e]. Section VIII.A.1.d, e, *supra*.

10. Claim 10: "The integrated device of claim 7, wherein the ID code is transmitted to the third-party trusted authority over a network."

288. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VIII.A.10, *supra*.

11. Claim 12: "The integrated device of claim 7, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch, and a key fob."

289. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VIII.A.11, *supra*.

290. *See also* Claim 5. Section VIII.C.5, *supra*.

12. Claim 13:

(a) [13a]. "A system, comprising: an integrated hardware device that persistently stores biometric data of a legitimate user and an ID code in the integrated hardware device, and that wirelessly sends the—ID code; an authentication circuit that receives the ED [sic- ID] code and sends the ID code to a third-party trusted authority for authentication, and that receives an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code and allows the user to complete a financial transaction; and"

291. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VIII.A.12.a, *supra*.

292. *See also* Claim 1, elements [1a], [1d], [1e]. Section VIII.A.1.a, d-e, *supra*.

(b) [13b]. "the third-party trusted authority operated by a third party, the third-party trusted authority storing a list of legitimate codes and determining the authentication of the ID code received based on a comparison of the ID code received and the legitimate codes included in the list of the legitimate codes."

293. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VIII.A.12.b, *supra*.

294. *See also* Claim 1, elements [1d], [1e]. Section VIII.A.1.d-e, *supra*.

13. Claim 14: "The system of claim 11 wherein the integrated hardware device receives an authentication request from the authentication circuit, and in response, requests a biometric scan from a user to generate scan data and, when the integrated hardware device cannot verify the scan data as being from the legitimate user, the integrated hardware device does not send the ID code."

295. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VIII.A.13, *supra*.

296. *See* Claim 1, elements [1b], [1c]. Section VIII.A.1.b-c, *supra*.

14. Claim 15: "The system of claim 11, wherein the integrated hardware device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob."

297. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VIII.A.14, *supra*.

298. *See also* claim 5, Section VIII.C.5, *supra*.

15. Claim 16: "The system of claim 11, wherein the biometric data includes data based on one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition, and a voice recognition."

299. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VIII.A.15, *supra*.

300. *See also* claim 4, Section VIII.C.4, *supra*.

16. Claim 17: "The system of claim 11, wherein completing the financial transaction includes accessing one or more of a casino machine, keyless lock, an ATM machine, a web site, a file and a financial account."

301. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VIII.A.16, *supra*.

302. *See also* claim 7, Section VIII.C.7, *supra*.

17. Claim 18: "The system of claim 11, wherein completing the financial transaction includes accessing an application."

303. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section VIII.A.17, *supra*.

304. *See also* claim 6, Section VIII.A.6, *supra*.

D. SNQ 4: Ludtke in combination with Scott and Robinson Renders Claims 2 and 11 Obvious

1. The Proposed Combination

(a) The Prior Art Discloses the Claim Limitations

305. I believe the combination of Ludtke, Scott, and Robinson renders obvious the above claims. SNQ 4 relies entirely on Ludtke and Scott for the same reasons as outlined

in SNQ 3, but also relies on Robinson for the limitations in dependent claims 2 and 11. Both of these dependent claims involve registering an age verification.

306. In my opinion, Robinson, like Ludtke and Scott, discloses a system involving biometric verification that is concerned with ensuring the protection of sensitive information. Robinson further discloses authentication of a user's age, thereby disclosing the limitations in dependent claims 2 and 11.

307. In the proposed combination, a POSITA would have been motivated to reference other disclosures to learn about the different types of information that may need to be protected for authorization. To fully understand the state of the art, a POSITA would have referenced Robinson, which discloses age verification. POSITA would have understood the necessity and benefits of verifying the age of a user in a secure manner for access to age restricted content.

(b) A POSITA Would have been Motivated to Combine Robinson with Ludtke and Scott

308. In my opinion, age verification would have been a feature a POSITA would have readily considered. Indeed, the age of a user is important in various transactions relevant to Ludtke. For example, Ludtke is expressly directed to the FeliCa Card, *see e.g.*, Ex. 1005 at 11:1-6, which, as I note above, was implemented in Hong Kong's Octopus transit card. In my opinion, a POSITA would have recognized a need for age authentication to allow preferred pricing for minors, student, and/or seniors as is often done in public transit. As such, a POSITA would have been motivated to combine Robinson with Ludtke and Scott.

309. Again, as I noted above, I also provide explanation of the specific factors that I understand are considered. In my opinion, the scope and content of the prior art would have motivated a POSITA to combine Robinson with Ludtke and Scott. Like both Ludtke and Scott, Robinson discloses a way to improve security and to authenticate a user and device. Ex. 1007 at ¶¶27-29, 32, 66-67 Fig. 1.

310. As such, to me, all three of the references are therefore in the same field of endeavor, with Robinson specifically teaching improving security with an additional age-based authorization factor and to authenticate a user for age-restricted access or transactions initiated by a wireless device like Ludtke's transaction device. Ex. 1007 at ¶9-10. In my opinion, a POSITA would have recognized that the disclosure of Ludtke welcomes this modification with its stated aim to provide, for example, secure access to restricted areas. Ex. 1005 at 2:5-8, 10:24-28. Indeed, a POSITA would have also recognized that the age verification disclosed in Robinson would, for example, allow a way for the Ludtke system to ensure that the user is old enough to conduct a transaction, access a specific financial system or application, or to enter a restricted area.

311. In my opinion, a POSITA would also have had a reasonable expectation of success because age verification as disclosed in Robinson is a logical extension of the type of information that is exchanged. In my opinion, Robinson, like Ludtke and Scott, also discloses the use of biometric information to verify a user. Ex. 1007 at ¶39. To me, it would be logical to modify the system of Ludtke and Scott to also include the age of the user who was verified with biometric information. The age would logically be registered at

Ludtke's TPCH, where the age can also be kept confidential from third parties, consistent with Ludtke's goals.

2. Claim 2: "The method of claim 1, further comprising: registering an age verification for the user in association with the device ID code."

312. Ludtke in combination with Scott disclose all of the limitations of claim 1. *See* SNQ 3, Claim 1. Section VIII.C.2, *supra*.

313. However, in my opinion that neither Ludtke nor Scott expressly disclose "registering an age verification for the user" as recited in this limitation. Robinson discloses this limitation as described in SNQ 2. *See* Section VIII.B.2.a.

3. Claim 11: "The integrated device of claim 7 [sic – 9], wherein an age verification is registered in association with the device ID code."

314. Ludtke in combination with Scott disclose all of the limitations of claim 9. *See* SNQ 3, claim 9. Section VIII.C.9, *supra*.

315. In my opinion, Robinson in combination with Ludtke and Okereke disclose all of the limitations of claim 11 for the same reasons as described in conjunction with claim 2. SectionVIII.D.2, *supra*.

VIII. '989 PATENT

A. SNQ 1: Ludtke in combination with Okereke Renders Claims 1-9 of the '989 Patent Obvious

1. The proposed combination

(a) The Prior Art Discloses the Claim Limitations

316. I believe the combination of Ludtke and Okereke renders obvious the above claims. As I explain below, SNQ 1 relies on Ludtke as the base reference, which discloses

a mobile device used for performing financial transactions. Ludtke discloses all of the limitations in claims 1-9 except the "unique Device ID" and storage of "secret information." Specifically, Ludtke discloses the system as shown below in figure 1:

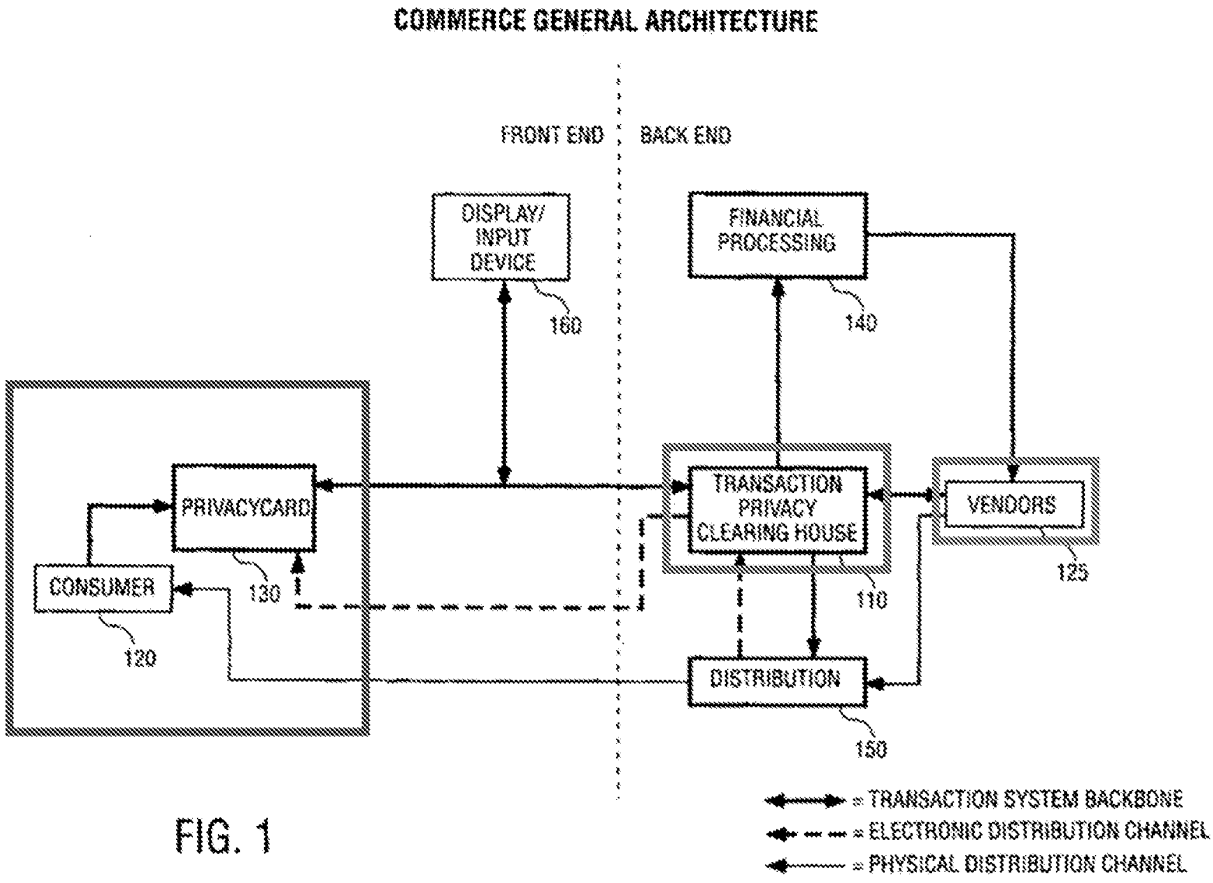


FIG. 1

Figure 1 shows one embodiment of the system in Ludtke. Ludtke discloses a "transaction device," which is seen above as the Privacy Card 130. Ex. 1005 at 6:36-44, Fig. 1. The transaction device is a device that the consumer 120 uses and includes a number of embodiments, including a privacy card , and digital wallet . *Id.* at 5:1-5, 11-14, 6:36-44. The transaction device also authorizes the consumer 120 using biometric data, including a

fingerprint and other biometric information. Ludtke's transaction device includes and discloses a persistent, tamper proof storage. Ludtke also discloses the process to authenticate a financial transaction between the consumer 120 and a vendor 125. The financial transaction is authorized through the transaction privacy clearing house 110, which is a third party, independent of the consumer 120 and the vendor 125. Ludtke emphasizes the third-party aspect of the transaction privacy clearing house 110 because the third party ensures that private information is not exchanged between the consumer 120 and the vendor 125. *Id.* at 6:45-49, 29:43-53.

317. The claims require storage of "secret information" in the user's device. Although Ludtke does not explicitly disclose this "secret information," it does disclose (1) a storage location for this information, (*id.* at 10:46-49, 24:61-65), as well as (2) the importance of maintaining the confidentiality of private information (*id.* at 3:45-47; 5:30-31, 6:45-49). Okereke discloses this "secret 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. Ex. 1006 at ¶25.

318. The claims also require an "ID code" that is unique and identifies the user's device that is communicated to the third party trusted authority for authorization of the device. Ludtke discloses "transaction device information" that is communicated from the consumer's transaction device 130 to the transaction privacy clearing house 110 for authorization, but Ludtke does not explicitly indicate that this "transaction device information" is a unique code identifying the consumer's transaction device. Okereke,

however, does disclose this unique device ID code information, in the form of a unique serial number or SIM number for the user device. *Id.*

(b) A POSITA Would be Motivated to Combine Ludtke and Okereke

319. In my opinion, not only would a POSITA have been motivated to combine Ludtke and Okereke, a POSITA implementing Ludtke would have most likely done so according to Okereke. Such an implementation would have resulted in a product that meets all the limitations I discuss below. As I note above, the Ludtke reference meets most of the limitations of the claims of the '989 Patent with the exception of the "ID Code" limitations. Instead Ludtke discusses using "transaction device information" as part of the described encrypted transaction without explaining how to implement such information. A POSITA would naturally have used public key cryptography to fill in this gap. As I describe above, public key cryptography is the standard for encrypted transactions and as such it would have been natural for a POSITA to implement it were a reference in this field not to provide detailed instructions. Okereke would have been a natural choice as it is an implementation of public key cryptography itself. *See* Ex. 1006 at Abstract.

320. In my opinion, not only would a POSITA have been motivated to combine Ludtke and Okereke, a POSITA implementing Ludtke would have most likely done so according to Okereke. Such an implementation would have resulted in a product that meets all the limitations I discuss below. As I note above, the Ludtke reference meets most of the limitations of the claims of the '989 Patent with the exception of the "unique Device ID" and storage of "secret information" limitations. Instead Ludtke discusses using

"transaction device information" as part of the described encrypted transaction without explaining how to implement such information. A POSITA would naturally have used public key cryptography to fill in this gap. As I describe above, public key cryptography is the standard for encrypted transactions and as such it would have been natural for a POSITA to implement it were a reference in this field not to provide detailed instructions. Okereke would have been a natural choice as it is an implementation of public key cryptography itself. *See* Ex. 1006 at Abstract.

321. In my opinion the scope and content of the prior art would have motivated POSITA to combine Ludtke and Okereke. As explained above, Ludtke discloses almost all of the limitations of the claims except for "secret information" and the "unique" nature of a device ID.

322. Ludtke discloses a persistent, tamper-proof memory, and in my opinion a POSITA would have been motivated to combine the secret key disclosed in Okereke with the system disclosed in Ludtke. As I note above, *supra* § IV.A, a POSITA would have already known, as of the priority date of the '989 patent, that encryption using a secret key such as that as part of a PKI would have been obvious when communicating confidential information. A POSITA specifically recognized the importance of encrypted communication when engaging in communications regarding financial information and especially when authenticating financial transactions. The use of secret information to perform this type of encryption was well-known ***decades*** before the filing date of the '989 patent, and was a well-established, well-known method for implementing encryption.

Public key encryption was developed in the 1970s, and serves as a well-known way to encrypt and authenticate secret or confidential information. *Id.* A POSITA would have recognized that such encryption is important to many applications, including financial information where it is particularly important to keep the information secret. In my opinion, a POSITA would therefore recognize that the use of PKI encryption, which is disclosed in Okereke, would make the system of Ludtke even more secure. Okereke simply demonstrates this knowledge prior to the '989 patent's priority date.

323. Ludtke discloses transaction device information communicated between the transaction device and the transaction privacy clearing house for authorization of a financial transaction. In my opinion, a POSITA would have combined the teachings of Okereke's unique Device ID with Ludtke's system. As discussed above, Ludtke explicitly teaches communication of "transaction device information" with the TPCH. Ex. 1005 at 6:38-51. A POSITA would have recognized that such transaction device information necessarily includes unique device identifiers such as a serial number or a SIM. Okereke explicitly discloses this fundamental information. Ex. 1006 at ¶25.

324. I understand the legal examination of motivation to combine is often performed by examining particular factors. I analyze some of these factors separately here, but these factors are important in my analysis above. In my opinion a POSITA would have been motivated to combine Ludtke and Okereke because they are both in the same field of endeavor. Indeed, both references are in the same field of endeavor as the '989 patent, *i.e.*, authentication of a user and device, including use of biometric information, for the purpose

of exchanging sensitive information over a network. *See* Ex. 1001 at 1:35-38 ("The present invention relates generally to computerized authentication, and more specifically, to an authentication responsive to biometric verification of a user being authenticated"); Ex. 1005 at Abstract ("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"); Ex. 1006 at Title ("System and method for secure wireless communication using PKI"); *id.* ¶31 ("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 password or biometric signature.").

325. Likewise, in my opinion, a POSITA would also have reasonably expected the combination of Ludtke and Okereke to succeed and yield predictable results. Ludtke's system already discloses a persistent and tamper-proof memory and discusses the use of sensitive information. Ludtke also discloses transaction device information. Ex. 1005 at 6:38-51. Given this disclosure in Ludtke, a POSITA would have expected the combination to result in Ludtke's financial system storing the secret information in Ludtke's memory and using the unique device ID disclosed in Okereke as the transaction device information. A 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 authorized device using unique device identifying information such as a serial number or SIM, and would have expected this combination to succeed.

326. For example, Ludtke describes a protected memory to keep the type of important and sensitive information described in Okereke. Ex. 1005 at 19:37-40. Moreover, a POSITA would be familiar with the PKI-compliant encryption system because it had long been used as a way to encrypt and decrypt information and share such information only for authorized users. §IV.A *supra*. In my opinion, implementing such a system with Ludtke would have been logical and obvious to a POSITA. Finally, both systems have similar types of mobile devices, and have similar goals. It would make sense to a POSITA to use the type of information identified in Okereke in the Ludtke system to further complement Ludtke's features.

2. Claim 1

(a) [1a] "A method comprising: receiving, at a smartphone, an identification (ID) code from a third-party trusted authority, the ID code uniquely identifying the smartphone among a plurality of smartphones;"

327. In my opinion, Ludtke and Okereke disclose this limitation.

328. ***A smartphone***. Both Ludtke and Okereke disclose a smartphone. Ludtke discloses a "transaction device." Ex. 1005 at 3:34-5. Ludtke's transaction device, or consumer access device, provides a number of different integrated functions, including maintaining bills and bill paying on the device (*id.* at 4:4-6), online shopping (*id.* at 4:7-35), and downloading and accessing electronic catalogs (*id.* at 4:36-39). The transaction device includes a number of hardware options such as a magnetic stripe generator (*id.* at 3:49-51), a screen (*id.* at 55-57), and a bar code reader (*id.* at 3:61-63). Figure 28 shows some of these functions, including a screen and touchpad:

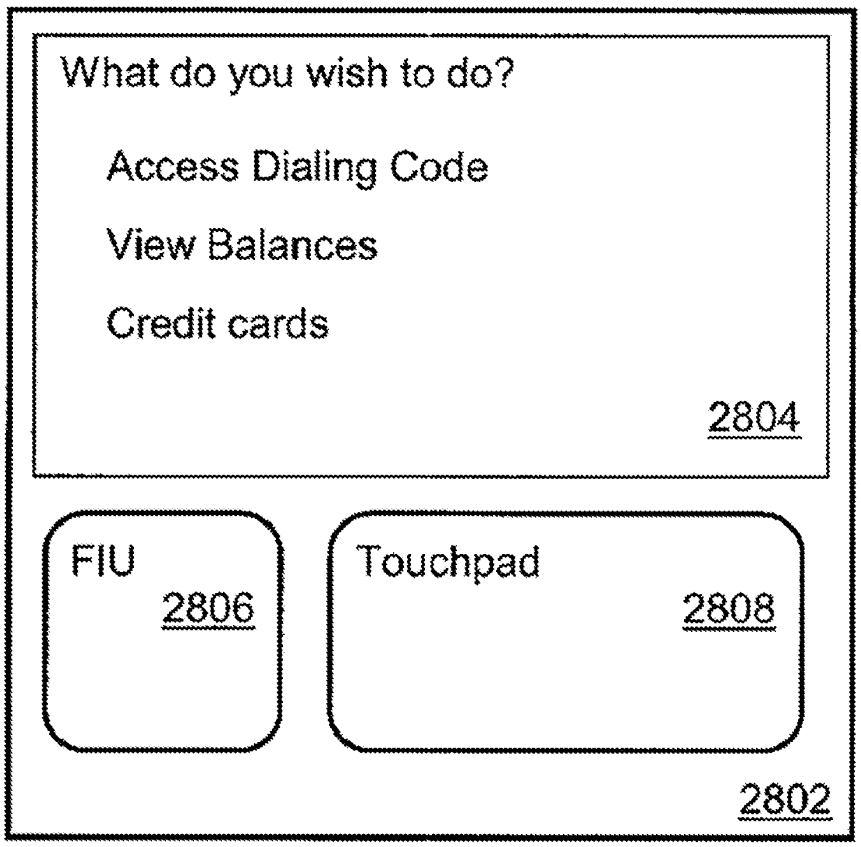


FIG. 28

Id. at Fig. 28. Ludtke teaches that the "consumer access device" shown in Fig. 28 "implements the method" in the patent. *Id.* at 39:19-21. In my opinion, a POSITA would recognize that this consumer access device, having functions allowing a user to see balances and credit cards, and also to "Access Dialing Codes" is a smartphone.

329. Okereke also discloses a smartphone. Okereke discloses wireless and mobile devices. Ex. 1006 at Abstract. "The wireless product 165 can be a personal digital assistant (PDA), laptop, cellular telephone or any other device capable of remote wireless

communication". *Id.* at ¶25. A POSITA would recognize that a smartphone is a cellular telephone with PDA functionality.

330. Even assuming neither Ludtke or Okereke disclose a smartphone, in my opinion, it would have been obvious to a POSITA to implement the functionality described in Ludtke and Okereke in a smartphone. Indeed, at the time of the invention, smartphones were common, and cellular telephones were gaining more and more functionality. A POSITA would recognize that a smartphone just combined the functionality already disclosed in the devices in Ludtke and Okereke.

331. ***Third party trusted authority***: In my opinion, Ludtke describes a transaction processing [or privacy] clearing house (TCPH) which is a third party trusted authority. The TPCH "may access relevant account information to authorize transactions." *Id.* at 3:40-45. Figure 1 of Ludtke shows how the TPCH is a third party:

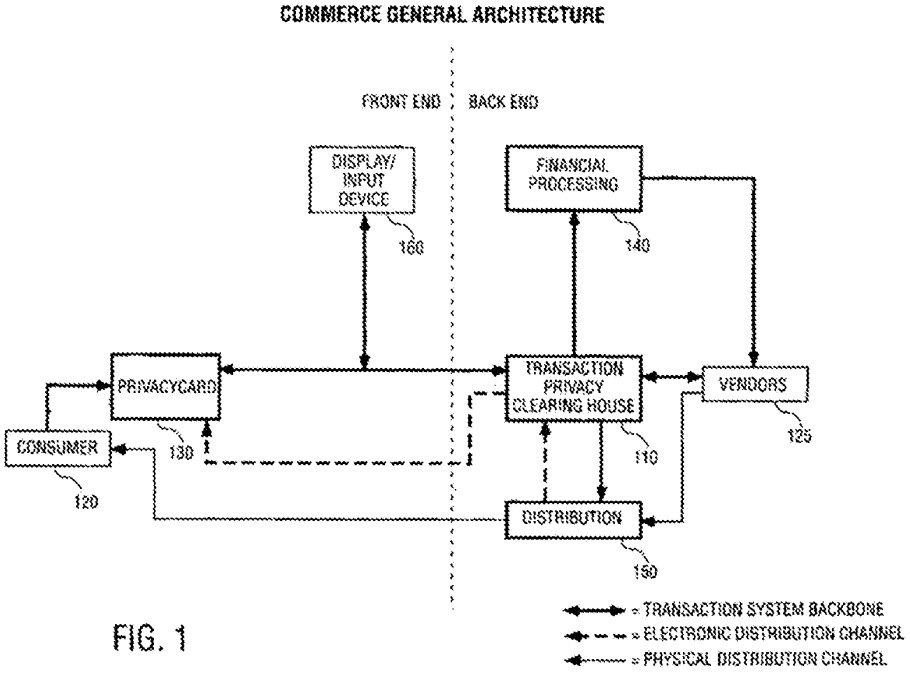


FIG. 1

Ex. 1005 at Figure 1. Figure 1 shows the commerce general architecture. *Id.* at 6:36-8:24. Figure 1 shows a consumer 120 who wishes to complete a purchase, *id.* at 6:36-64, and a vendor 125, who is selling something to the user 120. *Id.* "In this embodiment, a transaction privacy clearing house (TPCH) 110 interfaces a user 120 and a vendor 125." *Id.* at 6:36-39.

332. In my opinion, the TPCH is a third party to the transaction between the user/consumer 120 and the vendor 125. Ludtke explains that in "one embodiment of electronic distribution, the TPCH 110 functions as the middleman of the distribution channel. This allows TPCH 110 to retain user privacy by not exposing addressing information and possibly email addresses to third parties." *Id.* at 42-46. This demonstrates

that the TPCH acts as a middleman to ensure that only necessary information is exchanged between the consumer 120 and the vendor 125, but is not associated with either of them.

333. The TPCH is also a "trusted authority." Ludtke explains that 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." *Id.* at 6:41-44. The consumer 120 and vendor 125 therefore trust the TPCH to indicate whether the transaction may be complete.

334. ***Identification (ID) code uniquely identifying the smartphone among a plurality of smartphones***: Ludtke discloses the TPCH having "transaction device information" that is maintained in a secure database by the TPCH. *Id.* at 6:41-44. Ludtke does not further describe this "transaction device information." But, as explained above, Okereke discloses a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value. Specifically, Okereke discloses a device ID code in the form of a serial number or SIM number. Ex. 1006 at ¶25. As I discuss above, a POSITA would have been motivated to combine Ludtke with the teachings of Okereke, and would have recognized that the "transaction device information" would include a unique device serial number or SIM code, both of which identify the integrated device.

335. ***The smartphone receiving the ID code from the third party trusted authority***: Ludtke indicates that the "TPCH 110 maintains a secure database of device information and user information." Ex. 1005 at 6:49-51. In my opinion, it would have been obvious to

a POSITA that the third party trusted authority would send the ID code to the smartphone. The TPCH "functions as the middleman of the distribution channel." *Id.* at 7:44-46. The TPCH intent is to "retain user privacy by not exposing addressing information and possibly email addresses to third parties." *Id.* at 7:46-48. It would therefore be obvious that the ID code originate from the list of device information maintained by the TPCH and communicated to the smartphone. Not only could this communication be for purposes of assigning the ID code to the smartphone uniquely, but the TPCH would also include the ID code in communications to the smartphone to ensure verification.

(b) [1b] "persistently storing biometric data and the ID code on the smartphone, wherein the biometric data is one selected from a group consisting of facial recognition, a fingerprint scan, and a retinal scan of a legitimate user;"

336. ***Persistently storing biometric data and the ID code on the smartphone***: Ludtke discloses persistent storage on the smartphone. Specifically, the transaction device disclosed in Ludtke includes a process to use fingerprint data (biometric data of the user) to secure the device. Ludtke describes persistently storing the fingerprint data on the integrated device in a tamper-proof format that cannot be subsequently 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.

Id. at 19:35-40. This fingerprint data is persistently stored (write-once memory or other memory that is protected from accidental modification). This memory is persistent storage, because the information stored is not easily re-writable.

337. As I explain above, Okereke discloses a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value. Specifically, Okereke discloses a device ID code in the form of a serial number or SIM number. Ex. 1006 at ¶25.

338. As I discuss above, in my opinion, a POSITA would have been motivated to modify the system of Ludtke to incorporate the public/private key structure of Okereke and the unique serial numbers and SIMs. *see supra* §IV.A. Specifically, Ludtke includes the persistent storage area of the device where the ID code can be stored. POSITA would have been motivated to store permanent information, such as the unique device identifiers (serial number and/or SIM). Moreover, a POSITA would have recognized that the "transaction device information" disclosed within Ludtke could further include the unique device information in Okereke, which would ensure that the information used to authenticate the device only identifies the authorized device. POSITA would have stored the unique device identifiers in the persistent memory, because this is important information that needs to be maintained in the device.

339. ***Wherein the biometric data is selected from a group consisting of facial recognition, a fingerprint scan, and a retinal scan of a legitimate user***: Ludtke describes a number of different types of biometric information that may be used: "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." Ex. 1005 at 36:60-64.

(c) [1c] "receiving, at the smartphone, scan data from a biometric scan using the smartphone;"

340. Further, it is my opinion that Ludtke describes receiving scan data from a biometric scan using the smartphone. As I explain above, Ludtke describes using biometric verification – including a 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:

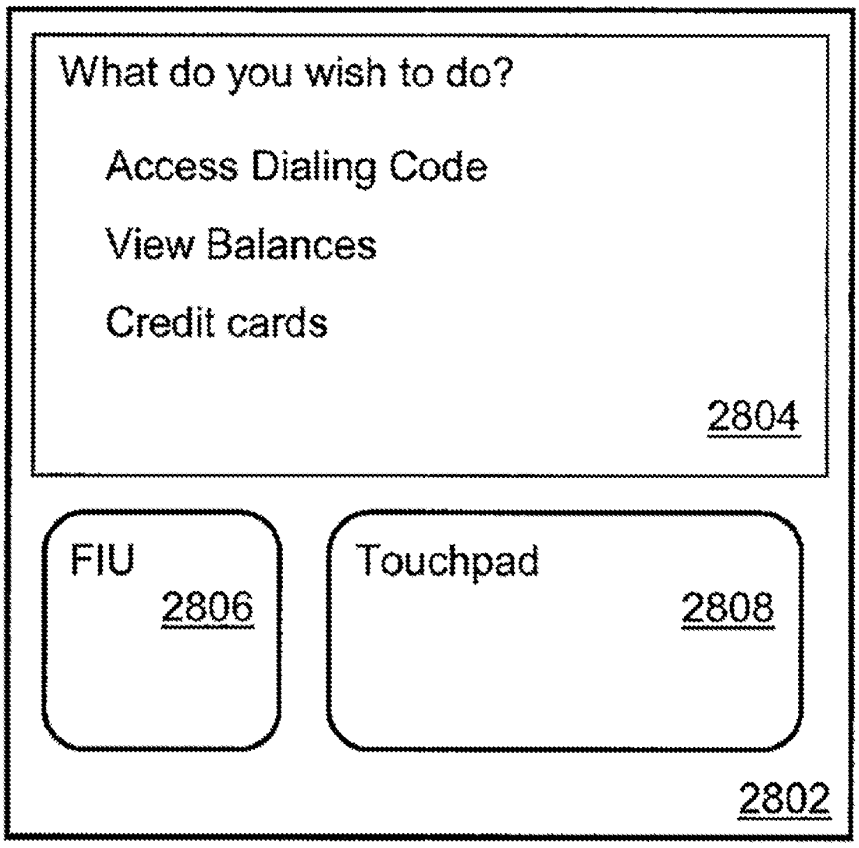


FIG. 28

Ex. 1005 at Fig. 28. "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." *Id.* at 39:24-27.

341. Figure 31 describes the process to verify a user of the integrated device (described in this embodiment as a digital wallet):

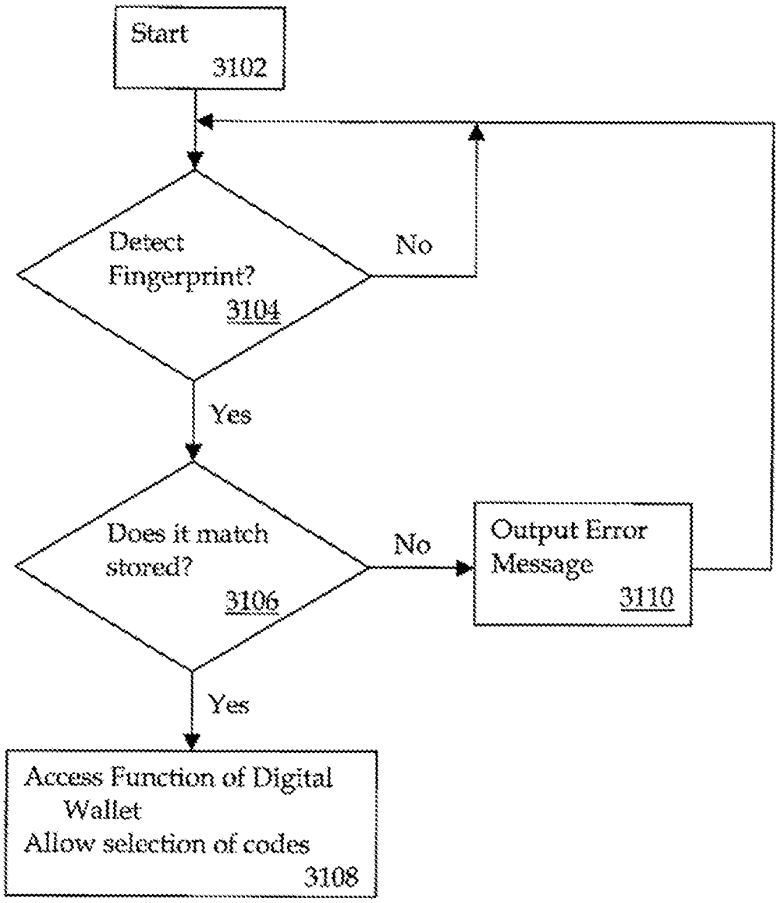


FIG. 31

Id. at Fig. 31. As can be seen in the flow chart, 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). *Id.* at 39:47-59.

(d) [1d] "comparing, using the smartphone, the scan data to the biometric data;"

342. Ludtke also shows this limitation in Figure 31:

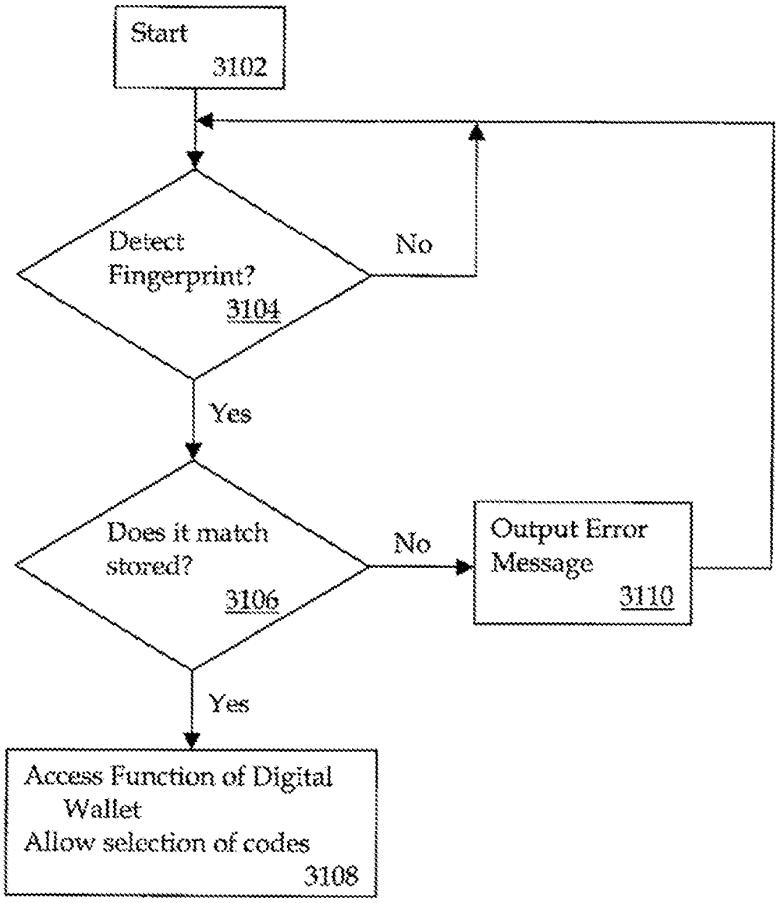


FIG. 31

Ex. 1005 at Fig. 31. Ludtke explains that 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 [Digital Wallet/Integrated Device] 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." *Id.* at 39:47-54.

(e) [1e] "determining whether the scan data matches the biometric data; and"

343. *See* element [1d], Section IX.A.2.d, *supra*.

(f) [1f] "responsive to a determination that the scan data matches the biometric data, wirelessly sending, from the smartphone, 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, a transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code, 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 website, a file and a financial account."

344. In my opinion Ludtke teaches this limitation.

345. ***Responsive to a determination that the scan data matches the biometric data***: As I explain in conjunction with limitation [1d], if the scanned fingerprint data matches the stored fingerprint, then access to functions of the integrated device, such as the digital wallet, is permitted. *Id*. at 39:47-54.

346. ***The third party trusted authority maintains one or more previously registered ID codes***: Ludtke also explains that the "TPCH 110 maintains a secure database of transaction device information and user information. In one embodiment, the TPCH 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." *Id*. at 49-55. And as I explain above, Ludtke explains that 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." *Id.* at 6:41-44. Therefore, the TPCH includes information that can be compared with information from the consumer and the consumer's device so the TPCH can determine whether the consumer 120 is authorized to complete a transaction with vendor 125. Indeed, the transaction device information that the TPCH compares to the received transaction device information must be stored within the TPCH as a list of codes (and specifically, a list of Device ID codes), in order to perform the comparison function that is disclosed. *Id.* at 30:19-27.

347. ***Wirelessly sending the ID code to the third party trusted authority for authorization***: Ludtke explains that "[t]he 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." *Id.* at 6:41-44. Ludtke also explains that "the transaction device may contain wireless data communication," and may also "closely resemble a standard credit card." *Id.* at 5:36-41. In describing the TPCH specifically, Ludtke indicates that a "variety of communication devices may be used, such as the Internet, direct dial-up modem connections, wireless or cellular signals, etc." *Id.* at 9:35-42.

348. ***A transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code***: Ludtke teaches that 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." *Id.* at 6:41-44. Therefore, once the TPCH authenticates the ID code, it provides notice to the parties to the transaction and the transaction can be completed.

349. Where the application is selected from a group consisting of a casino machine, a keyless lock, an ATM machine, a web site, a file, and a financial account: In Ludtke, access would be given applications of either computer software, a file (or both). In a number of embodiments, Ludtke describes the transaction device as including a "digital wallet" which, in my opinion, a POSITA would recognize as files that allow a user to digitally store credit card and other payment information and to make transactions with that card. Moreover, a POSITA would recognize that giving access to the digital wallet is providing access to a financial account.

3. Claim 2: "The method of claim 1, further comprising: Receiving a request for biometric verification, 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."

350. ***Receiving a request for biometric verification***: Ludtke discloses this limitation. As I explain above, Ludtke describes using biometric verification – including a fingerprint[9] – 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:

[9] I understand Samsung contends that a fingerprint is not within the scope of claim 1. However, in my opinion, Ludtke still discloses the elements of claim 1 in that it discloses different types of biometric information, including those covered by claim 1. *Id.*

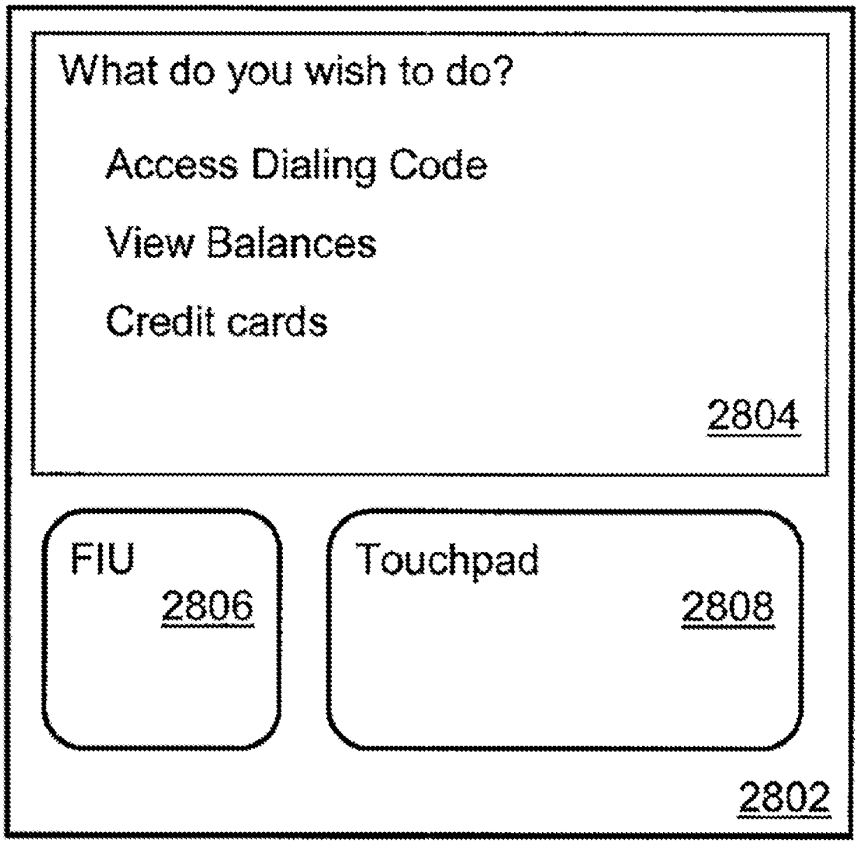


FIG. 28

Ex. 1005 at Fig. 28. "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." *Id.* at 39:24-27.

351. Figure 31 describes the process to verify a user of the integrated device (described in this embodiment as a digital wallet):

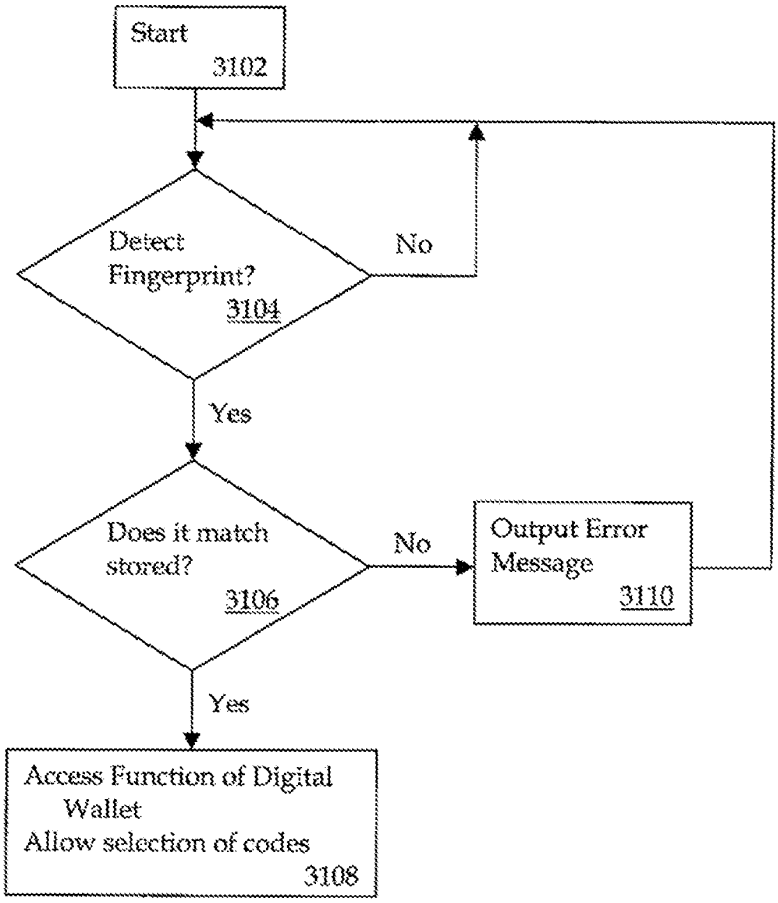


FIG. 31

Id. at Fig. 31. As can be seen in the flow chart, 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). *Id.* at 39:47-59.

352. 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: Ludtke discloses this limitation. Figure 31 describes the process to verify a user of the integrated device (described in this embodiment as a digital wallet):

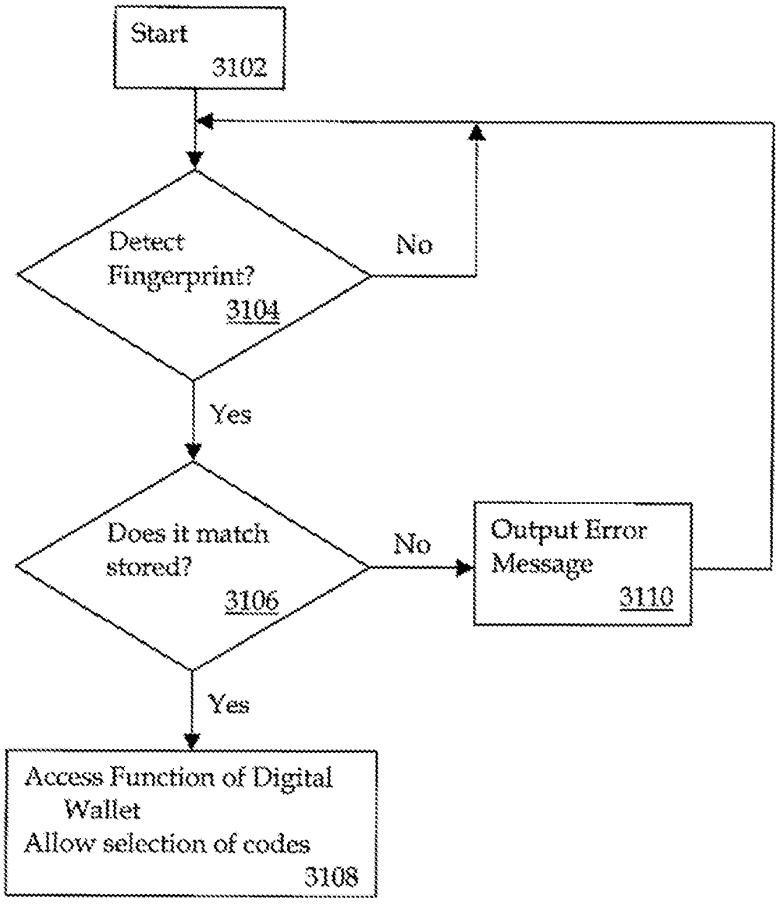


FIG. 31

Id. at Fig. 31. As can be seen in the flow chart, 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. *Id.* at 39:47-59.

4. Claim 3: "The method of claim 1, wherein completing the transaction includes accessing an application."

353. Ludtke discloses this limitation. In Ludtke, access would be given applications of either computer software, a file (or both). In a number of embodiments, Ludtke describes the transaction device as including a "digital wallet" which, in my opinion, a POSITA would recognize as an application and files that allow a user to digitally store credit card and other payment information and to make transactions with that card . *Id.* at Fig. 5a-b, 9:7-25.

5. 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 authority sending an indication that the third party trusted authority authenticated the ID code to another party."

354. In my opinion, Ludtke discloses this limitation. Ludtke teaches that 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." *Id.* at 6:41-44. Therefore, once the TPCH notifies both the smartphone (user) and the vendor (another party) that the TPCH authenticated the ID code, the transaction can be completed.

6. Claim 5:

(a) [5a] "a smartphone, comprising."

355. In my opinion, Ludtke and Okereke disclose a smartphone. *See* Claim 1, Element [1a], Section IX.A.2.a, *supra*.

(b) [5b] "a persistent storage having an input that receives an identification (ID) code from a third party trusted authority, and biometric data, wherein the biometric data is one selected from a group consisting of facial recognition, a fingerprint

scan, and a retinal scan, of a legitimate user, the ID code uniquely identifying the smartphone among a plurality of smartphones, the persistent storage storing the biometric data and the ID code, the persistent storage having an output configured to provide a first set of biometric data and the ID code for use on the smartphone;"

356. In my opinion, Ludtke and Okereke disclose this element. *See* Claim 1, Elements [1a-1b], Section IX.A.2.a-b, *supra*. The storage described in Ludtke would necessarily include an input (through which it receives the data that is stored there) and an output (where the data can be retrieved from the memory for use).

(c) [5c] "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; and"

357. In my opinion, Ludtke discloses this limitation. *See* Elements [1c-1e], Sections IX.A.2.c-e, *supra*.

358. The "validation module" will be the portion of the smartphone, including processors and instructions, that receives the scan and verifies the biometric information. In my opinion, a POSITA would recognize that the validation module would be in coupled with the memory, since the biometric information that the validation module compares with received biometric information is stored in the memory for comparison.

(d) [5d] a wireless transceiver 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, a transaction

being completed responsive to the third-party trusted authority successfully authenticating the ID code, 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.

359. In my opinion, Ludtke discloses this limitation. *See* Claim 1, Element [1f], Section IX.A.2.f, *supra*. A POSITA would recognize that any device capable of wireless communication would include a wireless transceiver.

7. Claim 6: "The smartphone of claim 5, wherein the ID code is transmitted to the third-party trusted authority over a network."

360. In my opinion, Ludtke and Okereke disclose this limitation. As explained above, Ludtke explains that "[t]he 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." *Id.* at 6:41-44. Ludtke also explains that "the transaction device may contain wireless data communication," and may also "closely resemble a standard credit card." *Id.* at 5:36-41. In describing the TPCH specifically, Ludtke indicates that a "variety of communication devices may be used, such as the Internet, direct dial-up modem connections, wireless or cellular signals, etc." *Id.* at 9:35-42. Therefore, the communications described above in conjunction with claim 1 (by both Ludtke and Okereke) to the agent are transmitted over a network.

8. Claim 7

(a) [7a]. "A system, comprising: a smartphone that persistently stores biometric data and an ID code, 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, and the ID code is received from a third-party

trusted authority, the ID code uniquely identifying the smartphone among a plurality of smartphones,"

361. In my opinion, Ludtke and Okereke disclose this limitation. *See* Claim 1, Elements [1a-1b]. Section IX.A.2.a-b, *supra*.

(b) [7b]. "the smartphone configured to indicate that a biometric authentication is requested,"

362. In my opinion, Ludtke and Okereke disclose this limitation. See Claim 1, Element [1c], Section IX.A.2.c, and claim 2, Section IX.A.3 *supra*. When the Ludtke smartphone receives a request for biometric authentication, it will necessarily include an indication that activates the touchpad.

(c) [7c] "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 biometric scan performed using the smartphone matches the biometric data of the legitimate user, wherein a transaction is completed responsive to successful authentication of the ID code by the third-party trusted authority, wherein the transaction being completed includes accessing one or more from a group consisting of a casino machine, a keyless lock, anATM machine, a web site, a file and a financial account; and"

363. In my opinion, Ludtke and Okereke disclose this limitation. *See* claim 1, element [1f], Section IX.A.2.f, *supra*.

(d) [7d] "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."

364. In my opinion, Ludtke and Okereke disclose this limitation. *See* claim 1, Elements [1a], [1f], sections IX.A.2.a, IX.A.2.f, *supra*.

9. 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 smartphone does not send the ID code."

