Application Data Sheet 37 CFR 1.76	Attorney Docket Number	W0537-701321
	Application Number	

Title of Invention	UNIVERSAL SECURE REGISTRY

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**
	Kenneth	P.	Weiss	

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

City	Newton	**State/Province**	MA	**Country of Residence** i	US

Mailing Address of Inventor:

Address 1	59 Sargent Street		
Address 2			
City	Newton	**State/Province**	MA
Postal Code	02458	**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	37462	
Email Address		Add Email Remove Email

Application Information:

Title of the Invention	UNIVERSAL SECURE REGISTRY		
Attorney Docket Number	W0537-701321	**Small Entity Status Claimed**	□
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	29	**Suggested Figure for Publication (if any)**	31

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	W0537-701321
	Application Number	
Title of Invention	UNIVERSAL SECURE REGISTRY	

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☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in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	37462		

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.

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13237184	Continuation in part of	13168556	2011-06-24	8271397	2012-09-18
Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13168556	Continuation of	11677490	2007-02-21	8001055B	2011-08-16

Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
11677490	non provisional of	60859235	2006-11-15
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
11677490	non provisional of	60812279	2006-06-09
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
11677490	non provisional of	60775046	2006-02-21

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	W0537-701321
	Application Number	
Title of Invention	UNIVERSAL SECURE REGISTRY	

Prior Application Status	Patented	Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13237184	Continuation of	12393586	2009-02-26	8234220	2012-07-31

Prior Application Status	Expired	Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
12393586	non provisional of	61031529	2008-02-26

Prior Application Status	Patented	Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
12393586	Continuation in part of	11760732	2007-06-08	7809651B	2010-10-05

Prior Application Status	Patented	Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
11760732	Continuation of	11677490	2007-02-21	8001055B	2011-08-16

Prior Application Status	Patented	Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
12393586	Continuation in part of	11760729	2007-06-08	7805372B	2010-09-28

Prior Application Status	Patented	Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
11760729	Continuation of	11677490	2007-02-21	8001055B	2011-08-16

Prior Application Status	Patented	Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
12393586	Continuation in part of	11677490	2007-02-21	8001055B	2011-08-16

Prior Application Status	Pending	Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation of	13237184	2011-09-20

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) ithe 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).

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	W0537-701321
	Application Number	
Title of Invention	UNIVERSAL SECURE REGISTRY	

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

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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	W0537-701321
	Application Number	
Title of Invention	UNIVERSAL SECURE REGISTRY	

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. □

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

Mailing Address Information:			
Address 1			
Address 2			
City		**State/Province**	
Country i		Postal Code	
Phone Number		Fax Number	
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

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	W0537-701321
	Application Number	
Title of Invention	UNIVERSAL SECURE REGISTRY	

If the Assignee is an Organization check here. ☒

Organization Name	UNIVERSAL SECURE REGISTRY, LLC

Mailing Address Information:

Address 1	59 Sargent Street		
Address 2			
City	Newton	**State/Province**	MA
Country i	US	Postal Code	02458
Phone Number		Fax Number	
Email Address			

Additional 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 H. Grady/			Date (YYYY-MM-DD)	2013-11-04
First Name	Matthew	Last Name	Grady	Registration Number	52957

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

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.

Electronic Acknowledgement Receipt

EFS ID:	17307687
Application Number:	14071126
International Application Number:	
Confirmation Number:	3814
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Customer Number:	37462
Filer:	Matthew H. Grady
Filer Authorized By:	
Attorney Docket Number:	W0537-701321
Receipt Date:	04-NOV-2013
Filing Date:	
Time Stamp:	16:25:09
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	Drawings-only black and white line drawings	-Parent-Dwgs_1.PDF	534913 fd4613e1911a3061050e1f7f3c025cd9601d2c9f	no	29

Warnings:

Information:

2		-_-Application_3.PDF	408291 20d5481796ead6b0d4c9195bdfe0dff158805cc4	yes	79

Multipart Description/PDF files in .zip description

Document Description	Start	End
Specification	1	74
Claims	75	78
Abstract	79	79

Warnings:

Information:

3	Application Data Sheet	EFSShowPDF.pdf	1516747 422fc6f6583f87a6ef19981ff3e930755fd32133	no	7

Warnings:

Information:

Total Files Size (in bytes):	2459951

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.

<u>New Applications Under 35 U.S.C. 111</u>
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.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
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.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
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.

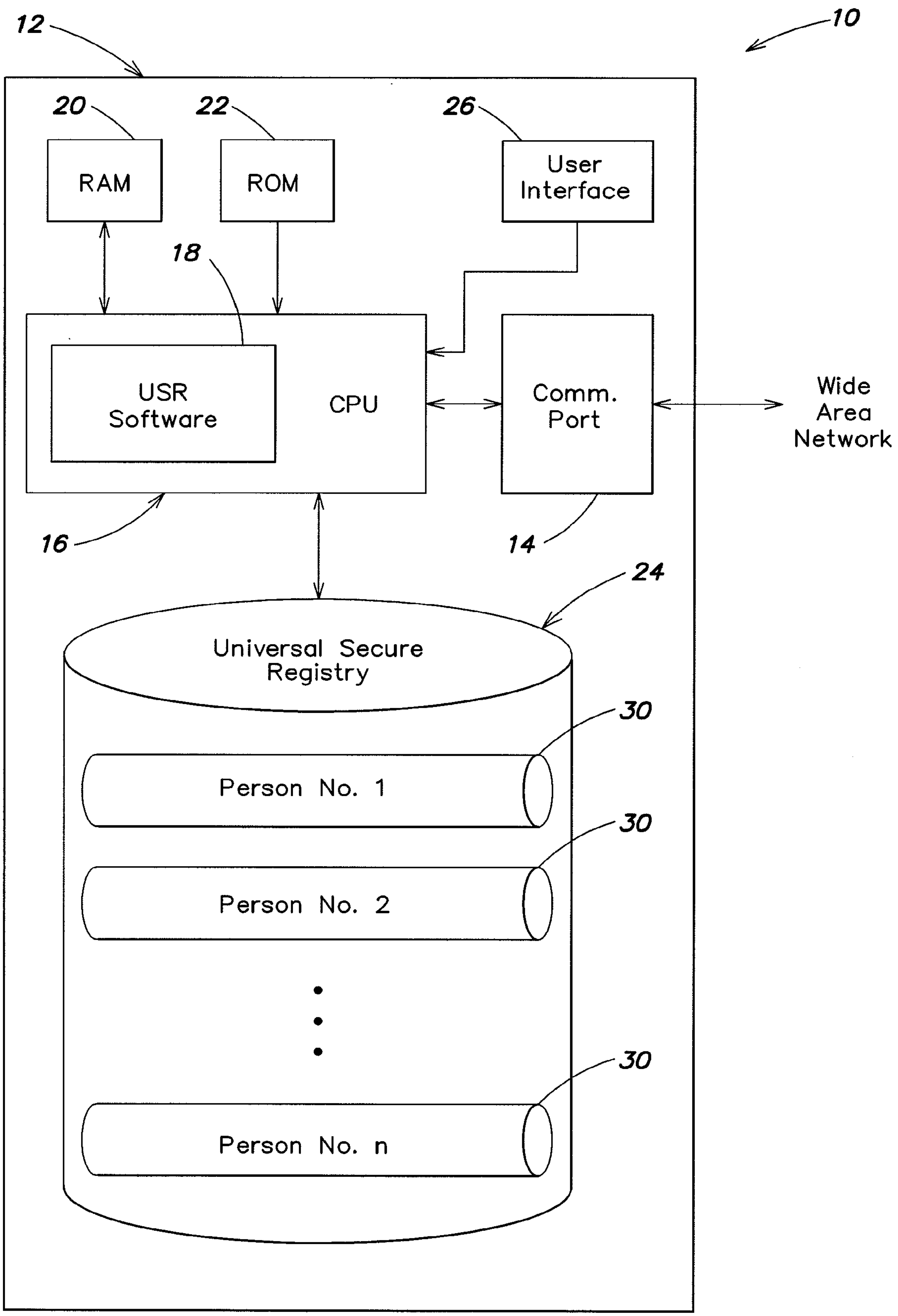
12
10
20
22
26
RAM
ROM
User Interface
18
USR Software
CPU
Comm. Port
Wide Area Network
16
14
24
Universal Secure Registry
30
Person No. 1
30
Person No. 2
30
Person No. n

FIG. 1

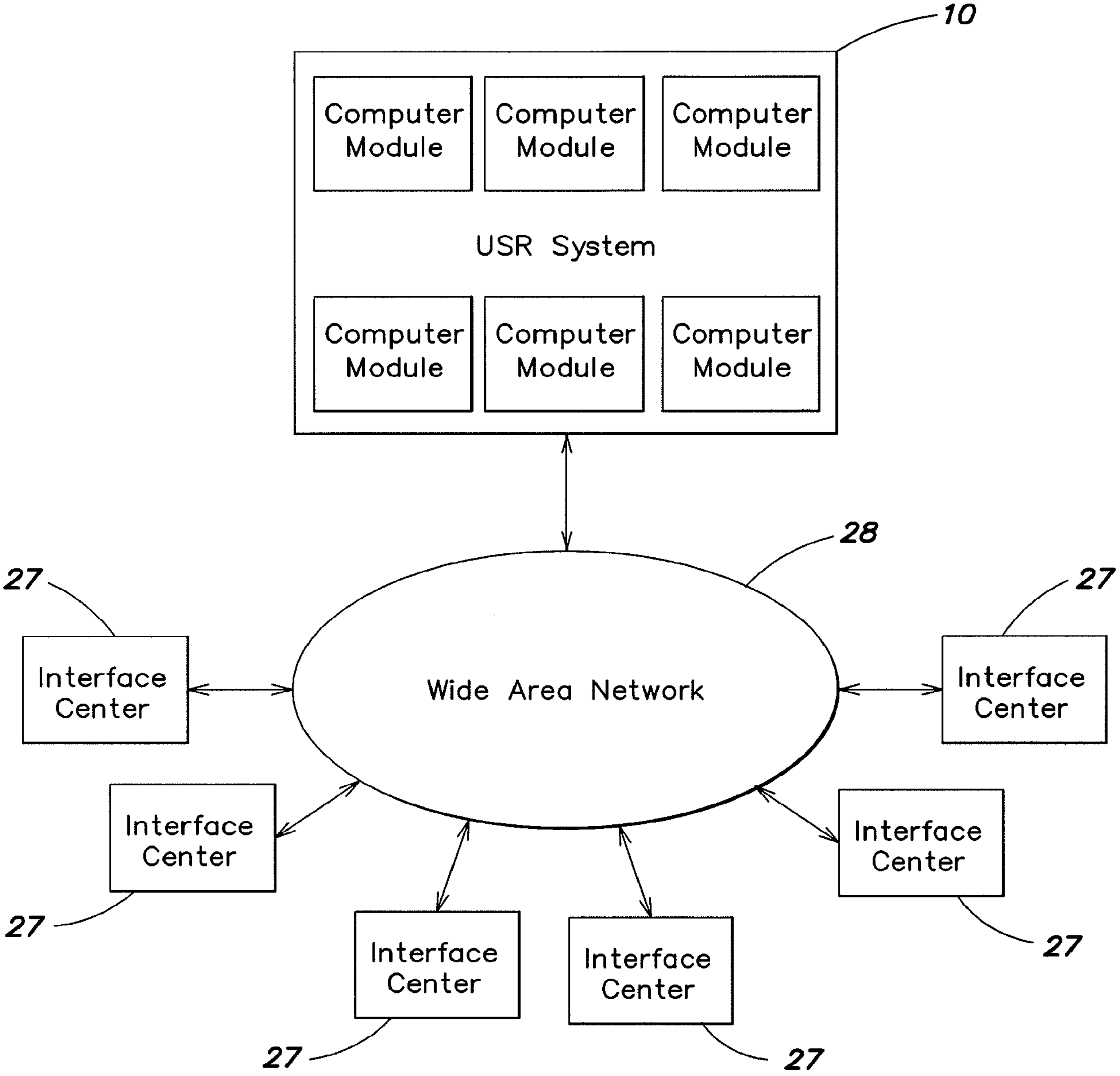
10
Computer Module
Computer Module
Computer Module
USR System
Computer Module
Computer Module
Computer Module
28
27
27
Interface Center
Wide Area Network
Interface Center
Interface Center
Interface Center
27
Interface Center
Interface Center
27
27
27

FIG. 2

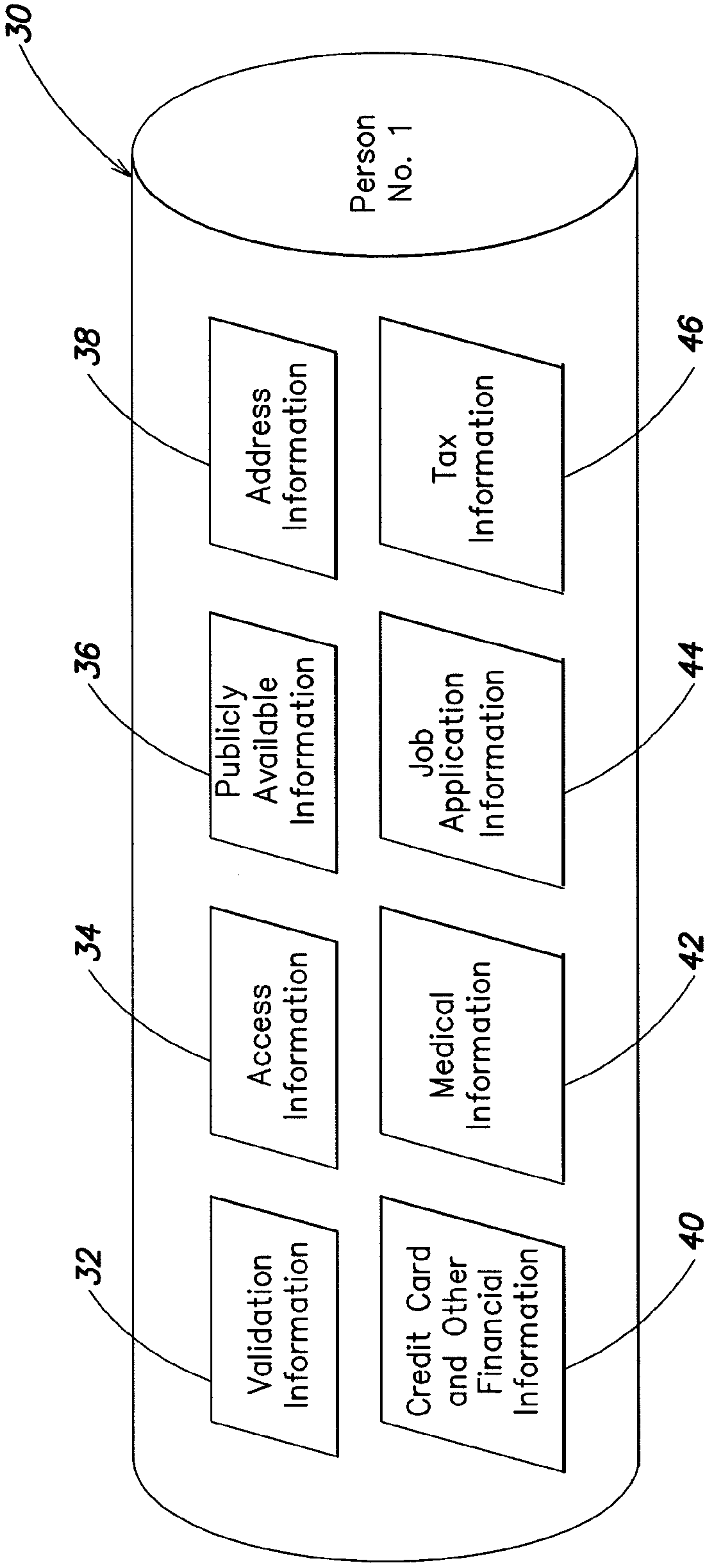
30
Person No. 1
38
Address Information
36
Publicly Available Information
34
Access Information
32
Validation Information
46
Tax Information
44
Job Application Information
42
Medical Information
40
Credit Card and Other Financial Information