365. In my opinion, Ludtke and Okereke disclose this limitation, *see* claim 2, Section IX.A.3, *supra*.

10. Claim 9: "The system of claim 7, wherein completing the transaction includes accessing an application."

366. In my opinion, Ludtke and Okereke disclose this limitation. *See* claim 3, Section IX.A.4, *supra*.

B. SNQ 2: Ludtke in combination with Scott Renders Claims 1-9 of the '989 Patent Obvious

1. The proposed combination

(a) The Prior Art Discloses the Claim Limitations

367. SNQ 2 relies on Ludtke as the base reference, which discloses a mobile device used for performing financial transactions. Ludtke discloses all of the limitations in claims 1-9 except the "unique Device ID" and storage of "secret information." Specifically, Ludtke discloses the system as shown below in figure 1:

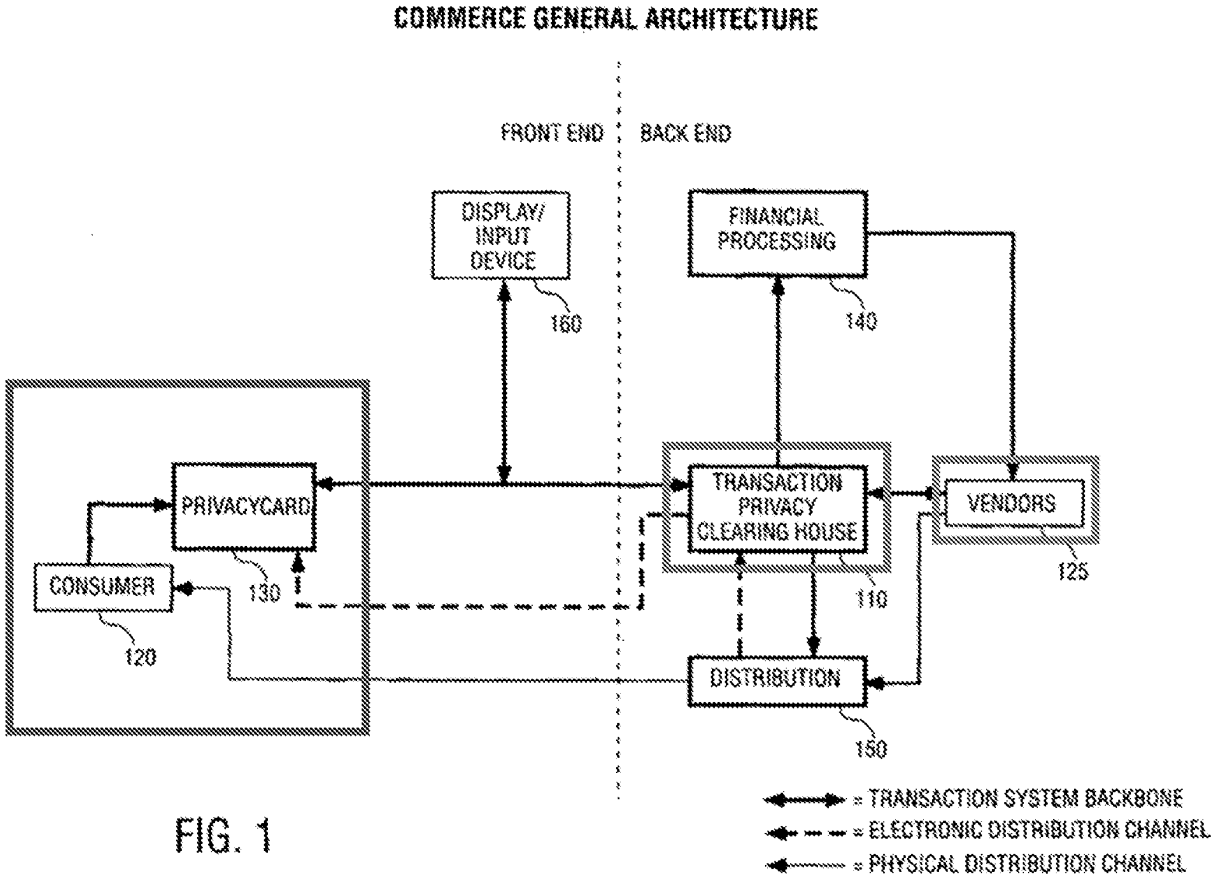


FIG. 1

Figure 1 shows one embodiment of the system in Ludtke. Ludtke discloses a "transaction device," which is seen above as the Privacy Card 130. Ex. 1005 at 6:36-44, Fig. 1. The transaction device is a device that the consumer 120 uses and includes a number of embodiments, including a privacy card, and digital wallet. *Id.* at 5:1-5, 11-14, 6:36-44. The transaction device also authorizes the consumer 120 using biometric data, including a fingerprint and other biometric information. Ludtke's transaction device includes and discloses a persistent, tamper proof storage. Ludtke also discloses the process to authenticate a financial transaction between the consumer 120 and a vendor 125. The financial transaction is authorized through the transaction privacy clearing house 110,

which is a third party, independent of the consumer 120 and the vendor 125. Ludtke emphasizes the third party aspect of the transaction privacy clearing house 110 because the third party ensures that private information is not exchanged between the consumer 120 and the vendor 125. *Id.* at 6:45-49, 29:43-53.

368. The claims require storage of "secret information" in the user's device. Although Ludtke does not explicitly disclose this "secret information," it does disclose (1) a storage location for this information, (*id.* at 10:46-49, 24:61-65), as well as (2) the importance of maintaining the confidentiality of private information (*id.* at 3:45-47; 5:30-31, 6:45-49). Scott discloses this "secret information." Specifically, Scott includes an extensive discussion regarding a secret key infrastructure. Scott discloses that the device's memory 20 also stores a private key unique to each device and used for encryption, which can be "set into memory by the manufacturer." Ex. 1008 at 11:24-30, 28:13-15, 4:14-18. Scott discloses that this "private key" used by the PID 6 is never disclosed. *Id.* at 8:21-22.

369. The claims also require an "ID code" that is unique and identifies the user's device that is communicated to the third party trusted authority for authorization of the device. Ludtke discloses "transaction device information" that is communicated from the consumer's transaction device 130 to the transaction privacy clearing house 110 for authorization, but Ludtke does not explicitly indicate that this "transaction device information" is a unique code identifying the consumer's transaction device. Scott, however, does disclose an ID code that uniquely identifies the PID 6. Ex. 1008 at 4:9-10 ("The memory can further 10 store an ID code indicative of the enrolled person or the

device."), 8:13-22, 11:14-20. Specifically, memory 20 stores information "specific to processing unit 16," including an ID code unique to the device, which may be set by the device manufacturer and can be the device serial number. *Id.* at 11:11-13. In my opinion, a serial number is a unique code that identifies the device it is attached to. Scott also discloses wherein the PID 6 stores other data values such as "a synchronization counter associated with the user device." *Id.* at 6:28-7:23, 13:10-15, 19:30-32.

(b) POSITA Would be Motivated to Combine Ludtke and Scott

370. In my opinion, a POSITA would have been motivated to combine Ludtke and Scott. As I note above, the Ludtke reference meets most of the limitations of the claims of the '989 Patent with the exception of the "unique Device ID" limitation. Instead Ludtke discusses using "transaction device information" as part of the described encrypted transaction without explaining how to implement such information. A POSITA would naturally have turned to a similar implementation which provides detailed instructions, particularly one implementing a well-known solution, such as public key cryptography. As I describe below, Scott describes a similar implementation in detail and describes public key cryptography, *see* Ex. 1008 at 4:6-8.

371. Again, as I noted above, I also provide explanation of the specific factors that I understand are considered. The scope and content of the prior art would have motivated a POSITA to combine Ludtke and Okereke. As I explain above, Ludtke discloses almost all of the limitations of the claims except for "secret information" and the "unique" nature of a device ID code. Similar to Ludtke, Scott discloses authenticating a user using a "personal

identification device" (PID) for protected applications such as opening a hotel room door or a conducting a point-of-sale transaction. *Id.* at 8:5-12. Scott specifically describes a system for authentication of a mobile device to protect information for financial transactions. *Id.* at 2:5-16

372. Ludtke discloses a persistent, tamper proof memory, and a POSITA would have been motivated to combine the secret key disclosed in Scott with the system disclosed in Ludtke. The secret key infrastructure disclosed in Scott is similar to that disclosed in Okereke, as discussed above. As discussed above, a POSITA would have already known, as of the priority date of the '989 patent, that encryption using a secret key such as that disclosed in Scott would have been obvious when communicating confidential information. A POSITA specifically would have recognized the importance of encrypted communication when engaging in communications regarding financial information and especially when authenticating financial transactions. The use of secret information (such as that in PKI encryption) to perform this type of encryption was well-known ***decades*** before the filing date of the '989 patent, and was a well-established, well-known method for implementing encryption. For example, public key encryption was developed in the 1970s, and serves as a well-known way to encrypt and authenticate secret or confidential information. A POSITA would have recognized that such encryption is important to many applications, including financial information where it is particularly important to keep the information secret. In my opinion, a POSITA would therefore recognize that the use of secret information, which is disclosed in Scott, would make the system of Ludtke even

more secure. Scott simply demonstrates this knowledge prior to the '989 patent's priority date.

373. Ludtke discloses transaction device information communicated between the transaction device and the transaction privacy clearing house for authorization of a financial transaction. In my opinion, a POSITA would have combined the teachings of Scott's unique Device ID with Ludtke's system. As discussed above, Ludtke explicitly teaches communication of "transaction device information" with the TPCH. Ex. 1005 at 6:38-51. In my opinion, a POSITA would have recognized that such transaction device information necessarily includes unique device identifiers such as a serial number or other number that is specific to the processing unit. Scott explicitly discloses this fundamental information. Ex. 1008 at 8:20-23.

374. A POSITA would have been motivated to combine Ludtke and Scott because they are both in the same field of endeavor. Indeed, both references are in the same field of endeavor as the '989 patent, *i.e.*, authentication of a device, including use of biometric information, for the purpose of exchanging sensitive information over a network. *See* Ex. 1001 at 1:35-38 ("The present invention relates generally to computerized authentication, and more specifically, to an authentication responsive to biometric verification of a user being authenticated"); Ludtke at Abstract ("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"); Scott at Abstract ("A portable, hand-held personal identification device (6) and method for providing secure access to a host facility…"); *id.*

¶31 ("Where absolute security is essential, some host facilities employ a biometric sensor to measure a biometric trait of a person requesting access to the host facility").

375. In my opinion, a POSITA would have reasonably expected the combination of Ludtke and Scott to succeed and yield predictable results. Ludtke's system already discloses a persistent and tamper-proof memory and discusses the use of sensitive information. Ludtke also discloses transaction device information. Ex. 1005 at 6:38-51. Scott similarly discloses a persistent, tamper-proof memory. Scott teaches that data is stored in a memory where, after biometric enrollment, "there is no going back or editing." Ex. 1008 at 16:11-12. Given these disclosures, a POSITA would have expected the combination to result in Ludtke's financial system storing the secret information in Ludtke's memory and using the unique device ID disclosed in Scott as the transaction device information. A POSITA would have expected this to yield the predictable result of the option to use secret key encryption and decryption with a private key (secret information), as well as the ability to ensure authentication of an authorized device using unique device identifying information such as a serial number, and would have expected this combination to succeed.

376. For example, Ludtke describes a protected memory to keep the type of important and sensitive information described in Okereke. Ex. 1005 at 19:37-40. Moreover, a POSITA would be familiar with the secret key encryption system because it had long been used as a way to encrypt and decrypt information and share such information only for authorized users. §IV.A *supra*. Implementing such a system with Ludtke would

have been logical and obvious to a POSITA. Finally, both systems have similar types of mobile devices, and have similar goals. It would make sense to a POSITA to use the type of information identified in Scott in the Ludtke system to further complement Ludtke's features.

2. Claim 1

(a) [1a] "A method comprising: receiving, at a smartphone, an identification (ID) code from a third-party trusted authority, the ID code uniquely identifying the smartphone among a plurality of smartphones;"

377. The disclosure of Ludtke is described above in SNQ 1. Section IX.A.2.a, *supra*.

378. ***A smartphone***. While Scott does not explicitly disclose the use of a smartphone, Scott renders using a smartphone obvious. Scott discloses a "portable, hand-held personal identification device" similar in size and shape to a cell phone. Ex. 1005 at 4:22-24, 8:23-24, 13:16-26. As well as the use of telephone lines and computer lines for communication with the PID 6. Ex. 1005 9:16-22. The combination of Ludtke and Scott provides a motivation to use a Smartphone because, in addition to the reasons cited above, Scott teaches the PID should be small enough to be able to fit on a user's person while still providing access to a secure location. Ex. 1005 22:6-8. Combining a user's cellphone, such as that disclosed in Ludtke with the PID 6 would reduce what a user is required to carry while keeping the PID 6 small.

379. ***Identification (ID) code uniquely identifying the smartphone among a plurality of smartphones***: Ludtke discloses the TPCH having "transaction device

information" that is maintained in a secure database by the TPCH. *Id.* at 6:41-44. Ludtke does not further describe this "transaction device information." But, as I explain above, Scott discloses that the memory 20 of the PID 6 persistently stores a plurality of codes and other data values including an ID code that uniquely identifies the PID 6. Ex. 1005 at 4:9-10 ("The memory can further 10 store an ID code indicative of the enrolled person or the device."), 8:13-22, 11:14-20. Specifically, memory 20 stores information "specific to processing unit 16," including an ID code unique to the device, which may be set by the device manufacturer and can be the device serial number. Ex. 1005 at 11:11-13. In my opinion, a serial number is a unique code that identifies the device it is attached to. Scott also discloses wherein the PID 6 stores other data values such as "a synchronization counter associated with the user device." *Id.* at 6:28-7:23, 13:10-15, 19:30-32. As I discuss above, a POSITA would have been motivated to combine Ludtke with the teachings of Scott, and would have recognized that the "transaction device information" would include the ID code disclosed in Scott.

(b) [1b] "persistently storing biometric data and the ID code on the smartphone, wherein the biometric data is one selected from a group consisting of facial recognition, a fingerprint scan, and a retinal scan of a legitimate user;"

380. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section IX.A.2.b, *supra*.

(c) Persistently storing biometric data and the ID code on the smartphone:

381. As I explain above, Scott discloses that the memory 20 of the PID 6 persistently stores a plurality of codes and other data values including an ID code that uniquely identifies the PID 6. Ex. 1005 at 4:9-10 ("The memory can further 10 store an ID code indicative of the enrolled person or the device."), 8:13-22, 11:14-20. Specifically, memory 20 stores information "specific to processing unit 16," including an ID code unique to the device, which may be set by the device manufacturer and can be the device serial number. Ex. 1005 at 11:11-13. In my opinion, a serial number is a unique code that identifies the device it is attached to. Scott also discloses wherein the PID 6 stores other data values such as "a synchronization counter associated with the user device." *Id.* at 6:28-7:23, 13:10-15, 19:30-32.

382. As I discuss above, a POSITA would have been motivated to modify the system of Ludtke to incorporate the public/private key structure of Scott and the unique serial numbers also disclosed in Scott. In my opinion, a POSITA would have been motivated to store permanent information, such as the secret key (private key) and unique device identifiers (serial number). Moreover, a POSITA would have recognized that the "transaction device information" disclosed within Ludtke could further include the unique device information in Scott, which would ensure that the information used to authenticate the device only identifies the authorized device. In my opinion, a POSITA would also have stored the unique device identifiers and the secret key in the persistent tamper-proof memory, because this is important information that allows authorization and sensitive

communications to take place, and POSITA would have recognized the need to take care to ensure it is not easy to tamper with and modify the information.

(d) [1c] "receiving, at the smartphone, scan data from a biometric scan using the smartphone;"

383. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section IX.A.2.c, *supra*.

(e) [1d] "comparing, using the smartphone, the scan data to the biometric data;"

384. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section IX.A.2.d, *supra*.

(f) [1e] "determining whether the scan data matches the biometric data; and"

385. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section IX.A.2.e, *supra*. *See also,* element [1d], Section IX.A.2.d, *supra*.

(g) [1f] "responsive to a determination that the scan data matches the biometric data, wirelessly sending, from the smartphone, 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, a transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code, 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 website, a file and a financial account."

386. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section IX.A.2.f, *supra*.

3. Claim 2: "The method of claim 1, further comprising: Receiving a request for biometric verification, 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."

387. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section IX.A.3, *supra*.

4. Claim 3: "The method of claim 1, wherein completing the transaction includes accessing an application."

388. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section IX.A.4, *supra*.

5. 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 authority sending an indication that the third party trusted authority authenticated the ID code to another party."

389. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section IX.A.5, *supra*.

6. Claim 5:

(a) [5a] "a smartphone, comprising."

390. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section IX.A.6.a, *supra*. *See also* Claim 1, Element [1a], Section IX.B.1.a, *supra*.

(b) [5b] "a persistent storage having an input that receives an identification (ID) code from a third party trusted authority, and biometric data, wherein the biometric data is one selected from a group consisting of facial recognition, a fingerprint scan, and a retinal scan, of a legitimate user, the ID code uniquely identifying the smartphone among a plurality of smartphones, the persistent storage storing the biometric data and the ID code, the persistent storage having an output configured to provide a first set of biometric data and the ID code for use on the smartphone;"

391. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section IX.A.6.b, *supra*. *See also* Claim 1, Elements [1a-1b], Section IX.B.1.a-b, *supra*.

(c) [5c] "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; and"

392. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section IX.A.6.c, *supra*. *See also* Elements [1c-1e], Sections IX.B.1.c-e, *supra*.

(d) [5d] "a wireless transceiver 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, a transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code, 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."

393. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section IX.A.2.d, *supra*. *See also* Claim 1, Element [1f], Section IX.B.1.f, *supra*.

7. Claim 6: "The smartphone of claim 5, wherein the ID code is transmitted to the third-party trusted authority over a network."

394. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section IX.A.7, *supra*.

8. Claim 7

(a) [7a]. "A system, comprising: a smartphone that persistently stores biometric data and an ID code, 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, and the ID code is received from a third-party trusted authority, the ID code uniquely identifying the smartphone among a plurality of smartphones,"

395. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section IX.A.8.a, *supra*. *See also* Claim 1, Elements [1a-1b]. Section IX.B.1.a-b, *supra*.

(b) [7b]. "the smartphone configured to indicate that a biometric authentication is requested,"

396. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section IX.A.8.b, *supra*. *See also* Claim 1, Element [1c], Section IX.B.1.c, and claim 2, Section IX.B.2 *supra*.

(c) [7c] "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 biometric scan performed using the smartphone matches the biometric data of the legitimate user, wherein a transaction is completed responsive to successful authentication of the ID code by the third-party trusted authority, wherein the transaction being completed includes accessing one or more from a group consisting of a casino machine, a keyless lock, anATM machine, a web site, a file and a financial account; and"

397. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section IX.A.8.c, *supra*. *See also* claim 1, element [1f], Section IX.B.1.f, *supra*.

(d) [7d] "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."

398. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section IX.A.8.d, *supra*. *See also* claim 1, Elements [1a], [1f], sections IX.B.1.a, IX.B.1.f, *supra*.

9. 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 smartphone does not send the ID code."

399. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section IX.A.9, *supra*. *See also* claim 2, Section IX.B.2, *supra*.

10. Claim 9: "The system of claim 7, wherein completing the transaction includes accessing an application."

400. The disclosure of Ludtke for this limitation is described above in SNQ 1. Section IX.A.10, *supra*. *See also* claim 3, Section IX.B.3, *supra*.

IX. SECONDARY CONSIDERATIONS

401. I have been informed that Patent Owner has not identified any evidence of secondary considerations, either in the prosecution history or in the related district court litigation. I am not aware of any evidence of secondary considerations supporting a finding of non-obviousness. The analysis above indicates that many of these researchers independently invented the same technology described and claimed in the Challenged Patents all within a relatively short period of time when faced with the same technical problem. I understand this observation heightens the obviousness of the Challenged Claims.

X. CONCLUSION

402. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on the information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.



Executed: June 8, 2022 Benjamin F. Goldberg

Curriculum Vitae

BENJAMIN F. GOLDBERG

200 Mercer Street #2F
New York, New York 10012
Phone: (917) 576-5127
goldberg@benjamingoldberg.com

Personal

Born January 31, 1961, Las Cruces, New Mexico.

U.S. Citizen.

Education

Ph.D. in Computer Science, Yale University, 1988. Dissertation: "Multiprocessor Execution of Functional Programs."

M.S. and M.Phil in Computer Science, Yale University, 1984.

B.A. with Highest Honors in Mathematical Sciences, Williams College, Cum Laude, Phi Beta Kappa, Sigma Xi, June 1982. Honors Thesis: "Theory and Implementation of an Automatic Program Verifier."

Employment

Associate Professor (Tenured), Courant Institute of Mathematical Sciences, Department of Computer Science, New York University. September 1994 – Present.

Invited Professor, Ecole Normale Supérieur, Paris, France. June 2007 – July 2007 and June 2003 – July 2003.

Director of Graduate Studies (for the MS programs), Department of Computer Science, New York University. September 2009 – August 2012 and September 2014 – present.

Director of Undergraduate Studies, Department of Computer Science, New York University. September 1995 – August 1998 and September 2003 – August 2006.

Visiting Professor, Institute National de Recherche en Informatique et en Automatique (INRIA), Rocquencourt, France. September 1994 – August 1995.

Assistant Professor, Courant Institute of Mathematical Sciences, Department of Computer Science, New York University. September 1987 - August 1994.

Expert Testimony at Trial or Deposition in the Past Five Years

Retained by Sheppard Mullin on behalf of Healthplan Services, Inc. in the matter of *Blue Shield of California v. Healthplan Services*, U.S. District Court for the Northern District of California, San Francisco Division. Case No. 3:18-cv-3730, August 2019-present.

Retained by Goodwin Proctor on behalf of 2Wire, Inc. in the matter of *TQ Delta v. 2Wire*. U.S. District Court for the District of Delaware, Case No. 13-cv-01835-RGA. February 2020-present.

Retained by Kirkland & Ellis on behalf of Samsung in the matter of *Certain Mobile Devices with Multifunction Emulators* (Dynamics v. Samsung). US International Trade Commission, Investigation No. 337-TA-1170. November 2019 – November 2020.

Retained by Quinn Emanuel on behalf of Opticon in the Matter of *Certain Barcode Scanners, Scan Engines, Products Containing the Same, and Components Thereof* (Honeywell v. Opticon). US International Trade Commission, Investigation No. 337-TA-1165. August 2019 – January 2020.

Retained by Duane Morris on behalf of Target in the matter of *Dyfan v. Target*, U.S. District Court for the Western District of Texas, Waco Division. Case No. 6:19-cv-00179-ADA, August 2019 – December 2019.

Retained by Morrison & Foerster on behalf of Spotify in the matter of *SISVEL v. Spotify* (*Inter Partes Review* before the USPTO). Case IPR2019-00521, October 2018 – October 2019.

Retained by Sidley Austin on behalf of Apple in the matter of *Omni MedSci v. Apple*, U.S. District Court for the Eastern District of Texas, Marshall Division. Case No. 2:18-cv-134, December 2018 – August 2019.

Retained by Morrison & Foerster on behalf of IEX Group in the matter of *Nasdaq v. IEX Group* (Covered Business Method patent review before the USPTO). Case CBM2018-00039, May 2018 – March 2020.

Retained by Kirkland & Ellis on behalf of Apple, by Sheppard Mullin on behalf of HTC, and by McDermott Will & Emery on behalf of ZTE in the Matter of *Certain LTE- And 3G-Compliant Cellular Communications Devices* (INVT v. Apple, HTC, and ZTE), US International Trade Commission Investigation No. 337-TA-1138. September 2018 – September 2019.

Retained by Seyfarth Shaw on behalf of Capstone Logistics in the matter of *Capstone Logistics v. Pedro Navarrete et al.* US District Court for the Southern District of New York, Civil Action No. 17-4819-GBD-BCM. June 2018 – July 2019.

Retained by Norton Rose Fulbright on behalf of Papa John's USA in the matter of *In Re Ameranth Patent Litigation*. U.S. District Court for the Southern District of California, Lead Case No. 3:11-CV-01810-DMS-WVG. December 2017-September 2018.

Retained by Latham & Watkins on behalf of Oracle in the matter of *Oracle v. Hewlett Packard Enterprise*. US District Court for the Northern District of California, San Francisco Division, Case No. 16-cv-01393-JST. July 2017 – Present.

Retained by Quinn Emanuel on behalf of StubHub in the matter of *Calendar Research v. StubHub et al.* US District Court for the Central District of California, Western Division – Los Angeles, Case No. CV 17-4062-SVW. September 2017-August 2018.

Retained by Arnold & Porter Kay Scholer on behalf of Google in the matter of *KlausTech v. Google*. US District Court for the Northern District of California, Oakland Division, Case No. C 10-05899 JSW. October 2015-January 2018.

Retained by Baker & Hostetler by intervenor IAC Search & Media in the matter of *Finjan v. Symantec*. US District Court for the Northern District of California, Oakland Division, Case No. 4:14-cv-02998-HSG. November 2017- January 2018.

Retained by Morrison & Foerster on behalf of Nikon in the Matter of *Certain Digital Cameras, Software, and Components Thereof* (Zeiss v. Nikon), International Trade Commission, Investigation No. 337-TA-1059. August 2017-January 2018.

Retained by Quinn Emanuel on behalf of Samsung, by Sheppard Mullin on behalf of HTC, and by Kilpatrick Townsend on behalf of Lenovo and Motorola Mobility in the matters of *Evolved Wireless v. Samsung*, *Evolved Wireless v. HTC*, and *Evolved Wireless v. Lenovo and Motorola Mobility*. US District Court for the District of Delaware, Civil Action Nos. 15--545--SLR-SRF, 15-543-SLR-SRF, and 15-544-SLR-SRF. November 2016- August 2017.

Retained by Norton Rose Fulbright on behalf of Priceline, Kayak, and Open Table in the matter of *IBM v. The Priceline Group et al.*, US District Court for the District of Delaware, Civil Action No. 1:15-cv-00137-LPS-CJB. June 2016-December 2017.

Retained by Andrews Kurth Kenyon on behalf of Viatech Technologies in the matter of *Viatech Technologies v. Microsoft.* US District Court for the District of Delaware, Case No. 14-1226-RGA. March 2015-June 2017.

Retained by Allen, Dyer, Doppelt, Milbrath & Gilchrist on behalf of Live Face on Web in the matter of *Live Face on Web v. Major League Builders*, US District Court for the Central District of California, Case No. CV15-9927 PA (AGRx), *Live Face on Web v. Full Service Vending*, US District Court for the Western District of Texas, San Antonio Division, Case No. 5:15-cv-00539-HJB, and *Live Face on Web v. Integrity Solutions*. US District Court for the District of Colorado, Case No. 1:16-cv-01627-KLM. October 2014-May 2020.

Retained by Cooley on behalf of Apple in the matter of *Odyssey Wireless v. Apple*. US District Court for the Southern District of California, Case No. 15-cv-1735-H-RBB. March 2016-October 2016.

Retained by Milbank Tweed on behalf of Apple in the matter of *Rembrandt Patent Innovations v. Apple*. US District Court for the Northern District of California, Case No. C 14-05094 WHA (Lead Case), Case No. C 14-05093 WHA (Consolidated Case). July 2015-May 2016.

Retained by Gibson Dunn & Crutcher on behalf of Facebook in the matter of *Campbell v. Facebook*. US District Court for the Northern District of California, Case No. 13-cv-05996-PJH (MEJ). October 2015-March 2016.

Retained by Kaye Scholer on behalf of Google in the matter of *ContentGuard v. Google* (Covered Business Method patent review before the USPTO). Case CBM2015-00040. August 2014 – January 2016.

Retained by Boies Schiller on behalf of InfoSpan in the matter of *InfoSpan v. Emirates NBD Bank*. US District Court for the Central District of California, Southern Division. Civil Action No. 8:11-CV-01062 JVS (ANx) September 2013 – August 2016.

Teaching Awards

New York University "Golden Dozen" Award, 1992. Awarded to twelve faculty members in the entire College of Arts and Sciences for excellence in teaching.

Professional Activities

Editorial Board, *The Computer Journal*. Published by Oxford University Press on behalf of the British Computer Society. 2007 – 2009.

Program Committee member: 2007 Symposium on Principles of Programming Languages (POPL)

External Review Committee member: 2013 Symposium on Principles of Programming Languages (POPL)

Program Committee member: 2001 Workshop on Practical Applications of Declarative Languages (PADL'01), ACM SIGPLAN'95 Conference on Programming Language Design and Implementation, 1995 ACM SIGPLAN Symposium on Partial Evaluation and Semantics-Based Program Manipulation (PEPM '95), 1995 International Workshop on Memory Management (IWMM'95), ACM SIGPLAN'93 Conference on Programming Language Design and Implementation.

Review Panel Member, National Science Foundation, January 1998 and January 2000.

Official Collaborator, Los Alamos National Laboratory, Computing and Communications Division.

Member, Association for Computing Machinery and ACM Special Interest Group on Programming Languages (SIGPLAN).

Referee for: ACM TOPLAS, IEEE Computer, International Journal of Parallel Programming, Software Practice and Experience, Computational Intelligence, ACM TOCS, ACM Computing Surveys, etc.

Referee for a variety of ACM and IEEE conferences.

Journal Papers

"Translation and Run Time Validation of Optimized Code", with L. Zuck, A. Pnueli, C. Barrett, Y. Fang, and Y. Hu, *Formal Methods in System Design*. 27(3): 335-360, November 2005

"VOC: A Methodology for Translation Validaton of Optimizing Compilers", with L. Zuck, A. Pnueli, and Y. Fang. *Journal of Universal Computer Science*, March 2003.

"A Syntactic Method for Finding Least Fixed Points of Higher-Order Functions over Finite Domains", with Tyng-Ruey Chuang. *Journal of Functional Programming*. Vol. 7, No. 4, pp. 357-394, July 1997

"Functional Programming Languages", in ACM 50th Anniversary Issue of Computing Surveys. March 1996.

"Order-of-demand analysis for lazy languages", with Young-Gil Park. Information Processing Letters, Vol. 55, 1995, pp. 343-348.

"Static Analysis for Optimizing Reference Counting", with Young-Gil Park. Information Processing Letters, Vol. 55, 1995, pp. 229-234.

"Multiprocessor Execution of Functional Programs", International Journal of Parallel Programming, Vol. 17, No. 5, October 1988.

"Distributed Execution of Functional Programs Using Serial Combinators," with P. Hudak, IEEE Transactions on Computers, Vol. C-34, No. 10, October 1985, pp. 881-891.

Books or Chapters in Books

"Functional Programming Languages", in Handbook of Computer Science and Engineering, CRC Press, Inc. 1996.

Publications in Proceedings of Refereed Symposia

"Translation Validation of Loop Optimizations and Software Pipelining in the TVOC Framework". Proceedings of the 17th International Static Analysis Symposium (SAS 2010), September 2010.

"TVOC: A translation validator for optimizing compilers", with C. Barrett, Y. Fang, Y. Hu, A.Pnueli, and L. Zuck. Proceedings of the 17th International Conference on Computer Aided Verification (CAV '05), July 2005.

"Theory and algorithms for the generation and validation of speculative loop optimizations", with Y. Hu and C. Barrett. Proceedings of the 2nd IEEE International Conference on Software Engineering and Formal Methods (SEFM), September 2004.

"Into the Loops: Practical Issues in Translation Validation for Optimizing Compilers", with L. Zuck and C. Barrett. Proceedings of the Third International Workshop on Compiler Optimization meets Compiler Verification (COCV). April 2004.

"Run-Time Validation of Speculative Optimizations using CVC", with C. Barrett and L. Zuck. Proceedings of the Workshop on Runtime Verification 2003, ENTCS 89(2). July 2003.

"Software Bubbles: Using Predication to Compensate for Aliasing in Software Pipelines", with E. Chapman, C. Huneycutt, and K. Palem. Proceedings of the PACT-2002 International Conference on Parallel Architectures and Compilation Techniques, September 2002.

"Translation and Run-Time Validation of Optimized code", with L. Zuck, A. Pnueli, Y. Fang, and Y. Hu. Proceedings of the Workshop on Runtime Verification 2002, ENTCS 70(4). July 2002.

"VOC: A Translation Validator for Optimizing Compilers". Proceedings of the Workshop on Compiler Optimization Meets Compiler Verification (COCV) 2002, ENTCS 65(2). April 2002.

"Formal Models of Distributed Memory Management", with Cristian Ungureanu. Proceedings of the ACM International Conference on Functional Programming, June 1997.

"Partial Evaluation of Concurrent Programs", with Mihnea Marinescu. Proceedings of the ACM Symposium on Partial Evaluation and Program Manipulation, June 1997.

"Real-Time Deques, Multihead Turing Machines, and Purely Functional Programming", with T-R. Chuang. Proceedings of the 1993 ACM Conference on Functional Programming Languages and Computer Architecture, June 1993.

"Polymorphic Type Reconstruction for Garbage Collection without Tags", with M. Gloger. Proceedings of the 1992 ACM Conference on LISP and Functional Programming, June 1992.

"A Syntactic Approach to Fixed Point Computation on Finite Domains", with T.R. Chuang. Proceedings of the 1992 ACM Conference on LISP and Functional Programming, June 1992.

"Escape Analysis on Lists", with Y.G. Park. Proceedings of the 1992 ACM SIGPLAN Conference on Programming Language Design and Implementation, June 1992.

"Incremental Garbage Collection without Tags", Proceedings of the 1992 European Symposium on Programming, February 1992.

"Reference Escape Analysis: Optimizing Reference Counting based on the Lifetime of References", with Y.G. Park. Proceedings of the 1991 ACM/IFIP Conference on Partial Evaluation and Program Manipulation, June 1991.

"Tag-Free Garbage Collection for Strongly Typed Programming Languages", Proceedings of the ACM SIGPLAN'91 Conference on Programming Language Design and Implementation, June 1991.

"Higher Order Escape Analysis: Optimizing Stack Allocation in Functional Program Implementations", Proceedings of the 1990 European Symposium on Programming, May 1990. Springer-Verlag LNCS 432, pp. 152-160.

"Generational Reference Counting: A Reduced-Communication Distributed Storage Reclamation Scheme", Proceedings of the SIGPLAN'89 Conference on Programming Language Design and Implementation, June 1989.

"A Reduced-Communication Storage Reclamation Scheme for Distributed Memory Multiprocessors", Proceedings of the Fourth Conference on Hypercubes, Concurrent Computers, and Applications, January 1989.

"Buckwheat: Graph Reduction on a Shared Memory Multiprocessor", Proceedings of the 1988 ACM Symposium on Lisp and Functional Programming, July 1988, pp. 40-51.

"Executing Functional Programs on a Hypercube Multiprocessor", Proceedings of the Third Conference on Hypercube Concurrent Computers and Applications, January 1988.

"Detecting Sharing of Partial Applications in Functional Programs", Proceedings of the Conference on Functional Programming Languages and Computer Architecture, September 1987. Published in the Springer-Verlag Lecture Notes in Computer Science, Vol. 274, pp. 408-425.

"Serial Combinators: "Optimal" Grains of Parallelism", with P. Hudak, Proceedings of the IFIP Conference on Functional Programming Languages and Computer Architecture, September 1985. Published in the Springer-Verlag Lecture Notes in Computer Science, Vol. 201, pp. 382-389.

"Experiments in Diffused Combinator Reduction," with P. Hudak, Proceedings of the ACM Symposium on Lisp and Functional Programming, August 1984, pp. 167-176.

Keynote Addresses, Invited Talks and Tutorials

Keynote Address, "Software Pipelining and Loop Optimizations in the Presence of Memory Aliasing", 8th Workshop on Compiler Techniques for High Performance Computing, Hualien, Taiwan, March 2002.

Invited Talk, "Translation Validation of Loop Optimizations", Ecole Normale Supérieur, Paris. July 2003.

Invited tutorial, "The Trimaran Compiler Research Infrastructure", given at at the following conferences:

- IEEE Symposium on Parallel Architectures and Compiler Techniques (PACT'98), Paris, October 1998.
- IEEE Symposium on Microarchitecture (MICRO-31), Dallas, December 1998.
- 1999 ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI'99), Atlanta, June 1999.

Tutorial, "Functional Programming", 1994 ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI'94). Orlando, June 1994.

Research Grants and Contracts

"Property-Based Development of reactive and Embedded Systems", with A. Pnueli and L. Zuck. National Science Foundation, August 2007 – May 2009.

"PTV: Translation Validation in the Phoenix Compiler Framework", with A. Pnueli (coordinated proposal with L. Zuck of U. Illinois-Chicago). Microsoft, April 2006.

"A Methodology for Establishing the Dependability and Security of Telecommunication Protocols", with A. Pnueli and L. Zuck. Office of Naval Research, July 2003 – June 2005.

"Towards a Seamless Process for the Development of Embedded Systems", with A. Pnueli and L. Zuck. National Science Foundation, September 2002 - August 2005.

"Translation Validation of Advanced Compiler Optimizations", with L. Zuck and A. Pnueli. National Science Foundation, June 2001 – May 2006.

"Algorithmic Techniques for Compiler Controlled Caches", with K. Palem. Air Force, July 1999 - June 2002.

"Parallel Extensions of the MSTAR System", with E. Freudenthal. AFOSR, August 1999 - July, 2001.

"A Computational Laboratory for Automatic Target Recognition", with D. Geiger and E. Freudenthal. AFOSR, March 1998 - March 1999.

"Mobile and Stationary Target Acquisition and Recognition", DARPA/Air Force, June 1997-March 2000.

"An Integrated Parallel Programming Environment for High Performance Parallel Computing on Workstation Clusters", Department of Energy. May 1994. With Los Alamos National Laboratory and IBM.

"GRIFFIN - A Common Prototyping Language: Design, Implementation, and Assessment", with R. Dewar, M. Harrison, E. Schonberg and D. Shasha. DARPA/Office of Naval Research, May 1992 - April 1995.

"Research Training in Software Prototyping Languages and Environments". DARPA/ONR May 1992 - April 1995.

"Studies in Automatic Dynamic Load Balancing on Large Loosely-Coupled Multiprocessors", National Science Foundation Research Initiation Award. September 1989 - June 1992.

"GRIFFIN: a Common Prototyping Language", with R.Dewar, E. Schonberg, M. Harrison, and D. Shasha. DARPA/ONR September 1989 - April 1992.

New Courses Developed

"Object Oriented Programming". An undergraduate course covering Java, C++, UML, and object oriented programming techniques. Also developed an MS-level OOP course.

"The Design and Programming of Embedded Systems". A graduate course addressing the computing hardware and software designs in handheld devices, cell phones, appliances, etc.

"Compilers for Advanced Computer Architectures". A graduate course in optimization techniques for emerging microprocessors.

"Honors Programming Languages". A Ph.D. course in Programming Language Design and theory.

US007188110B1

(12) **United States Patent**
Ludtke et al.

(10) **Patent No.: US 7,188,110 B1**
(45) **Date of Patent: Mar. 6, 2007**

(54) **SECURE AND CONVENIENT METHOD AND APPARATUS FOR STORING AND TRANSMITTING TELEPHONY-BASED DATA**

(75) Inventors: **Harold Aaron Ludtke**, San Jose, CA (US); **Brant L. Candelore**, Escondido, CA (US)

(73) Assignees: **Sony Corporation**, Tokyo (JP); **Sony Electronics Inc.**, Park Ridge, NJ (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 66 days.

(21) Appl. No.: **09/734,839**

(22) Filed: **Dec. 11, 2000**

(51) **Int. Cl.**
G06F 17/30 (2006.01)

(52) **U.S. Cl.** **707/10**

(58) **Field of Classification Search** 707/6, 707/10, 104.1; 704/273, 247; 705/51; 455/563, 455/411; 713/182, 178; 709/217, 219; 715/746
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,329,589	A	7/1994	Fraser et al.	
5,561,709	A	10/1996	Remillard	
5,634,746	A	8/1997	McMullan, Jr. et al.	
5,748,890	A	5/1998	Goldberg et al.	
5,815,665	A	9/1998	Teper et al.	
5,878,139	A	3/1999	Rosen	
5,933,811	A	8/1999	Angles et al.	
6,000,832	A	12/1999	Franklin et al.	
6,029,141	A	2/2000	Bezos et al.	
6,076,075	A	6/2000	Teicher	
6,119,101	A	9/2000	Peckover	
6,128,602	A	10/2000	Northington et al.	
6,144,848	A	11/2000	Walsh et al.	
6,148,241	A	11/2000	Ludtke et al.	
6,163,771	A	12/2000	Walker et al.	
6,166,730	A	12/2000	Goode et al.	
6,237,096	B1 *	5/2001	Bisbee et al.	713/178
6,263,311	B1 *	7/2001	Diddy	704/273
6,264,560	B1	7/2001	Goldberg et al.	
6,282,582	B1	8/2001	Thompson et al.	
6,311,214	B1	10/2001	Rhoads	
6,356,905	B1	3/2002	Gershman et al.	
6,393,305	B1 *	5/2002	Ulvinen et al.	455/563
6,434,403	B1	8/2002	Ausems et al.	
6,434,747	B1	8/2002	Khoo et al.	
6,609,113	B1	8/2003	O'Leary et al.	
6,668,322	B1 *	12/2003	Wood et al.	713/182
6,675,203	B1 *	1/2004	Herrod et al.	709/217
6,778,998	B2 *	8/2004	Kondo et al.	707/104.1
6,804,705	B2 *	10/2004	Greco et al.	709/219
6,895,558	B1 *	5/2005	Loveland	715/746

FOREIGN PATENT DOCUMENTS

TW	351799	2/1999

OTHER PUBLICATIONS

Tryllian Mobile Agents: Going Beyond the Web, A Commercial White Paper, Version 1.0- May 18, 2000, p. 1-21.

Alan Neibauer, "Running Microsoft Outlook 98", Microsoft Press, p. 44-55 (Copyright 1998).

About Gossip, http://www.Tryllian.com including Quickstart Guide, Products and Downloads (6 pgs.) (Copyright 1999-2000).

Alan Freedman, The Computer Desktop Encyclopedia (2nd Ed.), pp. 16, 86, 1029. The Computer Language Company Inc., Point Pleasant, PA (Copyright 1999).

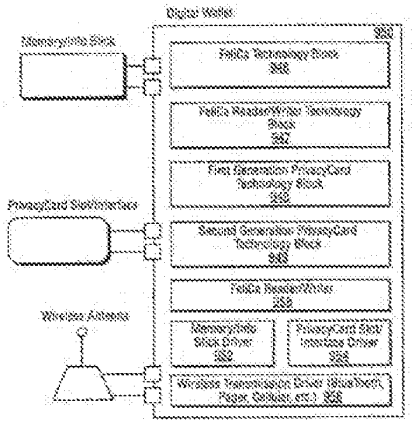
* cited by examiner

Primary Examiner—Diane Mizrahi
(74) *Attorney, Agent, or Firm*—Blakely, Sokoloff, Taylor & Zafman LLP

(57) **ABSTRACT**

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.

23 Claims, 31 Drawing Sheets



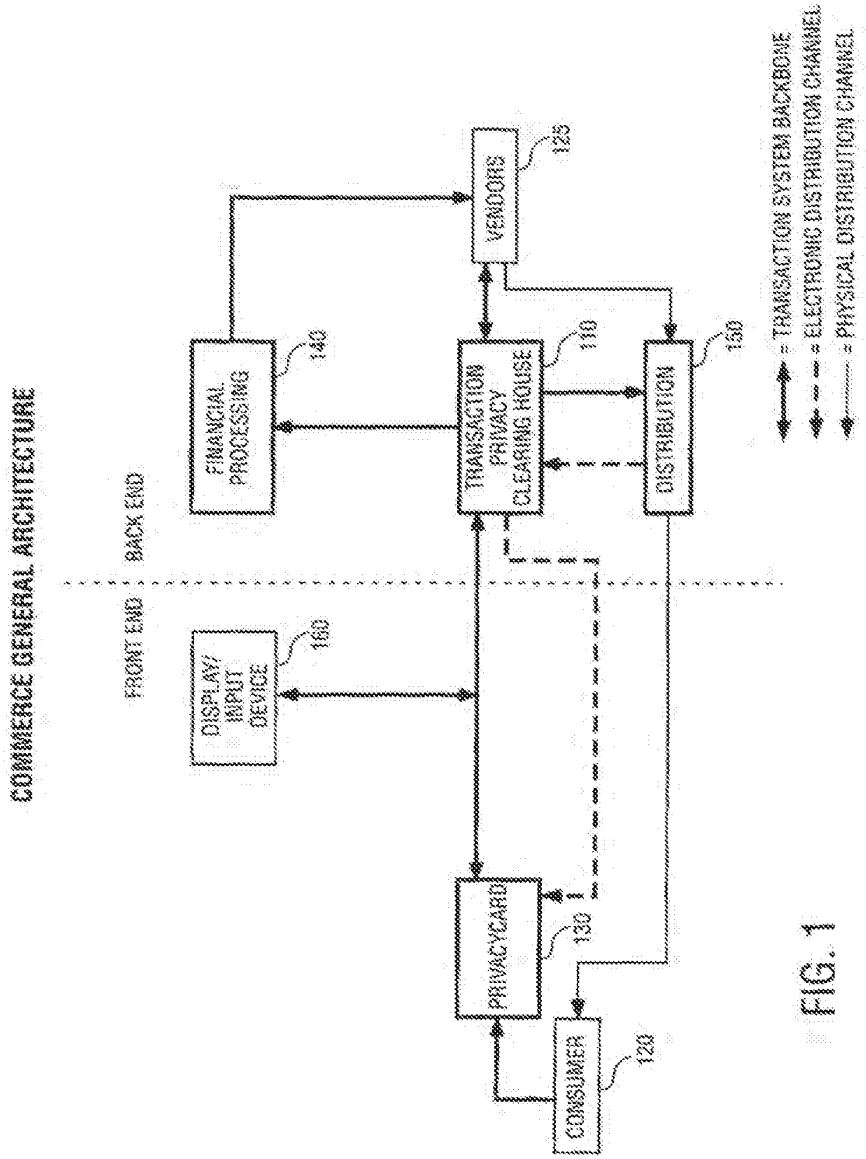

COMMERCE GENERAL ARCHITECTURE
FRONT END
BACK END
DISPLAY/ INPUT DEVICE
160
FINANCIAL PROCESSING
140
VENDORS
125
TRANSACTION PRIVACY CLEARING HOUSE
110
DISTRIBUTION
150
PRIVACYCARD
130
CONSUMER
120
= TRANSACTION SYSTEM BACKBONE
= ELECTRONIC DISTRIBUTION CHANNEL
= PHYSICAL DISTRIBUTION CHANNEL

FIG. 1

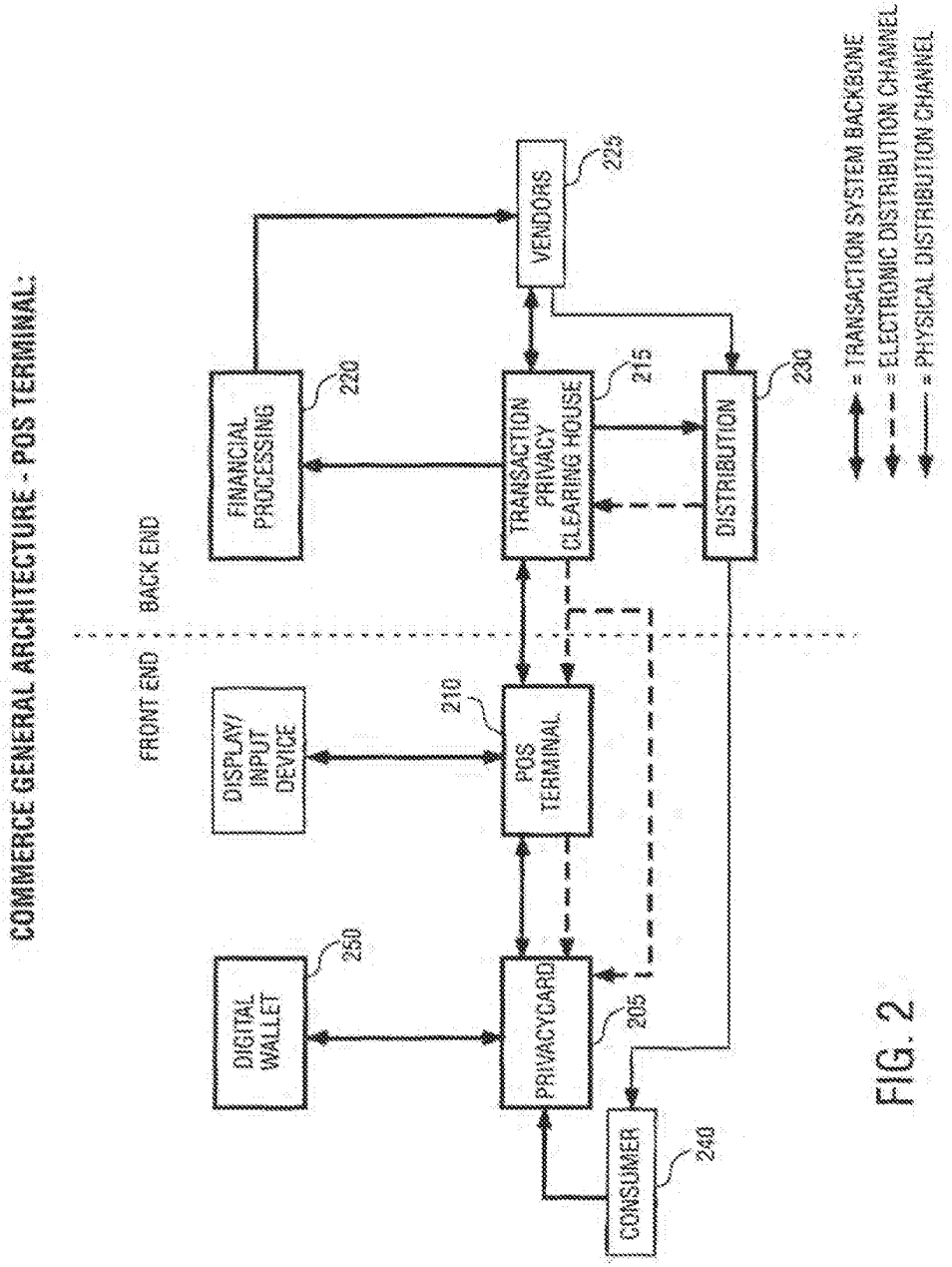

COMMERCE GENERAL ARCHITECTURE - POS TERMINAL:
FRONT END
BACK END
DIGITAL WALLET
250
DISPLAY/ INPUT DEVICE
210
POS TERMINAL
PRIVACYCARD
205
CONSUMER
240
FINANCIAL PROCESSING
220
TRANSACTION PRIVACY CLEARING HOUSE
215
VENDORS
225
DISTRIBUTION
230
= TRANSACTION SYSTEM BACKBONE
= ELECTRONIC DISTRIBUTION CHANNEL
= PHYSICAL DISTRIBUTION CHANNEL