FIG. 3

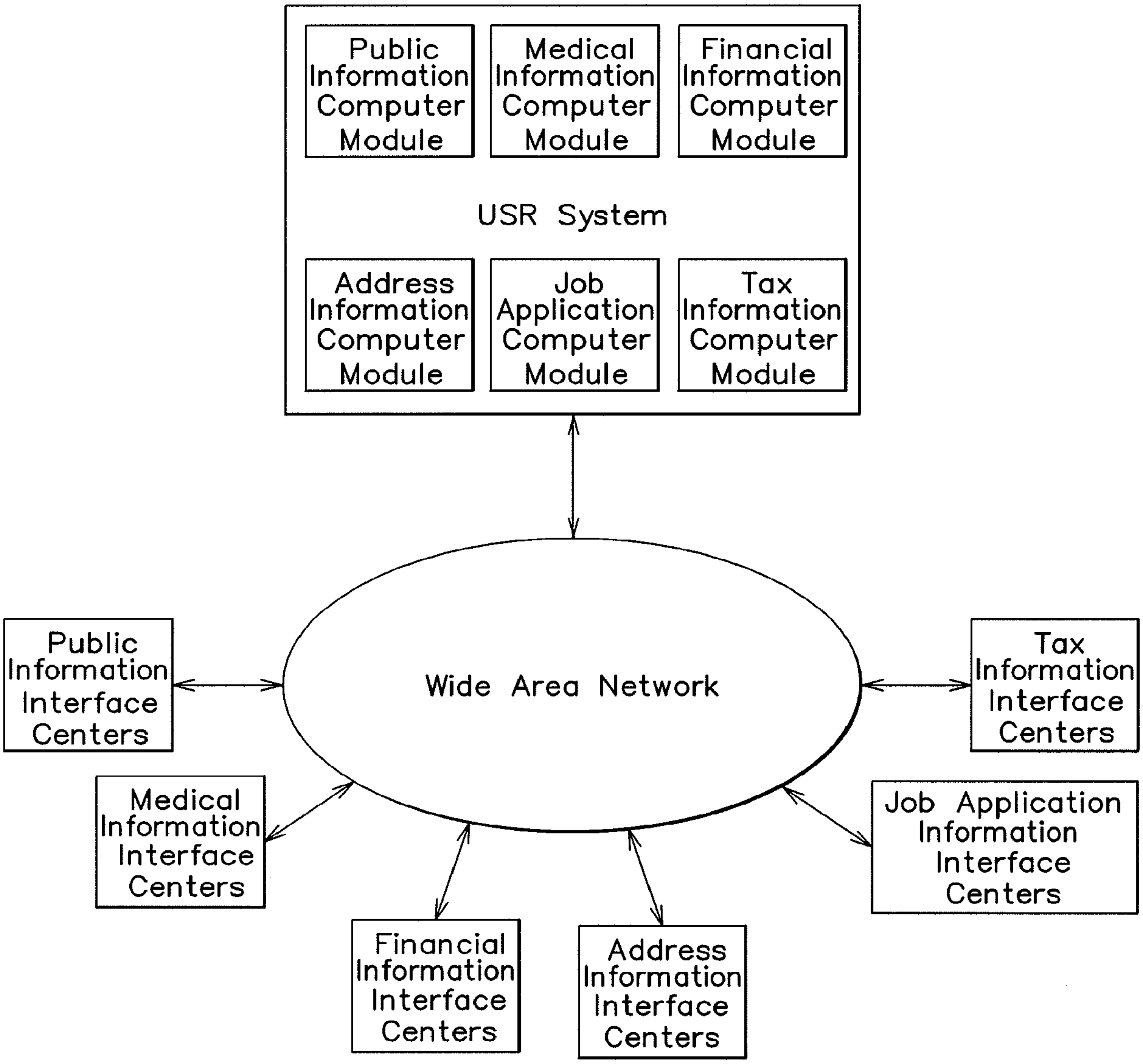
Public Information Computer Module
Medical Information Computer Module
Financial Information Computer Module
USR System
Address Information Computer Module
Job Application Computer Module
Tax Information Computer Module
Wide Area Network
Public Information Interface Centers
Tax Information Interface Centers
Medical Information Interface Centers
Job Application Information Interface Centers
Financial Information Interface Centers
Address Information Interface Centers

FIG. 4

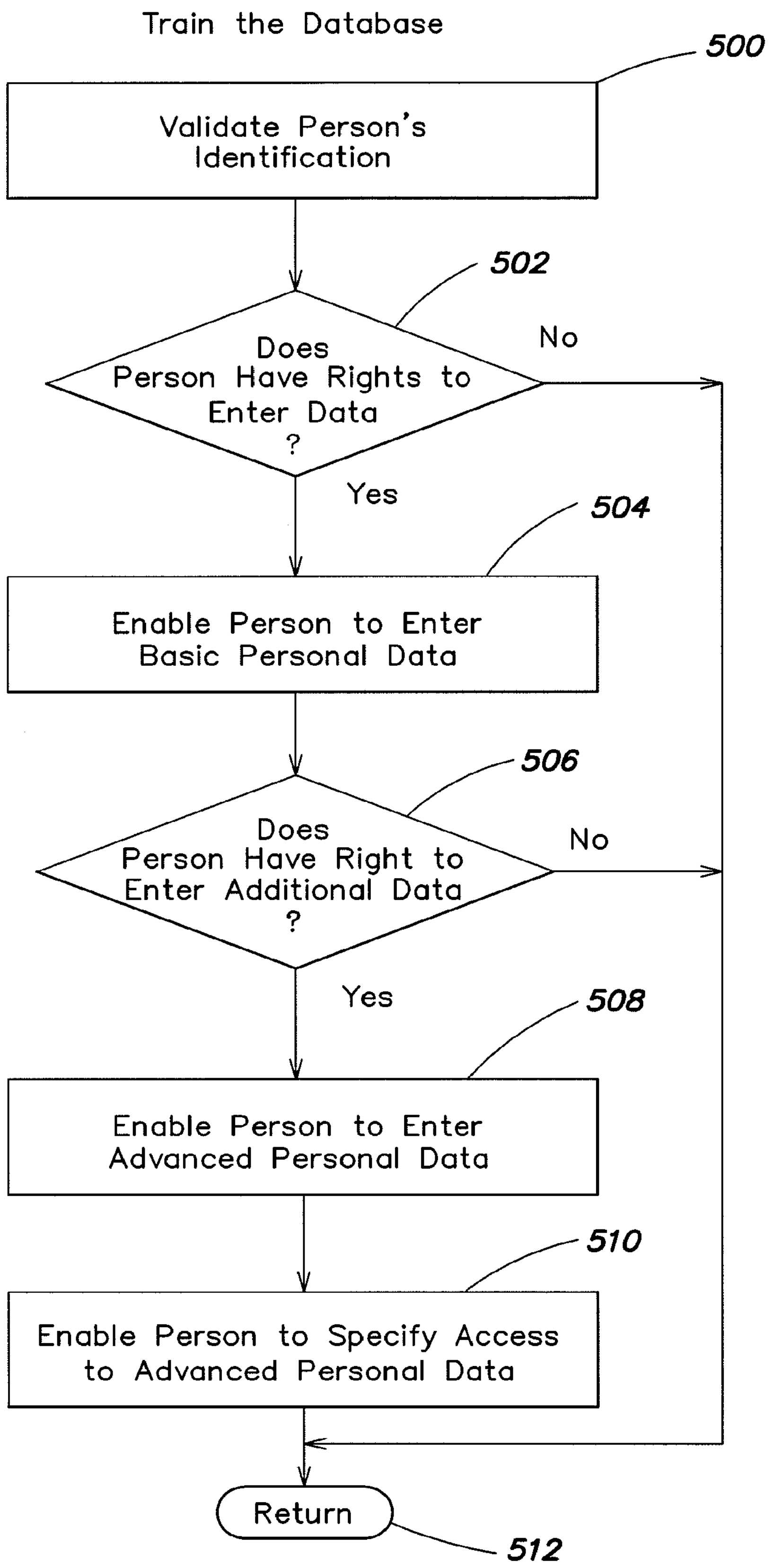
Train the Database
500
Validate Person's Identification
502
Does Person Have Rights to Enter Data ?
No
Yes
504
Enable Person to Enter Basic Personal Data
506
Does Person Have Right to Enter Additional Data ?
No
Yes
508
Enable Person to Enter Advanced Personal Data
510
Enable Person to Specify Access to Advanced Personal Data
Return
512