FIG. 2

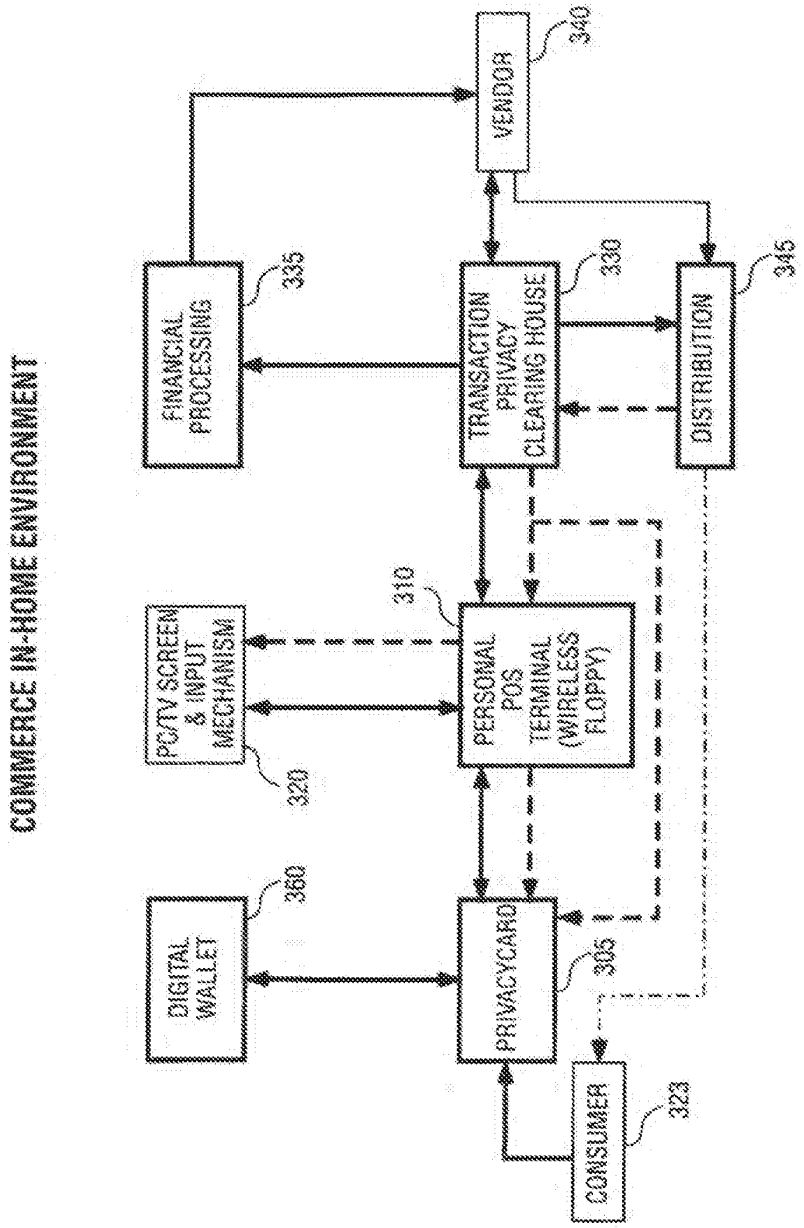

COMMERCE IN-HOME ENVIRONMENT
VENDOR
340
FINANCIAL PROCESSING
335
TRANSACTION PRIVACY CLEARING HOUSE
330
DISTRIBUTION
345
PC/TV SCREEN & INPUT MECHANISM
320
310
PERSONAL POS TERMINAL (WIRELESS FLOPPY)
DIGITAL WALLET
360
PRIVACYCARD
305
CONSUMER
323

FIG. 3

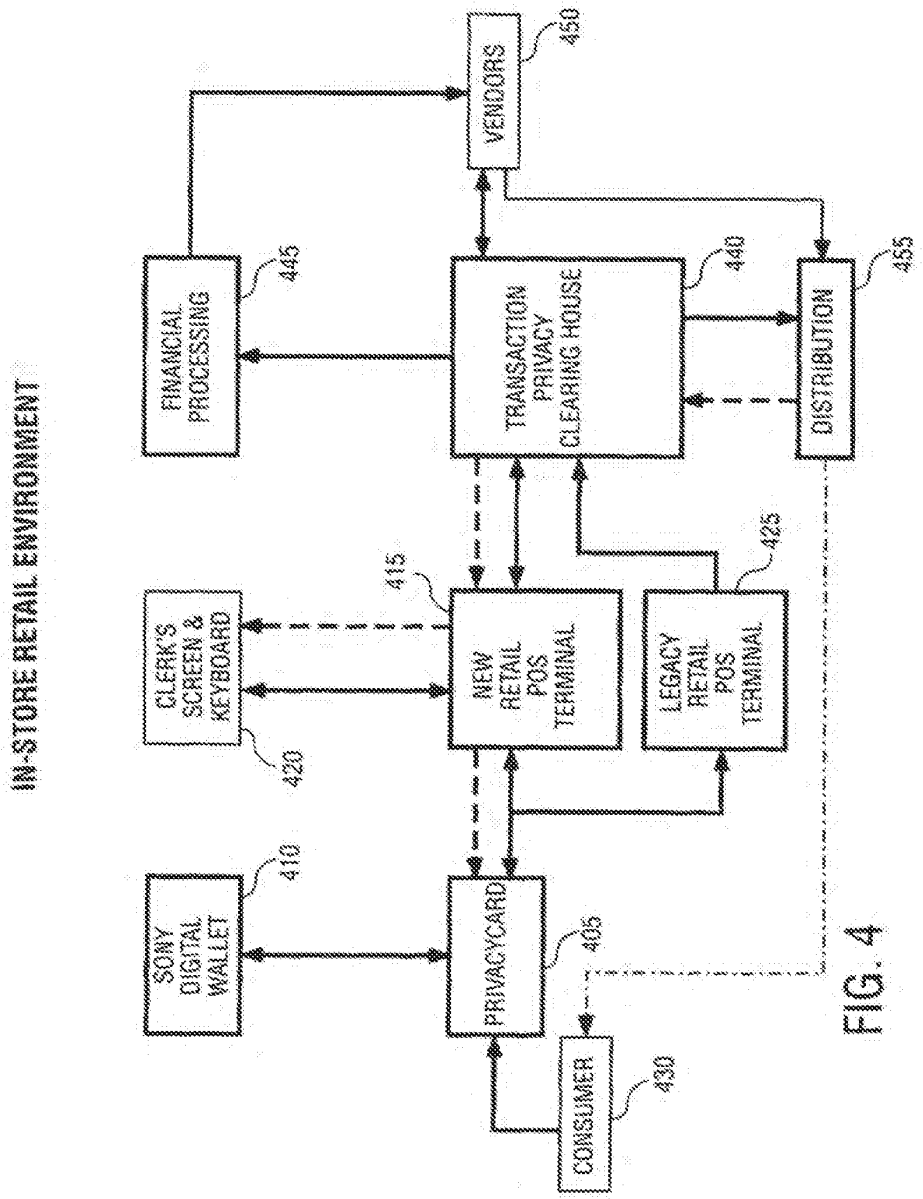
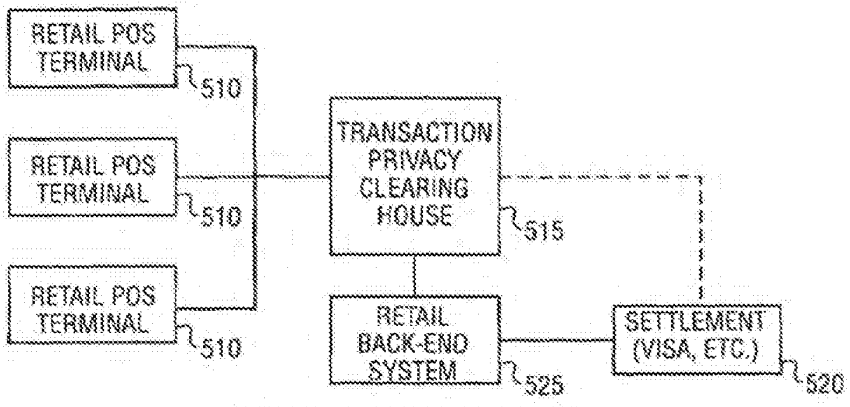
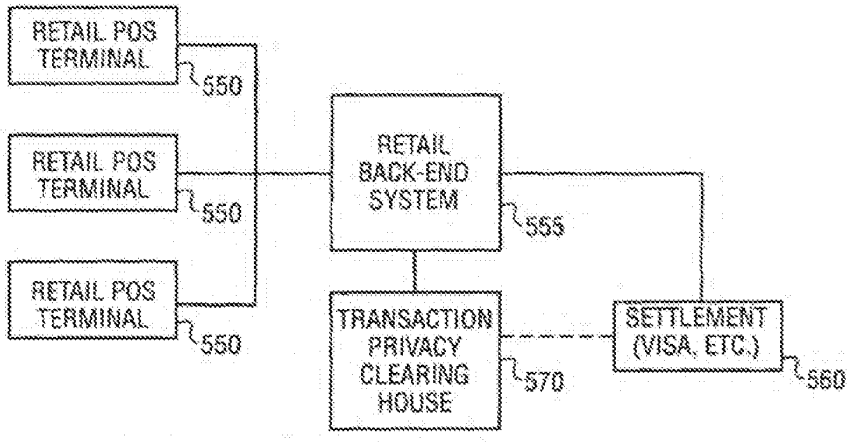

IN-STORE RETAIL ENVIRONMENT
VENDORS
450
FINANCIAL PROCESSING
445
TRANSACTION PRIVACY CLEARING HOUSE
440
DISTRIBUTION
455
CLERK'S SCREEN & KEYBOARD
420
415
NEW RETAIL POS TERMINAL
LEGACY RETAIL POS TERMINAL
425
SONY DIGITAL WALLET
410
PRIVACYCARD
405
CONSUMER
430

FIG. 4



A RETAIL SYSTEM MODIFIED TO SUPPORT THE INTERACTION OF LEGACY POS TERMINAL WITH THE DIGITAL WALLET SYSTEM

FIG. 5A



AN ALTERNATIVE EMBODIMENT OF THE RETAIL SYSTEM MODIFIED TO SUPPORT THE INTERACTION OF LEGACY POS TERMINALS WITH THE DIGITAL WALLET SYSTEM

FIG. 5B

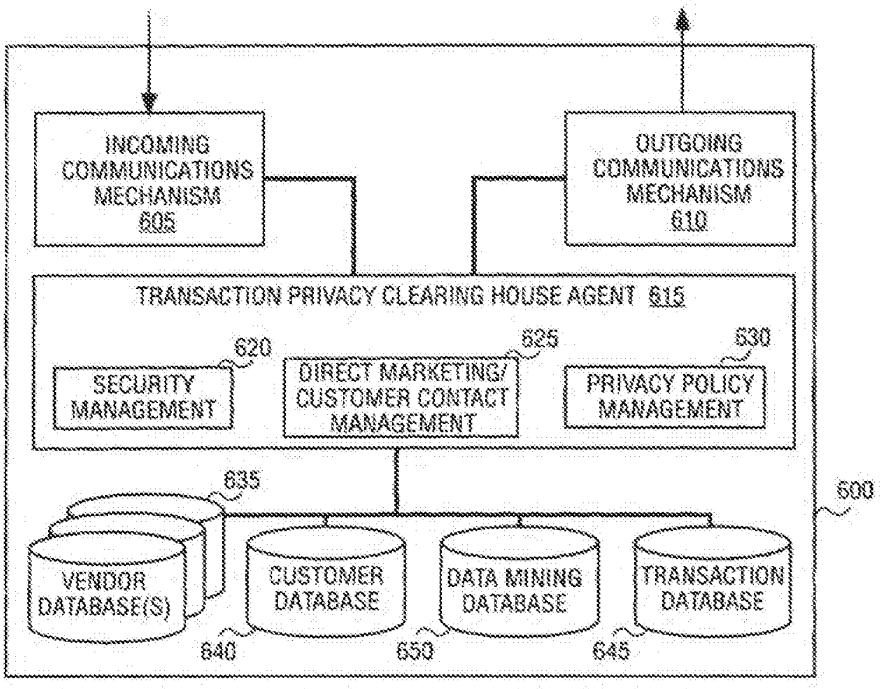

INCOMING COMMUNICATIONS MECHANISM 605
OUTGOING COMMUNICATIONS MECHANISM 610
TRANSACTION PRIVACY CLEARING HOUSE AGENT 615
620
SECURITY MANAGEMENT
625
DIRECT MARKETING/ CUSTOMER CONTACT MANAGEMENT
630
PRIVACY POLICY MANAGEMENT
635
600
VENDOR DATABASE(S)
CUSTOMER DATABASE
DATA MINING DATABASE
TRANSACTION DATABASE
640
650
645
TRANSACTION PRIVACY CLEARING HOUSE: MAJOR COMPONENTS

FIG. 6

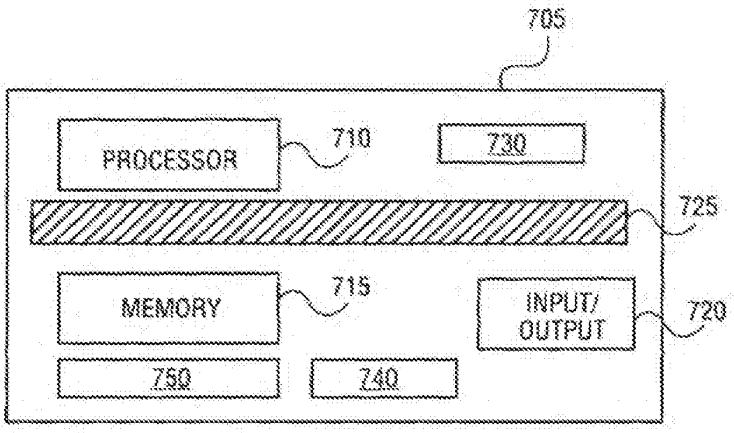

705
PROCESSOR
710
730
725
MEMORY
715
INPUT/
OUTPUT
720
750
740

FIG. 7A

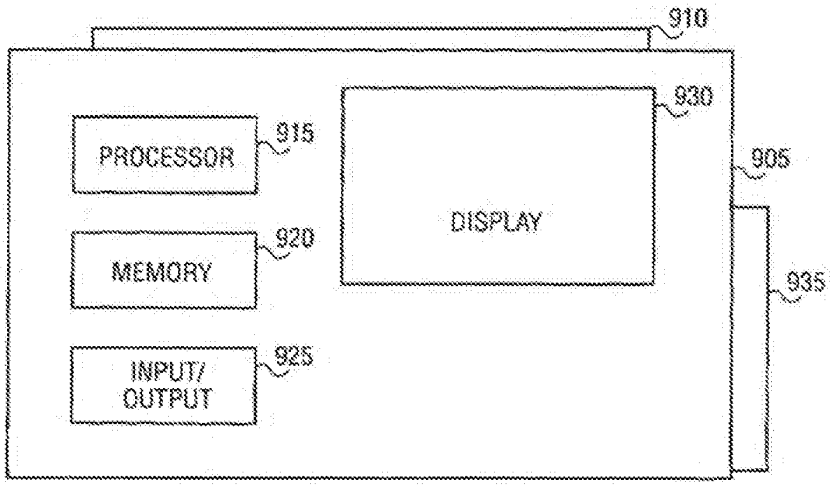

910
930
PROCESSOR
915
905
DISPLAY
MEMORY
920
935
INPUT/
OUTPUT
925

FIG. 9A

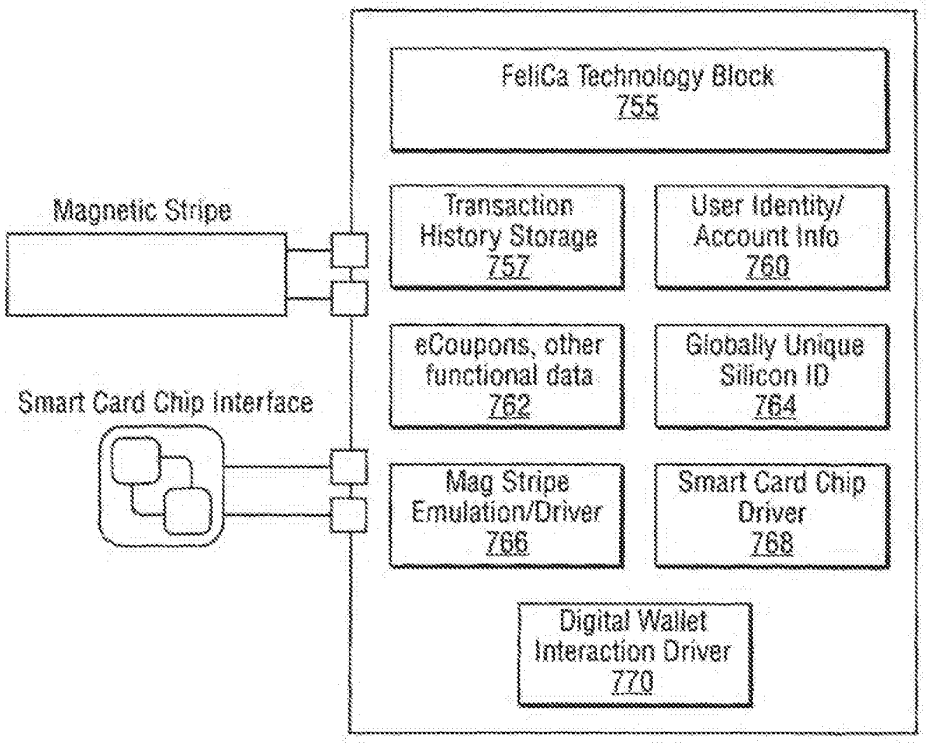

FeliCa Technology Block
755
Magnetic Stripe
Transaction History Storage
757
User Identity/ Account Info
760
eCoupons, other functional data
762
Globally Unique Silicon ID
764
Smart Card Chip Interface
Mag Stripe Emulation/Driver
766
Smart Card Chip Driver
768
Digital Wallet Interaction Driver
770

FIG. 7B

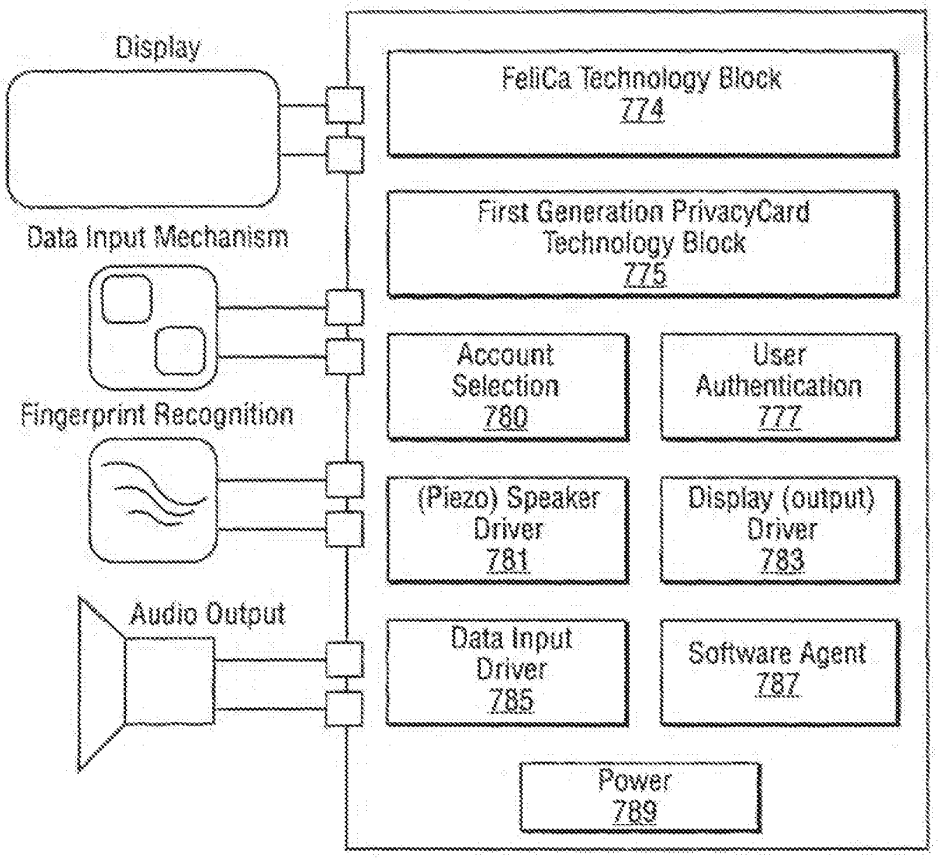
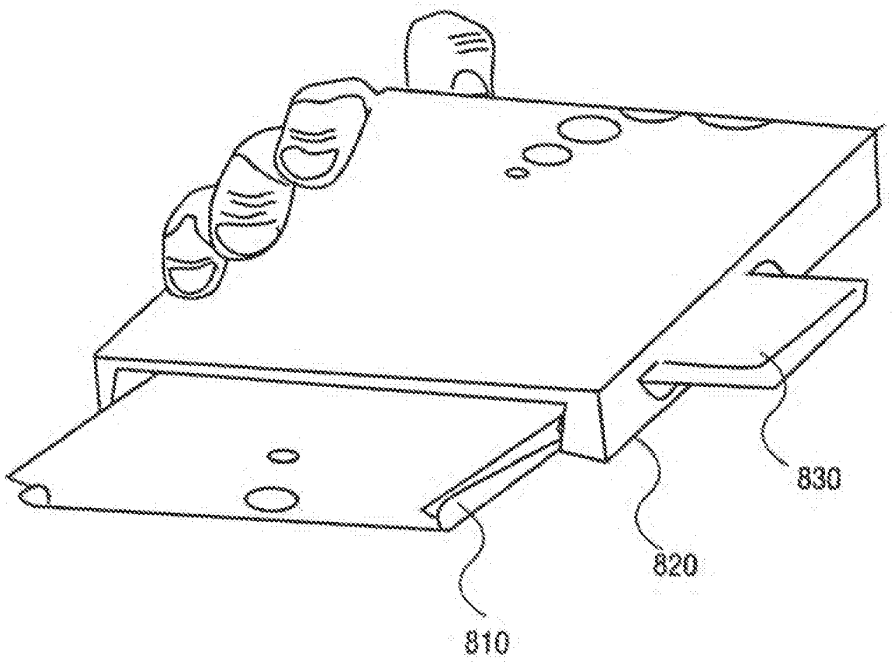

Display
Data Input Mechanism
Fingerprint Recognition
Audio Output
FeliCa Technology Block
774
First Generation PrivacyCard
Technology Block
775
Account
Selection
780
User
Authentication
777
(Piezo) Speaker
Driver
781
Display (output)
Driver
783
Data Input
Driver
785
Software Agent
787
Power
789

FIG. 7C



DIGITAL WALLET AND PRIVACY CARD

FIG. 8

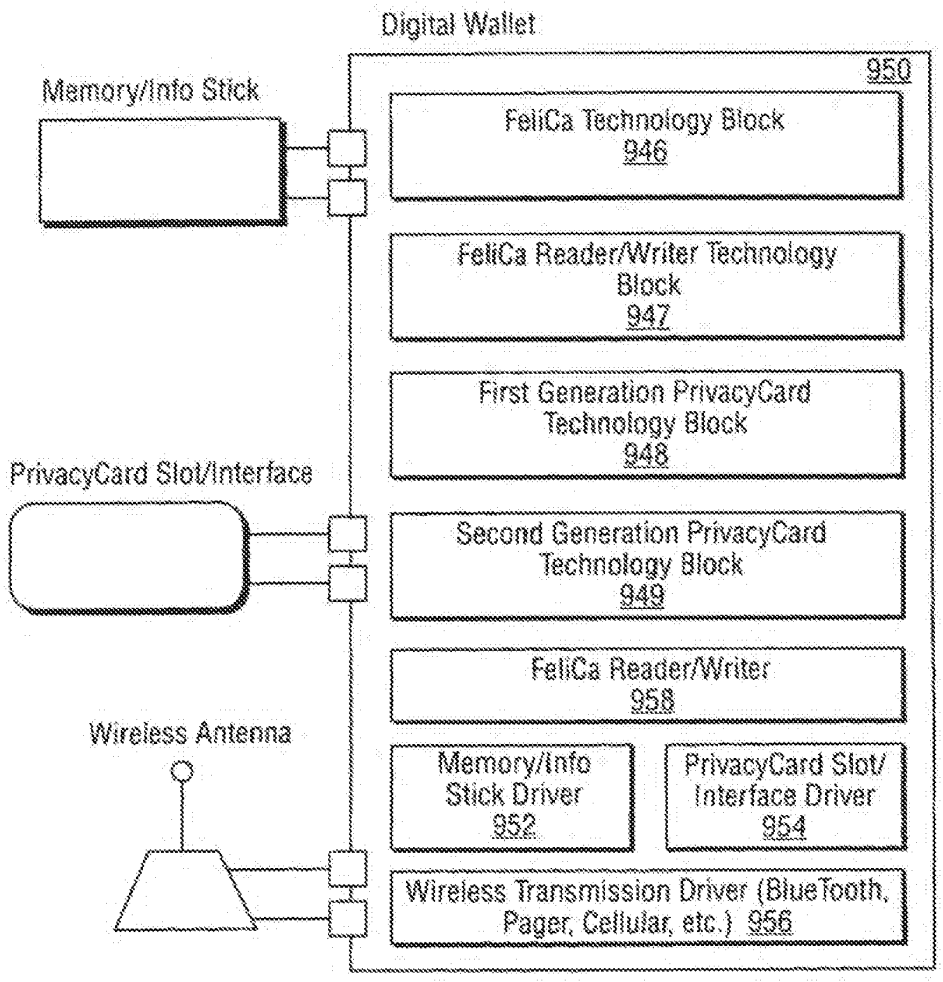
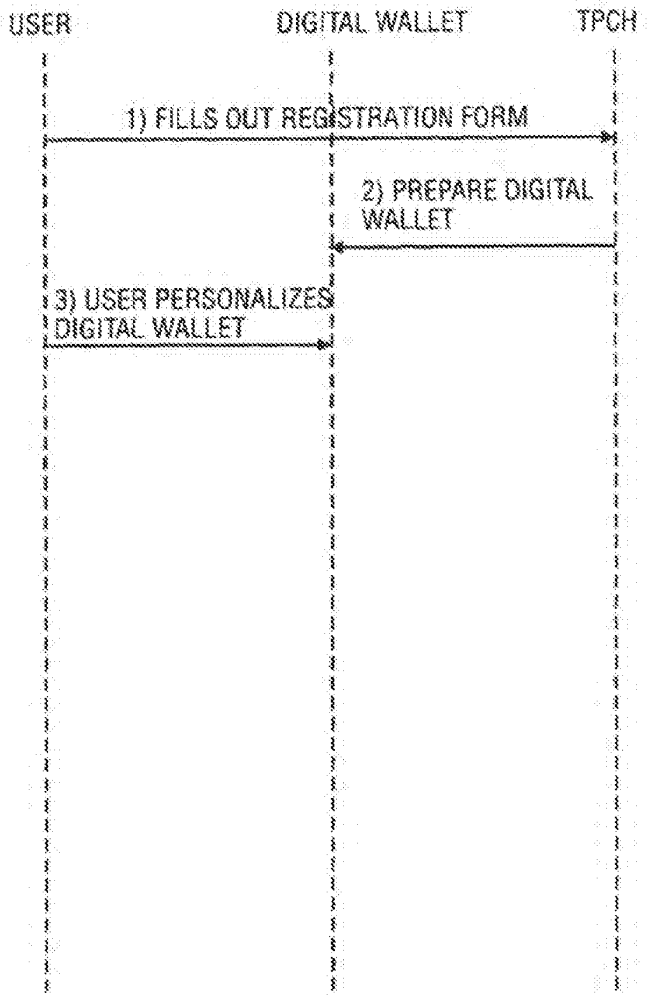

Digital Wallet
950
Memory/Info Stick
FeliCa Technology Block
946
FeliCa Reader/Writer Technology Block
947
First Generation PrivacyCard Technology Block
948
PrivacyCard Slot/Interface
Second Generation PrivacyCard Technology Block
949
FeliCa Reader/Writer
958
Wireless Antenna
Memory/Info Stick Driver
952
PrivacyCard Slot/ Interface Driver
954
Wireless Transmission Driver (BlueTooth, Pager, Cellular, etc.) 956

FIG. 9B



SETUP OF DIGITAL WALLET

FIG. 10

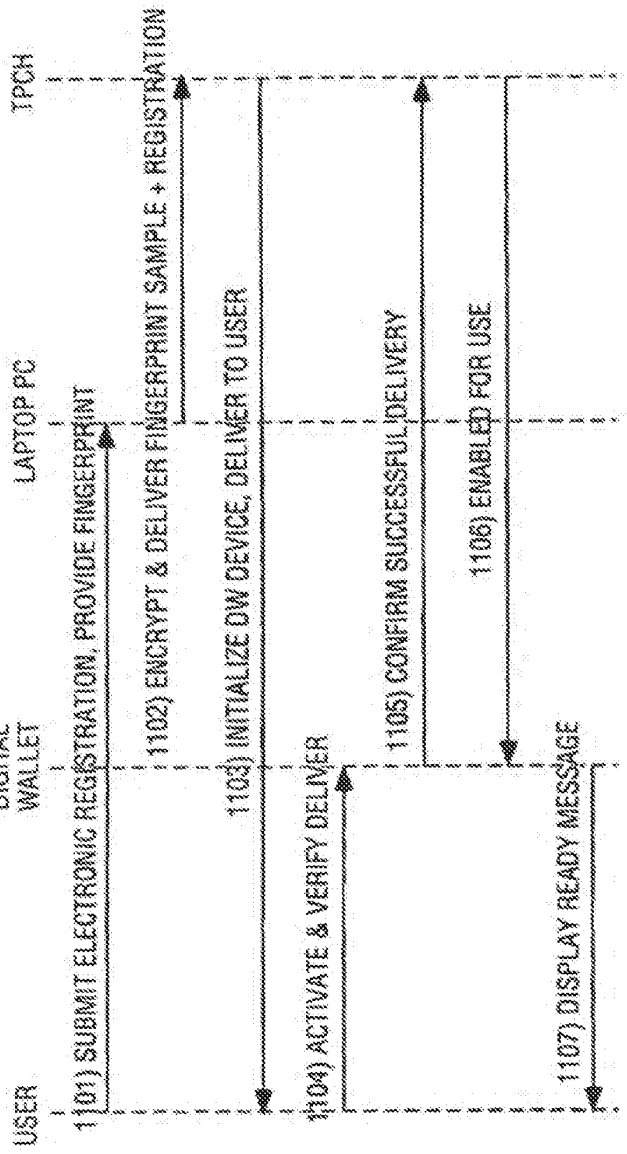

USER
DIGITAL WALLET
LAPTOP PC
TPCH
1101) SUBMIT ELECTRONIC REGISTRATION, PROVIDE FINGERPRINT
1102) ENCRYPT & DELIVER FINGERPRINT SAMPLE + REGISTRATION
1103) INITIALIZE DW DEVICE, DELIVER TO USER
1104) ACTIVATE & VERIFY DELIVER
1105) CONFIRM SUCCESSFUL DELIVERY
1106) ENABLED FOR USE
1107) DISPLAY READY MESSAGE
DIGITAL WALLET SETUP
(ALTERNATIVE EMBODIMENT)

FIG. 11

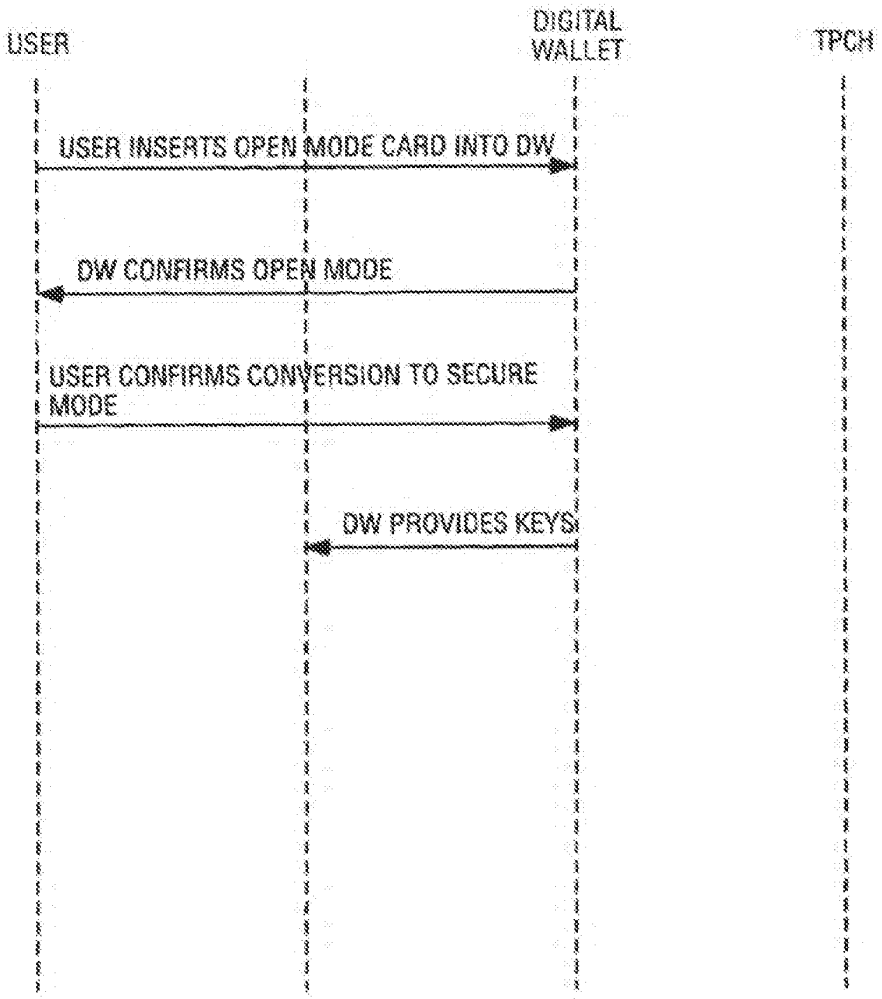

USER
DIGITAL WALLET
TPCH
USER INSERTS OPEN MODE CARD INTO DW
DW CONFIRMS OPEN MODE
USER CONFIRMS CONVERSION TO SECURE MODE
DW PROVIDES KEYS
CONVERSION OF CARD TO SECURE

FIG. 12

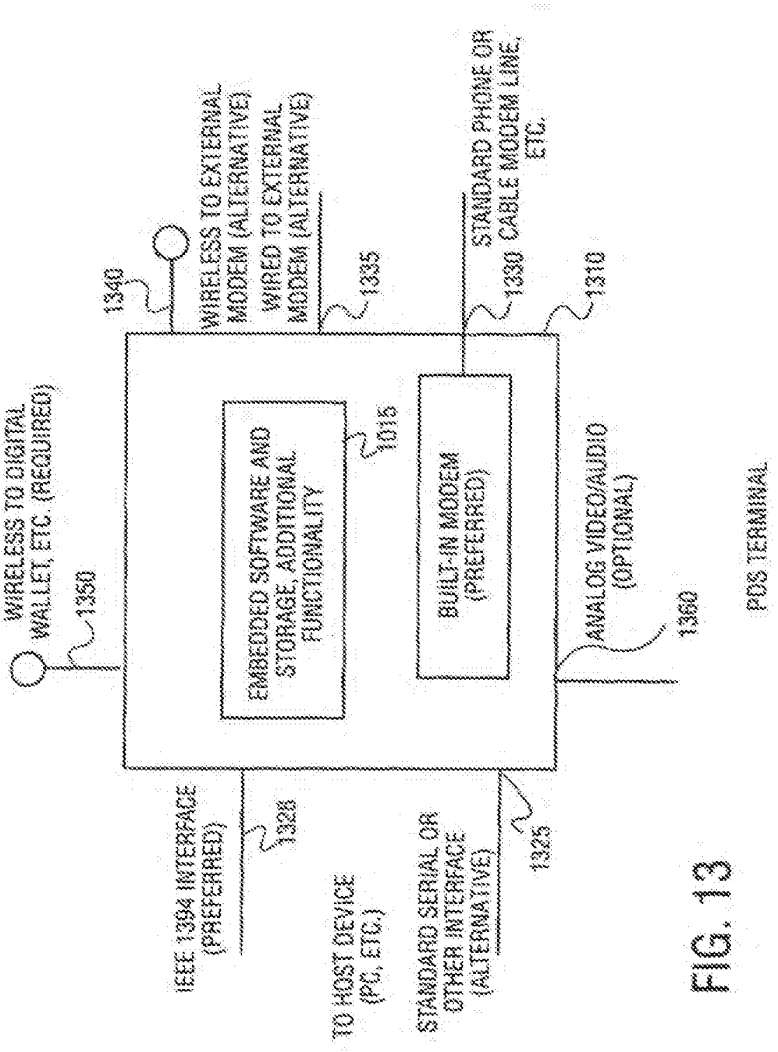

WIRELESS TO DIGITAL WALLET, ETC. (REQUIRED)
1350
1340
WIRELESS TO EXTERNAL MODEM (ALTERNATIVE)
WIRED TO EXTERNAL MODEM (ALTERNATIVE)
1335
STANDARD PHONE OR CABLE MODEM LINE, ETC.
1330
1310
EMBEDDED SOFTWARE AND STORAGE, ADDITIONAL FUNCTIONALITY
1015
BUILT-IN MODEM (PREFERRED)
ANALOG VIDEO/AUDIO (OPTIONAL)
1360
POS TERMINAL
IEEE 1394 INTERFACE (PREFERRED)
1328
TO HOST DEVICE (PC, ETC.)
STANDARD SERIAL OR OTHER INTERFACE (ALTERNATIVE)
1325

FIG. 13

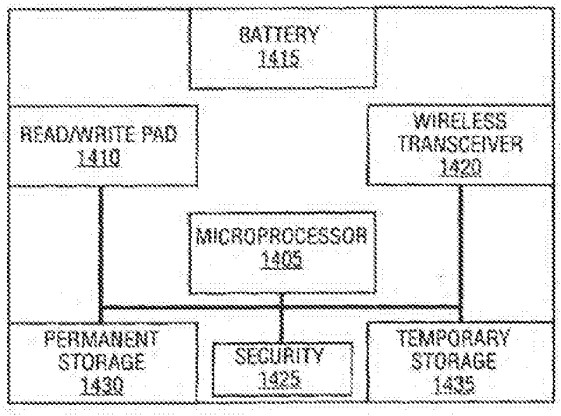


DIAGRAM OF THE MAJOR COMPONENTS OF THE PERSONAL POS, SHOWING THE DATA/ADDRESS BUS INTERCONNECT

FIG. 14

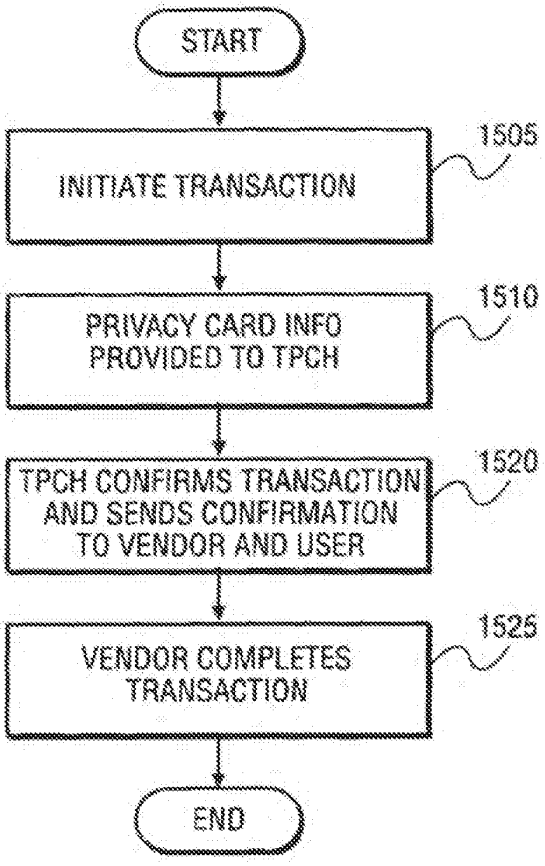

START
INITIATE TRANSACTION
1505
PRIVACY CARD INFO PROVIDED TO TPCH
1510
TPCH CONFIRMS TRANSACTION AND SENDS CONFIRMATION TO VENDOR AND USER
1520
VENDOR COMPLETES TRANSACTION
1525
END

FIG. 15

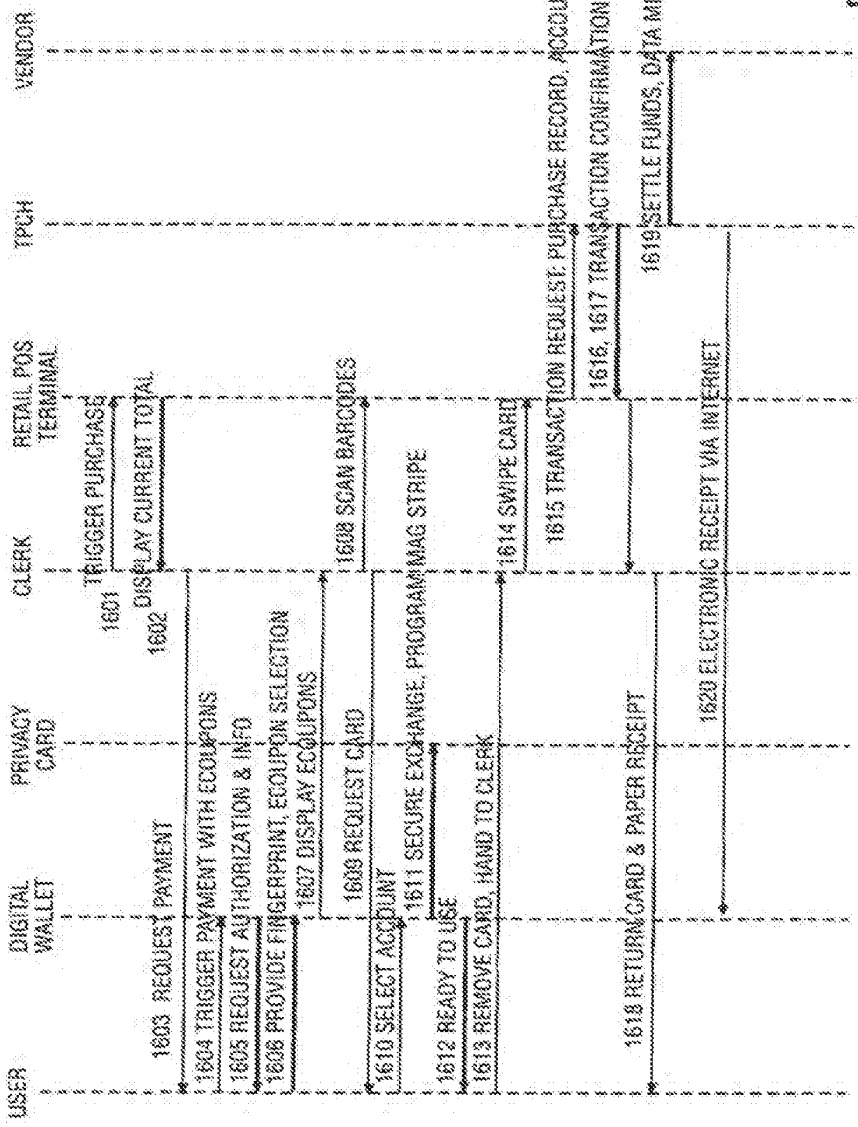

USER
DIGITAL WALLET
PRIVACY CARD
CLERK
RETAIL POS TERMINAL
TPCH
VENDOR
1601 TRIGGER PURCHASE
1602 DISPLAY CURRENT TOTAL
1603 REQUEST PAYMENT
1604 TRIGGER PAYMENT WITH ECOUPONS
1605 REQUEST AUTHORIZATION & INFO
1606 PROVIDE FINGERPRINT, ECOUPON SELECTION
1607 DISPLAY ECOUPONS
1608 SCAN BARCODES
1609 REQUEST CARD
1610 SELECT ACCOUNT
1611 SECURE EXCHANGE, PROGRAM MAG STRIPE
1612 READY TO USE
1613 REMOVE CARD, HAND TO CLERK
1614 SWIPE CARD
1615 TRANSACTION REQUEST: PURCHASE RECORD, ACCOUNT INFO
1616, 1617 TRANSACTION CONFIRMATION
1618 RETURN CARD & PAPER RECEIPT
1619 SETTLE FUNDS, DATA MINING INFO
1620 ELECTRONIC RECEIPT VIA INTERNET
RETAIL TRANSACTION

FIG. 16

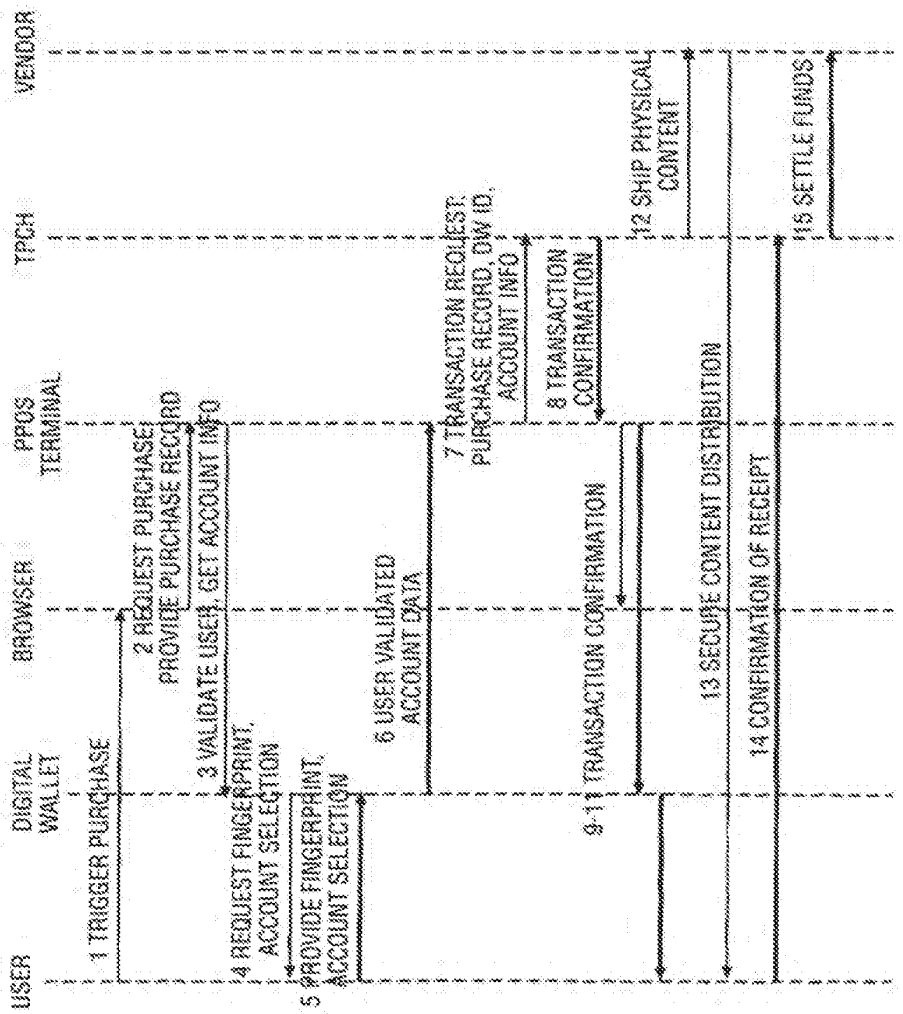

USER
DIGITAL WALLET
BROWSER
PPOS TERMINAL
TPCH
VENDOR
1 TRIGGER PURCHASE
2 REQUEST PURCHASE PROVIDE PURCHASE RECORD
3 VALIDATE USER, GET ACCOUNT INFO
4 REQUEST FINGERPRINT, ACCOUNT SELECTION
5 PROVIDE FINGERPRINT, ACCOUNT SELECTION
6 USER VALIDATED ACCOUNT DATA
7 TRANSACTION REQUEST, PURCHASE RECORD, DW ID, ACCOUNT INFO
8 TRANSACTION CONFIRMATION
9-11 TRANSACTION CONFIRMATION
12 SHIP PHYSICAL CONTENT
13 SECURE CONTENT DISTRIBUTION
14 CONFIRMATION OF RECEIPT
15 SETTLE FUNDS
WEB TRANSACTION

FIG. 17

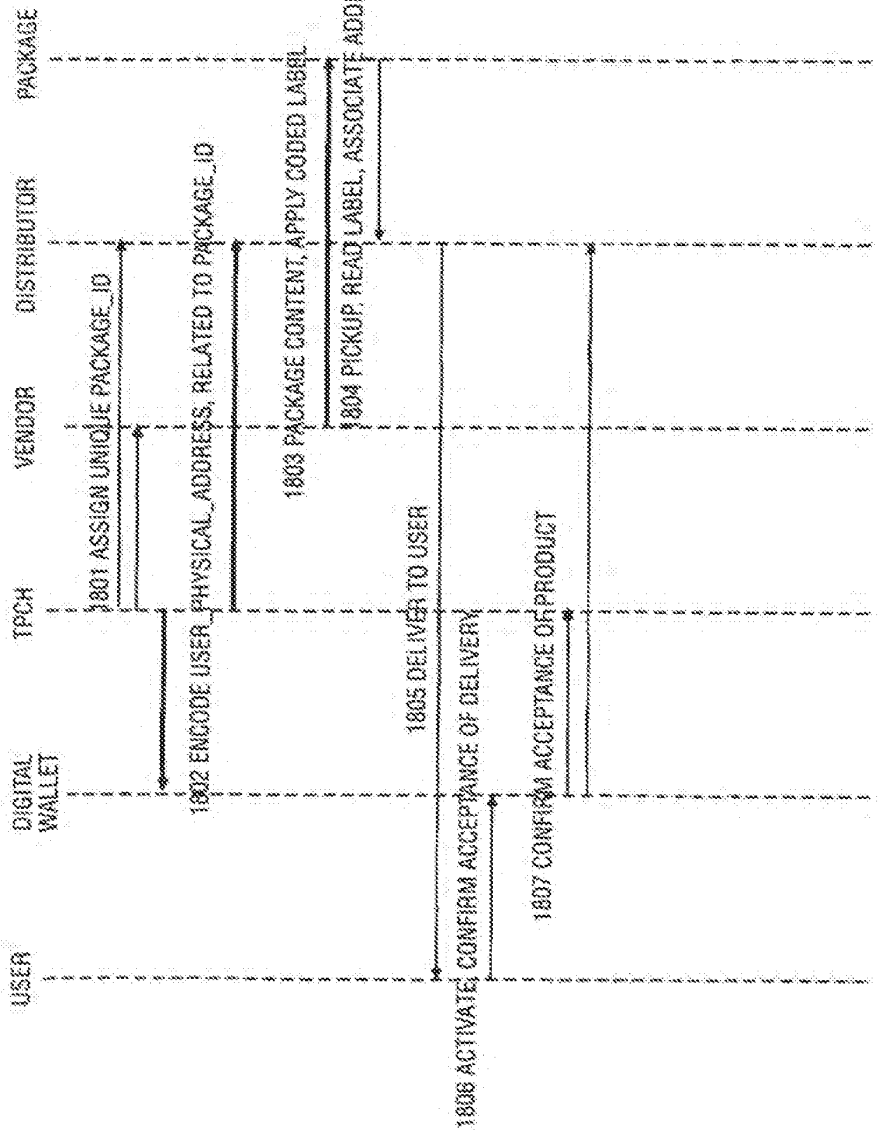

USER
DIGITAL WALLET
TPCH
VENDOR
DISTRIBUTOR
PACKAGE
1801 ASSIGN UNIQUE PACKAGE_ID
1802 ENCODE USER_PHYSICAL_ADDRESS, RELATED TO PACKAGE_ID
1803 PACKAGE CONTENT, APPLY CODED LABEL
1804 PICKUP READ LABEL, ASSOCIATE ADDRESS
1805 DELIVER TO USER
1806 ACTIVATE CONFIRM ACCEPTANCE OF DELIVERY
1807 CONFIRM ACCEPTANCE OF PRODUCT
DELIVERY OF PRODUCT