FIG. 5

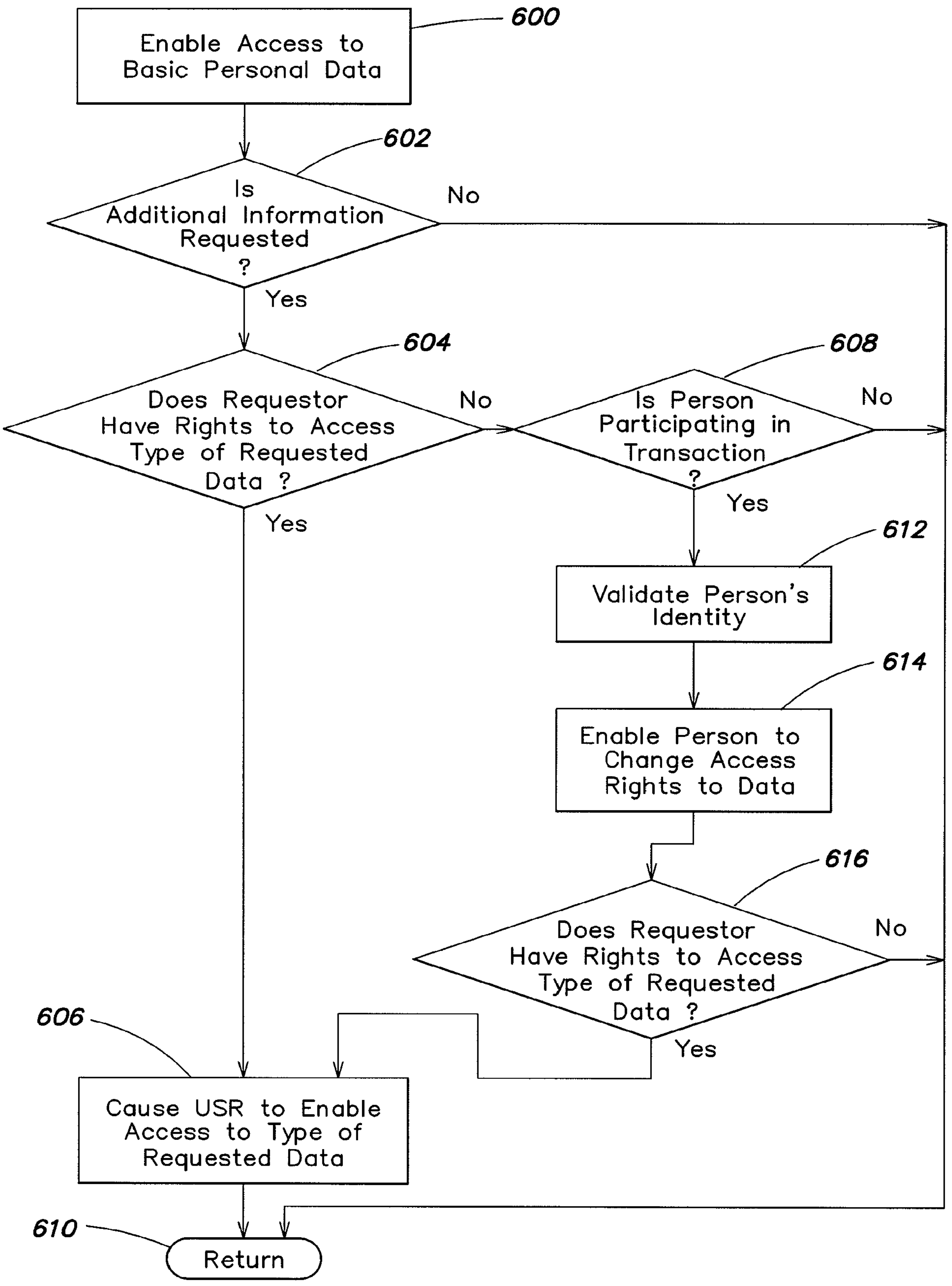
Enable Access to Basic Personal Data
600
Is Additional Information Requested ?
602
No
Yes
Does Requestor Have Rights to Access Type of Requested Data ?
604
No
Yes
Is Person Participating in Transaction ?
608
No
Yes
Validate Person's Identity
612
Enable Person to Change Access Rights to Data
614
Does Requestor Have Rights to Access Type of Requested Data ?
616
No
Yes
606
Cause USR to Enable Access to Type of Requested Data
610
Return

FIG. 6

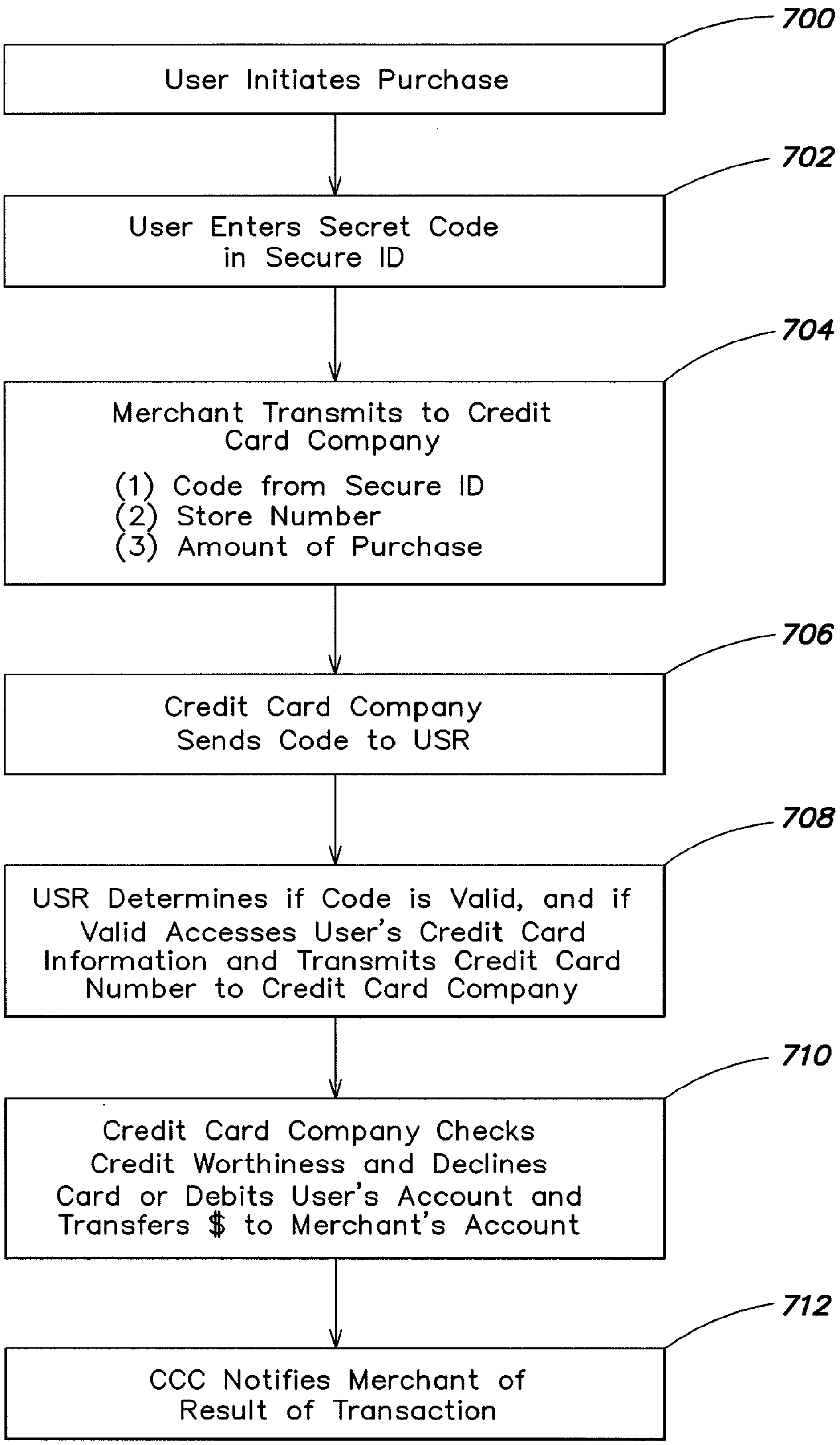
700
User Initiates Purchase
702
User Enters Secret Code in Secure ID
704
Merchant Transmits to Credit Card Company
(1) Code from Secure ID
(2) Store Number
(3) Amount of Purchase
706
Credit Card Company Sends Code to USR
708
USR Determines if Code is Valid, and if Valid Accesses User's Credit Card Information and Transmits Credit Card Number to Credit Card Company
710
Credit Card Company Checks Credit Worthiness and Declines Card or Debits User's Account and Transfers $ to Merchant's Account
712
CCC Notifies Merchant of Result of Transaction