FIG. 18

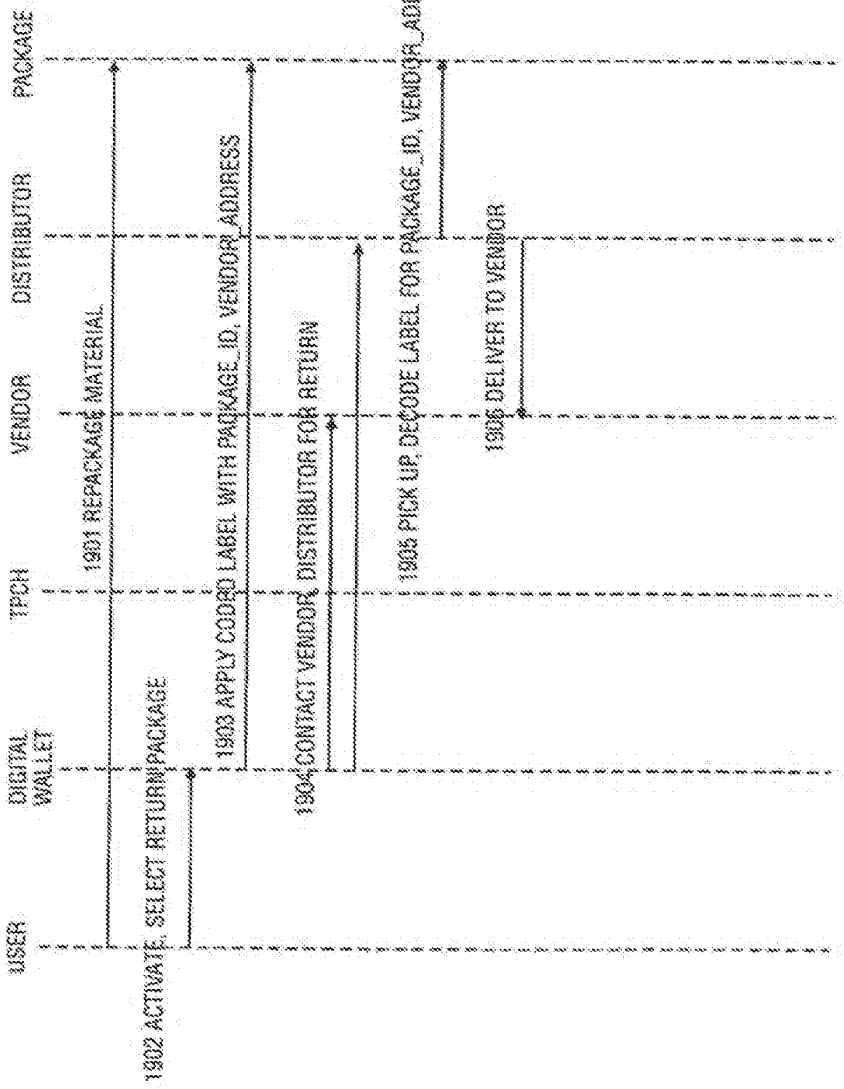

USER
DIGITAL WALLET
TPCH
VENDOR
DISTRIBUTOR
PACKAGE
1901 REPACKAGE MATERIAL
1902 ACTIVATE, SELECT RETURN PACKAGE
1903 APPLY CODED LABEL WITH PACKAGE_ID, VENDOR_ADDRESS
1904 CONTACT VENDOR, DISTRIBUTOR FOR RETURN
1905 PICK UP, DECODE LABEL FOR PACKAGE_ID, VENDOR_ADDRESS
1906 DELIVER TO VENDOR
RETURN OF PRODUCT

FIG. 19

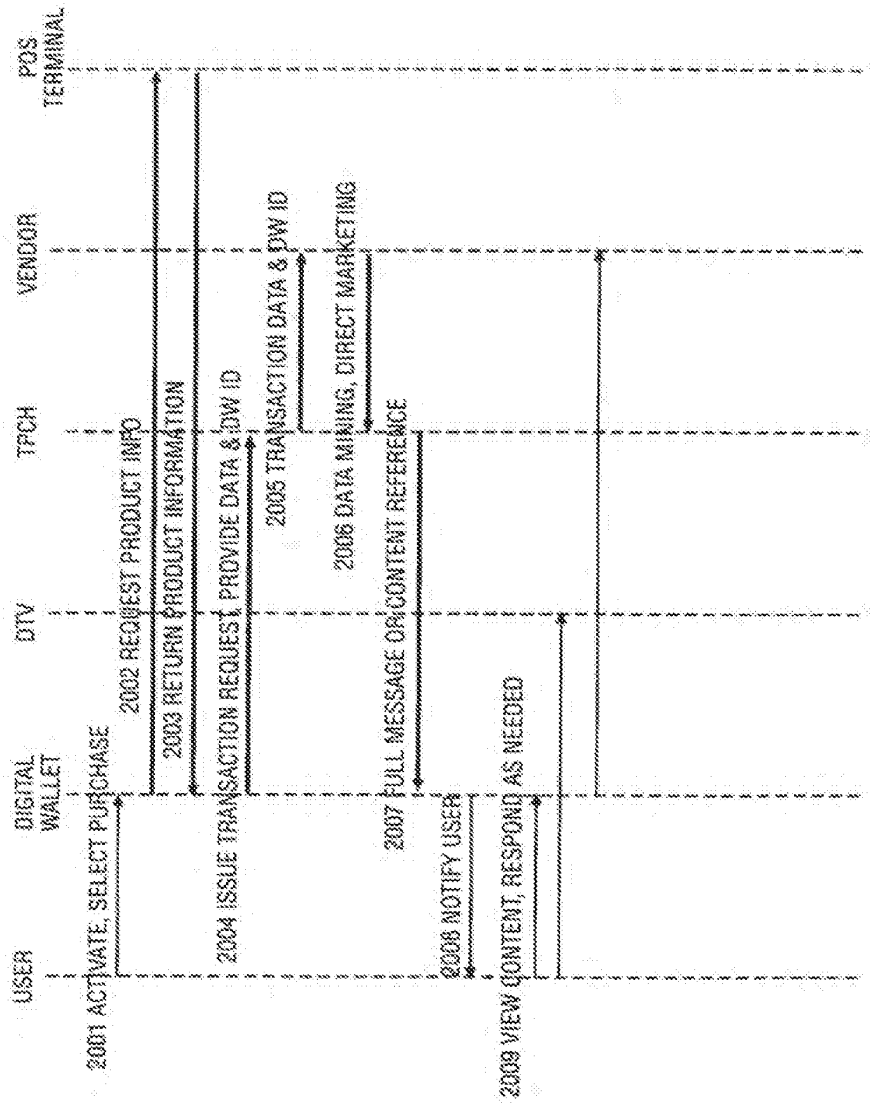

USER
DIGITAL WALLET
DTV
TPCH
VENDOR
POS TERMINAL
2001 ACTIVATE, SELECT PURCHASE
2002 REQUEST PRODUCT INFO
2003 RETURN PRODUCT INFORMATION
2004 ISSUE TRANSACTION REQUEST, PROVIDE DATA & DW ID
2005 TRANSACTION DATA & DW ID
2006 DATA MINING, DIRECT MARKETING
2007 FULL MESSAGE OR CONTENT REFERENCE
2008 NOTIFY USER
2009 VIEW CONTENT, RESPOND AS NEEDED
DATA MINING

FIG. 20

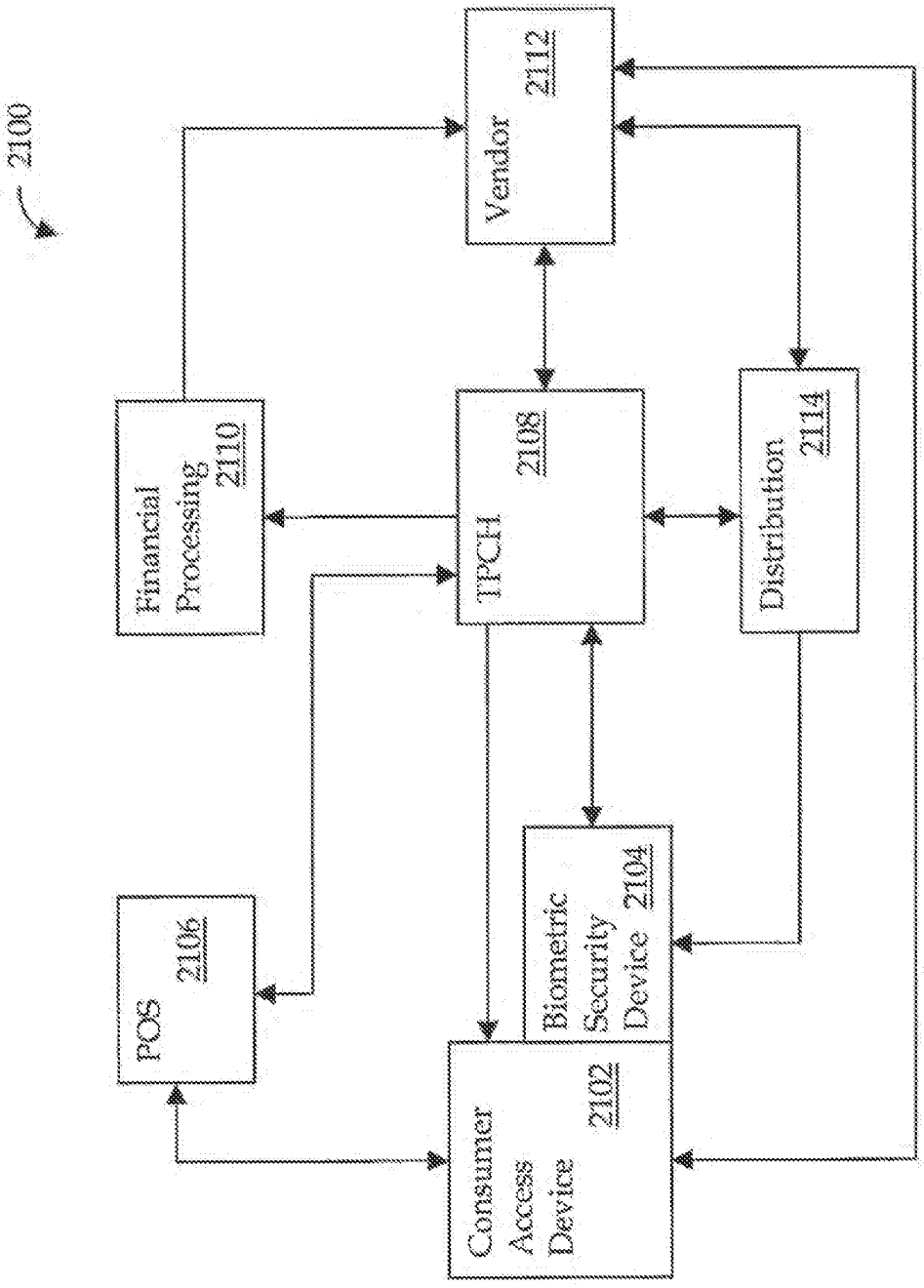

2100
Vendor 2112
Financial Processing 2110
TPCH 2108
Distribution 2114
POS 2106
Biometric Security Device 2104
Consumer Access Device 2102

FIG. 21

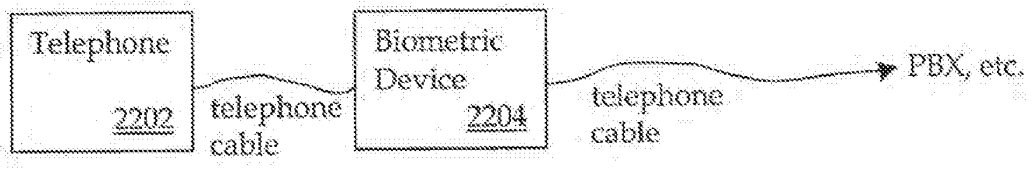


FIG. 22

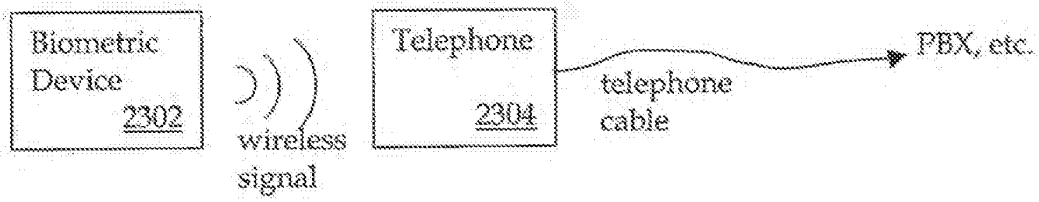


FIG. 23

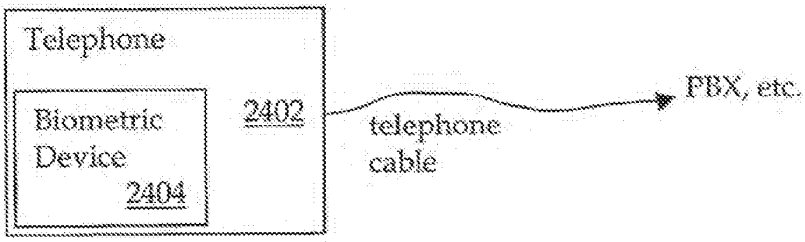


FIG. 24

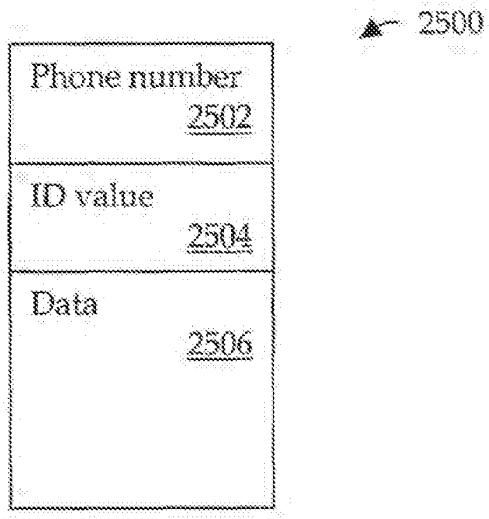

2500
Phone number
2502
ID value
2504
Data
2506

FIG. 25

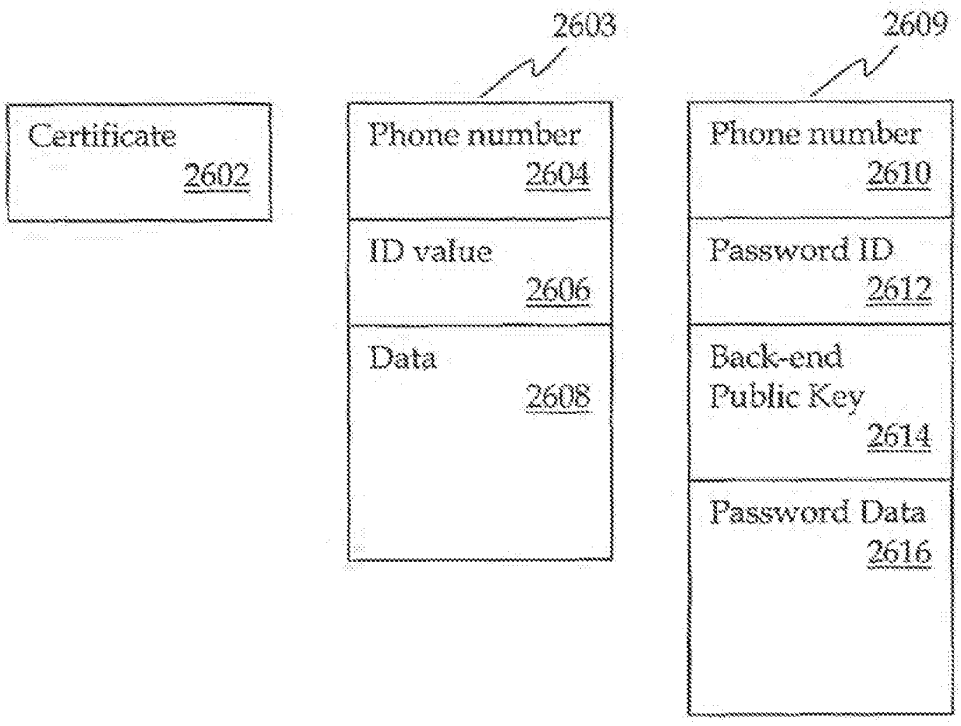

2603
2609
Certificate
2602
Phone number
2604
ID value
2606
Data
2608
Phone number
2610
Password ID
2612
Back-end
Public Key
2614
Password Data
2616

FIG. 26

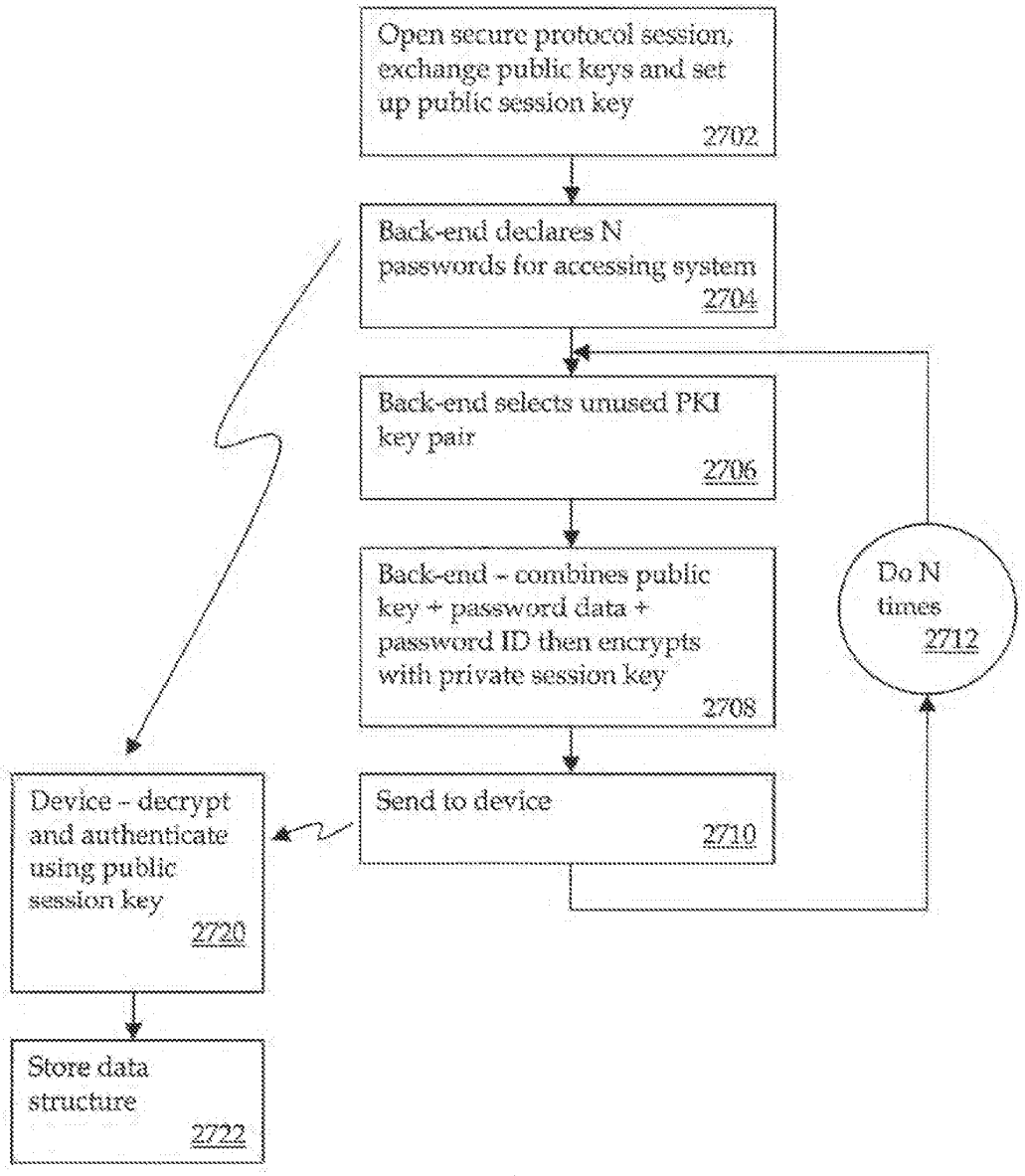

Open secure protocol session, exchange public keys and set up public session key
2702
Back-end declares N passwords for accessing system
2704
Back-end selects unused PKI key pair
2706
Back-end – combines public key + password data + password ID then encrypts with private session key
2708
Send to device
2710
Do N times
2712
Device – decrypt and authenticate using public session key
2720
Store data structure
2722

FIG. 27

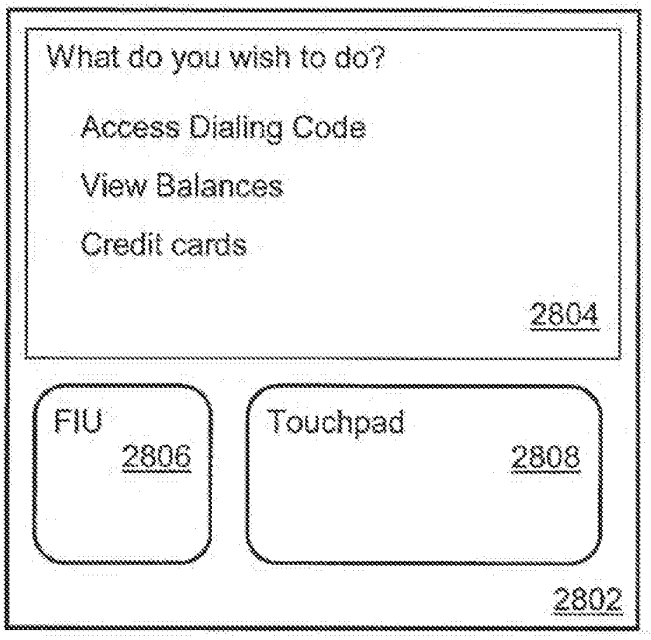

What do you wish to do?
Access Dialing Code
View Balances
Credit cards
2804
FIU
2806
Touchpad
2808
2802

FIG. 28

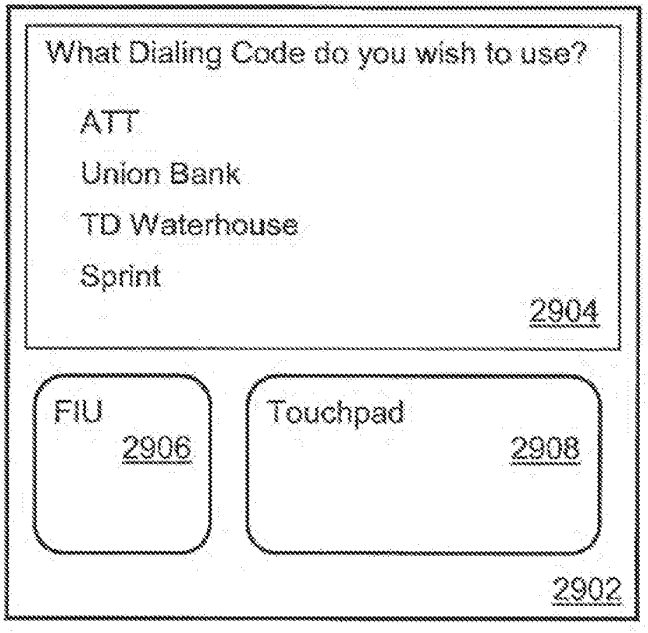

What Dialing Code do you wish to use?
ATT
Union Bank
TD Waterhouse
Sprint
2904
FIU
2906
Touchpad
2908
2902

FIG. 29

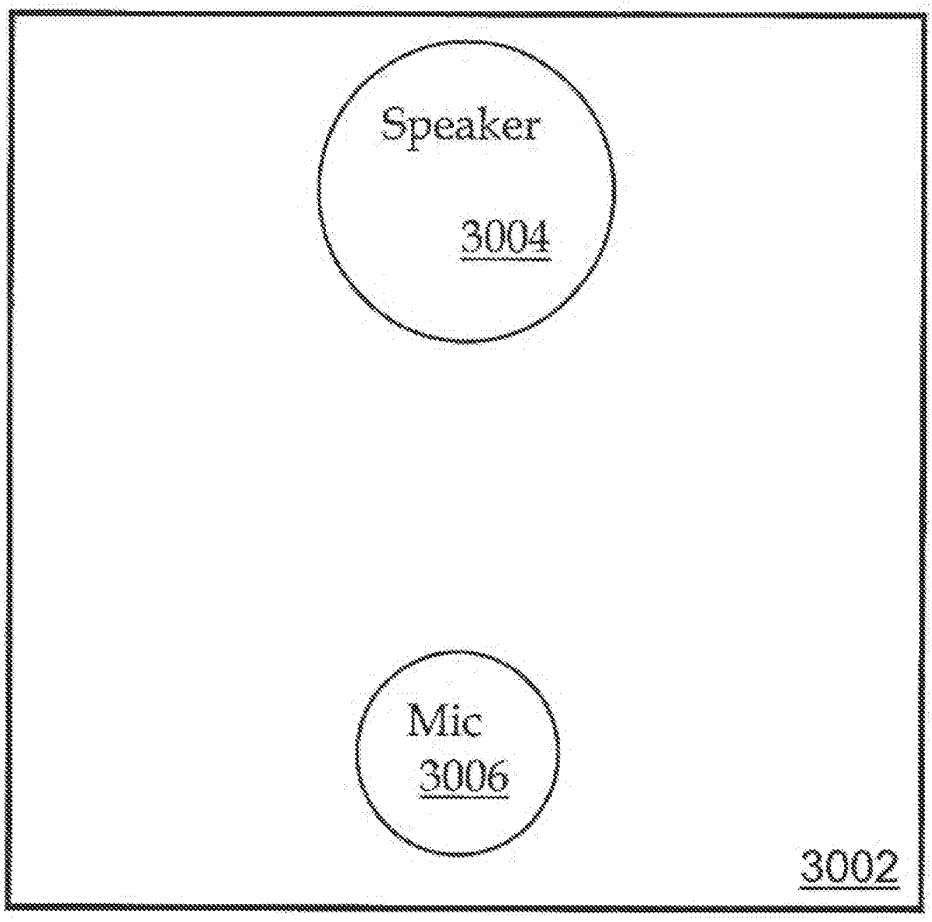


FIG. 30

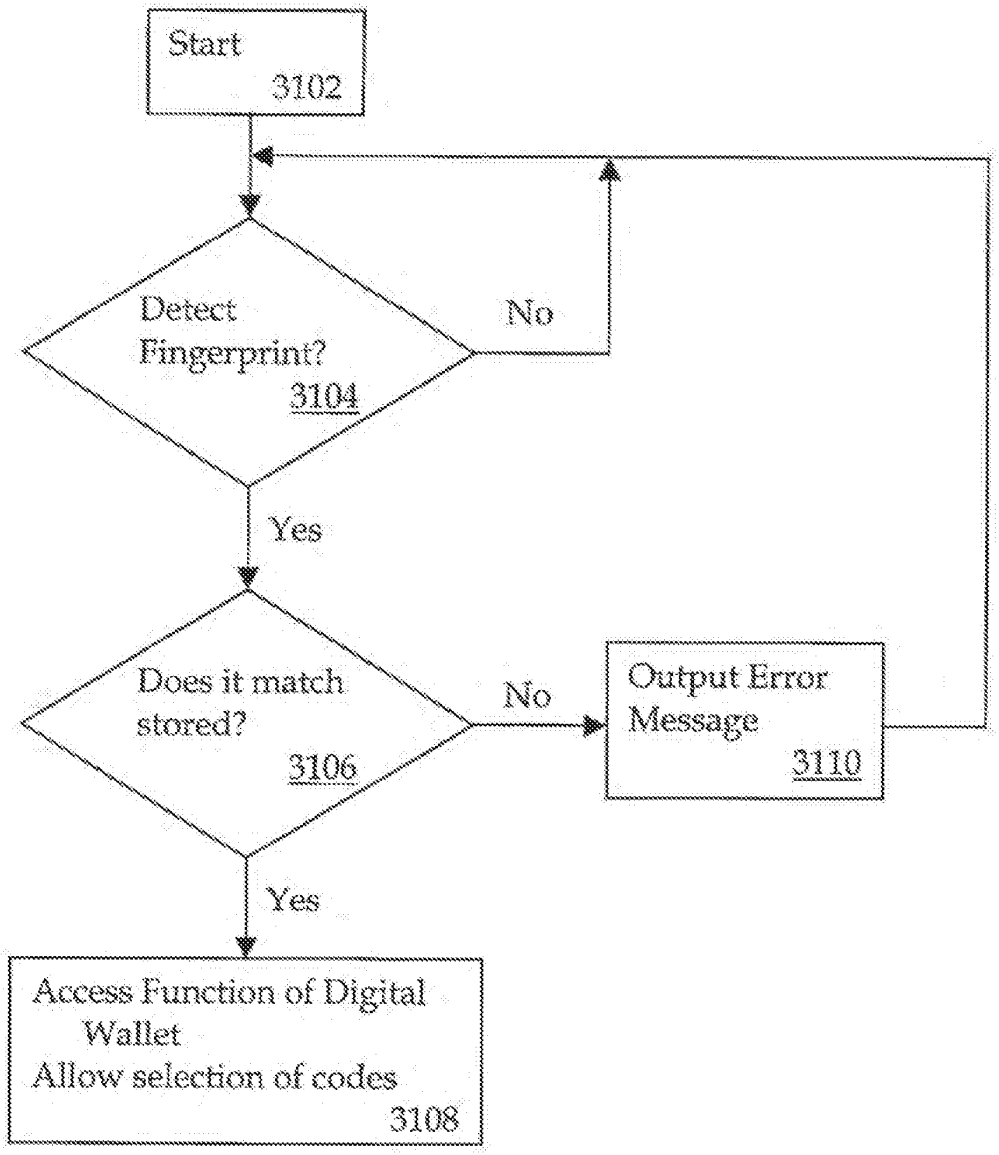

Start
3102
Detect Fingerprint?
3104
No
Yes
Does it match stored?
3106
No
Output Error Message
3110
Yes
Access Function of Digital Wallet
Allow selection of codes
3108

FIG. 31

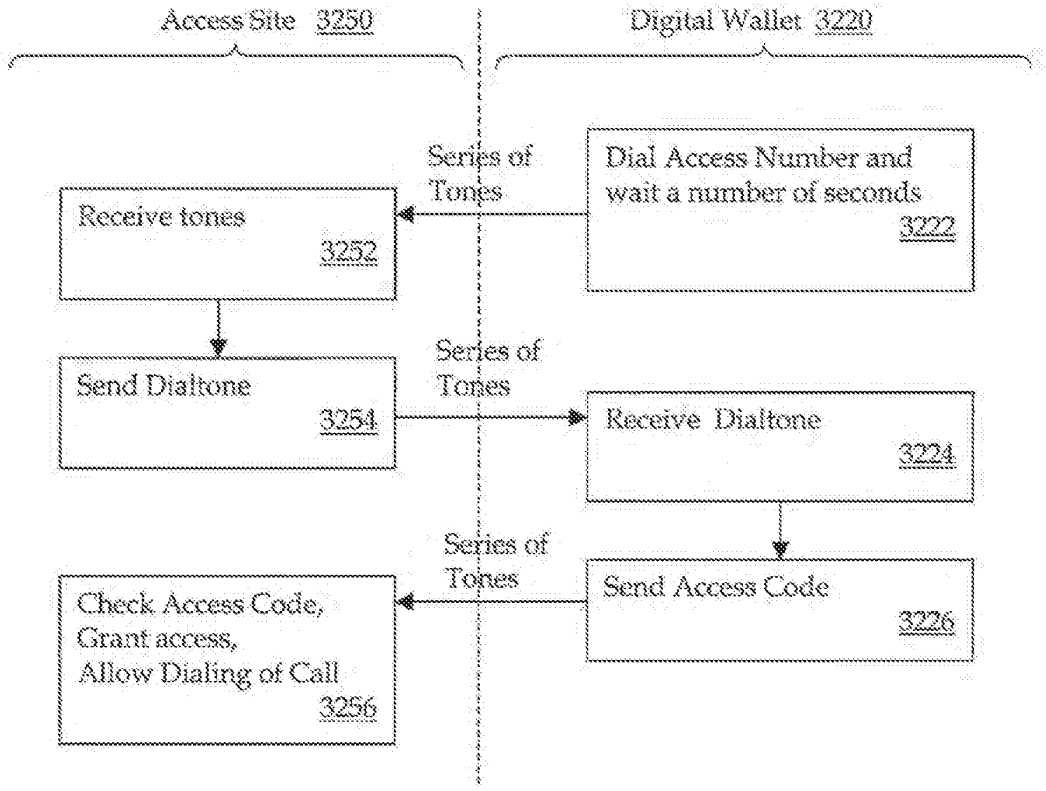

Access Site 3250
Digital Wallet 3220
Dial Access Number and wait a number of seconds 3222
Series of Tones
Receive tones 3252
Send Dialtone 3254
Series of Tones
Receive Dialtone 3224
Send Access Code 3226
Series of Tones
Check Access Code, Grant access, Allow Dialing of Call 3256

FIG. 32

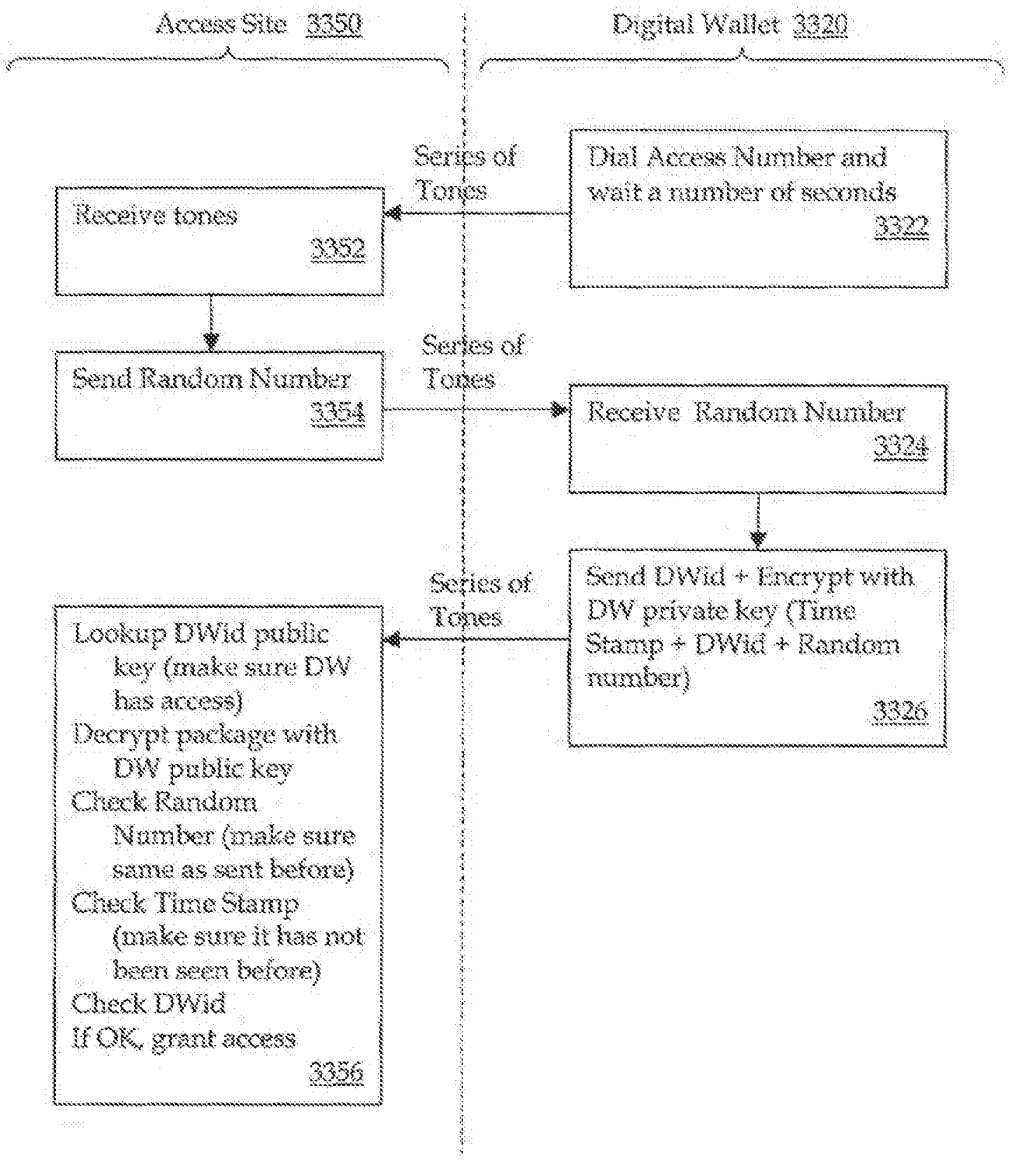

Access Site 3350
Digital Wallet 3320
Dial Access Number and wait a number of seconds 3322
Series of Tones
Receive tones 3352
Send Random Number 3354
Series of Tones
Receive Random Number 3324
Send DWid + Encrypt with DW private key (Time Stamp + DWid + Random number) 3326
Series of Tones
Lookup DWid public key (make sure DW has access)
Decrypt package with DW public key
Check Random Number (make sure same as sent before)
Check Time Stamp (make sure it has not been seen before)
Check DWid
If OK, grant access
3356

FIG. 33

SECURE AND CONVENIENT METHOD AND APPARATUS FOR STORING AND TRANSMITTING TELEPHONY-BASED DATA

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention pertains to the field of electronic communications.

2. Art Background

Electronic commerce is achieving widespread use. Transactions are performed everyday over the Internet and through point of sale (POS) or bank systems. Such systems are designed to maintain the integrity of the user's credit card, debit card, and account number. However, no measures are taken to ensure the privacy of the user. As the vendor retains information regarding the identity of the user, the user is open to receipt of marketing materials that may result from the data mining of transactions performed on a particular network.

The rapid growth of both wired and wireless communications has resulted in an increase in methods of communication. Along with the increase in the methods of communication has come the increase in access or control codes for accessing information. Often these control codes are personal identification numbers (PINs) and/or passwords. These codes may be used for accessing such information as: voice mail, bank balances, dialing cards, credit reports, paying for purchases, depositing money, accessing stored messages, logging onto computers, etc. For security reasons, generally the longer the access code the less likelihood of an unauthorized person guessing your code or password. Additionally, passwords or PINs that appear random are also likely to be more resistant to penetration. Remembering a series of long and/or random codes presents a problem for most people.

Additionally, once a service is accessed, there may be the need to then transfer information and/or data. For example, after successfully accessing a phone line via a calling card, the user may then need to enter a string of digits representing the destination telephone number. Again, people have difficulty in remembering a long series of, in this case, numbers.

Finally, when people enter access codes at public places, there is the possibility that someone may be watching with an intent to steal the codes for later use or sale. Once an access code has been stolen it may take the user time to discover this and billing corrects may be difficult. Because the access number are generally long in sequence, humans tend to write them down which may defeat the purpose of the code if someone copies or steals the code. Thus, a long sequence of numbers is difficult to remember and may lead to writing it down which may defeat some aspects of the security.

SUMMARY OF THE INVENTION

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.

BRIEF DESCRIPTION OF THE DRAWINGS

The objects, features and advantages of the present invention will be apparent from the following detailed description in which:

FIG. **1** is a simplified block diagram of an eCommerce system in accordance with one embodiment of the present invention;

FIG. **2** is an embodiment of an eCommerce system which utilizes a retail POS terminal;

FIG. **3** is an embodiment of the in-home eCommerce system;

FIG. **4** is a block diagram of an embodiment of an in-store retail system;

FIGS. **5***a* and **5***b* are simplified block diagrams illustrating embodiments of eCommerce systems that utilize POS terminals;

FIG. **6** is a simplified block diagram of a one embodiment of a transaction processing clearing house;

FIGS. **7***a*, **7***b*, **7***c* are simplified block diagrams of embodiments of a privacy card;

FIG. **8** is an embodiment illustrating a digital wallet and privacy card in accordance with the teachings of the present invention;

FIGS. **9***a* and **9***b* are simplified block diagrams of embodiments of a digital wallet;

FIG. **10** illustrates one embodiment of process for setup of a digital wallet;

FIG. **11** is an alternate embodiment of process for setting up a digital wallet;

FIG. **12** illustrates one embodiment of a process for conversion of an unsecured card to a secure card;

FIG. **13** is a simplified block diagram of one embodiment of a POS terminal;

FIG. **14** is a simplified block diagram of an alternate embodiment of a POS terminal;

FIG. **15** is a simplified block diagram of one embodiment of a process to perform a transaction in accordance with the teachings of the present invention;

FIG. **16** illustrates one embodiment of a process for performing a retail transaction;

FIG. **17** illustrates one embodiment of the process of performing a web-based transaction;

FIG. **18** illustrates one embodiment of a process for delivery of a product;

FIG. **19** illustrates one embodiment of a process for returning a product;

FIG. **20** illustrates one embodiment of a process for data mining and direct marketing;

FIG. **21** is a block diagram of one embodiment for a networked query information system;

FIG. **22** illustrates one embodiment of the system being utilized in a telephony based application;

FIG. **23** illustrates another embodiment of the system being utilized in a telephony based application;

FIG. **24** illustrates yet another embodiment of the system being utilized in a telephony based application;

FIG. **25** illustrates one embodiment of a record in a data structure;

FIG. **26** illustrates other embodiments of records and a certificate in a data structure;

FIG. **27** is a flow diagram illustrating one embodiment of securely sharing information;

FIG. **28** illustrates one embodiment of a consumer access device;

FIG. **29** illustrates one result from a selection by a user on a consumer access device;

FIG. **30** illustrates another embodiment of a consumer access device;

FIG. **31** illustrates one embodiment of a method to securely and conveniently store and transmit telephony-based data;

FIG. 32 illustrates one sequence of events; and

FIG. 33 illustrates another sequence of events using PKI.

DETAILED DESCRIPTION

In the following descriptions for the purposes of explanation, numerous details are set forth in order to provide a thorough understanding of the present invention. However, it will be apparent to one skilled in the art that these specific details are not required in order to practice the present invention. In other instances, well known electrical structures or circuits are shown in block diagram form in order not to obscure the present invention unnecessarily.

The system and method of the present invention enables a user to conduct electronic commerce transactions without compromising the user's personal identification information and identity, while also providing enhanced direct marketing for vendors. The following description discusses the invention in the context of Internet and point of sale (POS) networks. However, it is readily apparent that the invention is not limited to these particular networks, and are applicable to any network that is configured to perform a transaction.

In one embodiment of the system and method of the present invention provides a privacy feature in which no links or records are kept that relate items purchased with a specific user identity except in one highly secure location is provided. It is contemplated that the present invention is operable in a variety of types of eCommerce systems including those which do not provide a privacy feature as described herein. Although data can be collected to examine purchase patterns, personal information is not connected to this data for use outside the eCommerce system. The user connects to and performs transactions with the eCommerce system through a transaction device which has a unique identifier (ID). In one embodiment, a privacy card is used. In an alternate embodiment a digital wallet is used. In an alternate embodiment, a privacy card in conjunction with a digital wallet is used. The transaction device, e.g., the privacy card, is the identity that may be known to a vendor. The highly secured location, accessible through or part of a transaction processing clearing house (TPCH), provides the transaction processing clearing house the information necessary to authorize a transaction. For example, the transaction processing clearing house may access relevant account information to authorize transactions. However, the identity of the user is not revealed externally so that confidentiality of the user's identity is maintained.

In addition, a wide variety of convenient features can be offered to a user. For example, the transaction device can be configured to function compatibly with existing point of sale terminals at retail locations and provide encoded account information compatible with existing systems, for example, magnetic stripe and bar codes. In one embodiment, the magnetic stripe generator on the transaction device can be programmed to represent any account. Additionally, the screen on the transaction device can be used to display bar codes that can be scanned by existing POS terminals. Thus there is a capability to access multiple accounts from a single card, thereby eliminating the need to carry many different credit cards, such as debit and loyalty cards, but still providing the opportunity to use different accounts based on the user's choice. Furthermore, the transaction device may include a bar code reading device integrated therein. This feature would allow the user to scan product packaging and add that item to a purchase or an electronic shopping list.

In addition, the physical paper trail can be eliminated both for transaction receipts at the stores as well as monthly bills and bill paying on accounts by storing such information and providing access to such information through the transaction device. The automation of transaction record keeping at home can be enhanced as the receipts, bills and bill paying can be maintained on the transaction device or a coupled personal computing device.

Pay per use coupons may also be easily and automatically accessed from a variety of resources stored in the card and automatically cashed in when purchases are made using the card. Electronic coupons (eCoupons) are another example of eliminating paper (i.e, eliminating paper coupons) by adding value in electronic form. Additional value comes in the form of wider methods of distribution enhancements to the user experience and/or a more efficient processing on the vendor's side. For example, while shopping, an eCoupon stored in the transaction device can be used to pinpoint exact items the user wishes to purchase. In addition, at checkout the coupons may be automatically credited without intervention by the user. Alternately, the user may manually convey eCoupons through bar codes or the like by manual selection of the coupons. This causes the bar codes to be presented on the display of the transaction device, which are then scanned by the POS terminal. Check out clerks and administrative personal do not have to manually handle eCoupons so processing is more accurate and efficient for both the retailer and vendor. Because they are digital in nature, eCoupons benefit from flexible distribution opportunities across all forms of media, including: Internet, digital TV/radio broadcast, and packaged recorded media such as audio/computer/DVD recorded on tape or disk and accessed later on playback. By utilizing electronic coupons, real-time tracking usage provides vendors information regarding advertising channels that are returning results as eCoupons typically contain data structures that enable tracking of this information.

In addition, in one embodiment, electronic catalogs can be downloaded to the transaction device and the user may reference products/services by direct access of the catalog downloaded to the transaction device. The catalogs may also contain electronic coupons which are automatically "clipped" and added to the user's device for subsequent use during an applicable transaction. Automated shopping lists can be added to simplify the user's shopping experience. In addition, a directory of where things are located in a particular store may be located on the device to simplify the customer's shopping for items in a particular store environment.

Security of the user's identity may be achieved in a variety of ways. In one embodiment, a single trusted location, for example the TPCH, contains user data. The user interfaces with the TPCH using the user's transaction device. The user therefore does not fill out online electronic eCommerce purchase forms at every product vendor's website. The eCommerce system acts as a financial transaction middleman, stripping off user identity information from transactions. As a result, the user's private information is not stored in several databases across the Internet and in private business networks (e.g. grocery store networks). The fewer locations where the data is stored, the fewer the possibilities that hackers can access the data or that accidental releases of the data occur.

The transaction device enhances security by authenticating the user of the card prior to usage such that if a card is lost or stolen, it is useless in the hands of an unauthorized person. One means of authentication is some kind of PIN code entry. Alternately, authentication may be achieved by using more sophisticated technologies such as a biometric

solution (e.g., fingerprint recognition). In addition, in one embodiment in which multiple transaction devices, e.g., a privacy card and a digital wallet, are used, it may be desirable to configure the first device to enable and program the second device in a secure manner. Thus, the means of communication between the first device and the second device may include mutual device verification so that an unauthorized first device may not be used to enable a particular second device that does not belong to the same or authorized user.

In one embodiment, the transaction device(s), POS terminals and/or TPCH may function to verify the authenticity of each other. For example, a privacy card and digital wallet may be configured to verify the legitimacy of each other. Similarly, the transaction device may be configured to verify the legitimacy of the POS terminal and/or TPCH. A variety of verification techniques may be used. For example lists of devices with account and/or access issues may be maintained. For example, in one embodiment, the public key infrastructure (PKI) may be used to verify legitimacy.

Through the eCommerce system of the present invention, data mining and direct marketing services can also be offered to vendors. 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.

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 communicating with outside devices such as a digital wallet described herein, point of sale (POS) terminal or personal computer (PC) and digital televisions (DTV).

Communication protocols include those that allow the digital wallet to specify which of several possible data structures to use for a transaction and communication protocols that allow the digital wallet and other devices to securely share data with the transaction device. The transaction device may represent a single account such as a particular credit card, or it might represent multiple accounts such as a credit card, telephone card and debit card.

In one embodiment, the transaction device may include a full screen that covers one side of the card. Alternately, in one embodiment in which the transaction device is one embodiment of a privacy card, the privacy card may be coupled to a device, such as the digital wallet, described herein, that provides a display. In one embodiment the screen may be touch sensitive and therefore can be used for data input as well as output. In one embodiment, a user authentication mechanism such as a fingerprint recognition or other mechanism may be built directly into the card. Furthermore, the privacy card may have a wireless communication mechanism for input and output.

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.

In one embodiment, a tap-slide-tap user interface may be utilized. This uses a touch sensitive input mechanism, such as a touch sensitive screen. Alternately, a pen-based user interface such as Graffiti®. (Graffiti is a trademark of Palm Computing, Inc.) may be utilized. Alternately, a user slide, jog wheel or other pointing device on a touch screen may be used. The wheel may be used to cycle through candidate values of a particular data field. Data dials may also be used. The data dials are an abstraction for collection of data items through which the user cycles as the dial (spins). The data dials may be tailored to the data field for which they are being used. When a user taps on a field to activate data entry, the appropriate data dial is instantiated and linked to an on-screen slider. The slider enables the user to change a selected element.

As noted above, the transaction device acts as a user's worldwide proxy or alias. The transaction device contains a unique identifying value along with other information that allows the transaction privacy clearinghouse to track its use and assist in user transactions. The transaction devices themselves have an identity in the electronic commerce world, thus the cards are the entities with which outside parties communicate. For example, when a vendor wishes to send electronic coupons or other promotional material to a user who has been purchasing its products, the vendor specifies the transaction device identity as the target of distribution. The eCommerce system then uses various means of electronic distribution to ensure that this data is delivered to the transaction device. However, in some embodiments the user's true identity and direct contact information are not revealed.

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.

In order to maintain confidentiality of the identity of the user, the transaction device information does not provide user identification information. Thus, the vendor or other entities do not have user information but rather transaction device information. The TPCH **110** maintains a secure database of transaction device information and user information. In one embodiment, the TPCH **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. In addition, the TPCH **110** may also provide information through a distribution system **150** that, in one embodiment, can provide a purchased product to the user **120**, again without the vendor **125** knowing the identification of the user **120**. In 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 TPCH **110** functionality.

In one embodiment, the financial processing system (FP) **140** performs tasks of transferring funds between the user's account and the vendor's account for each transaction. In

one embodiment, the presence of the TPCH **110** means that no details of the transactions, other than the amount of the transactions and other basic information, are known to the FP **140**. The TPCH **110** issues transaction authorizations to the FP **140** function on an anonymous basis on behalf of the user over a highly secure channel. The FP **140** does not need to have many electronic channels receiving requests for fund transfer, as in a traditional financial processing system. In one embodiment, a highly secure channel is set up between the TPCH **110** and the FP **140**; thus, the FP **140** is less vulnerable to spoofing.

In one embodiment, the FP **140** is contacted by the TPCH requesting a generic credit approval of a particular account. Thus the FP **140** receives a minimal amount of information. In one embodiment, the transaction information, including the identification of goods being purchased with the credit need not be passed to the FP **140**. The TPCH **110** can request the credit using a dummy charge ID that can be listed in the monthly credit statement sent to the user, so that the user can reconcile his credit statement. Further, the transaction device can include functionality to cause the credit statement to convert the dummy charge ID back to the transactional information so that the credit statement appears to be a conventional statement that lists the goods that were purchased and the associated amount charged.

A display input device **160** may be included to enable the user, or in some embodiments the vendor **125**, to display status and provide input regarding the transaction device and the status of the transaction to be performed.

The system described herein also provides a distribution functionality **150** whereby products purchased via the system are distributed. In one embodiment, the distribution function **150** is integrated with the TPCH **110** functionality. In an alternate embodiment, the distribution function **150** may be handled by a third party. Utilizing either approach, the system ensures user privacy and data security. A variety of distribution systems are contemplated, for example, electronic distribution through a POS terminal coupled to the network, electronic distribution direct to one or more privacy cards and/or digital wallets, or physical product distribution.