FIG. 7

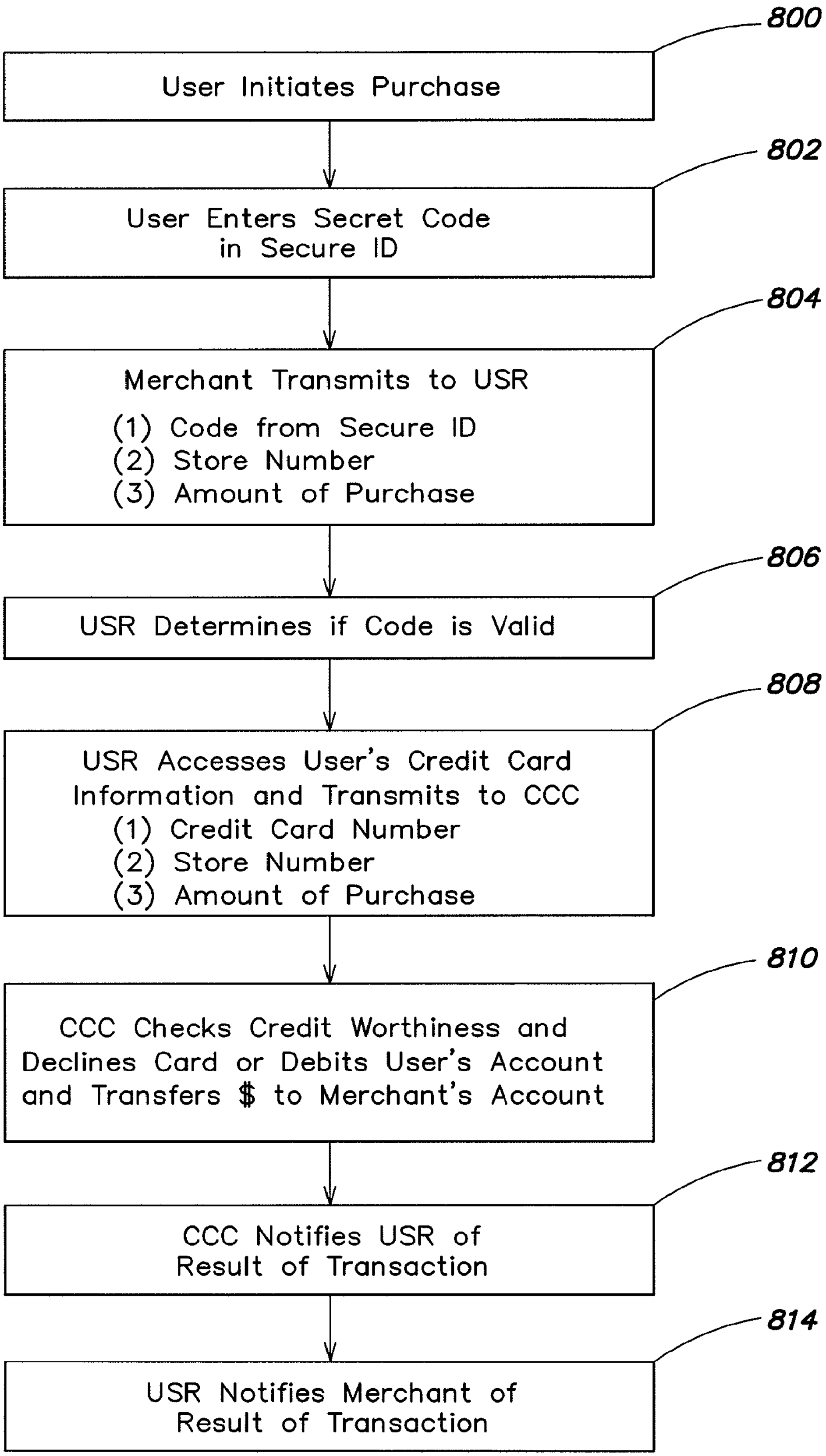
800
User Initiates Purchase
802
User Enters Secret Code in Secure ID
804
Merchant Transmits to USR
(1) Code from Secure ID
(2) Store Number
(3) Amount of Purchase
806
USR Determines if Code is Valid
808
USR Accesses User's Credit Card Information and Transmits to CCC
(1) Credit Card Number
(2) Store Number
(3) Amount of Purchase
810
CCC Checks Credit Worthiness and Declines Card or Debits User's Account and Transfers $ to Merchant's Account
812
CCC Notifies USR of Result of Transaction
814
USR Notifies Merchant of Result of Transaction

FIG. 8

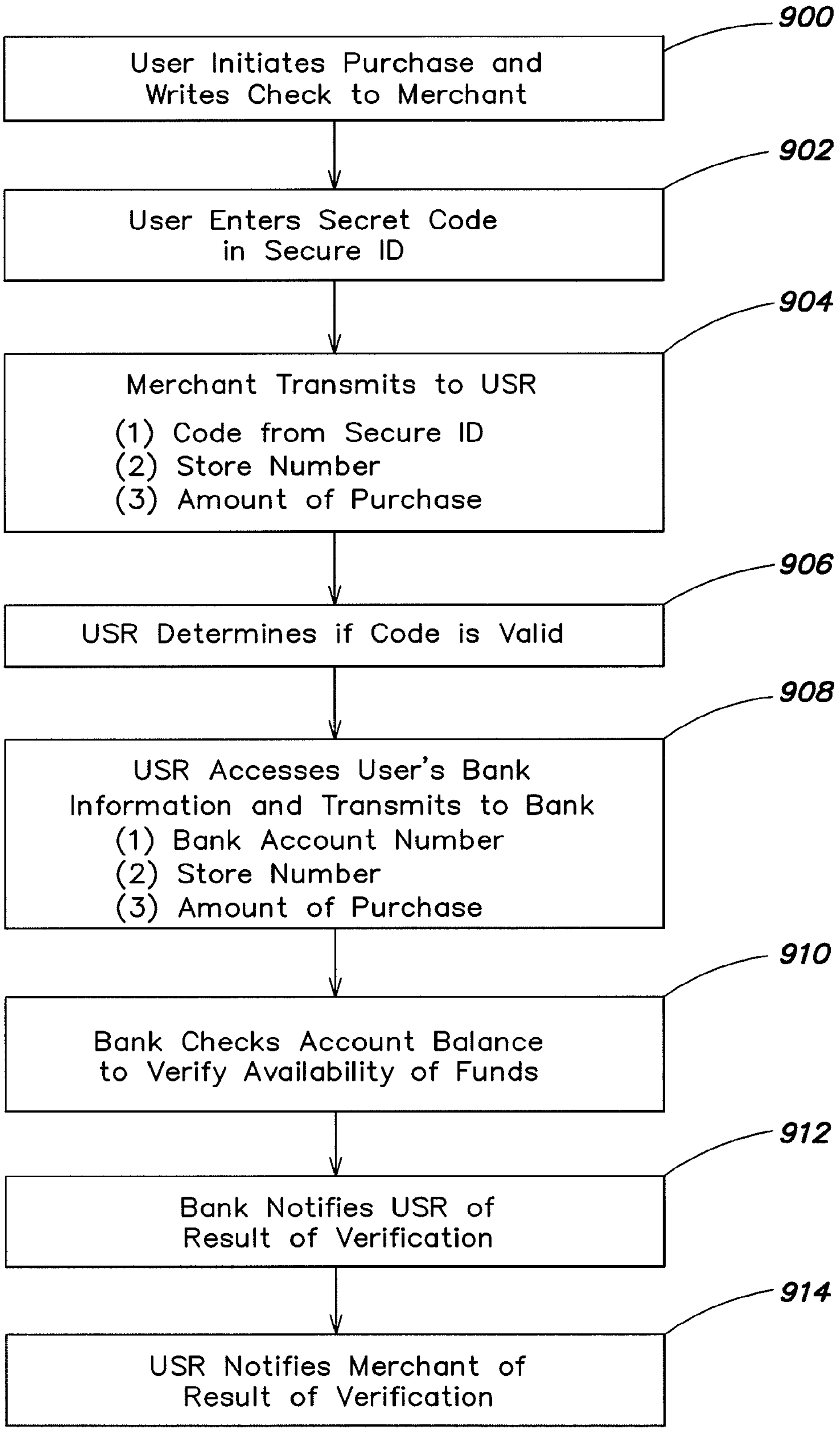
900
User Initiates Purchase and Writes Check to Merchant
902
User Enters Secret Code in Secure ID
904
Merchant Transmits to USR
(1) Code from Secure ID
(2) Store Number
(3) Amount of Purchase
906
USR Determines if Code is Valid
908
USR Accesses User's Bank Information and Transmits to Bank
(1) Bank Account Number
(2) Store Number
(3) Amount of Purchase
910
Bank Checks Account Balance to Verify Availability of Funds
912
Bank Notifies USR of Result of Verification
914
USR Notifies Merchant of Result of Verification

FIG. 9

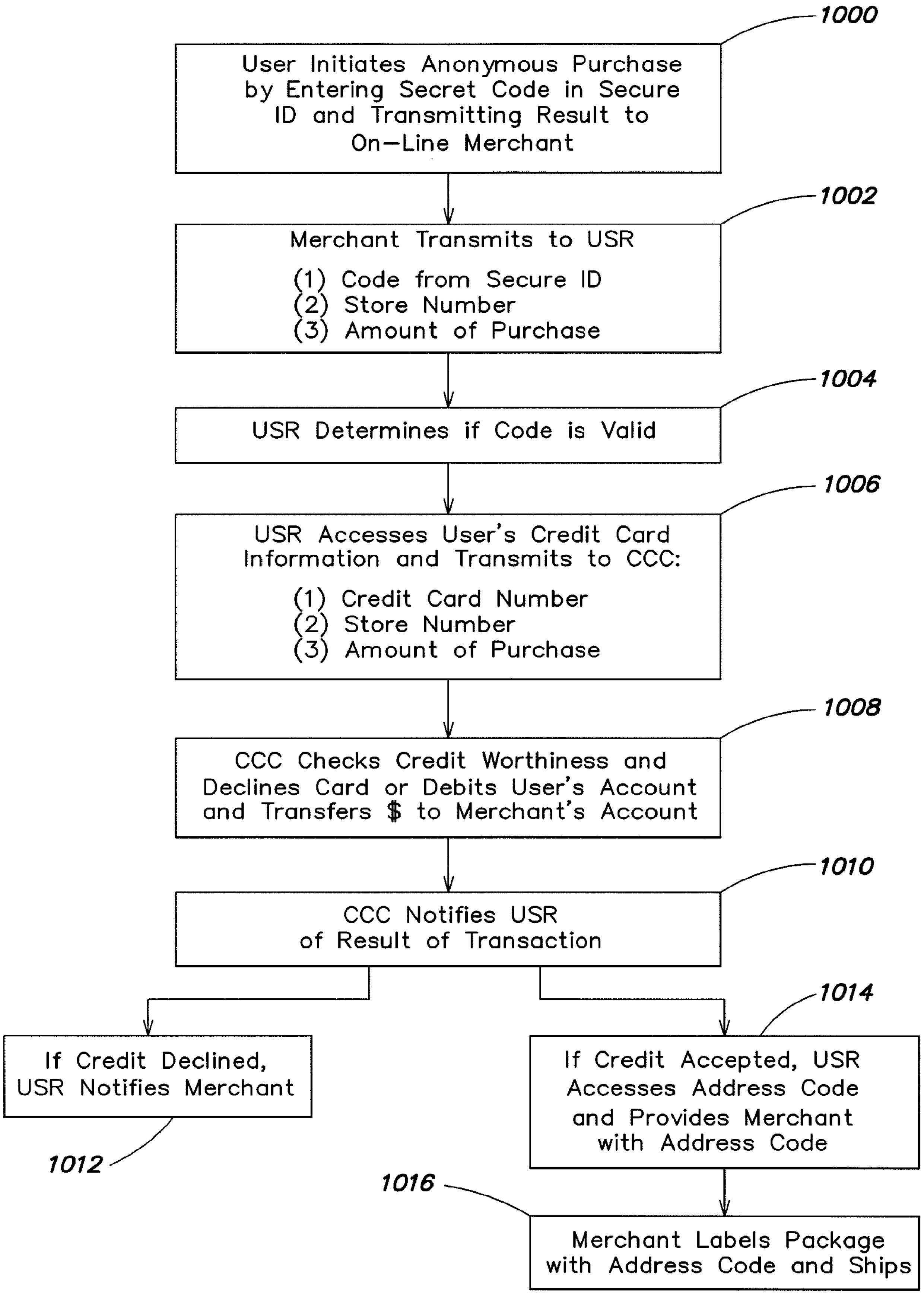
1000
User Initiates Anonymous Purchase by Entering Secret Code in Secure ID and Transmitting Result to On-Line Merchant
1002
Merchant Transmits to USR
(1) Code from Secure ID
(2) Store Number
(3) Amount of Purchase
1004
USR Determines if Code is Valid
1006
USR Accesses User's Credit Card Information and Transmits to CCC:
(1) Credit Card Number
(2) Store Number
(3) Amount of Purchase
1008
CCC Checks Credit Worthiness and Declines Card or Debits User's Account and Transfers $ to Merchant's Account
1010
CCC Notifies USR of Result of Transaction
1014
If Credit Declined, USR Notifies Merchant
1012
If Credit Accepted, USR Accesses Address Code and Provides Merchant with Address Code
1016
Merchant Labels Package with Address Code and Ships

FIG. 10

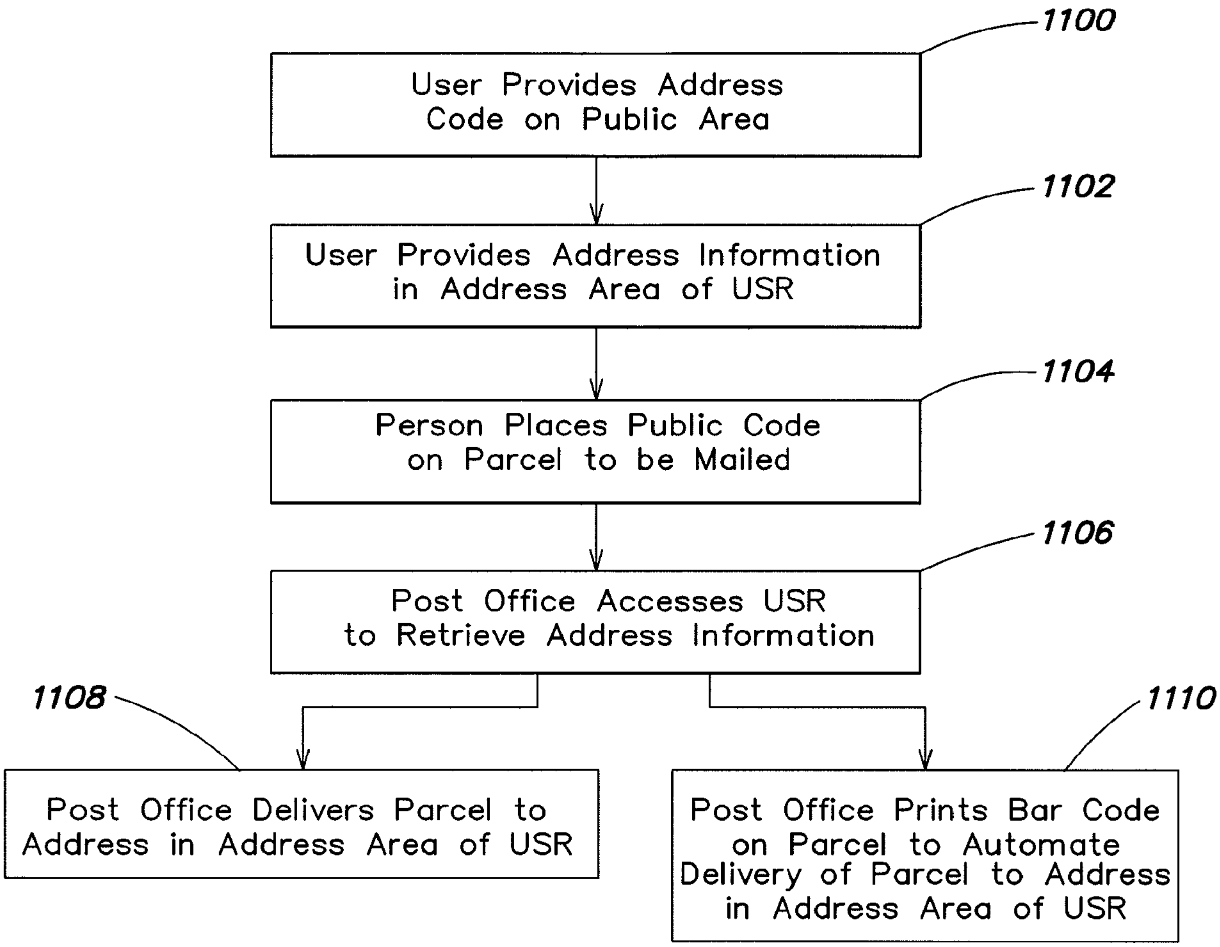
1100
User Provides Address Code on Public Area
1102
User Provides Address Information in Address Area of USR
1104
Person Places Public Code on Parcel to be Mailed
1106
Post Office Accesses USR to Retrieve Address Information
1108
Post Office Delivers Parcel to Address in Address Area of USR
1110
Post Office Prints Bar Code on Parcel to Automate Delivery of Parcel to Address in Address Area of USR