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

In one embodiment, the POS terminal may be a retail POS terminal. Alternately, the POS terminal may be a home-based personal POS terminal as described herein. Thus, a POS distribution channel may be configured to provide for secure transmission of large amounts of data. If small amounts of secured data or unsecured data are transmitted, the data may be directly transmitted to the transaction device, e.g., privacy card or digital wallet. In an alternative embodiment, the POS terminal functionality may be integrated into the transaction device eliminating the requirement of a coupling to a POS terminal. One use of the direct electronic distribution channel is for e-coupons and other promotional material distributed by vendors.

A physical distribution channel is used when the product purchased is physical (i.e., cannot be electronically transmitted to the user) in nature. Within the scope of physical distribution, two basic sub-categories will be discussed: products that are carried out by the user and products that are delivered from the vendor to the user via third party carrier. An example of a user distributed mechanism are actions such as carrying groceries out of a store. In these cases there is nothing for the system to handle regarding distribution and the electronic transaction mechanism described herein operates to ensure user privacy for the purchase.

However, when the product is to be delivered to the user, there should be a mechanism for retaining user privacy. In one embodiment, the eCommerce system provides a carrier with the necessary physical address information in a secure manner. In one embodiment, the system installs mechanisms at the point of packaging and distribution to ensure user privacy, while also ensuring that users receive what they pay for. Alternately, depending upon how distribution is handled, product packaging and addressing may occur at the vendor site and carriers may later pick a product up for delivery.

One embodiment of a system that utilizes a point of sale (POS) terminal is shown in FIG. **2**. In this embodiment, the privacy card **205** interfaces with the POS terminal **210** and the POS terminal **210** communicates with the TPCH **215**. The TPCH **215** interfaces with the financial processing system **220**, the vendor **225** and the distribution system **230**. The POS terminal may be an existing (referred to herein as a legacy POS terminal) or a newly configured POS terminal located in a retail environment. The user **240** uses the privacy card **205** to interface to the POS terminal in a manner similar to how credit cards and debit cards interface with POS terminals. Alternately, a digital wallet **250** may be used by itself or with the privacy card **205** to interface to the POS terminal **210**.

FIG. **3** illustrates an embodiment that may exist in home environments. In this embodiment, the privacy card **305** interfaces with a device **310** referred to herein as a personal POS terminal. The personal POS terminal interfaces with the system. The user may also have access using an input device such as a keyboard. An output device may also be provided, such as a computer display or a television monitor **320**. Utilizing this embodiment, the user may perform transactions in-home through the TPCH **330**. The TPCH **330** interfaces with financial processing system **335**, vendors **340**, and distribution systems **345** to authorize and perform the transaction. As noted above, in an alternate embodiment, a digital wallet may be used in conjunction with the privacy card to interface with the personal POS terminal **310**.

An alternate embodiment contemplated for the retail environment is shown in FIG. **4**. In this embodiment, the privacy card **405** interfaces with the digital wallet **410** and retail POS terminal **415**. Alternately, the privacy card **405** interfaces directly to the retail POS terminal **415**. The retail clerk may have a display and keyboard to perform input/output functions with respect to the POS terminal **415**. The user **430** provides the transaction device, e.g., privacy card **405** and digital wallet **410**, to the terminal **415**. The terminal may be a terminal configured particularly to operate with a privacy card. Alternately, the transaction device may interface to a legacy retail POS terminal **425** wherein the privacy card **405** and/or digital wallet **410** provides a bar code or magnetic code readable by the legacy retail POS terminal **425**.

Transaction privacy clearing house **440** receives the user's privacy card identification and determines whether the user has sufficient funds to perform the transaction. TPCH **440** interfaces with the financial processing system **445**, vendors **450**, and distribution systems **455** to complete the transaction.

As noted above, it is contemplated that the transaction device would operate in a home environment as well as in a retail environment. FIG. **5***a* is a simplified block diagram of a retail system modified to support the interaction of a legacy POS terminal with a transaction device. The terminal **510** interfaces to TPCH **515** which communicates with the financial provider, for example, a credit card company **520**, and the particular retailer **525**. Alternately, as shown in FIG. **5***b*, the POS terminal **550** interfaces to the retail system **555**, which then interfaces with the credit card company **560** and the TPCH **570**.

It is contemplated that the transaction device will be compatible with a variety of eCommerce system's POS terminals and therefore will provide magnetic stripe, bar-code information and/or smart card chip. The magnetic stripe on the card or digital wallet can be programmed to represent a new account; thus a single transaction device may be configured to represent a number of different accounts.

One embodiment of the TPCH is illustrated in FIG. **6**. In one embodiment, the TPCH is located at a secure location and is accessible to the transaction device. The TPCH functions to provide the user with authorization to perform transactions without compromising the user's identity. The TPCH may be embodied as a secure server connected to the transaction device in some form of direct connection or alternately a form of indirect connection over the Internet or point of sales networks.

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

The TPCH agent **615** handles system management and policy control, and forms the core functionality of the TPCH **600**. In one embodiment, within the entire system, there is one clearing house agent, which resides permanently at the clearing house. Among the responsibilities handled by the agent include internal system management functions such as data mining, financial settlement and allocation of payments to internal and external accounts, and registration of new users joining the system.

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

The TPCH agent **615** also provides a direct marketing and customer contact service **625**, which in one embodiment is a data access control mechanism that maintains separate, secure access between various clients and their database(s). The data access control mechanism ensures that vendors have access only to the appropriate data in order to carry out the tasks of the system. One of the key features of the TPCH, the ability to carry out focused direct marketing while maintaining the privacy and identity protection of the consumer, is handled by this mechanism.

The vendor databases **635** are a related to vendors and retailers that the TPCH is currently interacting with, or has previously interacted with. In one embodiment, there is a separate vendor database for each vendor, past and present. In an alternate embodiment, one database accumulates information about all vendors past and present.

In one embodiment, vendors use the database(s) to store a variety of information about the products and services that they offer through the TPCH and the transaction device. Some of the information in the database may be visible only to the vendor, such that even the TPCH may not be able to see all the entries.

The customer database **640** holds information regarding each customer of the TPCH. It is this database in which the only link between actual user identity information and the digital aliases provided by the transaction device exists.

The transaction database **645** is used by the TPCH to store records of all transactions facilitated by the TPCH. This database is used as a mirror backup for the transaction records that may exist in the transaction device.

In some systems, vendors have planned to use the Internet to send periodic financial records to their customers via email or other protocols. One of the problems with such a system is that the central data collection agency will ultimately be incurring potentially high transmission overhead by sending all of these transaction records to all users. Another problem is that users must wait for that periodic distribution to take place, and would normally be required to use means that are not truly convenient, such as email messages.

In one embodiment of the system of the present invention, the user collects a transaction record in the form of an electronic receipt immediately at the time of purchase, preferably by wireless communication between the POS terminal and the transaction device. The user then has the data readily available for use on demand, whether it is for a business expense report or for personal record keeping. However, if the transaction device is lost or stolen, all of that data is still replicated at the TPCH, for example, in the transaction database **645**. Therefore, an exact duplicate of the device, including its transaction history, can be manufactured and sent to the customer, thereby minimizing the inconvenience of a lost or stolen device.

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. In one embodiment, this backup action would happen automatically whenever the transaction device is coupled to the communication channel of the TPCH, for example, through a POS terminal. This would also facilitate the quick replacement of a lost or stolen transaction device along with all of its associated data, thereby further increasing the convenience of the user.

The data mining database **650** stores data mining rules and results. The rules can be in the form of scripts or query specifications, each of which has a label and other attribute information. One example of a rule may be "find all transaction device ID values that purchased product X in the recent week". These rules can be presented in an administrative application for human use, or triggered automatically by scheduled actions managed by the TPCH agent **615**.

The transaction device is a physical device, such as a card, containing an identification that maintains the confidentiality of the user's identity by employing the transaction device ID as the identity of the entity performing the transaction.

Thus, all transactions, from the vendor's perspective, are performed with the transaction device. One embodiment may be visualized in a form similar to Sony Corporation's (Japan) FeliCa Card. The FeliCa is a contactless (wireless) card execution platform. The privacy card, in one embodiment, may have a form similar to the FeliCa but would operate in accordance with the teachings set forth herein.

As described herein, the TPCH maintains secure information linking a user to a particular transaction card identification and interfaces among the transaction device, vendor and any financial systems to provide the user authorization to perform and complete a transaction.

In one embodiment in which the transaction device is a privacy card, the privacy card provides a basic functionality to perform eCommerce transactions as described herein. The privacy card may include one or more of the following features: wireless/non-contact communication technologies such as that found in the Sony FeliCa card; magnetic stripe emulation/simulation technology; smart card contact interface; and secure transaction capability to verify that the partner device, e.g., card reader, is legitimate.

The above technologies, in one embodiment, may be implemented in such a manner as to not require on-card battery power. Power may be provided by a local RF energy field provided by an external device such as a non-contact card reader, which is picked up by a loop antenna in the card and converted into energy to power the on-card circuitry. Alternately, the power may be provided by the smart card chip interface. In another embodiment, the power may be induced by an RF field and stored in an RC (resistance/capacitance) circuit that slowly releases power as it is consumed by on-card circuitry. This would be analogous to a "temporary battery" that lasts on the order of a few seconds of operation. Once this RC storage is depleted, it must be recharged by an RF field before the card device can become activated again.

In an alternate embodiment, the privacy card may further include on-card fingerprint recognition, on-card display technology, which may be enabled via thin LCD technologies, touch/pen/button input, and software agent technologies. These technologies, as a practical matter, may be operable with an on-card power supply so as to avoid having to be near an RF field in order enable the display and fingerprint functions and provide an on-demand functionality. One power source may be a lithium polymer battery which does not require the battery to be encased in a hard-shelled package and can be packaged into very thin formats. Thus one section of the card can be devoted to storing a lithium polymer power supply that can recharged by electrical induction.

In one embodiment, the privacy card is the size of a credit card. In one embodiment, to minimize the amount of circuitry and therefore the size of the card, a display is not provided. In addition, it is contemplated that network communication capabilities are not included on the privacy card. In such embodiments where desirable functionality is not included on the privacy card, a digital wallet, as described below, is provided to interface between the privacy card and the eCommerce network. The digital wallet, in an alternate embodiment, may be configured to function by itself. Alternately, such functionality is provided on the privacy card itself such that a device such as a digital wallet is not needed.

One embodiment of the privacy card is illustrated in FIG. **7***a*. As noted earlier, the privacy card **705** is configured to be sized for easy carrying and use. Thus, in one embodiment, the card **705** is configured to be the size of a credit card. The privacy card includes a processor **710**, memory **715** and input/output logic **720**. The processor **710** is configured to execute instructions to perform the functionality herein. The instructions may be stored in the memory **715**. The memory is also configured to store data, such as transaction data and the like. In one embodiment, the memory **715** stores the transaction ID used to perform transactions in accordance with the teachings of the present invention. Alternately, the processor may be replaced with specially configured logic to perform the functions described here.

The input/output logic **720** is configured to enable the privacy card to send and receive information. In one embodiment, the input/output logic **720** is configured to communicate through a wired or contact connection. In another embodiment, the logic **720** is configured to communicate through a wireless or contactless connection. A variety of communication technologies may be used.

In one embodiment, a display **725** is used to generate bar codes scannable by coupled devices and used to perform processes as described herein. The privacy card **705** may also include a magnetic stripe generator **740** to simulate a magnetic stripe readable by devices such as legacy POS terminals.

In one embodiment, fingerprint recognition is used as a security mechanism that limits access to the card **705** to authorized users. A fingerprint touch pad and associated logic **730** is therefore included in one embodiment to perform these functions. Alternately, security may be achieved using a smart card chip interface **750**, which uses known smart card technology to perform the function.

In another embodiment the privacy card may originate as a dumb device that includes minimal capabilities, referred to herein as an "open mode card". The open mode card may be configured to have a foundation of a secure access capability built in. Examples of open mode cards may be pre-paid phone cards or the like. However, in their original state (their state when obtained by the user), it is not secure and therefore can be used by anybody as is typical for dumb devices.

In one embodiment, the user purchases an open mode pre-paid phone card off the rack at a retail outlet, uses the card in open mode until the pre-paid value expires, then disposes of the card. In one embodiment, these cards have a business value because they can carry on-card images/text that act as free advertising for related services. If the user chooses to "upgrade", then the card can be converted to a secure device. However, if the user chooses not to upgrade, the same card still has a functional business and user value.

In an alternate embodiment, the open mode card may be converted to a secure card. In one embodiment the user converts the card to a secure mode device by inserting it into the digital wallet and performing a conversion/setup procedure. The main value is that the user's financial or other personal investment in the card now becomes more secure in the event of a lost or stolen card. Once converted, the card may not be used in open mode and is thus dedicated to the person who made the conversion. Additional capabilities of the card might be added or eliminated after conversion to secure mode, such as the ability for the card to be re-charged with a stored value.

Alternately, the card may be configured to operate in a dual mode wherein certain functionality may be accessed by anyone, and additional functionality that may only be accessed by specified users.

Alternately, a multi-mode may be established wherein use of the card is restricted to a specific set of people, or a specific set of functionality, or a specific set of host devices (digital wallets). For example, this may be a family card that

allows the parents to spend up to the credit limit, and the children to spend up to a limit set by the parents, and only for certain types of purchases or stores.

An alternate embodiment of the privacy card **750** is illustrated in FIG. **7***b*. In this embodiment, technology found in existing FeliCa cards is incorporated, represented by block **755**. This technology may include power using received RF signals picked up by a loop antenna. Alternately, the card **750** may include a battery (not shown).

The transaction history storage area **757** stores transaction records (electronic receipts) that are received from POS terminals. The ways for the data to be input to the card include wireless communications and the smart card chip interface which functions similar to existing smart card interfaces. Both of these approaches presume that the POS terminal is equipped with the corresponding interface and can therefore transmit the data to the card.

The magnetic stripe **759**, in one embodiment, may be designed as a two-way data interchange interface, allowing a POS terminal to write data onto the magnetic stripe, which is then captured by logic in the card and stored in the transaction history area **757**. However, it requires the POS terminal to have such capability and further requires a different mode of user interaction—holding the card stationary at the POS terminal instead of swiping the card through a slot.

The user identity/account information block **760** stores data about the user and accounts that are accessed by the card. Typically, in one embodiment, this data may only be changed by authorized devices such as an authorized digital wallet or TPCH. The type of data stored includes the meta account information used to identify the account to be used.

The eCoupons and other financial data storage block **762** is used for storing data that is to be used during financial transactions, such as eCoupons that are to be transmitted to the POS as part of the purchase activity. An example of other financial data might include account balances that are dynamically updated as transactions are performed.

The globally unique silicon ID (GUID) **764** is used to identify the privacy card among other existing transaction cards. There are several ways known in the art of assigning and tracking these values to ensure that they are unique across manufacturers and product lines.

The mag stripe emulation/driver block **766** dynamically generates a magnetic stripe data image for use in some POS terminals, such as legacy POS terminals. In one embodiment, the decision of what data to simulate on the magnetic stripe is made by the user when the privacy card is activated, for example when coupled to a digital wallet. The user is provided with a menu of accounts that can be used, and selects one of them. The digital wallet indicates which account was selected and the driver **766** programs the stripe accordingly.

The smart card chip driver **768** performs a similar function as the mag stripe driver **766** except that it uses the industry standard chip interface. This interface defines a simple serial data transmission between the card and the reader/writer device (e.g., POS terminal) and is known in the art. This is advantageous to enable the privacy card to be useful with devices, e.g., POS terminals, that have a smart card chip interface.

The digital wallet interaction driver block **770** manages the interaction of the privacy card with a digital wallet device. When the car is inserted into the digital wallet, this block initiates the card-side security algorithms of digital wallet validation. As the user interacts with the wallet's touch screen, the wallet will request data from and store data to the card, which may also be handled by block **770**. When the privacy card is removed from the wallet, the functional block takes care of all necessary security measures to protect the data and functionality of the card. Thus, for example, if the privacy card was inserted and activated, causing the magnetic stripe to be dynamically programmed with an account alias value and the card was then removed from the digital wallet to be swiped through a legacy POS terminal, then block **770** would initiate a timer, for example for 20 seconds. Once the timer expires, the block **770** would disable the magnetic strip emulator, effectively deleting the account alias from the magnetic stripe.

An alternate embodiment is shown in FIG. **7***c*. In this embodiment, the privacy card may include those functions set forth in FIG. **7***b*, referred to herein as first generation privacy card technology block **775** and FeliCa Technology block **774**, and further include the functions represented by blocks **777**, **780**, **781**, **783**, **785**, **787**, **789**.

The user identity info block **760**, which was described previously in FIG. **7***b* PrivacyCard, may contain the authorized fingerprint recognition samples. In one embodiment, those samples are entered into the device during its initialization phases, which have been described elsewhere.

The account selection functional block **780** presents a user interface on the card's display, allowing the user to select an appropriate account to use for a transaction. This functional block **780** would receive the user's selection, and then trigger the mag stripe driver, described previously, to create the account alias value on the magnetic stripe. This could also be used to provide an account alias through the smart card chip interface, or even the non-contact wireless interface.

The user authentication block **777** preferably includes a biometric solution of validating that the user interacting with the device is an authorized user. This can be achieved, for example, by using a fingerprint recognition pad. One example of such a technology is Sony's FIU (fingerprint identification unit), which is composed of a very thin silicon sensing pad along with the appropriate electronics. Since the silicon pad is so thin, it could be used on a card device. At various times during interaction, the user is prompted to supply a fingerprint recognition sample. This block captures the sample, and carries out a recognition algorithm against the authorized samples that are stored in the user identity block described above. If a match is found, the user is authorized to access the data and functionality of the device.

The piezo speaker driver **781** enables the card to use a very small piezo-electronic speaker, which is sufficient for generating various tones to assist with helping the user understand when the card needs attention, when a transaction has been completed, etc. Such speakers require only a very small amount of energy, and are therefore reasonable for use in limited-power environments such as a card device.

The display driver **783** manages the creation and display of images for the card's display device. As described earlier the privacy card can be enabled with the display using various technologies. One of them is a very thin LCD that requires no power to retain the data being displayed; only a small amount of power is required in order to set the pixels to a specific value. As the user interacts with the device, the display driver would generate the appropriate images, trigger the on-card power supply to set the screen, and then cycle the power off. In one embodiment, to minimize the amount of pixels that need to be changed, and therefore the amount of battery power that will be consumed, the driver calculates the pixel differences between the existing screen and the next screen; only changed pixels are actually modi-

fied on the screen, as opposed to generating an entire screen refresh of every pixel as in a typical computer display. This algorithm may be configured to use only a minimum amount of battery power, thus preserving energy and allowing the card to remain "active" for a longer amount of time between recharging.

The data input driver **785** manages the data input mechanism, which is preferably a touch mechanism built into the card. Alternative forms of data input include small buttons that can be built into the card, or even an external peripheral such as a keyboard that communicates through the non-contact wireless communications function. Alternately, a touch sensitive input mechanism such as a resistive film may be used.

The software agent **787** monitors the user's interaction with the device, performing various local data mining activities and keeping track of many aspects of the card's use. For example, the agent can monitor the various types of eCoupons that are redeemed over a period of time, and dynamically build up a profile of the user's preferences for various types of products. The agent can interact with other agents on other platforms (on PC's or DTV's, on web servers, etc.) to actively seek out additional eCoupons that the user might not be aware of, or to actively filter out incoming advertisements and eCoupons so that the user is not overwhelmed by a flood of data coming in and being presented on the device.

Thus, the agent **787** can be configured to actively look for content on behalf of the user as well as filter out unwanted incoming information. In one embodiment, the data may be described by XML and the agent may operate via Java applets. Other embodiments are also contemplated. Although the software agent is described with reference to FIG. **7***C*, it may also be implemented in alternate embodiments, including the embodiments described in FIGS. **7***A* and **7***B*.

Power for the privacy card, as described previously, may be a lithium polymer battery that supports very thin and flexible form factors. The battery can be recharged via inductive charging technologies, which thus does not require a physical connector to be attached to the card. This increases reliability and convenience for the user.

FIGS. **7***a*, **7***b* and **7***c* illustrate some embodiments of the privacy card. Other embodiments are also contemplated. For example, in an alternate embodiment, the privacy card may be viewed as a "virtual" device in the form of data structure that may be downloaded to the digital wallet and used through the digital wallet interface(s) to connect to a POS terminal.

FIG. **8** illustrates a physical embodiment of the digital wallet and privacy card. In this embodiment the privacy card **810** interfaces to the wallet **820**. The wallet **820** receives privacy card information and includes an interface to the TPCH. The wallet may also include extra memory **830** so that additional functions, not necessarily related to eCommerce transactions, can be performed. In this embodiment, the functionality of the privacy card may be limited with the digital wallet providing additional functionality not found on the privacy card. For example, the digital wallet may provide a display not found on one embodiment of a privacy card. The digital wallet may also provide the POS interface, e.g., wireless, bar code, smart card data, optical terminal, that legacy POS terminals may read in order to perform transactions.

One embodiment of the digital wallet is illustrated in FIG. **9***a*. The digital wallet **905** includes a coupling input **910** for the privacy card, processor **915**, memory **920**, input/output logic **925**, display **930** and peripheral port **935**. The processor **915** is configured to execute instructions, such as those stored in memory **920**, to perform the functionality described herein. Memory **920** may also store data including financial information, eCoupons, shopping lists and the like. The digital wallet may be configured to have additional storage. In one embodiment, the additional storage is in a form of a card that couples to the device through peripheral port **935**.

In one embodiment, the privacy card couples to the digital wallet through port **910**; however, the privacy card may also couple to the digital wallet through another form of connection including a wireless connection.

Input/output logic **925** provides the mechanism for the digital wallet to communicate information. In one embodiment, the input/output logic **925** provides data to a POS terminal or to the privacy card in a prespecified format. The data may be output through a wired or wireless connection.

The digital wallet may also include a display **930** for display of status information to the user. The display **930** may also provide requests for input and may be a touch sensitive display, enabling the user to provide the input through the display.

The digital wallet may also incorporate functionality not illustrated in FIG. **9***a*. For example, a fingerprint pad and associated logic may be included to secure the device; thus, to access the device, the user would have to touch the fingerprint pad and wait for the logic to determine that the user is authorized to access the device. The digital wallet may also be configured to generate bar codes and/or magnetic stripe data for interfacing with other devices including legacy POS terminals. For example, the magnetic stripe data may then be programmed into the privacy card for use with a legacy POS terminal.

An alternate embodiment of a digital wallet is illustrated in FIG. **9***b*. The digital wallet **950** may be built using any of the previous technology blocks, **946**, **947**, **948**, **949** represented by and discussed with reference to FIGS. **7***a*, **7***b*, and **7***c*, with the addition of Memory/Info Stick support block **952**, and the privacy card interface slot **954**. Of course, the physical manifestation of many of the technologies in the digital wallet will likely be different from those in the privacy card devices, mainly because of the availability of physical real estate in which to package technology. Examples of different physical representations would include the screen, fingerprint recognition unit, speaker, etc.

The various elements of the privacy card, such as the speaker, fingerprint recognition unit, screen, and battery, can all be included in the digital wallet **950**. However, they might be more robust or feature-rich in the case of the digital wallet, because there is more physical space in which to store the required technologies.

For example, the digital wallet screen could be a small, high resolution color LCD, while the privacy card's LCD screen would likely be only black & white, and of limited resolution.

The memory/info stick driver **952** allows the digital wallet to accept memory stick and info stick devices. The info stick is mechanism that puts a CPU, ROM/RAM, etc. on a memory stick device. By inserting an info stick into the digital wallet, the functionality of the wallet device can be extended with the functions of the info stick.

The privacy card slot driver **954** manages the wallet-side of interaction with a privacy card device. When a card is inserted into the slot, this driver will initiate the necessary security steps to ensure that the card is a legitimate device; query the card for its basic capabilities and information that

it might be holding; etc. The driver interacts with the FeliCa reader/writer mechanism to facilitate this communication.

The wireless transmission driver **956** manages the built-in wireless capabilities of the digital wallet. These wireless communications functions are longer-range that those of the FeliCa-type wireless, which is typically only a few inches. Examples of these wireless capabilities include cellular, pager, IEEE 802.3, etc. These allow the digital wallet to communicate over distances of a few meters to many miles, depending on the necessary application.

The FeliCa reader/writer block **958** allows the digital wallet to communicate with the privacy card device when it is inserted. Thus, the digital wallet acts as an external POS terminal as far as the privacy card is concerned, with respect to communications protocols. This mechanism is one embodiment for how the digital wallet communicates with its privacy card, and can be used for all interaction. Alternate forms of communication could be through the smart card chip, through the magnetic stripe contact, etc.

In one embodiment, the digital wallet is intended to be the means by which the privacy card interfaces with the user and eCommerce system. In one embodiment, the digital wallet stores eCommerce related data on behalf of the user including transaction histories and meta-account information needed to carry out a transaction using the transaction privacy clearing house function of the system. In one embodiment the meta account information may be an abstraction of the user's real identity as opposed to the actual user's name, address, etc. For example, the TPCH keeps records of the user's real bank account numbers, but assigns a different number for use by retailers and POS terminals. For example, an actual Bank Visa account number may be 1234 0000 9876 1423 could be represented as 9999 9999 9999 9999. This number, in association with the transaction card's ID, would enable the TPCH to know that the Bank's account 1234 0000 9876 1423 was actually the account being used.

The purpose of this data is to abstract the user's identity while at the same time providing the necessary information for the transaction to be completed.

A digital wallet may also support secure user authentication mechanisms such as PIN code, or fingerprint recognition, for the purposes of a user accessing data or carrying out a transaction.

In one embodiment, the digital wallet is configured to operate in conjunction with a POS terminal. In one embodiment the connection with the POS terminal can be a wireless connection. Alternately connections may be made through a wired connection, magnetic stripe emulation or smart card emulation or through using a coupled privacy card.

The digital wallet can also be used to reconcile data among several privacy card devices, so that all the devices share the same data history. In this embodiment, a convenient solution is provided for users who prefer to use several different cards and need to keep the cards in separate locations but have consistent information. For example, while traveling many people may keep one card in their carry-on luggage, and a separate one in a suitcase. This way if one is lost or stolen the other is available as backup. Thus, a user may have redundant transaction devices that are kept synchronized with each other.

In addition to the eCommerce functionality, the digital wallet may be configured to provide other functional capabilities. For example, the digital wallet can be configured to contain extra user information, such as passport numbers or medical records. The digital wallet may contain personal digital assistant functionality such as a calendar. An extra memory slot can be used to insert memory cards containing digital photo albums for viewing on the screen or a slot on the device may receive a card that has pager or cell phone functionality built-in.

In one embodiment the digital wallet may have a touch sensitive screen for data display and input, and a slot into which the privacy card may be inserted for communications with the privacy card. Optionally, it may also include a memory slot for insertion of memory devices. In one embodiment, the privacy card is inserted into the digital wallet for purposes of accessing privacy card data and for enabling it to be used with a legacy POS terminal (e.g., a terminal that requires a magnetic stripe or smart card contact).

The digital wallet may have a user authentication mechanism such as fingerprint recognition. This might be reflected as a fingerprint recognition pad on one surface of the device. In one embodiment, the digital wallet is configured to only work with an authorized privacy card. In an alternate embodiment, the digital wallet is configured to work with more than one privacy card.

In one embodiment, the privacy card is designed to work in conjunction with a specific digital wallet or similar type of device or devices. At the time of manufacture, or during an initial setup stage in a processing facility such as a bank, the card is configured with user and digital wallet-specific information. The card is then delivered to a specific user. Aspects of the card's features and functionality are hidden behind a security mechanism, rendering the card useless to unauthorized users.

One embodiment of a process to set up a digital wallet for operation with a privacy card to perform transactions is illustrated by FIG. **10**. The user or issuing facility (e.g., bank) may set up the digital wallet and/or privacy card. As noted above, in one embodiment of the privacy card, the privacy card is coupled to a digital wallet and the digital wallet couples to a POS terminal that interfaces with the TPCH to perform a transaction.

In one embodiment, the digital wallet, for security, is configured to only work with a specified authorized privacy card. In one embodiment the user visits a web site or alternately, an authorized entity such as a bank, and fills out a form to be a new user of the digital wallet, or fills out a paper form and sends it to a specified address. This may or may not involve some kind of requirement to purchase the device. As part of the registration process, the user may be required to answer a variety of questions that serve not only data mining purposes, but also security purposes. Also as part of the process, the user is requested to provide a variety of questions and answers that only the user would be able to know. Additional data that the user must provide might include existing financial accounts that will be accessed via this device (credit/debit accounts, savings/checking, loyalty cards, etc.).

At the processing facility, a device is prepared that includes some basic information about the target user and necessary account information. Also included is a set of questions (and the correct answers) that will be asked of the person who receives this device in the mail. The device may also be encoded with a secret PIN code that must be entered to begin the user-confirmation procedure.

The user receives a confirmation of registration, which includes a secret PIN code that may be used for the first-time setup procedure. The means of receiving this PIN code might be a secure email message or a standard paper-based

mail message. The confirmation message may not typically include any of the questions and answers that were used during the sign-up process.

Under separate cover, the user may receive the digital wallet with a simple set of instructions for how to personalize and activate the device. The instructions might be on paper, or might include instructions that are presented on the digital wallet screen as the process is carried out.

In one embodiment, the personalization process may be as described below. The user turns on the digital wallet (for example, touches the fingerprint recognition pad in order to turn on the power). The device performs its startup procedure, and detects that is has not yet been personalized. Thus, it first prompts the user to enter the secret PIN code. If the PIN code entry fails, the user is prompted again. Ideally, the user is given a finite number of chances to enter the data. After the last failure, the device permanently disables itself and thus becomes useless. It may also display a message requesting that the device be returned to an authorized facility.

Assuming successful PIN code entry, the user may then be prompted to answer several of the security questions that were entered into the device at the processing center. Some of the questions might require data entry, and others might be constructed as multiple-choice, with both the correct as well as incorrect answers supplied. Assuming successful response to these questions, the user may then be prompted to enter secure personal identification information such as fingerprint data. In one embodiment in which fingerprint data is used, the user is prompted to enter fingerprint data by successively pressing one or more fingers against the recognition pad. The device prompts the user for each fingerprint that must be entered, for example, using a graphical image of a hand with the indicated finger.

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. If confirmation fails, the user is prompted to start over with entry. Failure to reliably enter the fingerprint data after a finite number of tries will result in the device permanently disabling itself, and optionally providing an on-screen message to the user to go to a secure processing facility (such as a bank) to complete the process. After successful personalization, the device is then ready to be used for the initial set of services that the user requested during the registration process. Once the device has been initialized for secure transactions, additional services could be downloaded to the device.

An alternate embodiment for setting up a transaction device such as a digital wallet is shown in FIG. **11**. In this embodiment, the process illustrates how to securely get the user's fingerprint information into the device for personalization in a manner that does not require the user to go to a processing facility such as a bank and is thus more convenient for the user.

This method presumes that the user already has some kind of fingerprint scanning device that they can easily access. In the future, such devices are very likely to be built directly into PCs, in an effort to provide secure access to those machines and their content. By utilizing these devices, this alternative embodiment becomes quite practical.

The embodiment described assumes that the user has a PC with an integrated fingerprint recognition pad or an FIU peripheral device, and that the appropriate security software exists. It may be incorporated into a web browser on which a transaction device registration form was displayed and filled out by the user, or in a dedicated software application for registration.

At step **1101**, after filling out the transaction device registration form, the user presses the "submit form" button or other appropriate trigger mechanism. The user is prompted to touch the fingerprint recognition pad in order to provide non-repudiation data (the user is "signing" the form and verifying that the user wants to register), and is providing the fingerprint identity sample that will be stored in the transaction device by the processing facility, for example, the TPCH. At step **1102** the PC software encrypts all of the information and delivers it to the TPCH over a secure connection.

At step **1103** the processing facility creates a new transaction device and personalizes it with the fingerprint and other data that was collected during registration. The processing facility delivers the transaction device to the user.

At step **1104**, upon receiving the transaction device, the user activates it for the first time. The device goes through its startup procedure and determines that it has not yet verified successful delivery to the valid user. It notifies the user that the setup procedure should be finalized, which requires the user to supply a fingerprint sample by touching the recognition pad. It might also require the user to answer a few questions just as an extra precaution.

At step **1105**, once the software agent inside the transaction device is satisfied that the authorized user has received the device, it contacts the processing facility to confirm that delivery and authorization was successful. It might do this via a web browser on a PC or direct wireless connection.

At step **1106**, the processing facility finishes its registration procedure and transmits a final signal to the transaction device that it can enable itself for use. The transaction device notifies the user that setup has finished and that it can now be used, step **1107**.

Embodiments of processes for initially configuring a digital wallet are described above. It is apparent that the digital wallet can also have additional personalized information added in the future by visiting a secure facility such as a bank, DMV, etc. or interfacing remotely, either through the Internet or direct connection, to an authorized facility.

Similar processes may be performed to set up a privacy card. The user fills out registration data and provides it to an issuing or authorizing facility. If the privacy card is intended to work only with a specific digital wallet, then the issuing facility would obtain a unique identifier of the specific digital wallet. This can be obtained from the digital wallet issuing facility, or directly from the digital wallet itself via a secure electronic transaction. As an example of the latter, the digital wallet can interact with a web browser, providing the necessary digital wallet identification information to the browser or other network software, which is then transmitted to the issuing facility. The facility may contact the TPCH to confirm that everything is okay and then downloads new data. This entire transaction can be encrypted for security. In an alternative embodiment, the user may take the digital wallet to an issuing facility, where the digital wallet identification data can be directly obtained from the device in a secure manner.

Thus, in one embodiment, it is not necessary for the issuing facility to obtain user fingerprint or other identity information, because the digital wallet will not work, and will therefore not interact with the privacy card, unless the user is validated by the digital wallet during a transaction.

If the privacy card is intended to work with any digital wallet but with only specified users, then it is preferable for

the issuing facility to obtain the necessary user identification information. Normally this would be fingerprint data, but it might be any information that will satisfy security requirements. This data can be obtained in a manner similar to that described for the digital wallet identification value; in this case, the data being transmitted would be the fingerprint data.

The facility creates the privacy card device configured for the specified digital wallets and authorized users, recording the appropriate information into permanent storage in the privacy card.

As noted earlier, in one embodiment a privacy card may operate in an open mode and subsequently be converted to a secure mode. One embodiment of the process is described with reference to FIG. **12**.

The user receives a standard "non-secure" card such as a phone card from a retailer or a credit card from a bank, either by a purchase or registration procedure. When in open mode, the card does not contain the necessary user-specific information used in a secure mode. The user inserts the open mode card into a digital wallet. The digital wallet examines the card and determines that it is currently operating in open mode, and that it does not currently have a secure mode.

The digital wallet displays a message to the user, explaining that the card is currently in open mode, but it can be converted to a secure mode if desired. Alternatively, the digital wallet can have a menu option that triggers the conversion process, which can be selected by the user at any time.

Once the user confirms that conversion to secure mode is requested, the digital wallet requests configuration options from the user. This might include the option to leave the card in dual mode or multi-mode; the option to include or exclude specific individuals known to the digital wallet as valid users of the card; the option to use the card with only this digital wallet or with any digital wallet, etc.

Once the user supplies the necessary configuration information, the privacy card and digital wallet carry out a secure exchange, for example, with the digital wallet assigning the equivalent of one or more private keys to the card. These private keys can be composed of user-specific data obtained from fingerprint recognition, the digital wallet identification information, TPCH etc. These keys become the means by which the card is accessible only to specified individuals or only to the particular authorized digital wallet. The privacy card records the keys in its own permanent, secure memory. Thereafter, subsequent access to the privacy card by the user requires secure exchange between the card and digital wallet.

In one embodiment, a POS terminal is the link between the digital wallet or privacy card and the transaction privacy clearinghouse (TPCH) of the eCommerce system. The main purpose of the POS terminal is to establish a secure transaction connection between the transaction device and the TPCH and to transfer transaction data to the TPCH for completion of the transaction. The POS terminal can also be used to transfer data from the TPCH to the transaction device. An example of data that may be transferred, is the distribution of electronic contents such as electronic coupons, which might pass directly from the TPCH to the transaction device.

In one embodiment there is a level of consistency applied to home-based and in-store retail purchase functionality. To achieve this, there may be three types of POS terminals, the legacy Retail POS terminal, the New Retail POS terminal and the personal POS terminal.

The legacy Retail POS terminal represents existing terminals that use a bar code, a magnetic stripe or smart card input. The new retail POS terminal as referred to herein may include those terminals that are particularly configured to interface to the digital wallet or privacy card described herein and may not use a bar code, magnetic stripe or smart card contact input. The personal POS terminal, discussed herein, refers to a home-based POS terminal.

In one embodiment, the basic transaction experience is the same for each type of POS terminal. In a retail situation, the user or a store clerk specifies the items to be purchased. For example, this may be achieved by scanning items across a barcode scanner or a similar device. For an Internet-based purchase, the user clicks on several items to fill an electronic shopping cart or something similar on a website. Once the purchase has been specified, the user enables the transaction device. In one embodiment this may be the digital wallet, the digital wallet with a co-opted privacy card, or a privacy card with the communication functionality installed within the card.

In one embodiment, a user enables a transaction device with a security mechanism such as fingerprint recognition. Other secure solutions, such as a PIN entry, may also be used.

In one embodiment, if the POS terminal does not support wireless communication with a transaction device, the transaction device may include a magnetic stripe or barcode generator to generate the privacy card identification information to complete the transaction.

In one embodiment, if the POS terminal does not support electronic receipts (e.g., existing legacy POS terminals), the user may receive the standard paper receipt which must be signed by hand. Alternately, the system may be configured to be paperless wherein the receipt is electronically stored on the user's transaction device, transmitted to the user's email account, or placed at a location in a network, e.g., personal account information in a bank network, accessible by the user.

The signature, which in one embodiment may be a fingerprint, may be electronically captured and the system may be configured such that the display shows a confirmation message to enable the clerk to visually check for verification. The privacy card/digital wallet may be configured to be used with the legacy POS terminal and the terminal may process the transaction in a standard way, by dialing into a central authority to carry out the financial processing. In this situation it would be possible to preserve the user's identity because there is no requirement to expose name, address, etc.

In an alternate embodiment, it may be possible to preserve the user's privacy by using two different account numbers. One number may be for a standard account for use at existing legacy POS terminals as the legacy terminals do not need to provide user identity information and the system may be configured to not provide such information. The other number may be a new privacy account number for use with newer terminals which are compliant with the privacy card system.

In one embodiment, the legacy POS terminals are configured to dial into the TPCH, which then facilitates the transaction as usual. In return, the TPCH returns the basic purchase data such as a list of items purchased along with a reference to the transaction device (e.g., the digital wallet ID or privacy card ID) so that the store can keep track of its inventory usage and also have a record of the user who purchased the items. In this situation the user information is not the user's identity but an electronic alias reflective of the

transaction device, i.e., digital wallet or privacy card, used. An alternate modification would be to modify the legacy POS terminal software to treat the transaction in the same way that the traditional credit cards are used; the store keeps track of all data directly and dials into a location to carry out the transaction (in this situation the TPCH). In this embodiment the TPCH does not have to send back any data since the store already has it, but the store does need to send the purchase data to the TPCH, which needs this information to build its database of purchase histories.

To interface with existing legacy retail terminals, the transaction device may be configured to simulate a magnetic stripe media readable by the legacy retail terminals. In one embodiment, the transaction device is configured to provide dynamically generated bar codes readable by a POS terminal. Thus, when a user purchases items through a legacy retail terminal using the transaction device, the magnetic stripe and/or barcode generated data is forwarded along with details of the purchase to the TPCH for processing.

A retail POS terminal may also include a display device that is used by the clerk performing the transaction. The display device may display information that is received from the privacy card, such as the user's picture, etc. This is a security feature that allows the clerk to check on certain items of data that can help to initially confirm that the user is authorized. The transaction device may therefore contain an encoded encrypted image that is transmitted to the POS terminal. The terminal decodes the image and presents it on the clerk's display. This action may be performed concurrently with the transaction processing (i.e., verifying that the card is legitimate etc.). Fingerprint recognition may also be provided by the system for security.

In an embodiment that utilizes a new retail POS terminal that supports wireless communication, the user may enable the transaction device via a security mechanism and the transaction device may then communicate with the POS terminal directly through the wireless communication mechanism to carry out the transaction.

One embodiment of a POS terminal is shown in FIG. **13**. Terminal **1310** includes message logic and processing circuitry **1315** and may also include embedded software and storage and additional functionality to perform the functions of the POS terminal. A variety of interfaces may be utilized. For example, an IEEE 1394 interface **1320** may be configured to couple to a host device. A serial interface **1325**, modem **1330**, **1335**, **1340** and a connection to a transaction device **1350** may also be included in the terminal **1310**. The POS terminal **1310** may also drive an output video or audio signal device such as a display **1360**.

The POS terminal may collect the necessary information from the transaction device, e.g., the digital wallet, combine it with the purchase data, and send it to the TPCH. The TPCH may then authorize the transaction, store data relevant to the transaction in its records and trigger a financial transfer to the vendor's account. The POS terminal may then receive verification that the transaction is complete, and transfer the wireless receipt to the transaction device. Additional data can be transferred as well, such as electronic coupons and other promotional material.

Many retailers use a loyalty card system whereby the retailers award additional product discounts for their customers who use the card and purchase selected items. The main use of these programs is for data mining.

In one embodiment, the transaction device would be programmed with loyalty card account information, which would be an account maintained only by the retailer. This account is associated only with the transaction device, not with a specific human user, thus preserving the user's privacy and identity protection.

During a transaction, the clerk would request the loyalty card. The loyalty account information can be entered in a manner as is typically done today: either by a barcode which would be displayed on a screen of the user's transaction device, by an account number that is programmed into a magnetic stripe of the transaction device, or by wireless transmission.

The transaction device may be configured to carry both the payment and loyalty account information in the same magnetic stripe, because these stripes actually are composed of three separate bands. If the current legacy POS terminal in the retail store is able to read the other magnetic stripe bands, then it can read both accounts at the same time as the card is swiped through the reader.

In an embodiment of a system that uses a personal POS terminal, the user is likely to be making a purchase on-line while at home. The user specifies the items to be purchased on the appropriate web pages. When the items have been selected, the user clicks on a transaction device icon to trigger the transaction to be performed. One embodiment of the transaction device icon is displayed on the web page when the browser detects that a personal POS terminal is present. This detection may be handled by a custom browser plug-in or by a fully customized browser. The user may then be prompted to place the transaction device next to the user's computer or other device and enable it by using a built in security mechanism such as fingerprint recognition. The transaction device then communicates with the personal POS terminal, each of them authenticating the legitimacy of the other.

In one embodiment the vendor's website supports a standard such as ECML (electronic commerce markup language) that specifies a standard set of information for an electronic purchase. The web browser passes the ECML purchase order to the personal POS terminal which has verified through the security mechanism that the user is authorized to carry out this transaction.

In one embodiment, the personal POS terminal communicates with the TPCH on a dedicated connection, not the same Internet connection. This enhances security by not exposing the transaction data to any security weaknesses of the Internet.

The personal POS terminal accumulates transaction history data and either stores it locally or passes it to an appropriate location in the user's system, such as Quicken® (Quicken is a trademark of Intuit Corporation). If any electronic coupons or other related items are available they are also passed to the TPCH as part of the transaction.

In one embodiment, the personal POS terminal allows the user to have the equivalent of a retail POS terminal for use at home or wherever the user may wish to access it. The personal POS terminal may be configured to provide the same level of security for transactions as standard retail based POS terminals. It may allow non-retail, also referred to as "brick and mortar" electronic commerce transactions over a secured non-Internet connection. In one embodiment, it facilitates a portability solution and allows a user to carry out brick and mortar electronic commerce transactions from any location. 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.

The personal POS terminal may include data encryption technologies such as those used in retail-based POS termi-

nals. In addition, security protocols may be used including user authentication and authentication of the transaction devices themselves. By providing this additional security, an increased level of user confidence is provided. In one embodiment, the personal POS terminal is a physical device designed to be portable so that the users can have the same level of secure non-retail based transactions from almost any location they desire. The circuitry in the device may function as a small processing system to provide additional functionality.

The input/output of the personal POS terminal may function to transmit and receive wireless data between the terminal and an external device such as the transaction device. The terminal may store all electronic commerce transaction data within itself, for example, in flash memory, rather than transferring it to the coupled device, e.g., computer disk. This has several security benefits including greater reliability, less vulnerability to viruses and other hostile PC-based software, and the ability to have the data available when the POS terminal is configured as a transportable device. In an alternate embodiment, the terminal is used to transfer data from the transaction device to one or more destinations on the host device, such as accounting programs executing on the host device.

FIG. **14** is a simplified block diagram of one embodiment of a personal POS terminal. As described herein, a personal POS terminal is a POS terminal that may exist in the home environment. In the embodiment shown in FIG. **14**, the personal POS terminal includes a processor **1405**, input/output pad **1410**, power supply **1415**, wireless transceiver **1420**, which may be used to interface with the transaction device, security function **1425**, permanent storage **1430**, and temporary storage **1435**.

In one embodiment, the software executing on the personal POS terminal may include an internal driver software that executes locally to drive the wireless transceiver, software to store incoming data into memory and to control input/output to a computer (e.g., PC) coupled to the personal POS terminal.

Host application software may be stored on the personal POS terminal and uploaded by the host system for execution. The application may be written in a platform specific format or platform neutral code such as Java. Updated versions of the software may be stored on the personal POS terminal as needed. Application software may also be executed locally on the personal POS terminal. In one embodiment, a stored data file containing data accumulated from associated devices such as the privacy card and digital wallet may only be accessed by an authorized application executing on the personal POS terminal or host device (e.g., PC).

The personal POS terminal storage area may also contain a user application that gets uploaded to the PC and executed. This application, once a user-triggered data transfer is performed, performs the necessary authorization tasks to ensure that the data transfer is legitimate and sends the data to applications, such as Quicken® via an operating system specific interapplication communication (IAC) mechanism. It also allows the user to perform administrative tasks on the data, such as deleting all data from the remote (e.g., digital wallet) devices, to free up storage space. In one embodiment, the personal POS terminal can receive data from any remote device, including the transaction device, and pass it along to other authorized applications on the host device.

Security is always an issue as the transaction device, e.g., privacy card and/or digital wallet, contains sensitive information, such as financial transactions. The system may include a mechanism that prevents casual misuse or unauthorized access to that data. In one embodiment, the transaction device requires the user to activate it before the device is capable of transmitting data. The activation procedure may involve performing a security operation such as entering a PIN code on a numeric pad built into the device or opening a physical lock of some kind. Thus, if the personal POS terminal can receive data from the device, then it can assume that the user has authorized the transmission of data. In an alternate embodiment, a user authorization process is carried out by the personal POS terminal and the host application. In one embodiment, the personal POS terminal reads a PIN code or other authorization signature from the transaction device. The user enters in a corresponding value into the host application. The application then feeds the user's entered data to the personal POS terminal, the terminal then checks to see if the value entered by the user matches what was read from the device. Alternately, mutual device verification techniques may be utilized. Still, alternately, a combination of the above approaches may be used.

In one embodiment, the personal POS terminal is a self-contained mechanism with wireless communication capability for communicating with a transaction device. The personal POS terminal may also include software that is configured to communicate with the PC and the eCommerce system to perform the transaction. In one embodiment, the personal POS terminal includes a custom driver that gets uploaded from its internal storage to the host PC and executed. The custom driver can be configured to provide enhanced security. In addition, the custom driver may be configured to manage the display of information from the personal POS terminal to the PC screen and the input of data from the PC's keyboard to the personal POS.

In one embodiment, the personal POS terminal is configured in a self-contained execution environment that operates in parallel with the host (e.g., PC) platform. In one embodiment, the personal POS terminal may include data storage, memory and a processor that executes code that performs such support applications as web browsers and accounting systems. By keeping the applications and stored data on the personal POS system, the system provides enhanced levels of security and data protection for the user. More particularly, the user information and transaction data is never transferred onto the PC's hard disk. In addition, by utilizing a self contained execution environment, the eCommerce system is less dependent on the processing capabilities of the host platform (PC) that the user uses.

In one embodiment, certain functionality of the PC is utilized. In one embodiment, a coupled host device's keyboard is used for input and the host device's display is used for viewing. All other processing including communications is handled from within the secure environment of the personal POS terminal. For example, the personal POS terminal may rely on the PC having a modem that is used for connection to the TPCH.

The personal POS terminal may be configured to be mobile, such that the user may take it out of the home environment. For example, the user may take the personal POS on a business trip and from a portable PC continue to perform secure transactions from within a hotel room or business office. In such an embodiment, the records of the transactions are kept in the personal POS terminal just as if these were transactions that are carried out at home. In such a configuration, the external communications from the personal POS to the TPCH would have to accommodate various communications systems such as the business PBX system. In one embodiment, an adaptable soft modem architecture

resident on the personal POS terminal would be implemented. Alternately, a wireless (e.g., cellular) link may be used.

As noted above, by using the transaction device and the eCommerce system described herein, a user may be able to perform electronic commerce transactions without revealing the user's identity. A simplified flow diagram of one embodiment of the process to perform a transaction is as illustrated in FIG. **15**. At step **1505**, the user initiates the transaction. This transaction may be one over the Internet or through a retail store or bank. Other transaction networks may also be accessed. Privacy card information is provided to TPCH, step **1510**. The TPCH, at step **1520**, confirms the transaction and provides the confirmation to the vendor and the user. At step **1525** the vendor completes the transaction without knowledge of the identity of the user.

One embodiment of a transaction performed in the retail environment will be described with respect to FIG. **16**. At step **1601** a clerk triggers the purchase action, after having passed the items to be purchased through a checkout procedure, normally by scanning barcodes on the packaging. At step **1602** the retail POS terminal displays the current transaction total, and asks the clerk to continue processing the transaction. At step **1603** the clerk requests payment from the user. At step **1604**, the user activates the transaction device, requesting a payment transaction using any eCoupons that might have been collected by the transaction device prior to or during shopping. The transaction device requests the user to authenticate himself, for example, by fingerprint recognition, step **1605**. The user presses on the finger print recognition pad to continue, step **1606**. After verifying the user, the transaction device displays the collection of eCoupons that the user requested on its display screen, step **1607**.

The user hands the transaction device to the clerk, who successively scans the eCoupons barcodes into the legacy POS terminal in a manner similar to how paper coupons are scanned into the terminal. After each barcode is scanned, the clerk presses a "next" button, which indicates to the transaction device that the eCoupon was successfully entered. The transaction device then displays a bar code of a next eCoupon, and this process continues until all eCoupons have been entered for the transaction, step **1608**.

At step **1609**, payment is initiated. At step **1610** the user selects an account to use for payment by interacting with the transaction device, either by tapping on a text menu or on icons that represents the account to use. At step **1611**, the magnetic stripe generator of the transaction device is programmed with the appropriate account number information.

At step **1612**, the transaction device indicates to the user that the transaction device is now ready to be processed in the transaction. The transaction device is coupled to the magnetic stripe reader of the legacy POS terminal, just as it is currently done with typical credit or debit cards today to provide the necessary information.

The retail POS terminal establishes a secure connection with the TPCH, and requests that the transaction be carried out, step **1615**. it communicates the transaction record of items to be purchased, total, etc. and the requested account information. Assuming that the transaction is successful, the TPCH returns a confirmation message to the retail POS terminal, step **1616**, which in turn may display an appropriate message to the clerk, step **1617**. The clerk may then return the transaction device and perhaps a paper receipt of the transaction to the user, step **1618**.

The TPCH settles funds, transferring the appropriate amount into the vendor's account. It may also return any data mining information to the vendor's back-end system, for the use of the vendor in its own business management, step **1619**. The TPCH may also send an electronic receipt, step **1620**, to the transaction device via an alternate connection such as the Internet. The transaction device can store this information or communicate it to the personal POS terminal back at the user's home if they are two separate devices. This activity may not necessarily occur while the user is still in the store: the electronic receipt may arrive some time later, depending on the ability of the transaction device to establish some kind of network connection with the TPCH, such as through a web browser, direct dialup, etc.

An example of a web-based transaction performed in accordance with the teachings of the present invention is discussed with reference to FIG. **17**. The following sequence describes steps involved in a typical web-based transaction using a transaction device such as a privacy card and/or digital wallet and a personal POS terminal.

In the present example, the user may be at home with a PC, cable, satellite or digital television device, a web browser, and a personal POS terminal device as described herein. The user has selected items to be purchased and is ready to trigger a purchase. The user may either navigate to a web page by using the facilities of the web browser, or by triggering a shopping activity using the transaction device.

For example, if the transaction device is used to trigger shopping activity, the user may tap on an on-screen icon being displayed by the transaction device, e.g., digital wallet; and the digital wallet transmits a signal to the PC or DTV, via the personal POS terminal, which then transmits the signal to the web browser. The transmitted signal causes the web browser to launch if it is not already running, and to navigate to the desired web page indicated by the icon.

The user triggers the purchase, usually by clicking on a "Buy!" or similar button in the web browser. In this embodiment, the browser has been "customized" via a plug-in that allows it to communicate with the personal POS terminal, which is either integrated directly into the host PC or DTV, or has been added as a peripheral device via a known interface.

In an alternative embodiment of the system, the personal POS terminal functionality of providing secure communication and transactions with the Transaction Privacy Clearing House (TPCH) can be integrated into the digital wallet directly. In this embodiment, a remaining functionality to be provided is the communications interface between the digital wallet and the host PC or DTV. This can be implemented via a wired or wireless connection, for example, USB telephone, IEEE 1394, etc.

Once a transaction has been triggered, the browser communicates with the personal POS terminal, requesting it to initiate a transaction. The browser provides a transaction record, which includes all of the necessary data to support this transaction, including a list of items being purchased, unit cost and quantity, the vendor who will provide the items, etc.

When the personal POS terminal receives the transaction request, it communicates with the transaction device, asking the transaction device to validate the user, confirm that the user wants to make this transaction, and get the appropriate information for which account the user wants to use for payment.

The transaction device may request the user's attention, either via audio or video signals, or both. The transaction device screen, or alternately, a personal POS display, PC or DTV screen, displays the transaction amount, and requests the user to select which account to use for payment. When

the user has selected an account, the transaction device asks the user to confirm the entire transaction and that the user is authorized, for example, by entering a PIN or providing a fingerprint recognition sample.

The transaction device receives confirmation of the transaction and validates that the user is authorized. When information on the user's side of the transaction has been set up to perform a transaction, the personal POS terminal opens a secure communications session to the TPCH, requesting a transaction. The personal POS terminal provides the transaction record that it received from the web browser and the unique ID of the transaction device. The TPCH uses the unique ID of the transaction device to process the transaction.

After validating that the transaction device is in good standing and that the selected account has sufficient funds for the transaction, the TPCH issues a transaction confirmation back to the personal POS terminal. The personal POS terminal reflects the transaction confirmation back to the web browser and the transaction device. The transaction device may display a transaction confirmation to the user and may additionally record the transaction in its local storage. The personal POS terminal may also record the transaction in its local storage. In addition, in alternate embodiments, the personal POS terminal may enter the transaction directly into the user's personal finance program (e.g., Quicken) which may be executing on the user's PC or on the personal POS terminal.

Secure distribution of physical (or electronic) content to the user is performed once the transaction is authorized. Subsequently, the TPCH receives confirmation that the content was successfully shipped to the user and the user has acknowledged receipt of the content. Once the confirmation is received, the TPCH processes the settlement of funds.

The settlement of funds involves the transfer of the appropriate financial credit into the vendor's account. For the purposes of this example, it is assumed that the account is managed completely by the TPCH, and thus the funds transfer is handled completely inside of the TPCH. The vendor is not given any user identity information regarding the transaction; rather, the user is represented only by the transaction device identification information.

In an alternative embodiment, the TPCH may issue a funds settlement request to a third party financial institution on behalf of the user, causing the necessary funds to be transferred to the vendor from the user's account. In yet another alternative embodiment, the TPCH may act as a proxy for the user, whereby the TPCH takes the funds from the user's account as managed by a third party financial institution, and then issues a funds transfer from the TPCH account to the vendor's account. This embodiment further preserves the user's identity by not linking it with the funds transfer into the vendor's account.

It is possible to use the transaction device, e.g., privacy Card and/or digital wallet, for transactions that do not guarantee user privacy and identity protection. An example of this would be a web site that has its own proprietary eCommerce solution, which is not necessarily compliant with the policies of the digital wallet system.

A web browser plug-in can detect whether a web site is compliant with a transaction device as described herein. If it detects a non-compliant web site, then it displays a warning message to the user that the user's identity may be compromised and operates to perform the transaction while attempting to maintain the identity of the user as confidential.

In one embodiment, the transaction device may be configured to attempt to take a variety of steps to assist the user with preserving privacy and identity information. For example, the transaction device and web browser plug-in can attempt to determine what items are being purchased, for example by examining the current web page or the shopping cart in use. If the items are identified either by a name, a type (such as "book: sport: baseball"), or other such descriptive information, the browser plug-in can execute a web search to find a transaction device-compliant web site where this item can be purchased while maintaining the confidentiality of the identity of the user.

If an alternative purchase site can not be determined, the transaction device may then provide artificial information to the web site's purchase forms so that the user's identity is not revealed. Typically, the web browser has no way of knowing what is a valid name and what is not, and therefore may not object to such a string of characters not representative of the user's identity.

The transaction device may provide an account at the TPCH that is dynamically related to the particular web site and/or vendor. One means of achieving this is for the transaction device to be manufactured with several hundred unique transaction device ID values stored in its permanent memory. In this embodiment, the TPCH may maintain a copy of these values, so it knows that whenever a transaction arrives with one of these values, the TPCH knows which transaction device, and hence which user, the transaction it associated with.

Thus, when the transaction device determines that a transaction is to be performed with respect to a web site that is not transaction device-compliant, it searches its internal storage to find an alternate transaction device ID that has not yet been used, or one that has previously been used for this particular web site and/or vendor. The transaction device then uses this alternate ID as the account number that the web site vendor can charge for this purchase.

In this embodiment, vendors are prevented from sharing transaction history information, because there is no apparent common base of information by which to identify a user. Thus, for example, web site X might be carrying out transactions with transaction device ID=7, and web site Y may be carrying out transactions with a transaction device ID=9. Both of these sites may be dealing with the same user and same transaction device, but they don't know this. For this reason, the vendors are unable to successfully carry out any data mining operations that may jeopardize the user's identity or privacy.

Alternately the transaction device may provide the required information that might expose the user's identity, but the user would be enabled to allow or reject the transaction before it is carried out.

In one embodiment, a digital wallet can be used to enable/disable a privacy card device while it is coupled to the digital wallet. The privacy card may include a dynamically programmable magnetic stripe that can be enabled/disabled from the digital wallet, and programmed with an appropriate account number based on either the user's interaction with the digital wallet, or with the digital wallet automatically selecting the appropriate account info based on information received, such as wireless signals.

The transaction device may utilize software agent technologies to dynamically adapt to the user. The agent monitors the user's habits and activities with the transaction device, and might occasionally even pose a question to the user in order to help with this characterization process. Over time, the agent learns about the preferences of the user, and thus helps to either filter out undesirable information that

might be sent to the transaction device, or to actively search out information that the user might want (such as eCoupons, etc.)

In one embodiment, the transaction device may perform "local" data mining activities as part of its software agent activities. The local data mining information may occasionally be sent back to the TPCH, where it can be added to data mining information that had been generated there. In addition, the TPCH might update the transaction device with data mining information gathered by the TPCH.

In one embodiment, the transaction device can adapt to new services and functionality, either automatically by the transaction device or manually by the user. For example, on a web site the user might click a button that causes new functionality to be downloaded to the transaction device for access at a future time. The transaction device may also have wireless data transfer so it can detect the presence of a new service based on wireless data received.

The transaction device may have the ability to present the user with a "most likely" menu of functionality that the user wants to use at a given moment, based on the ability of the transaction device to detect its context (where it is, what the user might be doing at the moment, etc.). In one embodiment, a transaction device can potentially download and store a large amount of services and functionality, but not all of those services might be usable at any given time. For example, when arriving at a new location, the transaction device might download and store some services and functionality, but not all of those services might be usable at a particular moment. For example, when arriving at a new airport, the transaction device might download a new service that provides instructions for how to buy a train ticket to certain destinations. The dynamic adaptation to new services also includes the possibility of adapting to new settlement policies/mechanisms. For example, if the transaction device finds itself in the presence of a service that is managed by an alternate system, it can download not only the service software, but also the necessary underlying "transaction system" software. This might include new security protocols, etc.

For example, once a user has carried out a typical transaction to purchase electronic content, or has used the transaction device to register as a user of digital content that is delivered periodically, the content provider knows the transaction device ID and the electronic content distribution servers. The provider sends the content to the servers, along with a request to have it delivered to the transaction device itself, or to a proxy content viewing device. A "proxy content viewing device" may be something like a (digital television receiver) DTV. In one embodiment, the user receives the content or a reference to the content on the transaction device, but views that content on the DTV. This may be used for content that requires a larger screen or alternative viewing technologies that might not be provided on the transaction device itself.

In one embodiment, the distribution of physical content is performed through a product distributor, such as FedEx or UPS, who would participate in the user privacy protection policies of the eCommerce system. Furthermore, the distributor and vendor may act as independent entities such that they do not share information that links user identities with the product purchase data. One embodiment of physical content distribution process is illustrated by FIG. **18**.

At step **1801**, as part of a transaction, the TPCH assigns a unique package ID for the physical content item to be distributed. The TPCH transmits this ID along with the purchase record, to the vendor and to the distributor. At step **1802**, the TPCH looks into its secure databases to extract the user's physical address, encrypts this data, combines it into a data structure with the package ID, and securely transmits this data to the distributor.

The vendor puts the physical content into a package, and applies a coded label step **1803**. In one embodiment the coded label would be an electronic label that can be read from/written to using wireless transmission technology. Alternative embodiments may include bar code data, or other mechanisms that are preferably machine-readable. In this embodiment, the user's name and address are not displayed on the label, are not encoded in the electronic label and not known by the vendor.

At step **1804**, the distributor picks up the package and reads the electronic label using technology described above. Such technology could be added to existing devices commonly used by shippers such as UPS or FedEx, which already employ bar code scanning devices to streamline and optimize their shipping operations. The distributor has already received the necessary data from the TPCH which associates the user's physical address with the package ID, so the distributor's infrastructure processes the package as necessary, routing through delivery hubs, etc. The distributor takes the package to the user's physical address, step **1805**.

Upon receiving the package, the user can inspect it for accuracy and quality, etc. Once satisfied that the product is correct, the user activates the transaction device, and activates the "confirm acceptance of package" menu option, step **1806**. The transaction device carries out a secure message exchange with the distributor's handheld device (or other appropriate technologies) and with the TPCH, confirming that the product was successfully delivered and accepted, step **1807**.

An alternate embodiment for delivery provides a measure of convenience for the user, by having items delivered to any specified location. In this embodiment, the distributor may be a participant in the privacy protection policies of the eCommerce system; furthermore the distributor and vendor may act as independent entities, such that they don't attempt to share business data in order to link user identity with product purchase data.

In another embodiment for physical product distribution, an "anonymous drop-off point", such as a convenience store or other ubiquitous location is used. In one embodiment, it involves the use of a "package distribution kiosk" that allows the user to retrieve the package from the kiosk in a secure fashion.

In addition to providing a package ID to the vendor, the TPCH also provides the user's transaction device ID. Instead of providing the user's physical address to the distributor, the TPCH provides the address of a product drop-off location such as a convenience store.

Instead of delivering the package to the user's home or another address that identifies the user, the distributor takes the package to the specified drop-off location. In one embodiment the drop-off location has one or more package distribution kiosks, which in one embodiment are machines that can securely hold and release packages. The kiosk may automatically read the electronic label of the package in order to determine which transaction device is the legitimate owner of the package.

At some later time, the user goes to the kiosk, and activates the transaction device that carries out a secure exchange with the kiosk to release the appropriate package(s). The user can choose to inspect the product there and put it back into the kiosk if there is any damage, incorrect product, etc. The kiosk issues the delivery confir-

mation or rejection message to the TPCH, and the TPCH in turn passes the appropriate information to the vendor and distributor.

In some situations, a product must be returned to the vendor at some time after it was accepted on initial delivery. This can happen under many circumstances: the package might be left at the door and therefore does not get "real time" acceptance or rejection by the user while the delivery person is present; the device might break while under warranty, etc.

Once again, it is necessary to provide a solution that preserves the user's identity and privacy while at the same time allowing a very common activity to take place. One embodiment for returning a product is illustrated by FIG. **19**.

At step **1901**, the user re-packages the item, activates the transaction device and selects the "Return Package" function step **1902**. At step **1903**, the transaction device encodes a label with the package ID and vendor address, which is also stored in the transaction device. This label is applied to the package. The transaction device contacts the vendor and distributor to initiate the package return process, step **1904**.

The distributor picks up the package and reads the label, decoding the package ID and vendor address, step **1905**. The distributor returns the package to the appropriate vendor. The vendor has the necessary information to manage product warranty, tracking ownership via the transaction device ID, etc, step **1906**. Using this process, the user's privacy and identity information are not violated.

Another aspect of the present system is its ability to provide enhanced data mining and direct marketing for retailers while simultaneously providing user privacy and identity protection. Privacy is achieved by maintaining the user's identity information, such as name, address, etc. for limited access in a secure system such as the TPCH described herein.

When the user registers for and receives a transaction device, that device's globally unique ID value is associated with the user by the TPCH. Whenever the user carries out a transaction using the system, vendors receive only the transaction device ID in the transaction record. Thus, the transaction device acts as a digital alias for its user. When vendors need to contact the user who performed a transaction, they use the TPCH as an intermediary, requesting that it send the message to the transaction device with a given ID. Because the transaction device is an interactive device with communications capabilities, it can receive messages via the TPCH in a variety of ways, including wireless, Internet, a pager system, cellular, etc. It can then inform the user that a message is waiting. Depending upon the nature of the message, the user can view and respond to it directly on the digital wallet, or the user can view the message on an associated device such as a PC or DTV using the transaction device to gain access to the message.

A number of variations on data mining are contemplated. In one embodiment, the TPCH can compile an aggregate consumption profile of those users who use multiple transaction devices. In an alternate embodiment, one-to-one marketing is performed, which allows a vendor to communicate with a specific customer via the transaction device.

It is apparent that use of the transaction device enables a user to avoid unwanted solicitations. The TPCH may selectively provide consumption information. Alternately, a user may disassociate himself from their consumption profile by merely obtaining a new transaction device that would have a new device identification or by having a new ID associated with an existing device.

An example of how data mining and direct marketing may be performed is illustrated by FIG. **20**. At step **2001** the user activates the transaction device and requests a purchase action. The transaction device requests the necessary transaction information from the POS terminal (for example, a personal POS terminal or retail POS terminal), including information about the products being purchased, step **2002**. The information may include data such as item categories (dairy:milk:low fat), and other information that is useful for data mining purposes. Such information can be enabled using technologies such as the XML (Extensible Markup Language) protocol, which allows two or more parties to agree on an interpretation of flexible data structure mechanisms.

At step **2003**, the requested information is returned to the transaction device, where it is mined by the software agent technology resident in the transaction device. The results of the data mining may also be retained in the local storage of the transaction device. Alternatively, these results could be stored in a device coupled to the transaction device, such as a PC, another portable device such as a cell phone, etc. Such devices, assuming that they are always or typically in the proximity of the transaction device, would be able to offload some of the data storage requirements of the transaction device.

At step **2004**, the transaction device carries out the necessary secure transaction communication with the TPCH, providing the transaction data and its device ID. At step **2005**, as part of the transaction processing sequence, the TPCH delivers the necessary transaction information to the vendor. This includes basic information about the products being purchased and the ID of the transaction device being used for the transaction. Note that in this embodiment, it may not be necessary to provide an extensive amount of information about the products as is provided in step **2002**, because presumably the vendor has this information in its own databases.

At step **2006**, the vendor does its own data mining, associating the transaction device ID with the transaction and the details such as where the items were purchased (what store, what web site), when they were purchased, etc. At some time in the future, the vendor may want to follow up on this data mining activity by sending direct marketing material to the user. In one embodiment, the vendor can send materials by providing the materials and the transaction device ID to the TPCH, requesting a direct marketing distribution service.

At step **2007**, depending on the nature of the content, the TPCH sends the full content or a reference to that content, such as a web URL, to the transaction device. At step **2008**, the transaction device notifies the user that an incoming message has been received. This notification could be immediate, or delayed until the user has activated the transaction device for some reason. The means of notification could include audio and video signals.

At step **2009**, at some time in the future, the user may choose to view all pending messages. Alternatively, the transaction device might automatically detect that it is in proximity of a suitable viewing device such as the DTV, for example, and will remind the user that a message is waiting that is best viewed on the DTV. The user selects which items to review, and if appropriate, responds to the vendor.

A secure and convenient method and apparatus for storing and transmitting Telephony-based data is disclosed. In one embodiment, the method includes identifying an authorized user with a biometric device and enabling the authorized user to access private information over a voice network.

FIG. **21** is a block diagram of one embodiment for a networked query information system **2100**. System **2100**

includes a consumer access device **2102**. The consumer access device **2102** may be interfaced to a biometric security device **2104**. The user interfaces with the consumer access device **2102**. The consumer access device **2102** may interface with the POS **2106**, the TPCH **2108** directly or through the biometric security device **2104**. The consumer access device **2101** may also interface with the vendor **2112**. Additionally, the biometric security device **2104** may receive information from distributor **2114**. The TCPH **2108** is bidirectionally interfaced to distribution **2114** and vendor **2112**. Financial processing **2110** receives information from TCPH **2108** and sends information to vendor **2112**. Vendor **2112** interfaces bidirectionally with distribution **2114**, TCPH **2108**, and consumer access device **2102**.

FIG. **22** illustrates one embodiment of the system being utilized in a telephony based application. Here a standard telephone **2202** is interfaced via a telephone cable to a biometric device **2204** which in turn is connected via a standard telephone cable to, for example, a PBX, etc. In one example of operation, the user of the telephone **2202** is identified by the biometric device **2204** as an authorized user. Once identified as an authorized user, the biometric device **2204**, may for example allow the user to use the telephone **2202**. In another example, the biometric device **2204** may allow the transfer information in the form of tones to the PBX, etc., when requested by the user on the telephone **2202**. For example, the biometric device **2204** once having identified an authorized user may allow the transmission of tones representing such things as telephone numbers, access codes, PINs, etc.

FIG. **23** illustrates another embodiment of the system being utilized in a telephony based application. Here a standard telephone **2304** is interfaced via a telephone cable to, for example, a PBX, etc. The biometric device **2302** is interfaced to the telephone **2304** via a wireless connection. This wireless connection may be, but is not limited to, infrared, RF, audible tones, laser, etc. In one example of operation, the user of the telephone **2304** is identified by the biometric device **2302** as an authorized user. Once identified as an authorized user, the biometric device **2302**, may for example allow the user to use the telephone **2304**. In another example, the biometric device **2302** may allow the transfer information to the telephone **2304** which may then relay the received information in the form of tones to the PBX, etc. For example, the biometric device **2302** once having identified an authorized user may allow transmission of signals to the telephone **2304** representing such things as telephone numbers, access codes, PINs, etc.

FIG. **24** illustrates one embodiment of the system being utilized in a telephony based application. A standard telephone **2402** is interfaced via a telephone cable to, for example, a PBX, etc. The biometric device **2404** is integrated into the telephone **2402**. In one example of operation, the user of the telephone **2402** is identified by the biometric device **2404** as an authorized user. Once identified as an authorized user, the biometric device **2404**, may for example allow the user to use the telephone **2402**. In another example, the biometric device **2404** may, once an authorized user is identified, allow transmission of tones representing such things as telephone numbers, access codes, PINs, etc.

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.

The biometric device may have has stored within it some information representing for example, telephone numbers, passwords, etc., or this information may be stored external to the biometric device, yet, for example, only accessible one the biometric device has identified an authorized user. The information may be entered into the device either manually, for example, by the user, or automatically, for example, from reading a magnetic card or listening to tones on a telephone line. Sensitive information may be encrypted to enhance security.

FIG. **25** illustrates one embodiment of a record **2500** in a data structure for storage of information within a device. The record **2500** may have three fields. Field **2502** stores a phone number, field **2504** stores an identification (ID) value, and field **2506** stores data related to this record.

There may, of course, be multiple records within the data structure, and there may be other types of data structures within the device as well. For example, with respect to FIG. **25**, the first record may have these values: the phone field **2502** may have the telephone number of, for example, the user's bank. The ID value **2504** for this may be the number 1, and the data **2506** may be empty. The second record may have these values: the phone field **2502** may have the same telephone number of the user's bank. The ID value **2504** for this record may be the number 2, and the data **2506** may contain the user's PIN. In a sample use, the user may identify themselves via the biometric device and then select to call their bank as identified above. The device may then look at record number 1 having an ID=1 (from field **2504**), and transmit the bank phone number from field **2502**. Once dialed and when the bank is awaiting the entry of the PIN, the user may again identify themselves to the biometric device, which now would look for record number 2, ID=2 (from field **2504**), and recognizing that there is data in the data field **2506**, now transmit that data, which in this case represents the user's PIN. Thus, this technique may be used to enter passwords, access codes, PINs, and other information that may be difficult or hard for the user to remember.

What has been described above is a manual activation sequence, i.e. the user needed to activate the transfer of the information. An automatic transfer of information is also possible. For example, the user may have another two records with ID value 3, and data representing a password for access to a savings account, and another record with ID value 4, and respective data representing a password for a checking account. In the first record (ID=1), that the data field **2506** has data telling the bank that it may query the user's device automatically.

A sequence of events might then be: the user activates the biometric device that identifies him as an authorized user. He then selects the bank, the ID=1 record is selected, the telephone number **2502** is dialed and then the data **2506** is transmitted to the bank. Upon receiving this the bank sends a request to the device to transmit the record with ID=2. When the device sends the data **2506** in record 2, the bank will check and see that the password sent is correct. It may then request from the device the record with the ID=3. The data field **2506** containing the savings account password would then be sent.

The bank may then request more records each identified by the ID value **2504** until the device signals that there are no more records available. The bank may then transmit the information to the user on, for example, the balances in each account. Please note, that the ID value **2504** may be an index into any available data **2506** associated with that ID value **2504** and that the access does not need to be sequential. For example, after ID=1, the bank in the above example, may have requested data **2506** associated with the ID=3 (**2504**) and may have transmitted to user out of sequence information. That is, even though the checking account password

may be associated with an ID=4. The bank may recognize that this balance is more important to the user and may report the checking account balance before reporting the savings account balance.

The device, if properly activated, may be able to be programmed by the bank with additional or new information. For example, the user's bank may have a new telephone number. If the device is capable of receiving and storing this new information, then the bank upon being called on the old telephone number may automatically update the device and instruct it to store and dial the new number. In this instance user intervention is reduced and the device is automatically updated. Additionally, the back-end may update passwords, assign new passwords, etc. This may be done on a periodic basis or randomly, for example to increase security, or change passwords if the back-end determines that a security breach has occurred.

This automatic update or automatic transmission of data may be established for example, by a simple communication and/or command and control protocol to permit a back-end device (such as the bank in the above example) to coordinate with the front-end device (such as the device in the above example). For example, as part of the initial dialing procedure, the user may be required to be authenticated by the biometric device (commonly referred to as a "login"). All subsequent activity may be allowed until the call is ended, without requiring additional interaction between the user and the biometric device. Note that during the establishment of the connection, the back-end system communicates with the device, requesting individual pieces of data, using the ID value as described above. In this case then, the ID values do not necessarily represent sequential values, just unique identification for each piece of data.

The actual transmission of data may be by, for example, telephone-type signals, for example touch-tones. An advantage of touch-tones is that the back-end receives them in the same manner as if the user had entered them from the telephone keypad.

Because of the sensitive nature of the information being transferred, such as access codes, PINs, etc., it may be desired to use a secure communication means and/or encryption to lessen the possibility of unauthorized use of the information. Utilizing a public key (PKI) infrastructure, the device, may establish a secure connection to a back-end system. For PKI, additional information, such as, for example, a digital certificate issued by a certificate authority may be stored in the device. FIG. **26** illustrates how this might be stored as a value certificate at **2602**. For a single certificate **2602** there may be multiple records **2603** storing information as described above (for FIG. **25**), such as phone number **2604**, ID value **2606**, and data **2608**. Thus, for example, during a data exchange sequence, the device may encrypt the data field **2608** before sending it to the back-end. This has the advantage of preventing someone from snooping the phone line and directly capturing the data in clear text format.

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

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

One of the characteristics of the PKI technology is that a data structure encrypted with an entity's public key can only be decrypted with that entity's private key (the public key cannot be used to undo the encryption). This also holds in the reverse, with data that is encrypted with a private key only being capable of being decrypted with the public key.

When the back-end system receives the encrypted password, it can use its own private key to decrypt the password, thus helping ensure its validity. This process, along with other standard mechanisms of a PKI system such as message digest and digital certificates may be used to secure the exchange of passwords between the back-end and the device.

FIG. **27** is a flow diagram illustrating one embodiment of securely sharing information. In this example embodiment, the back-end system may be in possession of several PKI key pairs, one for each password to be assigned. The back-end distributes one public key with each password and the biometric device stores and associates these back-end public keys with the associated password and data as illustrated in FIG. **26** at **2609**.

At **2702** a protocol session is opened with a security mechanism and the telephone back-end system creating a secure connection and exchanging digital certificates to authenticate each other (back-end authenticating the biometric device and vice versa). The keys used for this purpose will be referred to as "session keys" for this explanation. The device and back-end system each have one pair of session keys a public key and a private key. The public keys have been exchanged along with digital certificates that authenticate them.

At **2704**, the beginning of the password configuration process, the back-end system informs the device that there will be "N" number of passwords required to access this system. Next for each password to be used, of which there are N, the following steps are repeated **2712**. At **2706** the back-end select an unused PKI key pair (one public, one private) from its internal database of keys. Alternatively, the back-end may contact its Certificate Authority and request a new key pair and certificate each time it needs one. At **2708** the back-end system combines the selected public key with the password data structure, adds a password ID, and encrypts this entire combination with its private session key. It then, at **2710**, transmits this to the device. Note that the back-end system has also creates an internal data structure that associates the key pair with the password.

As mentioned above, this sequence of steps **2706**, **2708**, and **2710** may be repeated N times **2712**. At **2720**, the device decrypts and authenticates the incoming data using the public session key of the back-end system and other elements of the PKI system that are well known to those skilled in the art. Once authenticated, the device stores the data structure **2722** as was illustrated in FIG. **26** at **2609**. This structure **2609** associates the telephone number **2610**, password ID **2612**, back-end public key **2614**, and password data **2616**.

Thus, the example embodiment above, describes a technique in which the back-end system assigns passwords and

public keys for a given access protocol, and the transfers them to the device for later use.

An alternative embodiment may allow the user of the device to choose passwords, send them to the back-end system, and receive back the back-end public key to utilize for future encryption of the password.

Yet another embodiment may be for the user of the device to chose the passwords and for the device to choose the PKI key pairs associated with those passwords. The device would then inform the back-end system about this key/password relationship, passing a "security mechanism public key" and password to the back-end. The back-end would then store this information. When the back-end issues a challenge for a password with a given ID, the device encrypts the password with its corresponding private key and transmits it to the back-end. The back-end utilizes the corresponding "security mechanism public key" to decrypt and authenticate the password.

FIG. **28** illustrates one embodiment of a device, as a consumer access device, **2802** that implements the method discussed above. 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**. FIG. **29** illustrates a response if in FIG. **28** the user was successfully identified and selected the "Access Dialing Code." In FIG. **29**, the consumer access device **2902** on the LCD screen **2904** now shows a series of dialing codes. The touchpad **2908** may be used to select an option, and the FIU **2906** may be used to activate the selection once the user, for example, presses his finger on the FIU **2906** and is recognized as an authorized user. Alternatively, the consumer access device, once the user has been identified may not require re-identification until the consumer access device is, for example, turned off.

FIG. **30** illustrates one embodiment of a consumer access device **3002**, which may have, on the back side of the device a microphone **3006**, and a speaker **3004**. In operation, this embodiment, may for example, once activated to dial a long distance carrier, emit from the speaker **3004** tones which when held up to a telephone receiver would allow accessing the long distance carrier. The microphone, may be used for voice identification or may be used to record a message, etc.

FIG. **31** illustrates one embodiment of a method to securely and conveniently store and transmit telephony-based data. At **3102** the user may start a device, such as a digital wallet (DW). At **3104** the DW checks to see if a fingerprint has been detected. If not then the DW loops back looking for a fingerprint. If a fingerprint has been detected, then at **3106** a check is made to see if it matches a stored authorized fingerprint. 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.

FIG. **32** illustrates one sequence of events. FIG. **32** illustrates communication and actions between two systems, the Access Site **3250** and the Digital Wallet (DW) **3220**. Initially, the DW at **3222** may dial, for example via tones, an access number and wait a number of seconds. These tones are received at **3252** on the Access Site **3250** side. Sometime later a dialtone **3254** is sent to the DW **3220** where it is received at **3224**. After receiving the dialtone the DW **3220** at **3226** will send the access code to the Access Site **3250** where it will be received at **3256** which will check the access code to see if it is valid, and if it is, will grant access and allow dialing of a call.

FIG. **33** illustrates another sequence of events using PKI. Again, FIG. **33** illustrates communication and actions between two systems, the Access Site **3350** and the Digital Wallet (DW) **3320**. Initially, the DW at **3322** may dial an access number and wait a number of seconds. These tones are received at **3352** on the Access Site **3350** side. Sometime later a random number **3354** is sent to the DW **3320** where it is received at **3324**. After receiving the random number the DW **3320** at step **3326** will send the DW identification (ID) plus an encrypted message using the DW private key that may contain such things as a time stamp, the DW ID, and a the random number, to the Access Site **3350** where it will be received at step **3356** which will lookup the DW ID to make sure this particular DW has access, then if so it will decrypt the message with the DW public key and check the random number to make sure it is the same as what was just sent, it will check the time stamp to make sure that it is a unique value not seen before (helps prevent against hijacking and later re-use), and will check the DW ID. If all of these check out then access may be granted (assuming such overriding things, such as bills for access being paid) and allow dialing of a call.

Thus, a secure and convenient method and apparatus for storing and transmitting telephony-based data have been described. Although the present invention has been described with reference to specific exemplary embodiments, it will be evident that various modifications and changes may be made to these embodiments without departing from the broader spirit and scope of the invention as set forth in the claims. Accordingly, the specification and drawings are to be regarded in an illustrative sense rather than a restrictive sense.

What is claimed is:

1. A computer-implemented method comprising:

authorizing, by a device, an authorized user access to the device based on biometric identification information associated with the authorized user, wherein the device is operable by only one authorized user at a time;

receiving, by the device, a message from a first remote source, the first remote source generating the message from the authorized user's private access information stored on the first remote source; and

automatically sending, by the device over a voice network, the message to a second remote source to enable the authorized user to access remote data stored on the second remote source, wherein the remote data is private information for the authorized user.

2. The computer-implemented method of claim **1** further comprising establishing a connection between the voice network and the device, wherein the device is a consumer access device.

3. The computer-implemented method of claim **2** wherein the consumer access device is selected from the group consisting of digital wallet devices, personal computers, personal digital assistants, electronic based organizers, watches, telephones, autodialers, wireless telephones, settop boxes, video game consoles, remote control units, personal radio communication units, telematic communication devices, information panels, and kiosks.

4. The computer-implemented method of claim **2** further comprising enabling the authorized user to conduct a transaction using the consumer access device.

5. The computer-implemented method of claim 1, further comprising:

accessing the remote data through a privacy clearing house server; and

transferring the remote data.

6. The computer-implemented method of claim 5, wherein the remote data further comprises:

a password associated with the authorized user.

7. The computer-implemented method of claim 5 wherein accessing further comprises establishing a secure communication channel using Public Key Infrastructure.

8. An apparatus comprising:

a biometric device to identify an authorized user based on biometric identification information associated with the user; and

a consumer access device connected to the biometric device to enable the authorized user to receive a message from a firt remote source, the first remote source generatig the message from the authorized user's private access information stored on the first remote source, and to automatically send, over a voice network, the message to a second remote source to enable the authorized user to access remote data stored on the second remote source, wherein the remote data is private information for the authorized user, and the consumer device is operable by only one authorized user at a time.

9. An apparatus comprising:

means for authorizing a user based on biometric identification information associated with the user, wherein the apparatus is operable by only one authorized user at a time;

means for receiving a message from a first remote source, the message generated by the first remote source from the authorized user's private access information stored on the first remote source; and

means for automatically sending, over a voice network, the message to a second remote source to enable the authorized user to access remote data stored on the second remote source, wherein the remote data is private information for the authorized user.

10. The apparatus of claim 9, further comprising means for presenting the information to the authorized user on a consumer access device selected from the group consisting of digital wallet devices, personal computers, personal digital assistants, electronic based organizers, watches, telephones, wireless telephones, setup boxes, video game consoles, remote control units, personal radio communication units, telematic communication devices, information panels, and kiosks.

11. A machine-readable program storage medium tangibly embodying a sequence of instructions executable by a machine to perform a method for communicating, the method comprising:

authorizing, by a device, an authorized user access to the device based on biometric identification information associated with the authorized user, wherein the device is operable by only one authorized user at a time;

receiving, by the device, a message from a first remote source, the message generated by first remote source from the authorized user's private access information stored on the first remote source; and

sending, by the device over a voice network, the message to a second remote source to enable the authorized user to access remote data stored on the second remote source, wherein the remote data is private information for the authorized user.

12. A system comprising:

a memory for storing computer program instructions and data; and

a processor coupled to the memory for processing the computer program instructions and data to:

authorize an authorized user based on biometric identification information associated with the authorized user, wherein the system is operable by only one authorized user at a time;

receive a message from a first remote source, the message generated by the first remote source from the authorized user's private access information stored on the first remote source; and

automatically send, over a voice network, the message to a second remote source to enable the authorized user to access remote data stored on the second remote source, wherein the remote data is private information for the authorized user.

13. An apparatus for communication, the apparatus comprising:

means for authorizing an authorized user based on biometric identification information associated with the authorized user, wherein the apparatus is operable by only one authorized user at a time;

means for receiving a message from a first remote source, the message generated by the first remote source from the authorized user's private access information stored on the first source and associated with a second remote source; and

means for automatically sending, over a voice network, the message to the second remote source to enable the authorized user to access remote data stored on the second remote source, wherein the remote data is private information for the authorized user.

14. The apparatus of claim 13, further comprising the device selected from the group consisting of digital wallet devices, personal computers, personal digital assistants, electronic based organizers, watches, telephones, wireless telephones, setup boxes, video game consoles, remote control units, personal radio communication units, telematic communication devices, information panels, and kiosks.

15. A system comprising:

a consumer access device operable by only one authorizal user at a time;

a biometric device to authorize a user access to the consumer access device; and

a storage unit to store a message received from a first remote source, the message generated by the first remote source from the authorized user's private access information stored on the first remote source, wherein the consumer access device automatically sends, over a voice network, the message to a second remote source to enable the authorized user to access remote data stored on the second remote source, and wherein the remote data is private information for the authorized user.

16. The system of claim 15 further comprising:

a communications unit coupled to the consumer access device to communicate prespecified information upon biometric identification of the authorized user.

17. The system of claim 16, wherein the output of the communications unit is encrypted.

18. The system of claim 15 wherein the consumer access device allows automatic receipt and updating of the private access information stored in the storage unit.

19. The system of claim 15 further comprising establishing a secure communication link with the consumer access device before allowing transfer of information.

20. The system of claim 15 further comprising a wireless communications unit.

21. An apparatus comprising:

means for biometric identification to authorize a user, wherein the apparatus is operable by only one authorized user at a time;

means for displaying information to an authorized user;

means for receiving a message from a first remote source, the message generated by the first remote source from the authorized user's private access information stored on the first remote source;

means for accepting authorized user input; and

means for automatically sending, over a voice network, the message to a second remote source to enable the authorized user to access remote data stored on the second remote source, wherein the remote data is private information for the authorized user.

22. The apparatus of claim 21 further comprising:

means for sending via tones.

23. The apparatus of claim 22 wherein the tones are communicated over a telephony-based system.

* * * * *

US 20030196084A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2003/0196084 A1

Okereke et al. (43) Pub. Date: Oct. 16, 2003

(54) SYSTEM AND METHOD FOR SECURE WIRELESS COMMUNICATIONS USING PKI

(76) Inventors: **Emeka Okereke**, Upland, CA (US); **Robert Thacher**, Newport News, VA (US); **Justin Good**, Upland, CA (US)

Correspondence Address:
Thomas F. Bergert
Williams Mullen, PC
Suite 700
8270 Greensboro Drive
McLean, VA 22102 (US)

(21) Appl. No.: **10/412,563**

(22) Filed: **Apr. 11, 2003**

Related U.S. Application Data

(60) Provisional application No. 60/371,736, filed on Apr. 12, 2002.

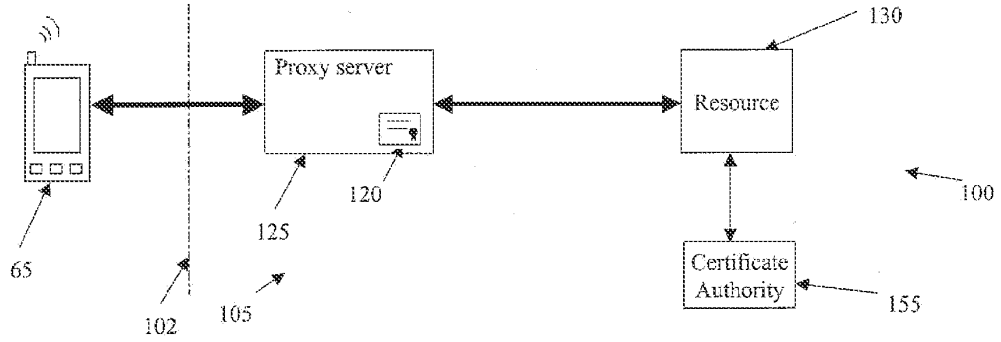
Publication Classification

(51) **Int. Cl.**[7] **H04L 9/00**

(52) **U.S. Cl.** **713/156**; 380/270

(57) **ABSTRACT**

A system and method for allowing users of wireless and mobile devices to participate in Public Key Infrastructure facilitates secure remote communications. The present invention allows wireless devices to participate in secure communications with secure networks without storing compromisable information on the wireless device. In one embodiment, the system allows wireless devices to participate in Public Key Infrastructure wherein no portion of the certificate, no information about the certificate, and no private or public key data are stored on the wireless device. In one embodiment, a certificate proxy server maintains the digital certificate and private for the client device in a secure fashion, and maintains connectivity with the wireless network. The mobile user can authenticate with the server in order to access resources that require the certificate to be presented.



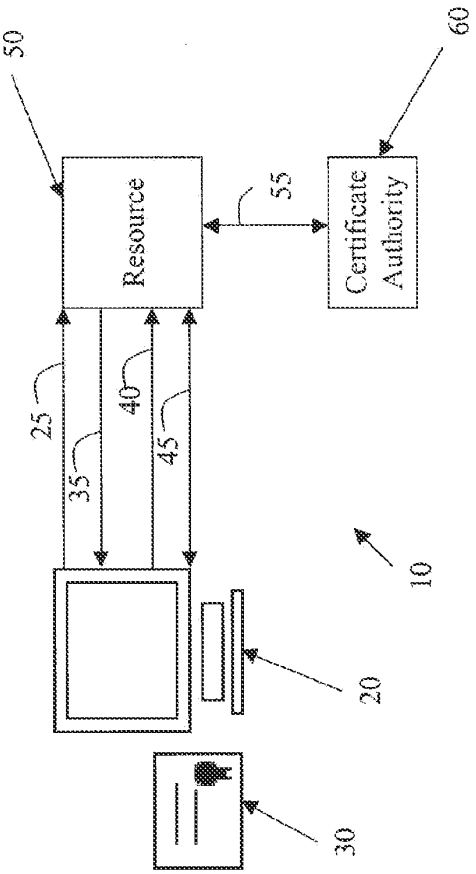

50
Resource
55
Certificate Authority
60
25
35
40
45
10
20
30

Fig. 1

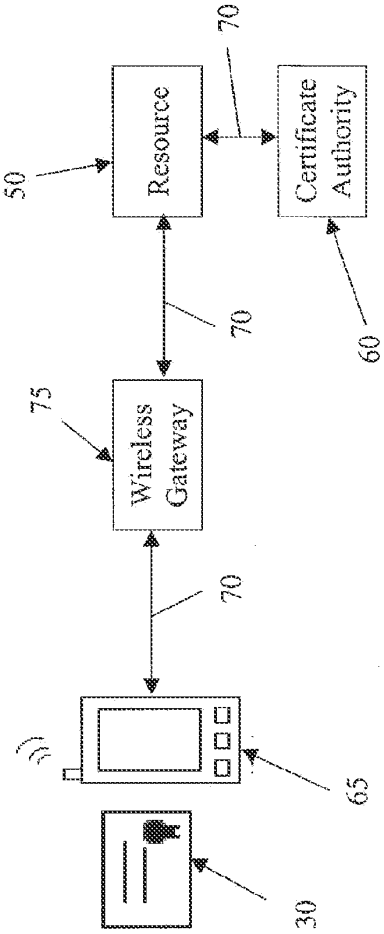

70
50
Resource
Certificate Authority
70
60
75
Wireless Gateway
70
65
30

Fig. 2

Fig. 3

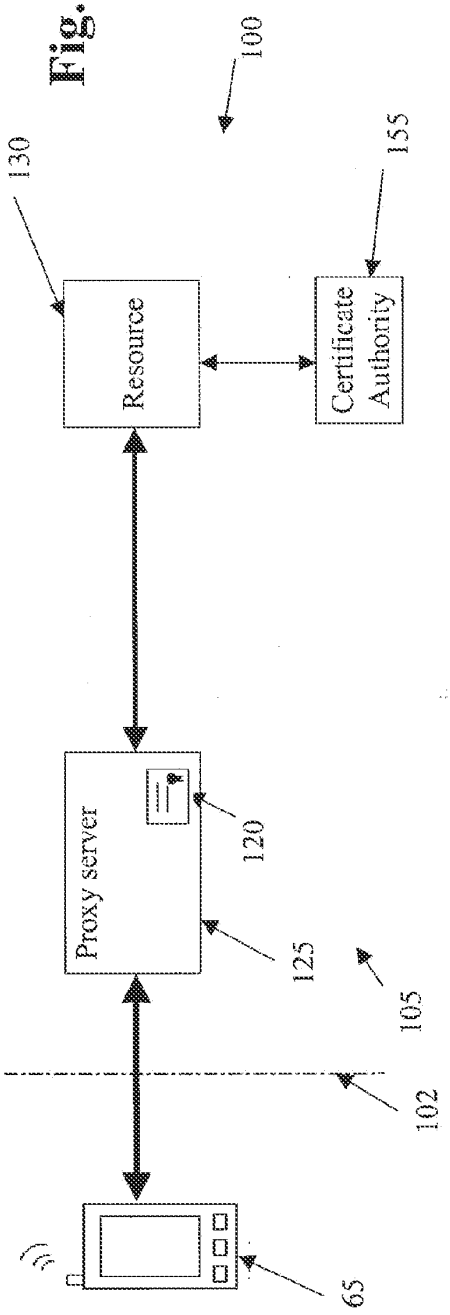

100
130
Resource
155
Certificate Authority
Proxy server
120
125
105
102
65

Fig. 4

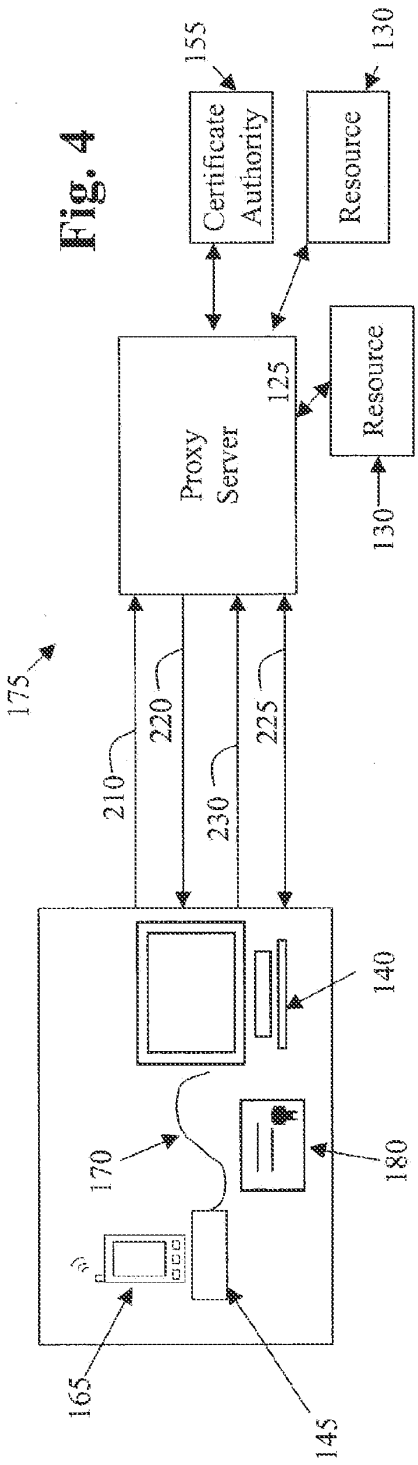

155
Certificate Authority
130
Resource
Proxy Server
125
Resource
130
175
210
220
225
230
140
170
180
165
145

Fig. 5

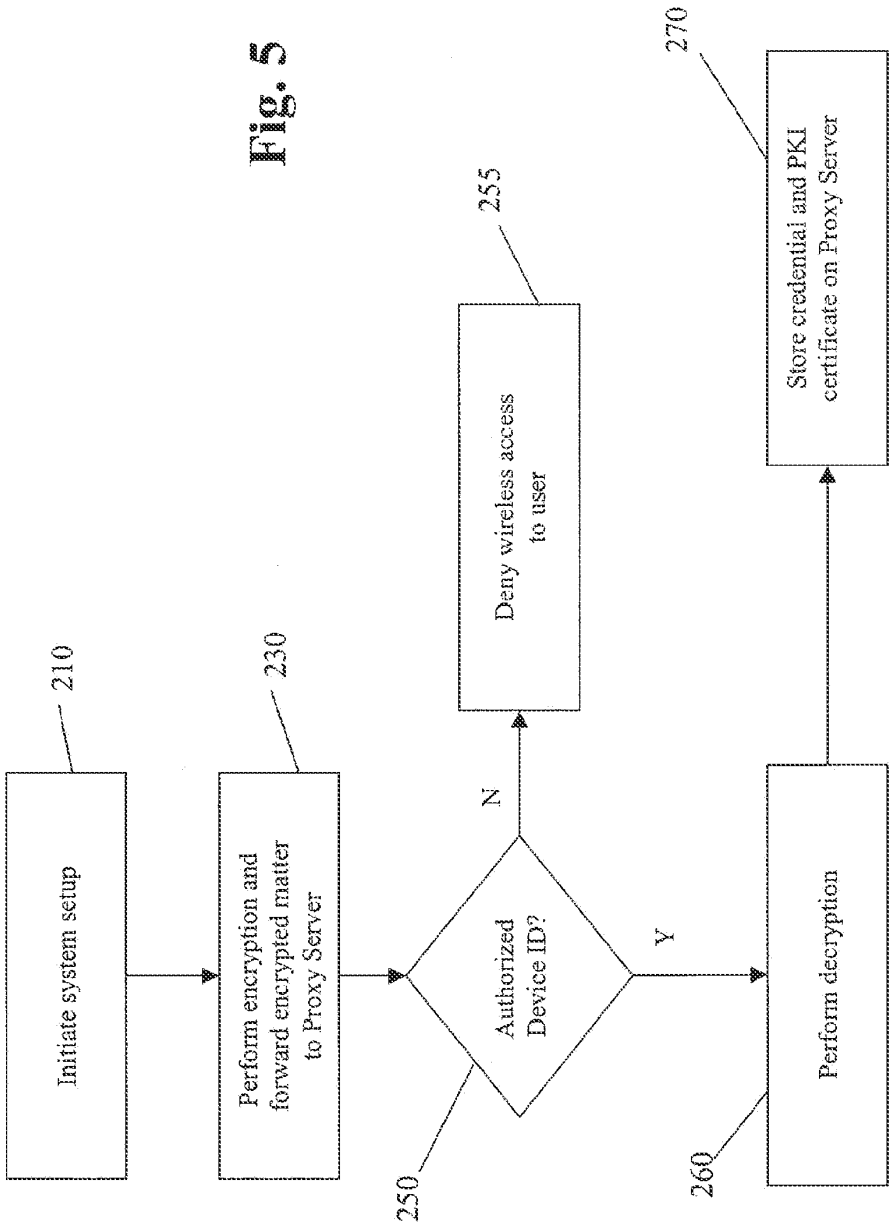
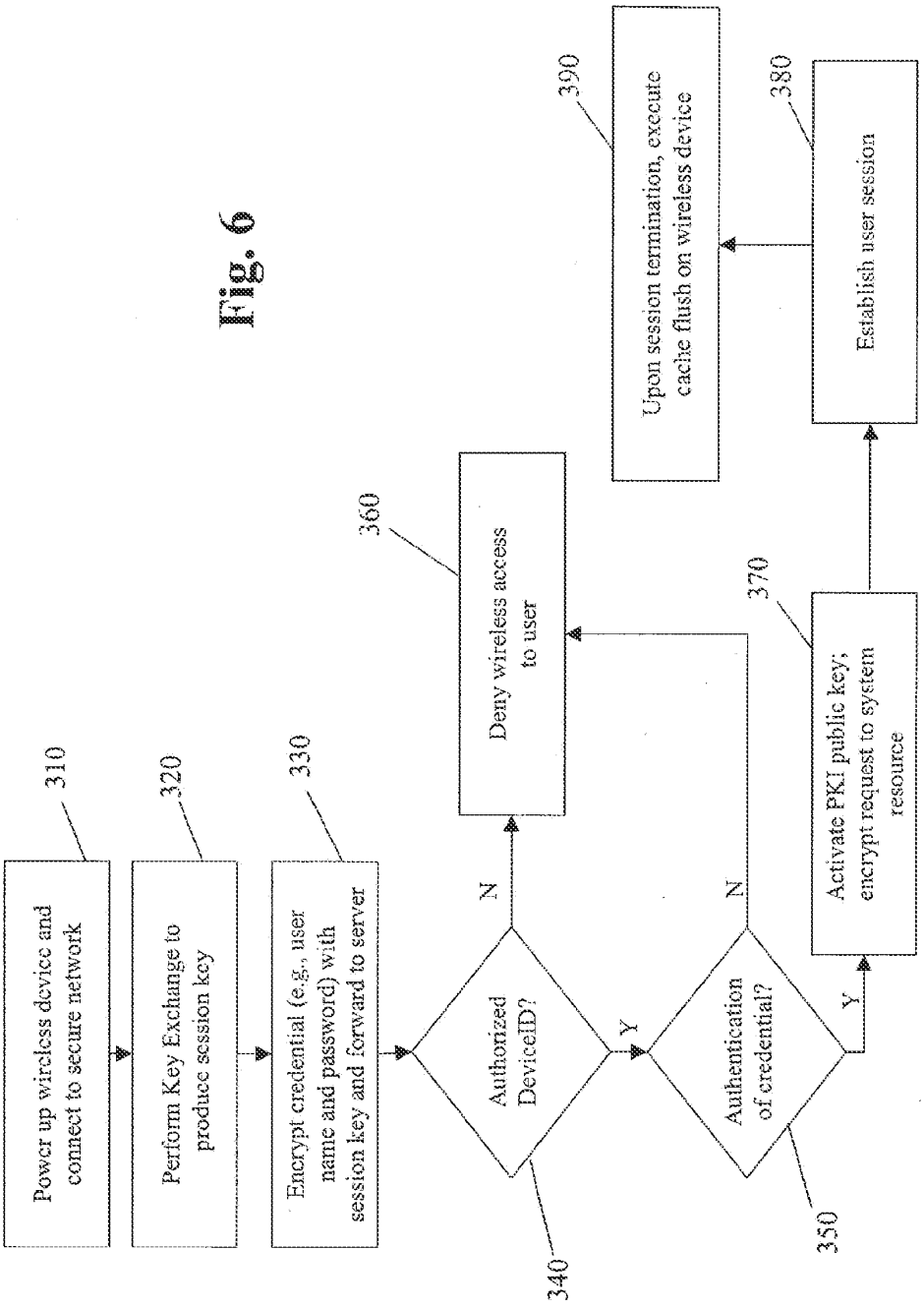

Initiate system setup
210
Perform encryption and forward encrypted matter to Proxy Server
230
Authorized Device ID?
250
N
Deny wireless access to user
255
Y
Perform decryption
260
Store credential and PKI certificate on Proxy Server
270

Fig. 6


Power up wireless device and connect to secure network
310
Perform Key Exchange to produce session key
320
Encrypt credential (e.g., user name and password) with session key and forward to server
330
Authorized DeviceID?
340
N
Y
Deny wireless access to user
360
Authentication of credential?
350
N
Y
Activate PKI public key; encrypt request to system resource
370
Establish user session
380
Upon session termination, execute cache flush on wireless device
390

SYSTEM AND METHOD FOR SECURE WIRELESS COMMUNICATIONS USING PKI

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority under 35 USC 119(e) of U.S. Provisional patent application Serial No. 60/371,736 filed on Apr. 12, 2002, entitled "System and Method for Secure Wireless Communications using PKI" which is hereby incorporated by reference in its entirety.