FIG. 11

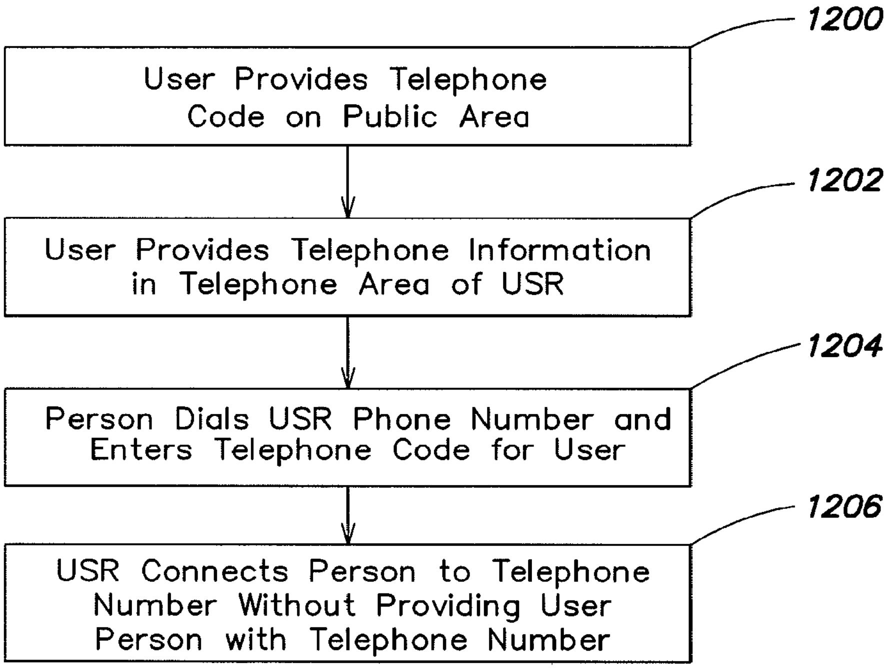
1200
User Provides Telephone Code on Public Area
1202
User Provides Telephone Information in Telephone Area of USR
1204
Person Dials USR Phone Number and Enters Telephone Code for User
1206
USR Connects Person to Telephone Number Without Providing User Person with Telephone Number

FIG. 12

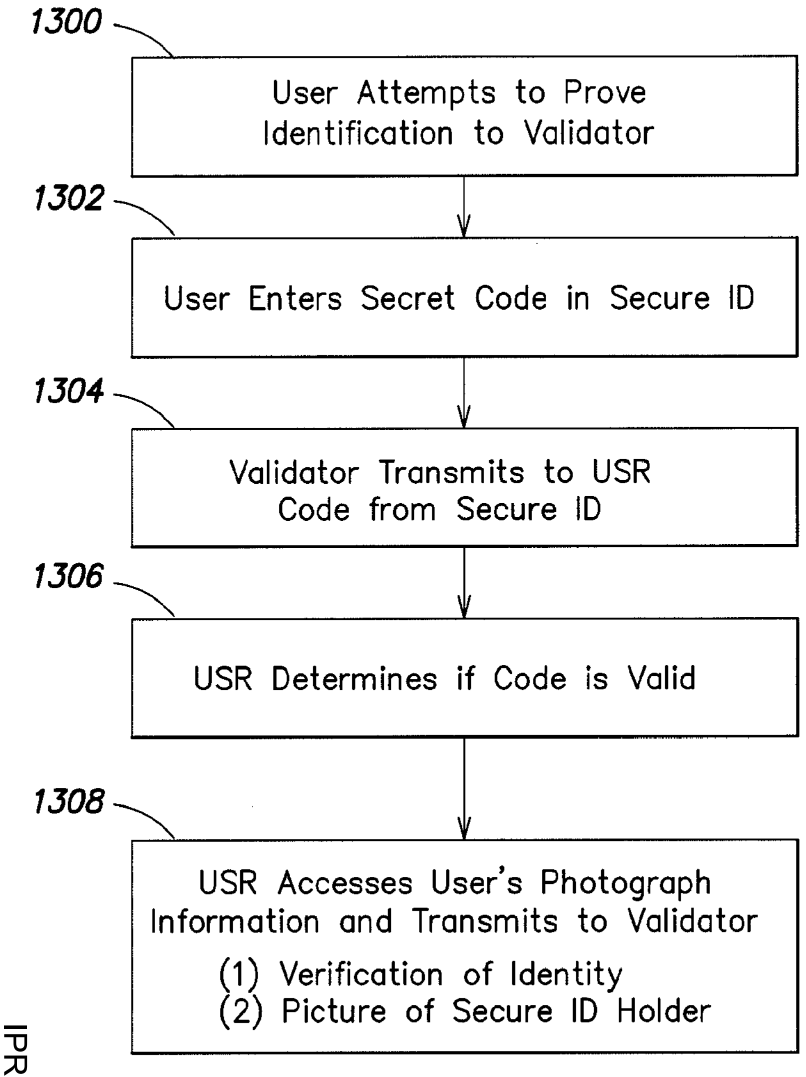
1300
User Attempts to Prove Identification to Validator
1302
User Enters Secret Code in Secure ID
1304
Validator Transmits to USR Code from Secure ID
1306
USR Determines if Code is Valid
1308
USR Accesses User's Photograph Information and Transmits to Validator
(1) Verification of Identity
(2) Picture of Secure ID Holder

FIG. 13

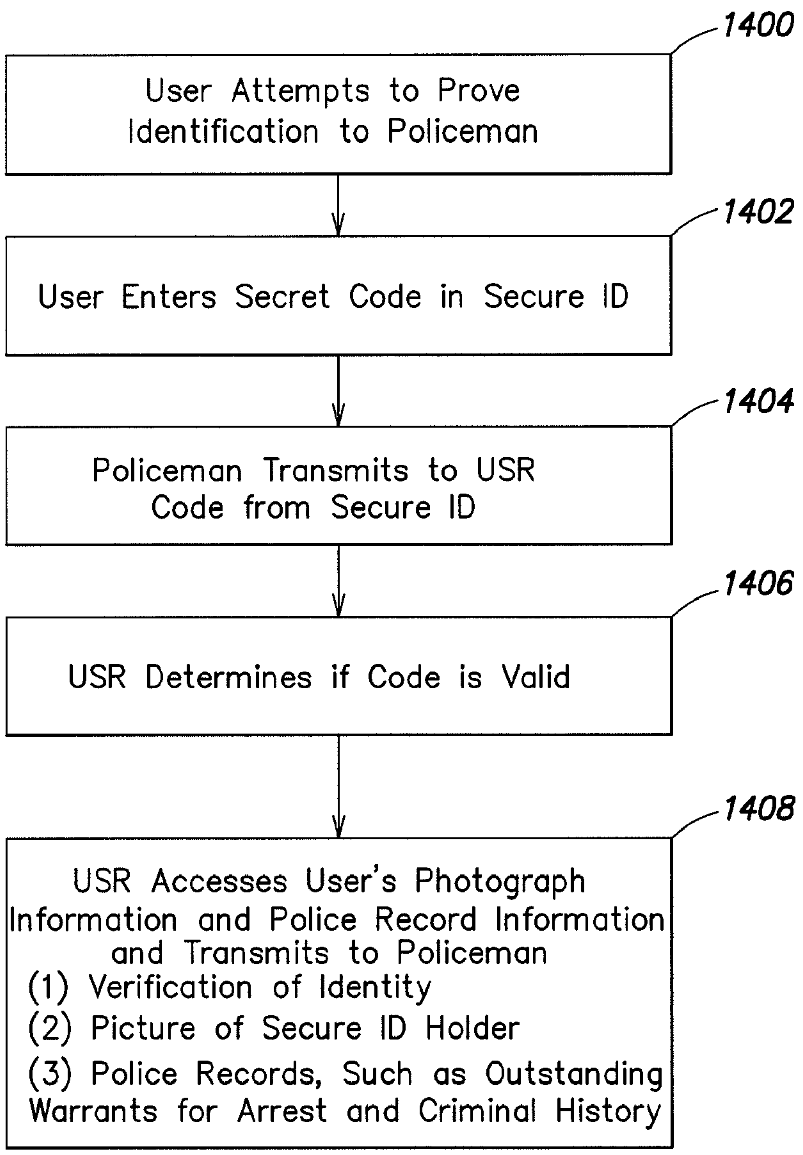
1400
User Attempts to Prove Identification to Policeman
1402
User Enters Secret Code in Secure ID
1404
Policeman Transmits to USR Code from Secure ID
1406
USR Determines if Code is Valid
1408
USR Accesses User's Photograph Information and Police Record Information and Transmits to Policeman
(1) Verification of Identity
(2) Picture of Secure ID Holder
(3) Police Records, Such as Outstanding Warrants for Arrest and Criminal History