TECHNICAL FIELD

[0002] The present invention relates to the field of mobile communications, and more particularly to the security of mobile communications using Public Key Infrastructure (PKI).

BACKGROUND ART

[0003] Both private and public entities rely on information technology systems to perform essential or mission-critical functions. Some computer information, such as defense, financial, medical, and personnel data, is sensitive and merits special or additional protection against unauthorized use or disclosure. As information technology becomes increasingly distributed and interconnected, the consequences of losing control of information become greater. For example, systems that perform electronic financial transactions or electronic commerce must protect against unauthorized access to confidential records and unauthorized modification of data. Sometimes, the value of the information lies in its limited distribution; wide spread knowledge and misuse could reduce the value of that information. In other cases, release of the information could lead to extrinsic harm, such as a violation of personal privacy. Easy access to sensitive information may also lead to malicious corruption of the information. Yet the distributed, collaborative, and open nature of early networks, including the Internet, encouraged the free flow of information in a manner that is not suited to information control.

[0004] Information security refers to those measures taken to protect information against unauthorized disclosure, transfer, modification, or destruction. Instead of returning to closed networks, computer security managers are seeking information security through reliably secure or trusted computer systems and communication methods. Both government and industry face a growing public concern for privacy, and the need for effective information security is compelling. At the same time, users want easy access to information from a variety of access devices, including desktop computers or workstations, as well as remote wireless devices.

[0005] Both wired and wireless information security systems seek to ensure authentication, confidentiality, nonrepudiation and integrity in communications. Wireless systems must also deal with inherent issues of limited bandwidth, high latency, and unstable connections.

[0006] Some have employed PKI (public key infrastructure) as a means to increase information security. PKI enables users of a basically insecure network such as the Internet to securely and privately exchange information through the use of a public and a private cryptographic key pair that can be obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization, and directory services that can store and, when necessary, revoke the certificates. A public key infrastructure consists of: (1) a certificate authority (CA) that issues and verifies a digital certificate, which includes the public key and/or information about the public key; (2) a registration authority (RA) that acts as the verifier for the certificate authority before a digital certificate is issued to a requester; (3) one or more directories where the certificates with their public keys are held; and (4) a certificate management system.

[0007] With PKI, a public and a private key are created simultaneously using the same algorithm by a certificate authority. Information encrypted with the private key can only be decrypted with the corresponding public key. Similarly, information encrypted with the public key can only be decrypted with the corresponding private key. The private key is given only to the requesting party and the public key is made publicly available as part of a digital certificate in a directory that all parties can access. The private key is never shared with anyone or sent across the network. In addition to encrypting messages for privacy assurance, authentication of the sending individual is possible if, for example, the individual uses their private key to encrypt a hash of the message contents. A hash results from the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string. For example, if user A is sending a message to user B, user A can use B's public key to encrypt the message, and can use A's own private key to encrypt a hash of the message contents. User B can decrypt the message with user B's own private key, and can decrypt this hash using user A's public key, thus authenticating user A as the sender of the message.

[0008] The ordinarily skilled individual in this field will recognize the pertinent features surrounding PKI technology. The working paper "Internet X.509 Public Key Infrastructure: Roadmap"(http://www.ietf.org) provides a detailed overview of PKI technology and is hereby incorporated by reference.

[0009] Several forms of public key infrastructure exist, including the WPKI for wireless devices. There also exist specialized PKI implementations for constrained storage devices such as smart cards. Current efforts aimed at allowing wireless devices to participate in Public Key Infrastructure operate so as to:

[0010] 1] store the entire certificate and private key on a wireless device in an unprotected fashion; or

[0011] 2] store the entire certificate and private key on a wireless device in a protected fashion; or

[0012] 3] store a digest or hash of the user's certificate solely for ID purposes on a smart card or similar constrained device, for example, and authenticate against a specialized security server.

[0013] None of these efforts completely address the security risk posed by theft or loss of the wireless device. For example, in the case where the entire certificate and private key is stored on a stolen wireless device in an unprotected manner, the thief can then access the formerly secure information through the compromised device. The thief can also copy the certificate and private key to another device for later use.

SUMMARY

[0014] The present invention allows wireless devices to participate in secure communications with secure networks without storing compromisable information on the wireless device. In one embodiment, the system allows wireless devices to participate in Public Key Infrastructure wherein no portion of the certificate, no information about the certificate, and no private key data are stored on the wireless device.

BRIEF DESCRIPTION OF DRAWINGS AND FIGURES

[0015] **FIG. 1** shows a traditional PKI.

[0016] **FIG. 2** shows a standard wireless PKI.

[0017] **FIG. 3** shows the wireless infrastructure in accordance with the PKI system of the present invention.

[0018] **FIG. 4** is a diagram showing information flow associated with initialization of a device in accordance with the present invention.

[0019] **FIG. 5** is a flow chart showing how a wireless device can be initialized for use in accordance with the present invention.

[0020] **FIG. 6** is a flow chart showing how an initialized device operates to access secure resources in accordance with the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0021] As shown in **FIG. 1**, there is provided a traditional PKI system **10**. The end user from the client workstation **20** sends a request **25** for a secure resource **50**, and before access is granted, the user is requested **35** to provide a digital certificate **30** for authentication. The secure resource can be data, applications or other information of value. In some cases, once the digital certificate **30** is provided **40** and verified **55** by a certificate authority **60**, access to the secure resource **50** will be granted as at **45**. In other cases, an additional form of authentication may be required, such as a user name and password, a smart card, or a fingerprint, for example. The digital certificate verification process occurs through a certificate authority **60**, normally a trusted third party.

[0022] In the wireless context, as shown in **FIG. 2**, the request for secure resource is made by wireless device **65** through a wireless gateway **75**, and similar communications **70** for authentication, verification and resource access ensue using certificate **30**.

[0023] In the system **100** of the present invention, as embodied in **FIGS. 3 through 6**, the user's digital certificate **120** is maintained on a proxy server **125** located within the system network identified at **105**. As shown in **FIG. 3**, the user can use wireless device **65** to establish connection with proxy server **125** within secure network **105**, and access secure resources **130** through the proxy server. A certificate authority **155** is also provided in communication with the network for certificate authentication purposes.

[0024] In a specific embodiment as shown in **FIG. 4**, the user is first provided with a network-connected device, such as a desktop computer **140**, along with one or more docking stations **145**. One or more wireless-capable devices **165** may be docked in the docking station for two-way communication with the desktop computer as indicated at **170**. The desktop computer includes a memory, processor, user interface, keyboard and mouse as is commonly known, and is preferably connected to a local area network (LAN) **175** for communication and use of shared resources as is commonly known. The user may be provided with a system PKI certificate **180** and private key for use with the desktop computer, in order to access and communicate to the extent authorized by the network administrator. As shown in **FIG. 4, a** certificate proxy server **125** can be placed within the system network in accordance with the present invention to provide for secure communications between and among the desktop computer **140**, the wireless device(s) **165**, the system resources **130** available on network **175** and a designated certificate authority **155**.

[0025] The establishment of mobile access to secure resources in accordance with the present invention can occur as shown in **FIGS. 4 and 5**. The proxy server can be provided with software designed in accordance with the present invention, and a thin client application can be installed and/or downloaded onto the user's desktop computer. 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 **165** can be a personal digital assistant (PDA), laptop, cellular telephone or any other device capable of remote wireless communication. The unique identifier can be a serial number or SIM. number, for example. If the unique identifier is one which the proxy server program identifies as being acceptable, the proxy server program will send approval as at **220** to the desktop **140**, which executes functionality to make a key exchange as at **225**, such as, for example, a Diffie Hellman Key Exchange. This key is used to encrypt information sent to the server using AES (Advanced Encryption Standard). AES is an encryption algorithm used by U.S. government agencies for securing sensitive but unclassified communications. In the preferred embodiment, this key is used to encrypt communication between the desktop and the server. In another embodiment, this key is used as part of a shared secret between the server and the client. This shared secret is used to generate a session key. The new session key ensures that conversations cannot be eavesdropped if the key has been compromised. The shared secret eliminates the possibility of a man-in-the-middle attack.

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

device, wherein the number changes in predetermined time intervals and is synchronized with programming on the proxy server so as to always match the corresponding number maintained on the proxy server.

[0027] Regardless of form, the credential information is forwarded to and stored on the proxy server, as at **230** in **FIG. 5**. If the device is an authorized device by virtue of appropriate identification provided and as determined at **250** in **FIG. 4**, the credential, PKI certificate and private key is decrypted as at **260** and the proxy server stores the credential, certificate and private key in a directory on the proxy server as at **270**. No PKI certificate, or public or private key information is ever passed to or stored on the wireless device. If the device is unauthorized, as determined at **250**, access is denied as at **255**.

[0028] As shown in **FIG. 6**, when the user attempts to access the system network through the wireless device as at **360**, the proxy server first authenticates the user. This can be, in one embodiment, with a two-form authentication, such as with a user name and password, smart card, or biometric identification, for example. In one embodiment, as shown in **FIG. 6**, a session key is produced as at **320** and the user's credentials are encrypted with the session key and forwarded to the server as at **330**. If the user is authenticated by the proxy server matching the device unique identifier with authorized device identifications as at **340**, and the credential information is authenticated as determined at **350**, the proxy server will activate the user's PKI public key and request the secure network resource for the user, as at **370**. If the device identification is not authorized, or the user's credential is not authenticated, access to the user will be denied as at **360**. The proxy server will then receive the request for digital certificate and private key, and provide the previously stored digital certificate and key, which can then be validated by the certificate authority, and the user's session can begin.

[0029] The user's information access capabilities during any given session can be determined by the network/resource administrator. For example, the user may have access to a Global Access Lookup directory for identification and contact information of others. When such information is presentable in browser-recognizable format, the appropriate page may be sent to the proxy server in HTML format, for example, and the proxy server can invoke programming functionality, which then pushes the same information to the wireless device.

[0030] The user can ensure secure communication between the wireless device and the Certificate Proxy Server (CPS) in various ways, including physically connecting the device to the server, or connecting securely over a known trusted network. As the user's certificate and private key are securely transferred to the CPS, the unique network identifier for the user's wireless device (such as a SIM number) is registered with the server. This network identifier registration can also be done in a number of ways, including over the wireless network, or over a physical network.

[0031] 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.

[0032] In one embodiment of the invention, desktop software is used to authenticate the user to the CPS, register the wireless device with the CPS, facilitate the initial key exchange and transfer the certificate and private key to the server. When the user wishes to access a resource from the wireless device outside of the secure network demarcation line (**102** in **FIG. 3**), they are prompted for a second means of authentication, which may be something the user has (such as a swipe card, synchronized password keychain or channel key, for example), something the user is (such as a fingerprint scan), or something the user knows (such as a password or pass phrase). In a preferred embodiment this second form of authentication is something the user knows. The CPS verifies both forms of authentication, locates the user's certificate and establishes a session.

[0033] In this way, the PKI is extended into the wireless domain without exposing the private key on the wireless device. Once a session is established, the CPS handles all interactions with entities that wish to authenticate the user. In the preferred embodiment, the CPS is capable of handling all wireless requests, including establishing and terminating a session, and general information requests.

[0034] In one embodiment of the invention, wireless access to the proxy server is not through a port in the network firewall, but rather through a separate private network connection, such as a leased line providing X.25 or IP over frame relay connectivity, for example. It will be appreciated that the network communication protocols can be varied without affecting the spirit or nature of the present invention. In one embodiment of the invention, once the user's session is complete, the proxy server can act to remove all locally cached information from the user's device for added security through conventional means, such as through a "cache flush" or "clear cache" instruction.

[0035] The invention may be embodied in other specific forms without departing from the spirit or essential characteristics thereof. The present embodiments are therefore to be considered in all respects as illustrative and not restrictive, the scope of the invention being indicated by the claims of the application rather than by the foregoing description, and all changes which come within the meaning and range of equivalency of the claims are therefore intended to be embraced therein.

What is claimed and desired to be secured by Letters Patent is:

1. A method for providing secure mobile communications, comprising the steps of:

(a) providing a secure network having a proxy server;

(b) initializing a wireless device within said secure network, said wireless device being associated with a user, said user having an associated digital certificate;

(c) storing said user digital certificate on said proxy server; and

(d) providing remote access to said secure network via said wireless device over an insecure network by transmitting at least two forms of authentication from said wireless device to said proxy server, said at least

two authentication forms not to include a digital certificate, a portion of a digital certificate or a hash of a digital certificate.

2. The method of claim 1 wherein the user is further provided with a private key and wherein step (c) includes the step of storing said user's private key on said proxy server.

3. The method of claim 1 including the further step of (e) clearing said device of locally cached information.

4. A method for providing secure mobile communications from a user's wireless device, comprising the steps of:

(a) storing user-associated information, including at least one digital certificate, on a proxy server;

(b) receiving a request from said device to access secure information accessible via said proxy server;

(c) authenticating the user of the wireless device to the server using at least two authentication measures; and

(d) servicing said request from the wireless device via the proxy server.

5. The method of claim 4 including the step of (e) removing all locally cached information from the wireless device.

6. The method of claim 4 wherein step (d) includes the step of presenting the user's certificate to at least one additional server.

7. The method of claim 4 wherein said at least two authentication measures in step (c) include a user-possessed authentication measure.

8. The method of claim 4 wherein said at least two authentication measures in step (c) include a session key issued from said proxy server which is stored in a memory of said wireless device.

9. The method of claim 4 wherein said at least two authentication measures in step (c) include a biometric identification form.

10. The method of claim 4 wherein said at least two authentication measures in step (c) include a user-known authentication measure.

11. The method of claim 4 wherein steps (a) and (b) are performed via secure network connection to said proxy server.

12. The method of claim 4 wherein step (d) is performed via secure communication over an at least partially non-secure network.

13. The method of claim 4 including the further step of (e) receiving a session termination signal from said wireless device.

14. The method of claim 4 wherein step (a) includes the step of storing a user-associated private key on said proxy server.

15. A wireless communication system, comprising:

(a) a first data network for receiving and transmitting communications signals, comprising:

a proxy server for storing digital certificates and user metadata, said server being programmed to issue at least one session key so as to allow user access to said server via a wireless communications device, said proxy server being further programmed to receive communications from said device, determine the authority of said device to access information accessible to said proxy server and determine the authenticity of user information received from said wireless device;

at least one second server programmed to retrieve information and programming upon receipt of access and request information from said proxy server; and

a program for enabling said retrieved information and programming to be transmitted for suitable display on said wireless device;

and

(b) a second data network adapted to transmit to and receive signals from at least one wireless communications device, said device having a memory for storing at least one authentication measure.

16. The system of claim 15 wherein said access information received from said proxy server includes a digital certificate stored on said proxy server.

17. The system of claim 15 wherein said at least one authentication measure does not include a digital certificate, a portion of a digital certificate or a hash of a digital certificate.

18. The system of claim 17 wherein said at least one authentication measure further does not include a public or private key.

19. A wireless communication system, comprising:

a proxy server for storing user-associated information, including at least one digital certificate and at least one private key, said proxy server further being capable of issuing at least one authentication measure and accessing and transmitting secure information;

a wireless communication device having a memory and programming for transmitting and receiving communication signals, including authentication information; and

an initialization device for transmitting to said proxy server at least one digital certificate and a private key associated with a user, as well as information attributed to said wireless communication device, said initialization device further being capable of receiving an authentication measure issued by said proxy server and transmitting said authentication measure to a memory of said wireless device, said authentication measure not to include a digital certificate, a portion of a digital certificate or a hash of a digital certificate.

20. A wireless communications system, comprising:

a proxy server programmed to store device identification, digital certificate and credential information, and to provide access to information and programming requested by at least one other device;

a first programmable device being programmed for receiving a unique device identifier associated with a second programmable device and at least one user identifier and transferring said identifiers to said proxy server for authentication against said stored information on said proxy server, said first device further being programmed to exchange at least one authentication measure between said second programmable device and said proxy server and to transmit a digital certificate and at least one access credential associated with said at least one user to said proxy server,

said second programmable device being programmed so as to communicate remotely with said proxy server only upon providing said device identifier and said credential.

21. A computer readable memory, comprising:

programming for:

accessing and transmitting secure information within a network;

storing device and user-associated information; receiving and processing requests for initializing a wireless device for use in accessing secure information;

determining the authority of a device to request secure information;

determining the authenticity of information delivered via a wireless device in connection with a user having stored user-associated information;

receiving and processing requests received via a wireless device for secure information;

transmitting user-associated information in exchange for secure information based on said received requests for secure information; and

transmitting secure information to a wireless device.

* * * * *

US 20030177102A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2003/0177102 A1

Robinson (43) Pub. Date: Sep. 18, 2003

(54) SYSTEM AND METHOD FOR BIOMETRIC AUTHORIZATION FOR AGE VERIFICATION

(76) Inventor: Timothy Robinson, Herndon, VA (US)

Correspondence Address:
ROBERTS ABOKHAIR & MARDULA
SUITE 1000
11800 SUNRISE VALLEY DRIVE
RESTON, VA 20191 (US)

(21) Appl. No.: 10/369,235

(22) Filed: Feb. 19, 2003

Related U.S. Application Data

(63) Continuation-in-part of application No. 10/251,308, filed on Sep. 20, 2002.

(60) Provisional application No. 60/324,229, filed on Sep. 21, 2001.

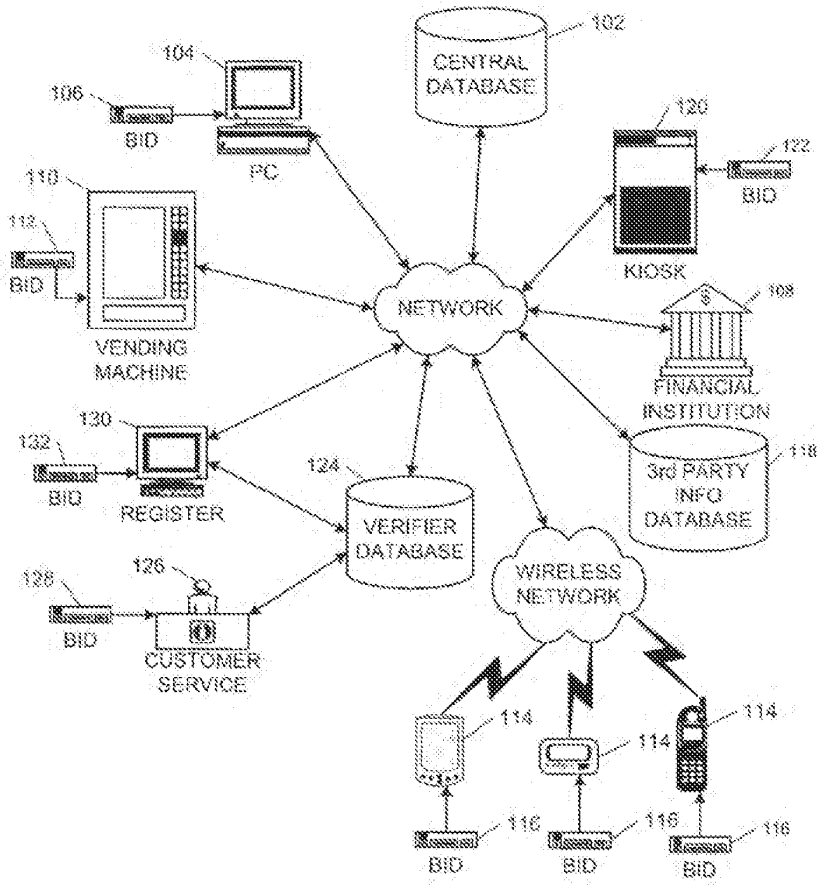
Publication Classification

(51) Int. Cl.[7] G06F 17/60

(52) U.S. Cl. 705/75

(57) ABSTRACT

The present invention is a system and method of biometric-based age verification for authorizing presenter access of age-restricted good or services between an age presenter and an age verifier. System presenters register at least one biometric identifier, at least one identification number, personal age-verifying data, and personal identity-verifying data. A presenter presents a biometric sample obtained from the presenter's person and the presenter's system ID number to conduct age verifications for purchase of or access to age-restricted goods or services. This data is used to authenticate the presenter's age and authorize access to purchase or obtain age-restricted goods or services by matching the presented transaction biometric with at least one registered biometric template and without the use of a man-made identity token.



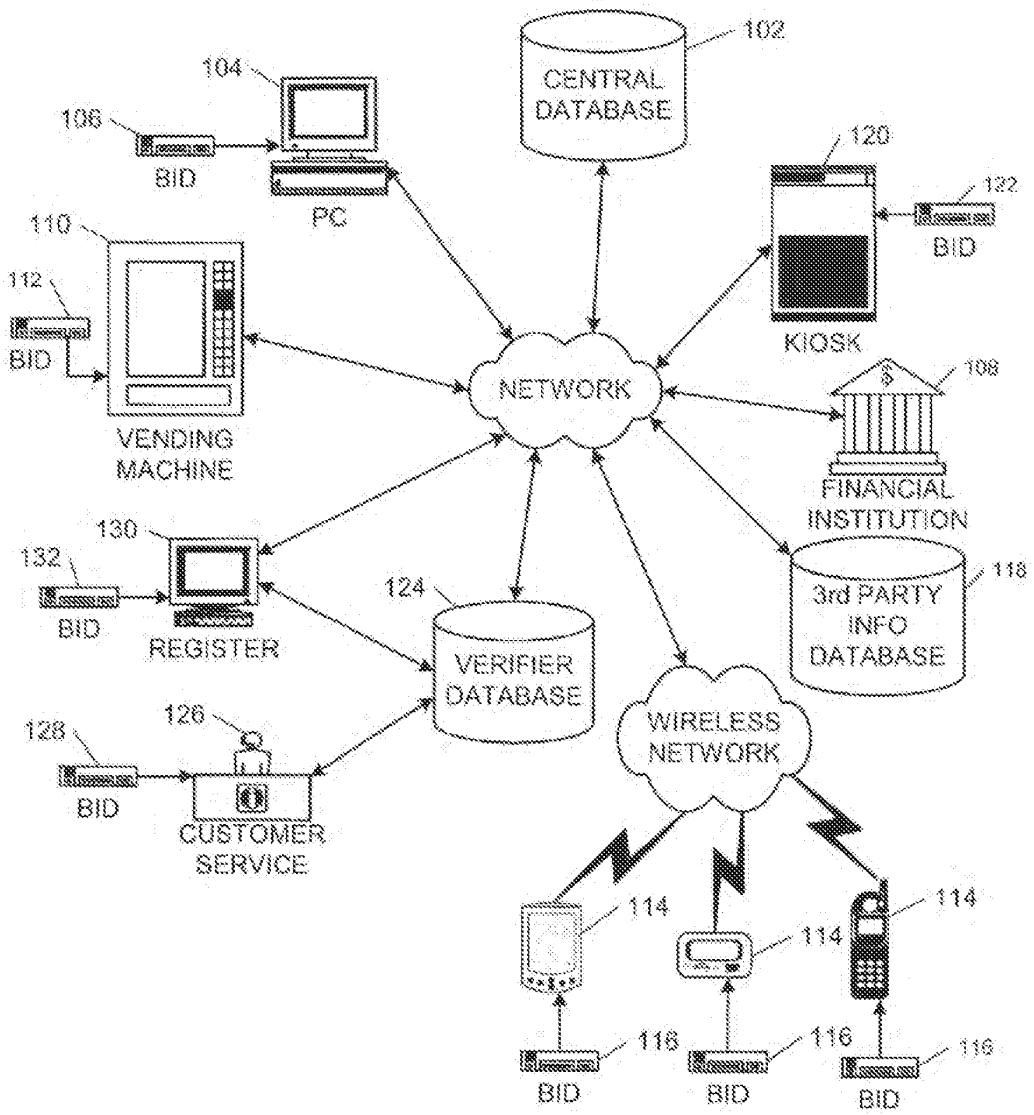

CENTRAL DATABASE
102
104
106
BID
PC
120
122
BID
KIOSK
110
112
BID
VENDING MACHINE
NETWORK
108
FINANCIAL INSTITUTION
130
132
BID
REGISTER
124
VERIFIER DATABASE
3rd PARTY INFO DATABASE
118
WIRELESS NETWORK
126
128
BID
CUSTOMER SERVICE
114
114
114
116
116
116
BID
BID
BID

FIG. 1

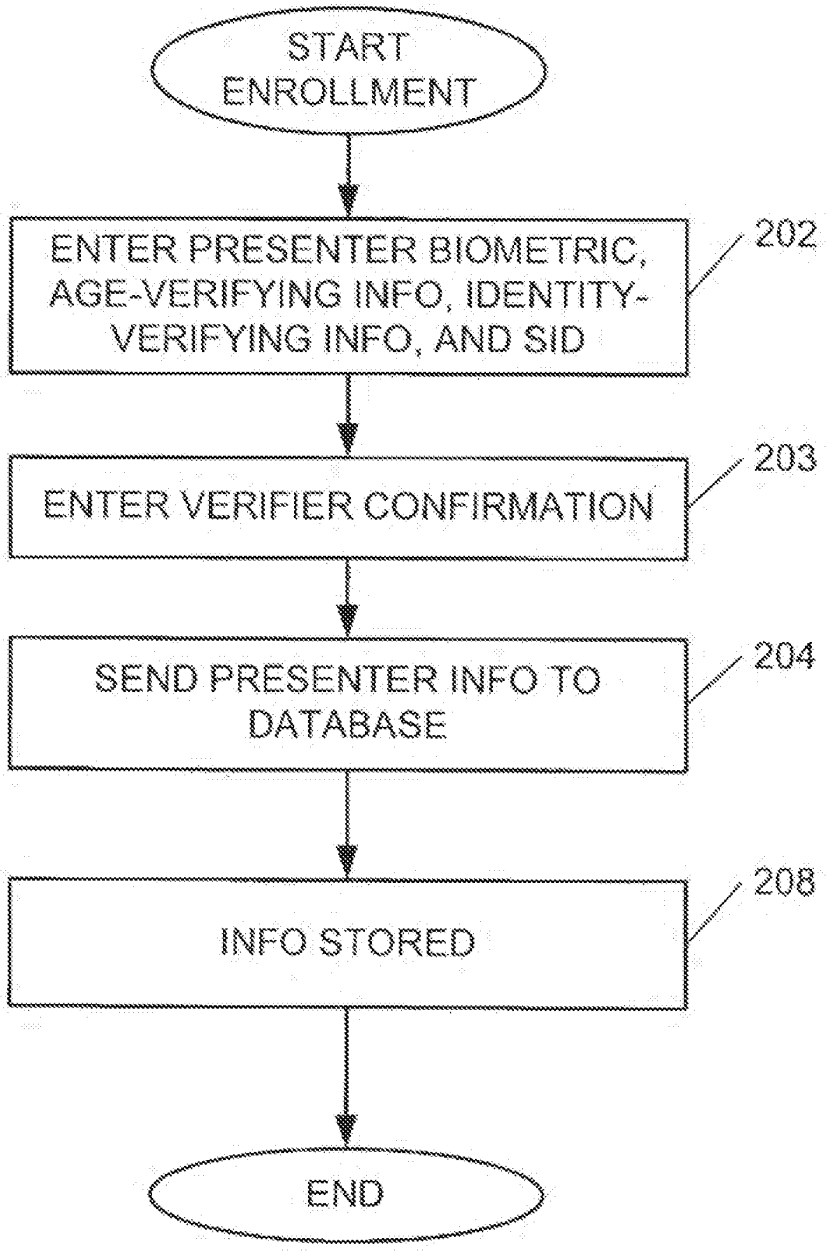

START ENROLLMENT
ENTER PRESENTER BIOMETRIC, AGE-VERIFYING INFO, IDENTITY-VERIFYING INFO, AND SID
202
ENTER VERIFIER CONFIRMATION
203
SEND PRESENTER INFO TO DATABASE
204
INFO STORED
208
END

FIG. 2

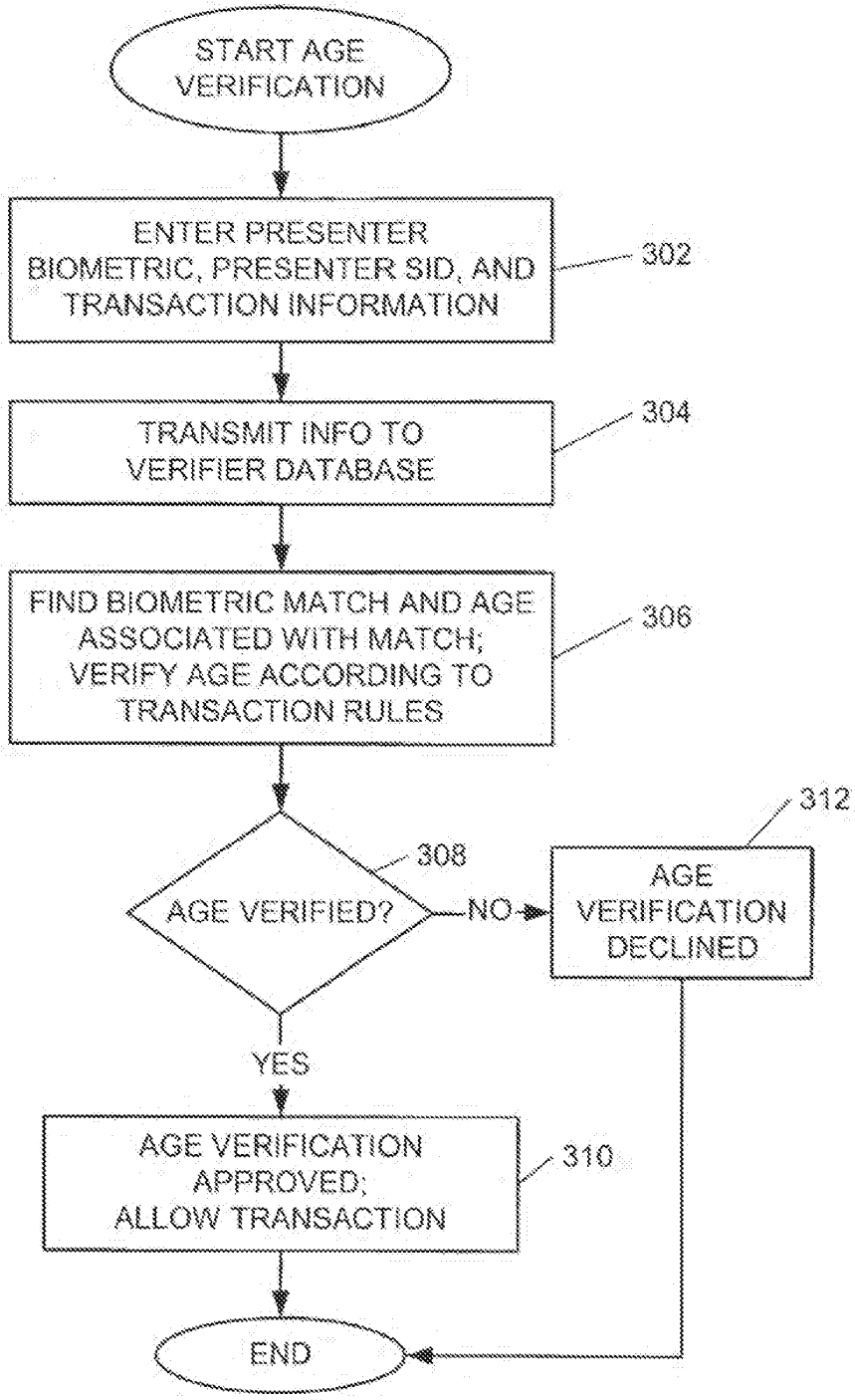

START AGE VERIFICATION
ENTER PRESENTER BIOMETRIC, PRESENTER SID, AND TRANSACTION INFORMATION
302
TRANSMIT INFO TO VERIFIER DATABASE
304
FIND BIOMETRIC MATCH AND AGE ASSOCIATED WITH MATCH; VERIFY AGE ACCORDING TO TRANSACTION RULES
306
AGE VERIFIED?
308
NO
AGE VERIFICATION DECLINED
312
YES
AGE VERIFICATION APPROVED; ALLOW TRANSACTION
310
END

FIG. 3

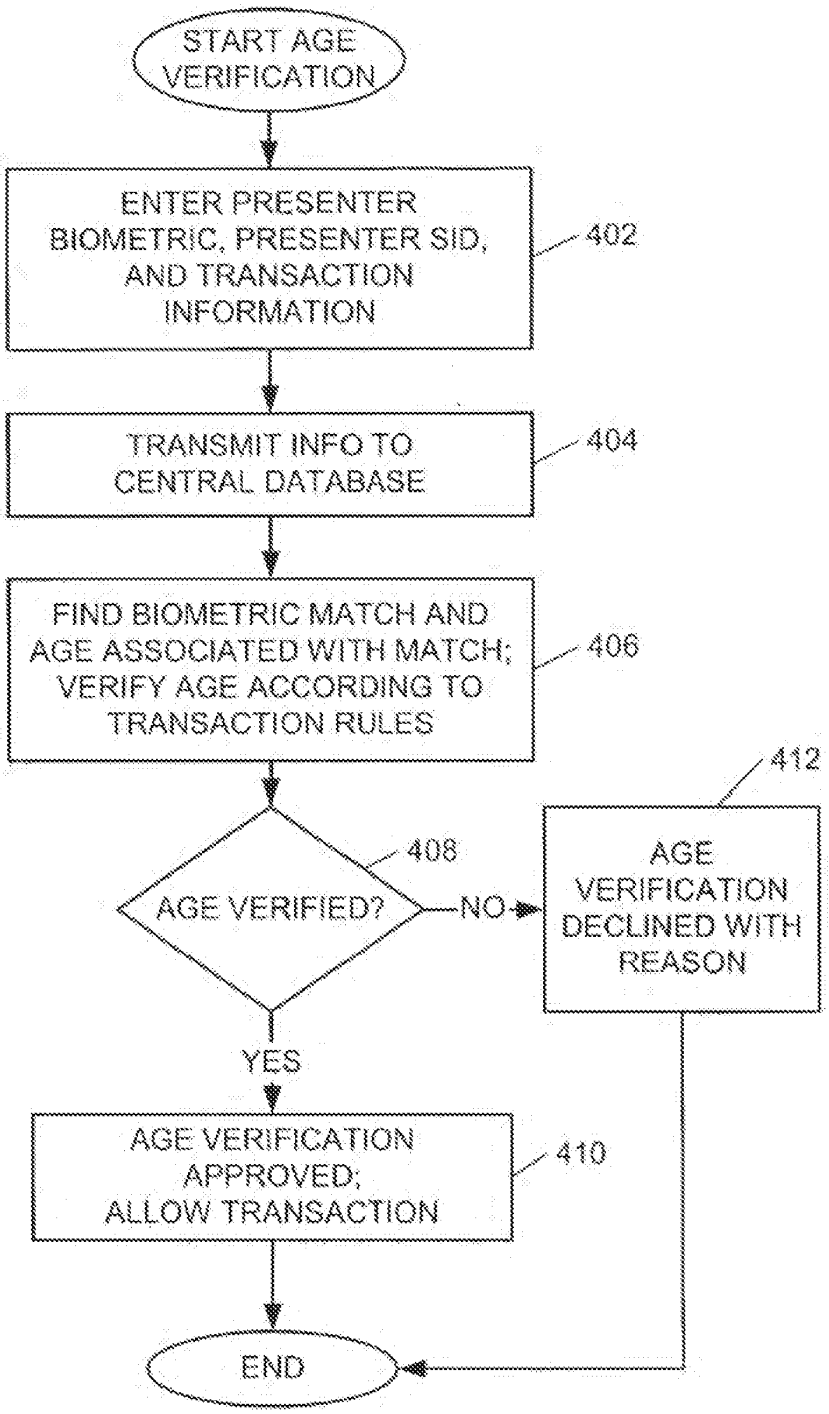

START AGE VERIFICATION
ENTER PRESENTER BIOMETRIC, PRESENTER SID, AND TRANSACTION INFORMATION
402
TRANSMIT INFO TO CENTRAL DATABASE
404
FIND BIOMETRIC MATCH AND AGE ASSOCIATED WITH MATCH; VERIFY AGE ACCORDING TO TRANSACTION RULES
406
412
AGE VERIFIED?
408
NO
AGE VERIFICATION DECLINED WITH REASON
YES
AGE VERIFICATION APPROVED; ALLOW TRANSACTION
410
END

FIG. 4

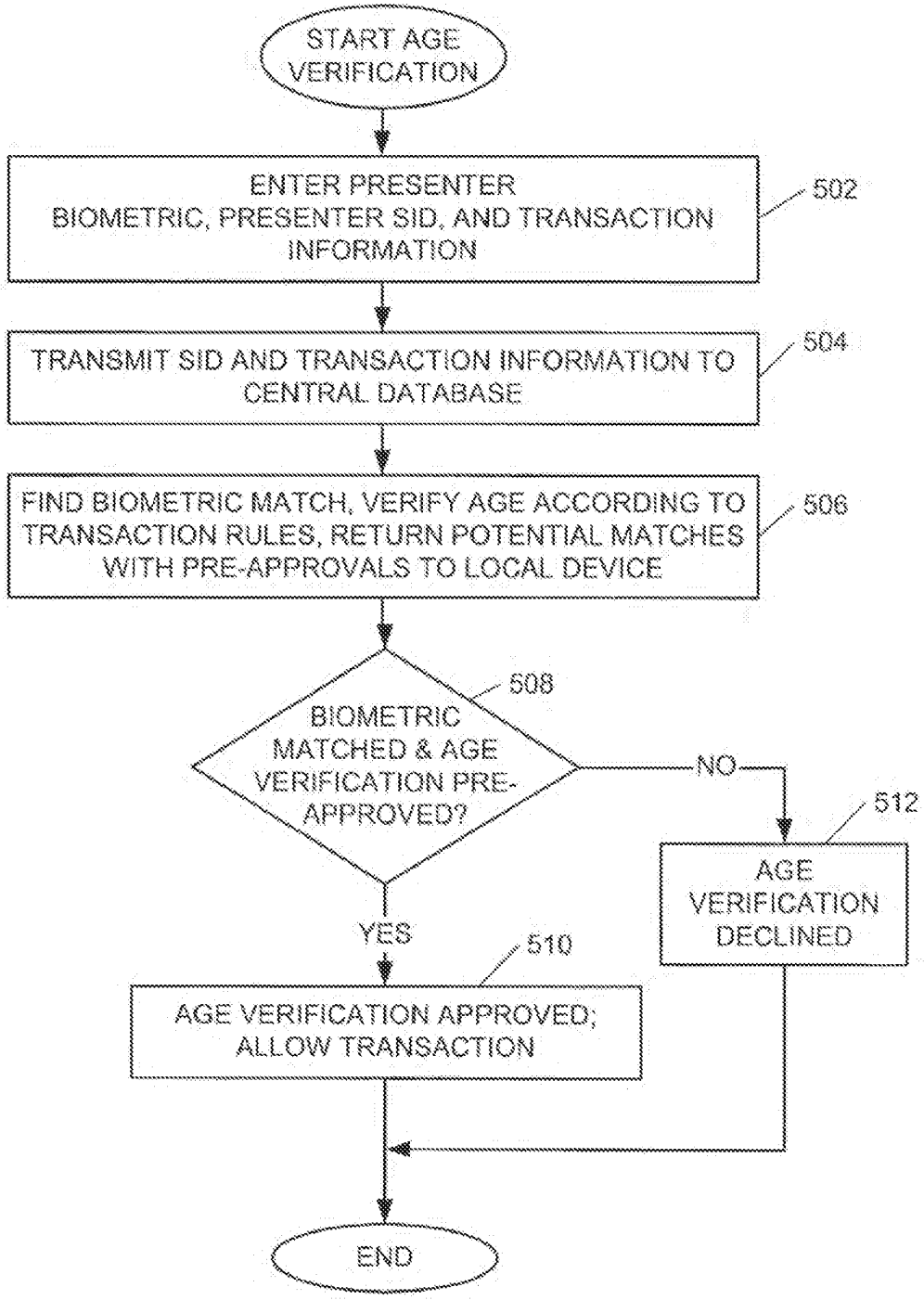

START AGE VERIFICATION
ENTER PRESENTER BIOMETRIC, PRESENTER SID, AND TRANSACTION INFORMATION
502
TRANSMIT SID AND TRANSACTION INFORMATION TO CENTRAL DATABASE
504
FIND BIOMETRIC MATCH, VERIFY AGE ACCORDING TO TRANSACTION RULES, RETURN POTENTIAL MATCHES WITH PRE-APPROVALS TO LOCAL DEVICE
506
BIOMETRIC MATCHED & AGE VERIFICATION PRE-APPROVED?
508
NO
YES
AGE VERIFICATION DECLINED
512
AGE VERIFICATION APPROVED; ALLOW TRANSACTION
510
END

FIG. 5

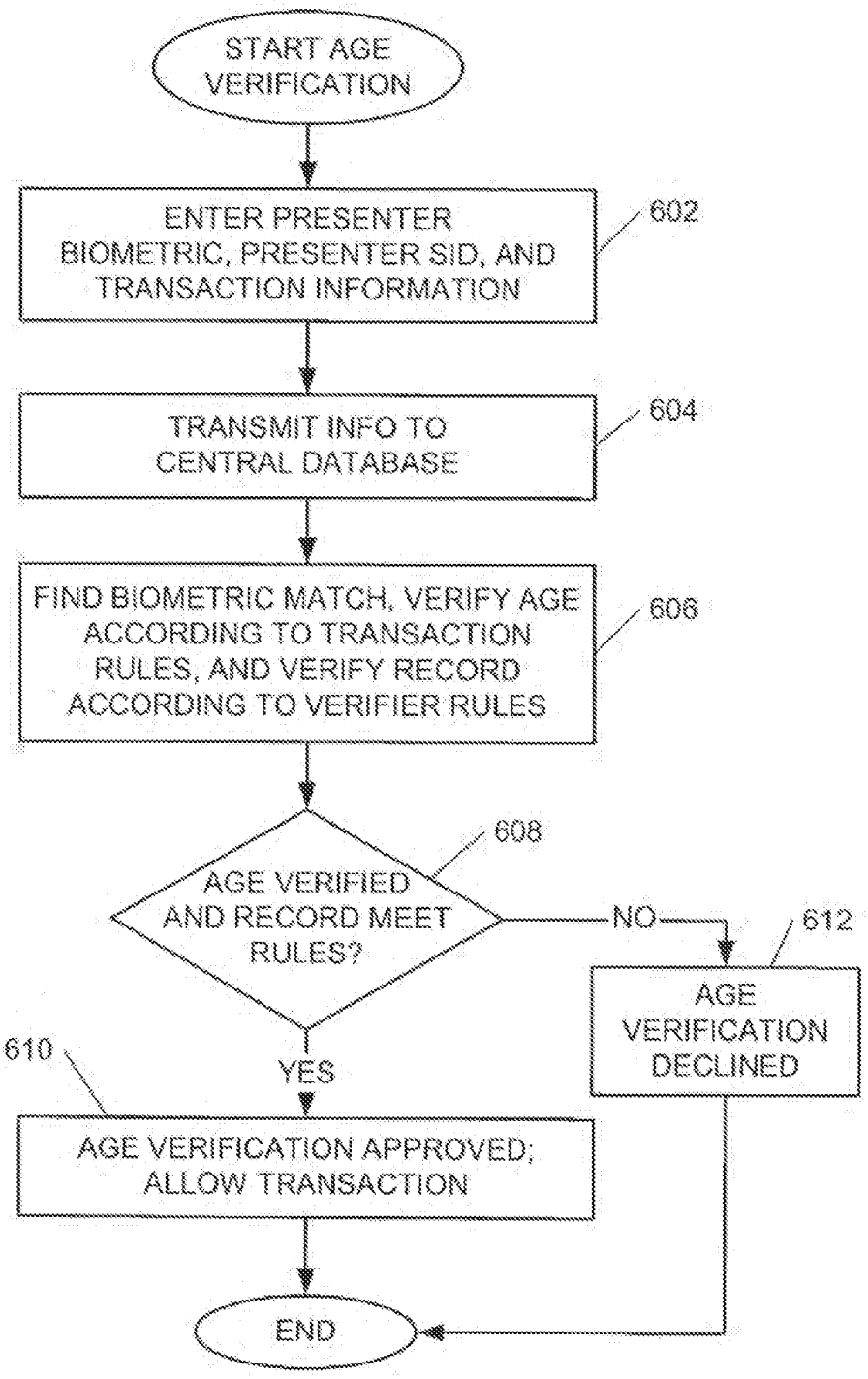

START AGE VERIFICATION
ENTER PRESENTER BIOMETRIC, PRESENTER SID, AND TRANSACTION INFORMATION
602
TRANSMIT INFO TO CENTRAL DATABASE
604
FIND BIOMETRIC MATCH, VERIFY AGE ACCORDING TO TRANSACTION RULES, AND VERIFY RECORD ACCORDING TO VERIFIER RULES
606
AGE VERIFIED AND RECORD MEET RULES?
608
NO
612
AGE VERIFICATION DECLINED
YES
610
AGE VERIFICATION APPROVED; ALLOW TRANSACTION
END

FIG. 6

SYSTEM AND METHOD FOR BIOMETRIC AUTHORIZATION FOR AGE VERIFICATION

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application is a continuation-in-part of application Ser. No. 10/251,305, filed Sep. 20, 2002, which claims domestic priority from provisional application No. 60/324,229, filed Sep. 21, 2001. The Ser. No. 10/251,305 application is incorporated by reference herein, in its entirety, for all purposes.

FIELD OF THE INVENTION

[0002] This application relates generally to age verification. More particularly, the present invention relates to a tokenless system and method for age verification using a biometric and a system identification number (SID).

BACKGROUND OF THE INVENTION

[0003] The U.S. Department of Health and Human Services (HHS) in their "1999 National Household Survey" reports underage tobacco and alcohol use is a persistent societal problem. At the time of the survey, an estimated 66.8 million Americans reported current use of a tobacco product, and 4.1 million, as reported by theantidrug.com, were between the ages of 12 and 17. Additionally, HHS estimated that 105 million Americans, 10.4 million of which were between the ages of 12 to 20, used alcohol at least once within the 30 day period preceding the survey.

[0004] As reported by the U.S. Department of Justice's "Guide to Conducting Alcohol Purchase Surveys," various surveys conducted across the U.S. have found that underage individuals were able to buy alcohol in 50 to 97 percent of stores, bars, and restaurants where attempts were made.

[0005] Although the government enforces fines and license suspension penalties on establishments that sell age-restricted goods to underage individuals, increased availability of inexpensive technology used to construct fake identifications for underage individuals to present in order to obtain age restricted goods makes age verification more difficult. Instances of selling age-restricted goods to under-age individuals also often results from careless employee verifications of a consumer's age before the consumer purchases age-restricted goods. Commonly, employees who are supposed to be verifying a consumer's age will not even look at the consumer's identification, and in systems that prompt employees to enter the consumer's birth date, employees often enter a fictitious birth date. Such careless age verification may go unnoticed by a store manager or owner. However, if authorities catch an employee selling age-restricted products to underage consumers, the manager or owner is often held responsible for the employee's actions in addition to the employee. Depending on state and federal laws, both the employee and merchant may suffer monetary penalties and/or the merchant may even have their license to sell age-restricted goods revoked as a result of their employee's careless behavior. In many states, merchants may lose their license to sell age-restricted goods for up to sixty days.

[0006] One of the main problems with the current system of age verification is that it relies too heavily on a token-based verification system. Currently, individuals seeking age verification present a state issued identification token for age verification purposes in an age-restricted transaction or access. However, such systems are easy prey to presenters bearing fake IDs or careless employees who lack a conscientious work attitude.

[0007] In addition to the age verification procedures described above, other age verification systems have been proposed that rely on tokens. Since they rely on tokens, they do not solve the problems associated with the token-based age verification systems described above. For further details, refer to U.S. Pat. No. 6,332,134 and U.S. Pat. No. 6,196,460.

[0008] What is needed is a tokenless age verification system that requires an individual seeking age verification to present biometric identification rather than token-based identification. Such a tokenless system would provide age verifiers with a more secure and accurate system for verifying age. Since age verification in such a system would be tied to an individual's biometric rather than a token, the chances are minimized that an individual can successfully present false age verification, or that a careless employee can bypass the system. Additionally, such a system would present a form of age verification that could not be lost, stolen, or fabricated. What would be quite useful would be a system and method that links an individual's biometric with age verifying information and allows the individual to verify their age at any participating point of verification by presenting a registered biometric and SID (System IDentification number).

SUMMARY OF THE INVENTION

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

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

[0011] It is another aspect of the invention to provide a system and method to help deter individuals from presenting fraudulent identification during an age-verification transaction by linking age verification to biometric identification and by monitoring verifier activity within the system.

[0012] It is also an object of the present invention to create a system that allows an individual to present age verifying and identity verifying documents once upon enrollment and then to use a SID and biometric sample to verify their age thereafter at participating devices in the system.

[0013] A system implementing the present invention uses at least one database that stores information concerning a plurality of age presenters (i.e., individuals seeking age verification). The system uses at least one point of verification (POV) terminal that has connections to necessary peripherals for biometric scanning and has communication lines for connection to the database where the presenter information is stored.

[0014] To register in the system, an individual presents at least one biometric sample, identity-verifying information, and age-verifying information. The biometric sample may be, for example and without limitation, a fingerprint, a retinal scan, a face geometric scan, or a voice print. The identity-verifying information may be, for example and without limitation, a name, a home address, a telephone number, or a government ID number and state of issue. The age-verifying information may be, for example and without limitation, age, date of birth, or a driver's license scan. The individual also registers with the system a system identification number (SID) that is used in conjunction with their biometric scan for age verification.

[0015] An individual who has already registered in the system may verify their age at any participating POV by entering the individual's SID and biometric sample. This information is sent to a database where it is used to find the individual's age verifying record. Once the age verifying record is found, the individual's age is evaluated to determine whether or not it is at or above the level pre-set for the particular verification. If the individual's age is at or above the pre-set level, the individual's age is verified, and the individual is granted access. This access may be used for (but is not limited to) purchasing age-restricted goods, accessing age-restricted areas, or purchasing age-restricted services.

[0016] These and other aspects of the present invention will become apparent to those skilled in the art by a review of the following detailed description. Although a number of salient features of the present invention have been described above, the detailed description that follows provides a more detailed exposition of additional features of the invention as it is embodied in various forms.

[0017] In this respect, before explaining at least one embodiment of the invention in detail, it is to be understood that the invention is not limited in its application to the details of construction and to the arrangements of the components set forth in the following description or illustrated drawings. The invention is capable of other embodiments and of being practiced and carried out in various ways. Also, it is to be understood that the phraseology and terminology employed herein are for the purposes of description and should not be regarded as limiting.

BRIEF SUMMARY OF THE DRAWINGS

[0018] Additional objects and advantages of the present invention will be apparent in the following detailed description read in conjunction with the accompanying drawing figures.

[0019] **FIG. 1** illustrates a block diagram overview of the general architecture of a system for age verification according to an embodiment of the present invention.

[0020] **FIG. 2** illustrates a flowchart of a process for enrollment into an age verification system according to an embodiment of the present invention.

[0021] **FIG. 3** illustrates a flowchart of a process for an age verification transaction using an age verification system according to an embodiment of the present invention.

[0022] **FIG. 4** illustrates a flowchart of a process for age verification with remote biometric matching using an age verification system according to an embodiment of the present invention.

[0023] **FIG. 5** illustrates a flowchart of a process for age verification with local biometric matching using an age verification system according to an embodiment of the present invention.

[0024] **FIG. 6** illustrates a flowchart of a process for age verification with approval rules being set by the verifier using an age verification system according to an embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0025] As previously noted, the present invention encompasses a system and method for verifying an individual's age using a biometric sample and an identification number.

[0026] Referring to **FIG. 1**, a general architecture overview of a system for age verification using biometric and system ID matching is illustrated. The system includes a verifier database **124**, wherein age verification records are stored, as well as information about authorized points of verification (POVs). The age verification records contain information related to individuals seeking age verification (that is, possessors). Various other records and databases may also be held in the verifier's database.

[0027] Alternatively (or redundantly), the central database **102** holds information related to presenters and authorized POVs. The central database **102** may further hold one or more databases that store various system data. In such an embodiment, age presenter data, verifier data, and other system data may be distributed across multiple databases within the central database **102**.

[0028] Age verifying records hold presenter age verifying and identity verifying information, such as a presenter's age, date of birth, government ID number and state of issue, home address, or a telephone number; at least one biometric template; and at least one ID number (SID) that identifies the presenter within the system. A presenter may choose a SID from any of the previously listed personal identification numbers, provided the number is unique. They may select their own SID, provided the number is unique, or they may choose from among system-suggested ID numbers.

[0029] POV information comprises information useful in recognizing, identifying and/or authenticating a POV station for accessing the age-verification system. Such information may include, but is not limited to, address of the POV location, POV identification number, and POV manufacturer.

[0030] The system may be configured so that the central database **102** is connected to a network, such as, but not limited to, the Internet. This network comprises connections to at least one POV device, such as but not limited to a computer **104** having a connected or integrated biological identification device (BID) **106**, a vending machine **110** having a connected or integrated BID **112**, a wireless device **114** having a connected or integrated BID **116**, a kiosk **120** having a connected or integrated BID **122**, a verifier database **124** having a connected age-verification devices such as a presenter service computer **126** having a connected or integrated BID **128** and/or a transaction register **130** with connected or integrated BID **132**. The transaction register **128** may be embodied so as to have a direct connection to the network through which it may communicate with the

central database **102**. However, such a direct connection is not strictly required in order to practice the present invention.

[0031] According to an alternate embodiment, the system also includes connections to one or more financial institution **108** and one or more third party information database **118**. Such connections enable presenters to perform financial transactions with their age-verifying records. Structure and processes for effecting such financial transactions are disclosed in detail in co-pending utility application Ser. No. 10/251,305 filed on Sep. 20, 2002. By way of illustration and not as a limitation, the type of information held in the third party database(s) includes government, financial, public, and private information. Examples of third party databases that would be useful for implementing this alternate embodiment are TransUnion, Experian, and Equifax.

[0032] Presenters interested in enrolling in the age verification system further have the option to pre-enroll, that is provide a partial enrollment, by providing only a portion of enrollment information, for the age verification services via a computer **104**, a vending machine **110**, a wireless device **114**, a kiosk **120**, or a verifier device **126**, **130**. Pre-enrollment records are stored as partial records that cannot be used until the remainder of enrollment information is collected. Such partial records are marked pre-enrollment. Pre-enrollment records are stored in the central database **102** but may be accessed by any participating verifier for enrollment completion. According to one embodiment, pre-enrollment records are stored only in a verifier's database **124**. Such an embodiment asks presenters to choose a verifier to send their pre-enrollment information to. According to an alternative embodiment, a pre-enrollment record may be stored in both the central database **102** and a verifier database **124**.

[0033] Pre-enrollments may be conducted at system devices with or without a BID. If the presenter pre-enrolls at a device in the system that does not have an attached BID, they may finalize enrollment at any participating device with an attached or integrated BID by selecting an option on the device nominated as "finish enrollment." The device then prompts the presenter to enter their pre-enrolled SID and present one or more designated biometrics for scanning. This information is sent to the central database to locate the presenter's partial system record. If a partial record matching the presenter's SID is found, the biometric sample entered is stored and the central database sends the presenter notice of enrollment.

[0034] Other forms of pre-enrollment may include registering with the age verification system's central database various presenters' information that is purchased or acquired database information. By way of illustration and not as a limitation, the central database operator purchases driver's license data from a state or government database and uses that information during presenter pre-enrollment, wherein the information is checked when the presenter pre-enrolls, is checked during enrollment finalization wherein the presenter is seeking to complete their enrollment into the system, or is checked during a complete enrollment. Said information could be easily entered into the central database so that when a presenter whose information was recorded in one of those databases wants to pre-enroll or enroll in the system of the invention, some or all of that information contained within said purchased or acquired database would already be available within the system. The already stored information would not need to be entered at the time of enrollment, thus saving time for the presenter during enrollment.

[0035] Age verifications are conducted within the system through a number of devices including but not limited to verifier devices connected to a verifier database **124**, such as a register **130** or presenter service computer **126**. In another embodiment, the system is also configured to conduct age verifications through devices such a vending machine **110** with an attached BID **112**, a kiosk **120** with an attached BID **122**, a PC **104** with an attached BID **106**, and a wireless device **114** with an attached BID **116**.

[0036] Presenters are free to manage their system records through a record management function that allows individuals to update personal information registered in their system record. These changes may be conducted at any of the following: a computer **104** with a BID **106**, any participating vending machine **110** with a BID **112**, a wireless device **114** with a BID **116**, a participating kiosk **120** with a BID **122**, or any participating verifier's device **126** with a BID **128**, or a register **130** with a BID **132**.

[0037] Referring to **FIG. 2**, a flowchart of an enrollment process according to an embodiment of the present invention is illustrated. The presenter is prompted to provide identity and age verifying information, a SID, and at least one biometric sample **202**. According to an optional embodiment, the presenter also provides information on one or more financial accounts to link to the age verifying record for which they are enrolling. This financial account would enable the presenter, once enrolled in the system, to authorize payment for purchases through biometric authorization.

[0038] By way of illustration and not as a limitation, one way of presenting the age verification information during enrollment is for driver's license data to simply be read from a magnetic stripe or bar code on the driver's license, from which date of birth information is pulled and used to calculate the presenter's age. Examples of suitable identity-verifying information are: a government ID number and state of issue, social security number, address, phone number, digital scans of information documents presented for identification, and other personal information about the enrolling presenter. This information may be card-swiped, scanned, hand-keyed, or entered by another means by the presenter or verifier. Optionally, identity documents such as a driver's license or identification card are digitally imaged and stored in the respective presenter's age verifying record. Digitally imaging identity documents would provide the system of the invention a security feature that would enable verifiers to view digital images of the identity documents presented for initial age verification. Such a feature would also enable authorized individuals (such as verifiers and law enforcement) who challenge an age verification to view the identifying documents the presenter presented upon enrollment into the system.

[0039] An additional feature of the present invention is the availability of further verifying age verification information, identity verification information, or biometric information stored with at least one participating third party database. Further verifying age and/or identity information adds to the system's security but is not strictly required to practice the present invention. By way of illustration and not as a

limitation, retrieving further verifying information from a third party database includes the device accessing the third party database for out-of-wallet information, such as where the presenter went to college, asking the presenter questions related to that out-of-wallet information, such as "which college did you attend: a, b, or c?" Such information is commonly stored in credit databases as a result of student loan information.

[0040] Yet another embodiment of the invention comprises checking presenter age verification information against presenter age verification information that may already be recorded in the central database as a result of the central database owner obtaining or purchasing information from private, public, or government databases. Examples of such information include, but are not limited to, driver's license data, employment data, and biometric data. All information obtained or purchased from such databases by the central database owner may be utilized for verification or confirmation of presenter information.

[0041] The presenter's biometric sample is entered via a biometric scanner. This sample is then translated to and stored in template form. Template forms of scanned biometrics are generally used for biometric comparisons. In an additional embodiment, the digital scan of the biometric is itself stored in the invention's central database. Such an embodiment that also stores the biometric digital scan is useful for reasons such as, but without limitation, biometric matching purposes, security procedures (in the case of an individual attempting to fraudulently access the system), or information protection in the event database information is lost or templates need to be re-constructed due to hardware revisions.

[0042] The system may optionally be configured to allow a presenter to register more than one type of biometric sample or two or more of the same type of biometric during enrollment. For example, the invention's system may be configured to accept a fingerprint biometric along with a face scan biometric, or the system may be configured to allow the presenter to register finger scans from more than one finger. Storing a biometric template in the presenter's system record that includes data from more than one biometric sample type enables that presenter the convenience of presenting any one of the presenter's previously scanned biometrics for age verification, record access authorization, and/or funds transfer.

[0043] The SID is a number used to help identify registered individuals in the invention's system. This SID is not equivalent to a PIN (Personal Identification Number) used for financial ATM and debit transactions. Rather, the SID simplifies the verification of the biometric sample. The SID may be a unique number (a number with no chance of being honestly duplicated, e.g. social security number), reasonably unique number (a number with a statistically small chance of being duplicated, e.g. phone number), or a non-unique number (a number with a large chance of being duplicated). While a SID comprising a unique number will inherently provide more security, the present invention is not so limited.

[0044] According to another alternative embodiment, a secondary ID number is utilized in the event that an individual does not remember the SID. In this embodiment, the secondary ID number is any number a registered individual registered during enrollment, such as, but not limited to, a home phone number, work phone number, social security number, or driver's license number.

[0045] According to yet another alternative embodiment, no SID number is used for verification of the presenter's age or identity. This is enabled when the biometric reading device conducts a reliably accurate read of a presenter's biometric that contains only a small fraction of error or no error. Additionally, an embodiment that allows a presenter to enter only their biometric might store presenter biometric sample and SID information on a device or database locally networked to the device. The device could then search the locally stored biometric templates for a match to the presenter's transaction biometric. Once a match was found, the transaction would proceed from that step, either accessing the system's central database or the local database depending on the configuration of the system. In this embodiment, the device or local database would store biometric sample and SID information for a set number of customers or would store such information for a set number of frequent customers.

[0046] In an additional embodiment, presenter personal information may be obtained for initial age verification and not stored in the presenter's age verifying record. Such an embodiment would provide presenters with a form of anonymous identification since the system would still recognize the presenter via biometric scan and SID but the biometric and SID would only be linked to age-related information and not personal information, such as home address and phone number.

[0047] In a further embodiment, if the presenter chooses to link a financial account with their age verifying record, financial account information is entered via magnetic stripe read, hand keying, or another input method. Checking record information is entered by a magnetic ink character recognition (MICR) read, an optical character recognition (OCR) read, hand keying, or entered by another method of input. The method of information input is also recorded for each enrollment. In an alternate embodiment, the system is configured to take a digital image of the monetary-representative token the presenter normally uses to access the presented financial account and store this digital scan in the presenter's system record. In an additional embodiment, the history of the presenter's financial transactions may be stored in their system record. Storing this information would enable the system to recognize the presenter's buying patterns for marketing purposes. By way of illustration and not as a limitation, it is feasible that biometrically authorized financial transactions be conducted in a system and method such as that described in utility application Ser. No. 10/251,305, filed Sep. 20, 2002, having common inventorship with this application.

[0048] Continuing with the enrollment process, the verifier enters confirmation into the system that they have reviewed and accepted the presenter's enrollment information **203**. To aid the security of the system, this confirmation is entered into the system by a verifier entering verifier identifying data, such as a biometric and/or ID number. Such verification allows the system to track verifier behavior within the system, so that if a particular verifier falls under suspicion of fraudulent verification activity, each enrollment that verifier has confirmed may be evaluated. A presenter can

then have their records re-verified in the event their records were previously verified by a verifier who is now under suspicion. Additionally, such verifier confirmation helps discourage presenters from attempting to enroll in the system with false identification and helps discourage dishonest verifiers from confirming fraudulent presenter information. However, the present invention is not so limited. The present invention may alternatively be configured such that the verifier simply presses a designated confirmation key or button on the device.

[0049] After presenter data and verifier confirmation is entered, all data entered is transmitted to the verifier database **204** where it is stored **208**. In an additional embodiment, other information may also be transmitted to the verifier database, such as but without limitation, the TID of the device the presenter is using to enroll into the system, the time of day, and the device location.

[0050] In an additional embodiment, verification information (all information entered into the system such as presenter enrollment information, verifier information, or age verification transaction information) is transmitted and stored in the system's central database. Such a system is referred to as an "open" system. An open system allows presenters to verify their age at any verifier registered in the system regardless of where they enrolled in the system because open systems comprise sharing presenter information stored in the central database with all registered verifiers. Open systems may also allow registered verifiers to choose whether or not to accept open sharing of verification information stored in the central database by setting rules that age verifying records must meet before a verification of that record and the information contained therein is verified. By way of illustration and not as a limitation, such verifier rules might include declining previous verifications of presenters in the system who enrolled at other specific verifiers, declining verifications of presenters who enrolled in the system over a year previous to the transaction, or declining verifications of presenters who have not verified their age at any verifier in a set amount of time.

[0051] Another embodiment of the system stores verification information only in the verifier database or verifier system wherein a presenter enrolls. This is referred to as a "closed" system because presenters enrolled in one verifier's database must enroll in each additional verifier database wherein they would like to verify their age with the system. Verification information is not shared among verifiers in a closed system, nor is verification information shared with the central database. Verifier databases in closed systems may query other databases, such as the central database or a third party database, for presenter verifications. However, all verification information that is entered into a particular verifier database is stored in that database. In an alternate embodiment of the closed system, information stored on a verifier database is additionally stored on the central database. Such an embodiment is useful for a reason such as, but without limitation, information protection in the event database information is lost.

[0052] In yet a further embodiment of the present invention, verification information is stored in select multiple verifier databases. In this embodiment, a system of verifiers will have chosen whether or not to share system information with the invention's central database. Such a system is referred to as a "multi-verifier" system. This system allows a chain of verifiers owned by the same entity or linked in some other manner to share verification information obtained at one or more of the linked locations amongst themselves without sharing that information with all other or non-designated other verifiers registered in the system. Verification information in a multi-verifier system is stored in either the central database or one or more of the select verifier databases in the verifier system. Information in such a system may be shared between verifier databases and the central database freely or sharing may be monitored by rules set in the verifier databases, central database, or both. By way of illustration and not as a limitation, one verifier might only want to share verification information with one of five verifiers in a multi-verifier system or all verifiers might not want to send or store verification transaction information in the central database.

[0053] In an additional embodiment of the present invention, POV devices monitored by automated verifiers may also be used for enrollment and age-verification. By way of illustration and not as a limitation, devices such as a vending machine **110**, a PC **104**, a kiosk **120**, or a wireless device **114** are configured as automated POVs, requiring no human verifier present during system enrollments or system age verifications. For security and accuracy purposes, the system would optionally have presenters enrolling at an automated POV to enter their personal and age verifying information into the system via MAG stripe read, bar code read, OCR read, or digital image read from a government or state identification document, such as a driver's license or ID card. However, the present invention is not so limited. Additionally, presenters enrolling or conducting an age verification transaction at an automated POV may be monitored by the operating database via digital video.

[0054] Referring to **FIG. 3**, a flowchart of an age verification transaction according to an embodiment of the present invention is illustrated. The presenter enters their SID and their biometric sample (herein referred to as the "transaction biometric") and transaction information is entered **302**. For example (and not as a limitation), transaction information sent to the database includes a rule code(s) mapped to the age-restricted action(s) for which the presenter has requested access. Such a code(s) indicates the presenter's requested access, which in turn indicates the rule(s) by which the presenter's age is evaluated. In an additional embodiment, such a rule(s) includes determining the presenter's allowance to access age-restricted goods/services with different age-restrictions. In such a system, it is possible that a presenter might be verified to access goods/services in one age-restricted group and not in another, even though the presenter requested to access goods/services from both groups. For example, a 19 year old presenter desiring to purchase items from both a group restricted to 18 and older presenters and a group restricted to 21 and older presenters would be verified to access the 18 and older goods/services but would be declined access to the 21 and older goods/services. Additional transaction information may also be sent to the verifier database such as terminal ID and time.

[0055] Continuing with the transaction, the presenter SID, presenter biometric, and transaction information are sent to the verifier database **304**. The presenter's age verification record is found **306**. The transaction biometric and the

registered biometric data of the selected record are compared, and if the transaction biometric and stored biometric data match, the linked presenter age is evaluated according to a rule(s) linked to the transaction information sent to the database **306**.

[0056] In an alternative embodiment, the transaction information sent to the database does not contain a code indicating the presenter's requested age-restricted access(es). In a closed system of such an embodiment, it is assumed that the verifier only offers access to age-restricted goods/services restricted to the same age group.

[0057] If the presenter's age is verified **308**, the presenter's access to purchasing age-restricted goods and/or services or accessing an age restricted area is approved **310**. In an additional embodiment, the presenter is automatically notified of the transaction approval. If for some reason the age verification is declined **312**, or part of the age verification is declined, the presenter is notified.

[0058] Once an approval or decline has been made, the local device optionally informs the presenter of their age verification results via digital display or printed receipt. The system is also optionally configured to print or display to the presenter a reason that their age verification was declined and a phone number to the invention's service center to call for further explanation.

[0059] Referring to **FIG. 4**, a flowchart of an age verification transaction according to an embodiment of the present invention is illustrated. The presenter enters their SID and their transaction biometric and transaction information is entered **402**. This information is sent to the central database **404**. Additional transaction information may also be sent to the central database such as transaction type, transaction reference number, terminal ID, and time. The presenter's age verification record is found **406**. The transaction biometric and the registered biometric data of the selected record are compared **406**. If the transaction biometric and stored biometric data match, the linked presenter age is evaluated according to rules, also known as "transaction rules," linked to the transaction information received **406**. The presenter age is then verified according to rules **408**, and the presenter's access to purchasing age-restricted goods and/or services or accessing an age restricted area is approved **410**. In an additional, optional embodiment, the presenter is automatically notified of the approval. If for some reason the age verification is declined **412**, or part of the age verification is declined, the presenter is notified.

[0060] Once an approval or decline has been made, the local device optionally informs the presenter of their age verification results via digital display or printed receipt. The system may also be optionally configured to print or display to the presenter a reason that their age verification was declined and a phone number to the invention's service center to call for further explanation.

[0061] Referring to **FIG. 5**, a flowchart of an age verification transaction with local biometric matching according to an embodiment of the present invention is illustrated. Local biometric matching refers to the transaction biometric and registered biometric matching process taking place at a device or database in the local network of the verifier system wherein the age verification is requested. The presenter enters their SID and their transaction biometric and transaction information is entered **502**. The presenter's SID and the transaction information are sent to the central database **504**. Additional transaction information may also be sent to the system's central database such as transaction type, transaction reference number, device ID, and time. Once the presenter's age verifying record is found in the central database, the biometric data stored therein is pulled and the presenter age associated with it is evaluated according to rules linked to the transaction information that was sent to the database to determine whether the age verification will be approved or declined **506**. If the age associated with the pulled biometric data is at or above the pre-set level for the age verification according to the rules, the biometric data that is sent back to the local device for matching is flagged to indicate that the age verification is pre-approved. However, if the age associated with the pulled biometric data is not at or above the pre-set level for age verification according to the rules, the biometric data sent to the local device will not be flagged, which will indicate to the device that the age verification is pre-declined. Additionally, if the transaction information initially sent to the central database includes more than one rule code, which potentially indicates to the system that the presenter is attempting to access various goods/services restricted by different age restriction rules, the ages linked to the potentially matching biometrics are pre-approved/pre-declined for each rule code. Each rule code is either flagged or not flagged, indicating to the local device pre-approval/pre-decline for each age-restricted access the presenter has requested, and returned to the device with their corresponding potentially matching biometric data.

[0062] In an additional embodiment, the age-restricted rules are optionally held at a database locally networked to the biometric device. In this embodiment, the central database might simply return the potentially matching biometric templates and their associated ages to the device. The device would then determine whether or not the presenter meets age-restricted rules by evaluating the age related to the biometric template that matches the transaction biometric provided by the presenter.

[0063] With continued reference to **FIG. 5**, the potentially matching biometric data and its pre-approval/pre-decline indication are returned to the device **506**, where the biometric data is compared to the transaction biometric temporarily held at the local device **508**. If a pre-approval indication was returned to the device, the age verification is approved **510**. Once a pre-approval indication is associated with potentially matching biometric data, if that biometric data matches transaction biometric information, the age verification is automatically approved.

[0064] Once an approval or decline has been made, the local device optionally informs the presenter of their age verification results via digital display or printed receipt. The system may also be optionally configured to print or display to the presenter a reason that their age verification was declined and a phone number to the invention's service center to call for further explanation.

[0065] Referring to **FIG. 6**, a flowchart of an age verification transaction with verifier approval rules according to an embodiment of the present invention is illustrated. Verifier approval rules refer to rules a verifier or verifier system sets within the central database or verifier database that

monitors presenter age verifications based upon certain criteria. By way of illustration and not as a limitation, such criteria includes evaluating where the presenter enrolled in the system, the identity of the verifier that enrolled the presenter into the system, when the presenter enrolled, how often the presenter uses their age verifying record, and/or how many times the presenter's age has been verified. For example, a presenter enrolls in the system at convenience store A. In an open system, the presenter should be able to verify their age at any verifier location in the system. However, convenience store B may not wish to trust an initial age verification conducted by convenience store A. Therefore, convenience store B would set rules that would decline age verifications of presenters who were initially verified at convenience store A. In such a system, convenience store B might offer to re-verify the presenter for future use of the system in their store.

[0066] Continuing with the verification process, the presenter enters their SID and transaction biometric and transaction information is entered **602**. The presenter's SID, transaction biometric, and transaction information is sent to the central database **604**. Additional transaction information may also be sent to the system's central database such as transaction type, transaction reference number, device ID, and time. Once the presenter's age verifying record is found in the central database, the biometric data stored therein is compared to the transaction biometric, the presenter age associated with it is evaluated according to rules linked to the transaction information the database received from the device, and if the age meets rules, the age verifying record is evaluated according to the verifier set rules **606**. If the transaction biometric and stored biometric data match, the linked presenter age is acceptable according to transaction linked rules, and the age verifying record meets verifier set rules, the presenter's age is verified **608**, and the presenter's access to purchasing age-restricted goods/services or accessing an age restricted area is approved **610**. If for some reason the age verification is declined **612**, or part of the age verification is declined, the presenter is notified.

[0067] Once an approval or decline has been made, the local device optionally informs the presenter of their age verification results via digital display or printed receipt. The system may also be optionally configured to print or display to the presenter a reason that their age verification was declined and a phone number to the invention's service center to call for further explanation. Additionally, if the presenter was declined age verification because their record did not meet pre-set rules, the presenter may be given instructions on how to meet these rules.

[0068] In an additional embodiment, open system age verification transactions regulated by verifier set rules, as illustrated in **FIG. 6**, are configured to match biometrics at the verifier device, as illustrated in **FIG. 5**. In such an embodiment, verifier rules would be stored in the central database and the pre-approval/pre-decline check would include verifying the chosen records according to those stored verifier set rules. Various additional embodiments and methods of the system are described as follows.

[0069] In an alternate embodiment of the invention, the system comprises utilizing an identification system wherein presenter records are associated with personal identifying information and a score which indicates the reliability of the information stored in the record and verifications performed with the record. This embodiment allows a presenter to verify their identity and age in one system access. Additionally, this embodiment also provides a presenter record score that is useful to determine the degree of reliability of the presenter's identity and/or age verification. This feature also allows the system to monitor the reliability of verifiers by requiring verifiers to identify themselves during supervision of an age verification transaction. This feature is useful to track the reliability of verifier actions within the system.

[0070] In another alternate embodiment, verifiers set the rules of age verification on goods and services which are not regulated by the government. For example, a verifier located at a movie theater would set various rules of age verification for purchase of age-related discount movie tickets or tickets to movies rated for a specific age. These rules are set in the verifier's local database and/or the central database of the invention, depending on whether the embodiment of the invention's system is open, semi-open, or closed.

[0071] An additional embodiment of the invention encrypts information transferred between two points in the system. For purposes of example and without limitation, information is encrypted at one point and sent across a non-secure connection between the points or not encrypted at a point of communication but sent to the other point of communication across a secure connection. Encryption and decryption of said messages may be monitored by services provided by a company such as VeriSign, Inc. As an added level of security, one alternate embodiment encrypts even information internal to a terminal and which is never transmitted in a communication. This prevents retrieval of sensitive information (e.g., data corresponding to a biometric scan) from a stolen terminal.

[0072] A hybrid embodiment of the invention enables presenters to verifying their age, verifying their identity, and/or paying for purchases with biometric authorization at various types of automated POV and POS stations. By way of illustration and not a limitation, such stations include linked or networked vending machines and linked or networked kiosks.

[0073] An additional feature of the present invention is giving an individual enrolling in a system according to an embodiment of the invention the ability to register a password that in conjunction with their system ID # would allow them to perform record maintenance of their system record over the Internet from a device without a BID.

[0074] Another embodiment of the invention includes the verifier and central databases providing presenters with system ID suggestions if their entered system ID is already registered within the system. These suggested IDs are preferably (but not necessarily) selected from system IDs that are not already registered in the system but are similar to the system ID the presenter originally entered.

[0075] An additional feature of the system allows direct transition from an enrollment into a POV or POS transaction without starting a new transaction. This would allow a presenter to enroll into the system just before they verify their age or purchase an item without having to reenter their biometric and SID.

[0076] A hybrid feature that is a useful option for use with any or all of the disclosed enrollment and identification

methods is to print a paper receipt of the system activity performed during the system access. Information included on this receipt would be any information including but not limited to the transaction type, date, transaction number, record used, the system's customer service phone number, instructions on how to contact the system's customer service, or other transaction information.

[0077] It is also an alternate embodiment of the present invention to provide verifiers with presenter and verifier profile reports in case of suspected fraudulent activity. These reports are customizable to display select information from a presenter's age verifying record history or record.

[0078] According to another hybrid embodiment, the system is configured to send a POV's TID along with transaction information for presenter security purposes. If the TID is not registered with the central or verifier database, the presenter's information is not processed. Optionally, the POV display gives the presenter a system customer service number to call and a transaction code to reference during the call, so they may find out why the transaction was declined.

[0079] An age verification system using biometric identification and a system ID number has been illustrated. It will be appreciated by those skilled in the art that the systems and methods of the present invention can be used to perform more secure and reliable age verifications, and in addition, allows presenters to verify their identity and pay for merchandise with the same biometric used to verify their age. It is anticipated that the present invention will especially find utility in preventing underage individuals from accessing age-restricted goods. Although the age-restricted goods and services referred to in the invention's description are primarily tobacco and/or alcohol related, the system is not limited to verifying age for access to these specific age-restricted goods and services. Age-restricted goods and services are additionally those designated by the verifier. It will thus be appreciated by those skilled in the art that other variations of the present invention will be possible without departing from the scope of the invention as described.

What is claimed is:

1. A method of using a transaction system to provide approval of an age-restricted transaction between an age presenter and an age verifier, the transaction system having at least one database that has stored therein a biometric record associated with the age presenter via an age presenter identification code, and at least one age verification station configured to access the at least one database, and wherein the at least one database is adapted to apply transaction rules, wherein the method comprises:

receiving, at the age verification station, a biometric sample proffered by the age presenter via a biometric identification device;

receiving, at the age verification station, an identification code proffered by the age presenter;

receiving, at the age verification station, transaction information;

sending the biometric sample proffered by the age presenter from the age verification station to the at least one database;

sending the identification code proffered by the age presenter from the age verification station to the at least one database;

sending transaction information from the age verification station to the at least one database;

comparing, at the at least one database, the proffered identification code to age presenter identification codes stored in the at least one database;

making a first determination, at the at least one database, whether the proffered identification code matches an age presenter code stored in the at least one database;

in the event the proffered identification code matches an age presenter code stored in the at least one database, making a second determination whether the proffered biometric sample matches an age presenter biometric record stored in the at least one database;

in the event the proffered biometric sample matches an age presenter biometric template record in the at least one database, making a third determination whether the age information mapped to said biometric record meets the transaction rules; in the event the age information mapped to said biometric record meets the transaction rules, approving the transaction at the at least one database; and

receiving, at the age verification station, confirmation of the transaction approval.

2. The method of using a transaction system as claimed in claim 1, wherein the age presenter identification code comprises one or more of: a unique number, a reasonably unique number, and a non unique number.

3. The method of using a transaction system as claimed in claim 1, wherein the biometric sample comprises one or more of: a fingerprint scan, an iris scan, a facial scan, a voice scan, a retinal scan, a hand architecture scan, a vein pattern scan, a signature sample, and a DNA sample.

4. The method of using a transaction system as claimed in claim 1, wherein transaction data is encrypted and the communications between the age verification station and the at least one database are encrypted.

5. The method of using a transaction system as claimed in claim 1, wherein the transaction information comprises at least one alphanumeric code indicating in at least one database the transaction rules to apply to the transaction.

6. The method of using a transaction system as claimed in claim 5, wherein transaction information further comprises one or more of: the terminal identification number associated with an age verification station, the age verification station location, and the time of the transaction.

7. The method of using a transaction system as claimed in claim 1, wherein the age approval station is located at a location selected from the group consisting of: a verifier, a kiosk, an ATM, a telephone, a self-checkout POS register station, an automated cash register, a computer, a wireless device, and a vending machine.

8. The method of using a transaction system as claimed in claim 1, wherein system user information is stored in more than one database.

9. The method of using a transaction system as claimed in claim 8, wherein transaction information is compared to information stored in more than one database.

10. The method of using a transaction system as claimed in claim 1, wherein the age-restricted transaction comprises a financial transaction.

11. The method of using a transaction system as claimed in claim 10, wherein financial transaction settlement is conducted via a financial transaction system comprising biometric authentication of payors.

12. A method of using a transaction system to provide approval of an age-restricted transaction between an age presenter and an age verifier, the transaction system having a central database that has stored therein a biometric record associated with the age presenter via an age presenter identification code, the central database being adapted to apply transaction rules, and at least one age verification station configured to access the central database, wherein the method comprises:

receiving, at the age verification station, a biometric sample proffered by the age presenter via a biometric identification device;

receiving, at the age verification station, an identification code proffered by the age presenter;

receiving, at the age verification station, transaction information;

sending the biometric sample proffered by the age presenter from the age verification station to the central database;

sending the identification code proffered by the age presenter from the age verification station to the central database;

sending the transaction information from the age verification station to the central database;

comparing, at the central database, the proffered identification code to age presenter identification codes stored in the central database;

making, at the central database, a first determination whether the proffered identification code matches an age presenter code stored in the central database;

in the event the proffered identification code matches an age presenter code stored in the central database, making a second determination whether the proffered biometric sample matches an age presenter biometric record stored in the central database;

in the event the proffered biometric sample matches an age presenter biometric record stored in the central database, making a third determination whether the age information mapped to the biometric record meets transaction rules;

in the event the age information mapped to the biometric record meets transaction rules, approving, at the central database, the transaction; and

receiving, at the age verification station, confirmation of the transaction approval.

13. The method of using a transaction system as claimed in claim 12, wherein the age presenter identification code comprises one or more of: a unique number, a reasonably unique number, and a non unique number.

14. The method of using a transaction system as claimed in claim 12, wherein the biometric sample comprises one or more: a fingerprint, an iris scan, a facial scan, a voice scan, a retinal scan, a hand architecture scan, a vein pattern scan, a signature sample, and a DNA sample.

15. The method of using a transaction system as claimed in claim 12, wherein transaction data is encrypted and the communications between the age verification station and the central database are encrypted.

16. The method of using a transaction system as claimed in claim 12, wherein the transaction information comprises at least one alphanumeric code indicating at the central database the transaction rules to apply to the transaction.

17. The method of using a transaction system as claimed in claim 16, wherein transaction information further comprises one or more of: the terminal identification number associated with an age verification station, the age verification station location, and the time of the transaction.

18. The method of using a transaction system as claimed in claim 12, wherein the age verification station is located at a location selected from the group consisting of: a verifier, a kiosk, an ATM, a telephone, a self-checkout POS register station, an automated cash register, a computer, a wireless device, and a vending machine.

19. The method of using a transaction system as claimed in claim 12, wherein the age-restricted transaction comprises a financial transaction.

20. The method of using a transaction system as claimed in claim 19, wherein financial transaction settlement is conducted via a financial transaction system comprising biometric authentication of payors.

21. The method of using a transaction system as claimed in claim 12, wherein system user information is stored in more than one database.

22. The method of using a transaction system as claimed in claim 21, wherein transaction information is compared to information stored in more than one database.

23. A method of using a transaction system to provide approval of an age-restricted transaction between an age presenter and an age verifier, the transaction system having a central database that has stored therein a biometric record associated with the age presenter via an age presenter identification code, the central database being configured to apply transaction rules, and at least one age verification station configured to access the central database, wherein the method comprises:

receiving, at the age verification station, a biometric sample proffered by the age presenter via a biometric identification device;

receiving, at the age verification station, an identification code proffered by the age presenter;

receiving, at the age verification station, transaction information;

sending the identification code proffered by the age presenter from the age verification station to the central database;

sending the transaction information from the age verification station to the central database;

comparing, at the central database, the proffered identification code to age presenter identification codes stored in the central database;

making, at the central database, a first determination whether the proffered identification code matches the age presenter code stored in the central database;

in the event the proffered identification code matches the age presenter code stored in the central database, making, at the central database, a second determination whether an age presenter age mapped to the biometric record corresponding to the age presenter code meets transaction rules;

in the event the at least one presenter age meets transaction rules, pre-approving, at the central database, the biometric record as a potential matching biometric record for age verification approval at the age verification station;

receiving, at the age verification station, the potential matching biometric record from the central database;

comparing, at the age verification station, the proffered biometric sample to the potential matching biometric record received from the central database;

making, at the age verification station, a third determination of whether the proffered biometric sample matches the potential matching biometric record;

in the event that the proffered biometric sample matches the at least one potential matching biometric record, making, at the age verification station, a fourth determination of whether the matching biometric record was pre-approved at the central database; and

in the event the matching biometric record was pre-approved at the central database, approving, at the age verification station, the transaction.

24. The method of using a transaction system as claimed in claim 23, wherein the method further comprises:

the age verification station sending to the central database confirmation of completion of the transaction.

25. The method of using a transaction system as claimed in claim 23, wherein the age presenter identification code comprises one or more of: a unique number, a reasonably unique number, and a non unique number.

26. The method of using a transaction system as claimed in claim 23, wherein the biometric sample comprises one or more of: a fingerprint, an iris scan, a facial scan, a voice scan, a retinal scan, a hand architecture scan, a vein pattern scan, a signature sample, and a DNA sample.

27. The method of using a transaction system as claimed in claim 23, wherein transaction data is encrypted and the communications between the age verification station and the central database are encrypted.

28. The method of using a transaction system as claimed in claim 23, wherein the transaction information comprises at least one alphanumeric code indicating at the central database the transaction rules to apply to the transaction.

29. The method of using a transaction system as claimed in claim 28, wherein transaction information further comprises one or more of: a terminal identification number associated with an age verification station, age verification station location, and the time of the transaction.

30. The method of using a transaction system as claimed in claim 23, wherein the age verification station is located at a location selected from the group consisting of: a verifier, a kiosk, an ATM, a telephone, a self-checkout POS register station, an automated cash register, a computer, a wireless device, and a vending machine.

31. The method of using a transaction system as claimed in claim 23, wherein the age-restricted transaction comprises a financial transaction.

32. The method of using a transaction system as claimed in claim 31, wherein financial transaction settlement is conducted via a financial transaction system comprising biometric authentication of payors.

33. The method of using a transaction system as claimed in claim 23, wherein system user information is stored in more than one database.

34. The method of using a transaction system as claimed in claim 33, wherein the transaction information is compared to information stored in more than one database.

35. A method of using a transaction system to provide approval of an age-restricted transaction between an age presenter and an age verifier, the transaction system having a central database that has stored therein a biometric record associated with the age presenter through an age presenter identification code, the central database being adapted to apply central transaction rules and to apply verifier transaction rules, and at least one age verification station configured to access the central database, wherein the method comprises:

receiving, at the age verification station, a biometric sample proffered by the age presenter via a biometric identification device;

receiving, at the age verification station, an identification code proffered by the age presenter;

receiving, at the age verification station, transaction information;

sending the biometric sample proffered by the age presenter from the age verification station to the central database;

sending the identification code proffered by the age presenter from the age verification station to the central database;

sending the transaction information from the age verification station to the central database;

comparing, at the central database, the proffered identification code to age presenter identification codes stored in the central database;

making, at the central database, a first determination whether the proffered identification code matches an age presenter code stored in the central database;

in the event the proffered identification code matches an age presenter code stored in the central database, making, at the central database, a second determination whether the proffered biometric sample matches an age presenter biometric record stored in the central database;

in the event the proffered biometric sample matches an age presenter biometric record stored in the central database, making, at the central database, a third determination whether an age presenter information record mapped to the matching presenter biometric record meets the verifier transaction rules;

in the event the age presenter information record mapped to the matching presenter biometric record meets the verifier transaction rules, making, at the central database, a fourth determination whether the age information mapped to said biometric record meets the central transaction rules;

in the event the age information mapped to said biometric record meets the central transaction rules, approving, at the database, the transaction; and

receiving at the age verification station confirmation of the transaction approval.

36. The method of using a transaction system as claimed in claim 35, wherein the age presenter identification code comprises one or more of: a unique number, a reasonably unique number, and a non unique number.

37. The method of using a transaction system as claimed in claim 35, wherein the biometric sample comprises one or more of: a fingerprint, an iris scan, a facial scan, a voice scan, a retinal scan, a hand architecture scan, a vein pattern scan, a signature sample, and a DNA sample.

38. The method of using a transaction system as claimed in claim 35, wherein the transaction data is encrypted and the communications between the age verification station and the central database are encrypted.

39. The method of using a transaction system as claimed in claim 35, wherein the transaction information comprises at least one alphanumeric code indicating at the central database the transaction rules to apply to the transaction.

40. The method of using a transaction system as claimed in claim 39, wherein transaction information further comprises one or more of: a terminal identification number associated with an age verification station, the age verification station location, and the time of the transaction.

41. The method of using a transaction system as claimed in claim 35, wherein the age verification station is located at a location selected from the group consisting of: a verifier, a kiosk, an ATM, a telephone, a self-checkout POS register station, an automated cash register, a computer, a wireless device, and a vending machine.

42. The method of using a transaction system as claimed in claim 35, wherein the age-restricted transaction comprises a financial transaction.

43. The method of using a transaction system as claimed in claim 35, wherein financial transaction settlement is conducted via a financial transaction system comprising biometric authorization of payors.

44. The method of using a transaction system as claimed in claim 35, wherein system user information is stored in more than one database.

45. The method of using a transaction system as claimed in claim 44, wherein the transaction information is compared to information stored in more than one database.

46. A method of using a transaction system to provide approval of an age-restricted transaction between an age presenter and an age verifier, the transaction system having a central database that has stored therein a biometric record associated with the age presenter, the central database being configured to apply transaction rules, and at least one age verification station configured to access the central database, wherein the method comprises:

receiving, at the age verification station, a biometric sample proffered by the age presenter via a biometric identification device;

receiving, at the age verification station, transaction information;

sending the biometric sample proffered by the age presenter from the age verification station to the central database;

sending the transaction information from the age verification station to the central database;

comparing, at the central database, the proffered biometric sample to age presenter biometric records stored in the central database;

making, at the central database, a first determination whether the proffered biometric sample matches any age presenter biometric record stored in the central database;

in the event the proffered biometric sample matches an age presenter biometric record stored in the central database, making a second determination whether the age information mapped to the biometric record meets transaction rules;

in the event the age information mapped to the biometric record meets transaction rules, approving, at the central database, the transaction; and

receiving at the age verification station confirmation of the transaction approval.

47. The method of using a transaction system as claimed in claim 46, wherein the biometric sample comprises one or more of: a fingerprint scan, an iris scan, a facial scan, a voice scan, a retinal scan, a hand architecture scan, a vein pattern scan, a signature sample, and a DNA sample.

48. The method of using a transaction system as claimed in claim 46, wherein the transaction data is encrypted and the communications between the age verification station and the central database are encrypted.

49. The method of using a transaction system as claimed in claim 46, wherein the transaction information comprises at least one alphanumeric code indicating at the central database the transaction rules to apply to the transaction.

50. The method of using a transaction system as claimed in claim 46, wherein the age approval station is located at a location selected from the group consisting of: a verifier, a kiosk, an ATM, a telephone, a self-checkout POS register station, an automated cash register, a computer, a wireless device, and a vending machine.

51. The method of using a transaction system as claimed in claim 46, wherein system user information is stored in more than one database.

52. The method of using a transaction system as claimed in claim 51, wherein the transaction information is compared to information stored in more than one database.

53. The method of using a transaction system as claimed in claim 46, wherein the age-restricted transaction comprises a financial transaction.

54. The method of using a transaction system as claimed in claim 53, wherein financial transaction settlement is conducted via a financial transaction system comprising biometric authorization of payors.

55. A method of using a transaction system to provide approval of an age-restricted transaction between an age presenter and an age verifier, the transaction system having a central database that has stored therein a biometric record associated with the age presenter via an age presenter

identification code, and at least one age verification station configured to access the central database, the age verification station being configured to apply transaction rules, wherein the method comprises:

receiving, at the age verification station, a biometric sample proffered by the age presenter via a biometric identification device;

receiving, at the age verification station, an identification code proffered by the age presenter;

receiving, at the age verification station, transaction information;

sending the identification code proffered by the age presenter from the age verification station to the central database;

sending the transaction information from the age verification station to the central database;

comparing, at the central database, the proffered identification code to one or more age presenter identification codes stored in the central database;

making, at the central database, a first determination whether the proffered identification code matches any age presenter identification codes stored in the central database;

in the event the proffered identification code matches at least one age presenter code stored in the central database, sending to the age verification station as one or more potential matching biometric records the one or more biometric records corresponding to any matched age presenter codes;

sending to the age verification station one or more presenter ages that correspond to the one or more potential matching biometric records;

receiving, at the age verification station, the one or more potential matching biometric records sent from the central database;

receiving, at the age verification station, the one or more presenter ages mapped to the one or more potential matching biometric records sent from the central database;

making, at the age verification station, a second determination of whether the proffered biometric sample matches any of the one or more potential matching biometric records;

in the event that the proffered biometric sample matches any of the one or more potential matching biometric records, making, at the age verification station, a third determination whether a presenter age mapped to a matched biometric record meets the transaction rules; and in the event the presenter age mapped to the matched biometric record meets transaction rules, providing, at the age verification station, approval of the age-restricted transaction.

56. The method of using a transaction system as claimed in claim 55, wherein the age presenter identification code comprises one or more of: a unique number, a reasonably unique number, and a non unique number.

57. The method of using a transaction system as claimed in claim 55, wherein the biometric sample comprises one of: a fingerprint scan, an iris scan, a facial scan, a voice scan, a retinal scan, a hand architecture scan, a vein pattern scan, a signature sample, and a DNA sample.

58. The method of using a transaction system as claimed in claim 55, wherein the transaction data is encrypted and the communications between the age verification station and the at least one database are encrypted.

59. The method of using a transaction system as claimed in claim 55, wherein the age station is located at a location selected from the group consisting of: a verifier, a kiosk, an ATM, a telephone, a self-checkout POS register station, an automated cash register, a computer, a wireless device, and a vending machine.

60. The method of using a transaction system as claimed in claim 55, wherein system user information is stored in more than one database.

61. The method of using a transaction system as claimed in claim 55, wherein transaction information is compared to information stored in more than one database.

62. The method of using a transaction system as claimed in claim 55, wherein the age-restricted transaction comprises a financial transaction.

63. The method of using a transaction system as claimed in claim 62, wherein financial transaction settlement is conducted via a financial transaction system comprising biometric authorization of payors.

64. A method for authorizing a system user to use a transaction system, the transaction system having at least one database that receives and stores therein enrollment data associated with authorized system users through a system identification code, the method comprising:

prompting a prospective system user to proffer enrollment data comprising age information, personal information, a system identification code, and one or more biometric samples;

prompting a system operator to proffer verification of the enrollment data the prospective system user proffers;

transmitting to at least one database the proffered enrollment data;

transmitting to at least one database the proffered verifier verification of the proffered enrollment data; and

storing in the at least one database the proffered enrollment data and proffered verifier verification.

65. The method for authorizing a system user to use a transaction system according to claim 64, wherein the age information comprises one or more of: driver's license data, passport data, birth certificate data, and credit data.

66. The method for authorizing a system user to use a transaction system according to claim 64, wherein the personal information comprises one or more of: driver's license data, social security number, address, and phone number.

67. The method for authorizing a system user to use a transaction system according to claim 64, wherein the personal information is acquired via a process selected from the group consisting of: swiping, scanning, and hand-keying.

68. The method for authorizing a system user to use a transaction system according to claim 64, wherein the proffered biometric sample is entered via a biometric scanner.

69. The method for authorizing a system user to use a transaction system according to claim 64, wherein the prospective user proffers enrollment data at a location selected

from the group consisting of: a verifier's station, a merchant's store, a kiosk, a self-checkout POS register station, and at a government office.

70. The method for authorizing a system user to use a transaction system according to claim 64, wherein the age presenter identification code comprises one of: a unique number, a reasonably unique number, and a non unique number.

71. The method of using a transaction system as claimed in claim 64, wherein the biometric sample comprises one of: a fingerprint, an iris scan, a facial scan, a voice scan, a retinal scan, and a hand architecture scan.

72. The method for authorizing a system user to use a transaction system according to claim 64, wherein saving the proffered enrollment data in at least one database comprises:

converting a biometric sample into a biometric template; and

saving the biometric template to at least one database in association with the system identification code.

73. The method for authorizing a system user to use a transaction system according to claim 72, wherein proffered enrollment data further comprises a record maintenance password.

74. The method for authorizing a system user to use a transaction system according to claim 73, wherein said a record maintenance password allows a system user to access a system user record to change system user information.

75. The method for authorizing a system user to use a transaction system according to claim 64, wherein the method further comprises:

in the event the proffered system identification code matches a system identification stored in at least one database, sending to the prospective system user one or more suggested system identification codes; and

receiving from the prospective system user a system identification code selected from the one or more suggested system identification codes.

76. The method for authorizing a system user to use a transaction system according to claim 64, wherein the method further comprises:

in the event the proffered system identification code matches a system identification stored in at least one database, assigning the prospective user an alternate system identification code.

77. The method for authorizing a system user to use a transaction system according to claim 64, wherein the proffered enrollment data further comprises a digital image of the biometric sample.

78. The method for authorizing a system user to use a transaction system according to claim 64, wherein the proffered enrollment data further comprises a digital image of the at least one document presented for system user identification or system user age verification.

79. The method for authorizing a system user to use a transaction system according to claim 64, wherein the proffered enrollment data further comprises financial account information.

80. The method for authorizing a system user to use a transaction system according to claim 64, wherein system user information is stored in more than one database.

81. A method for authorizing a system user to use a transaction system, the transaction system having at least one database that receives and stores therein enrollment data associated with authorized system users through a system user biometric record, the method comprising:

prompting a prospective system user to proffer enrollment data comprising age information, personal information, and one or more biometric sample;

prompting a system operator to proffer verification of the enrollment data the prospective system user proffers;

transmitting to at least one database the proffered enrollment data;

transmitting to at least one database the proffered verifier verification of the proffered enrollment data; and

storing in at least one database the proffered enrollment data and proffered verifier verification.

82. The method for authorizing a system user to use a transaction system according to claim 81, wherein the age information comprises one or more of: driver's license data, passport data, birth certificate data, and credit data.

83. The method for authorizing a system user to use a transaction system according to claim 81, wherein the personal information comprises one or more of: driver's license data, social security number, address, and phone number.

84. The method for authorizing a system user to use a transaction system according to claim 81, wherein the personal information is acquired via a process selected from the group consisting of: swiping, scanning, and hand-keying.

85. The method for authorizing a system user to use a transaction system according to claim 81, wherein the proffered biometric sample is entered via a biometric scanner.

86. The method for authorizing a system user to use a transaction system according to claim 81, wherein the prospective user proffers enrollment data at a location selected from the group consisting of: a verifier's station, a merchant's store, a kiosk, a self-checkout POS register station, and at a government office.

87. The method for authorizing a system user to use a transaction system according to claim 81, wherein the biometric sample is selected from the group consisting of: a fingerprint, an iris scan, a facial scan, a voice scan, a retinal scan, and a hand architecture scan.

88. The method for authorizing a system user to use a transaction system according to claim 81, wherein saving the proffered enrollment data in at least one database comprises:

converting a biometric sample into a biometric template; and

saving the biometric template to at least one database in association with the system identification code.

89. The method for authorizing a system user to use a transaction system according to claim 81, wherein the proffered enrollment data further comprises an account maintenance password.

90. The method for authorizing a system user to use a transaction system according to claim 81, wherein the proffered enrollment data further comprises a digital image of the biometric sample.

91. The method for authorizing a system user to use a transaction system according to claim 81, wherein the proffered enrollment data further comprises a digital image of the at least one document presented for system user identification or system user age verification.

92. The method for authorizing a system user to use a transaction system according to claim 81, wherein the proffered enrollment data further comprises financial account information.

93. The method for authorizing a system user to use a transaction system according to claim 81, wherein system user information is stored in more than one database.

* * * * *