FIG. 14

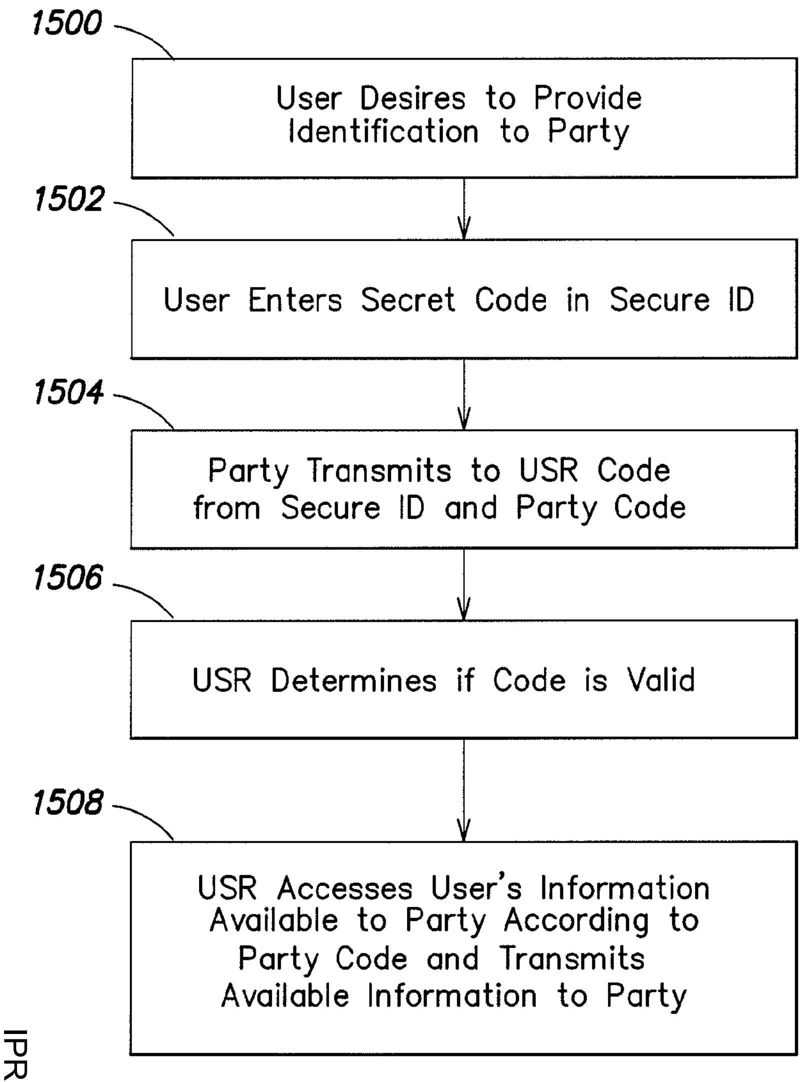
1500
User Desires to Provide Identification to Party
1502
User Enters Secret Code in Secure ID
1504
Party Transmits to USR Code from Secure ID and Party Code
1506
USR Determines if Code is Valid
1508
USR Accesses User's Information Available to Party According to Party Code and Transmits Available Information to Party

FIG. 15

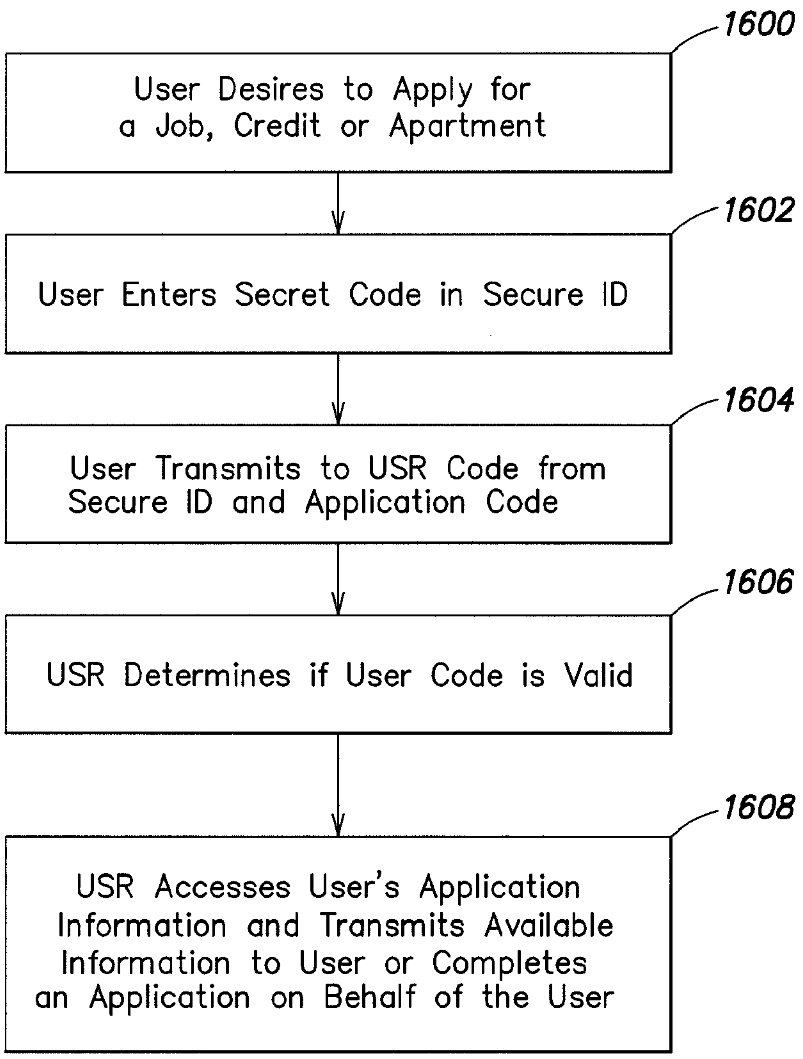
1600
User Desires to Apply for a Job, Credit or Apartment
1602
User Enters Secret Code in Secure ID
1604
User Transmits to USR Code from Secure ID and Application Code
1606
USR Determines if User Code is Valid
1608
USR Accesses User's Application Information and Transmits Available Information to User or Completes an Application on Behalf of the User

FIG. 16

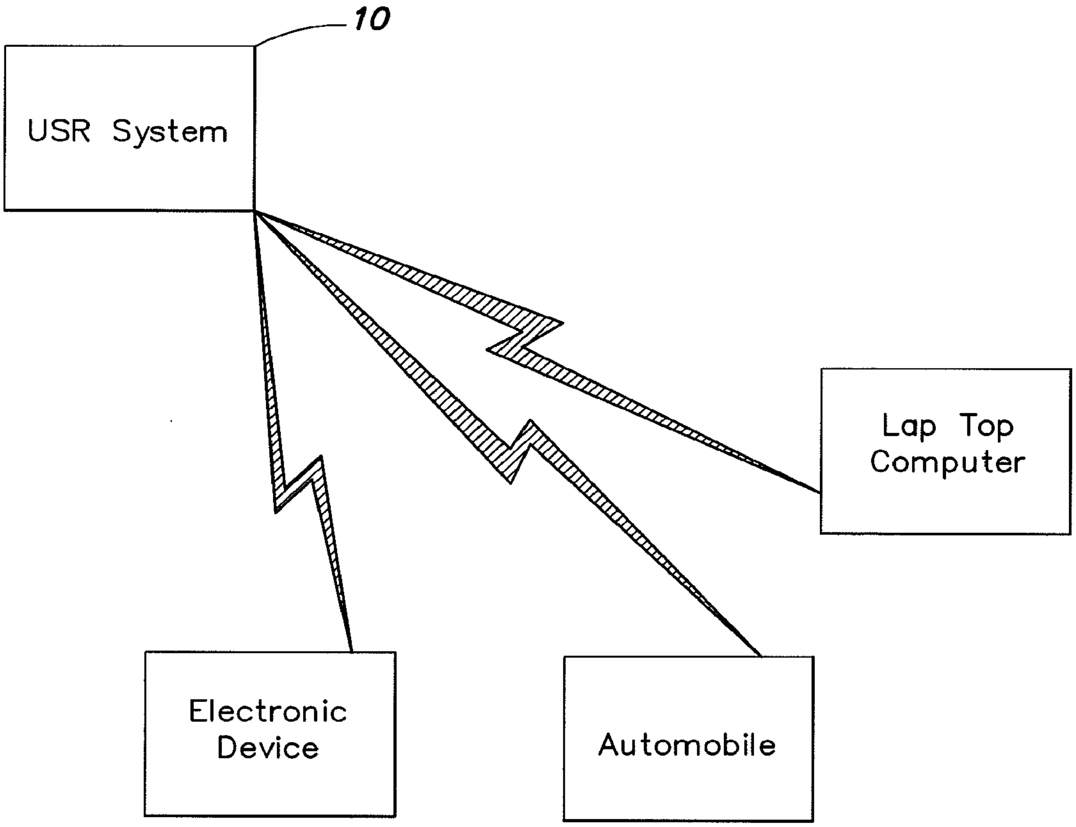
10
USR System
Lap Top Computer
Electronic Device
Automobile

FIG. 17

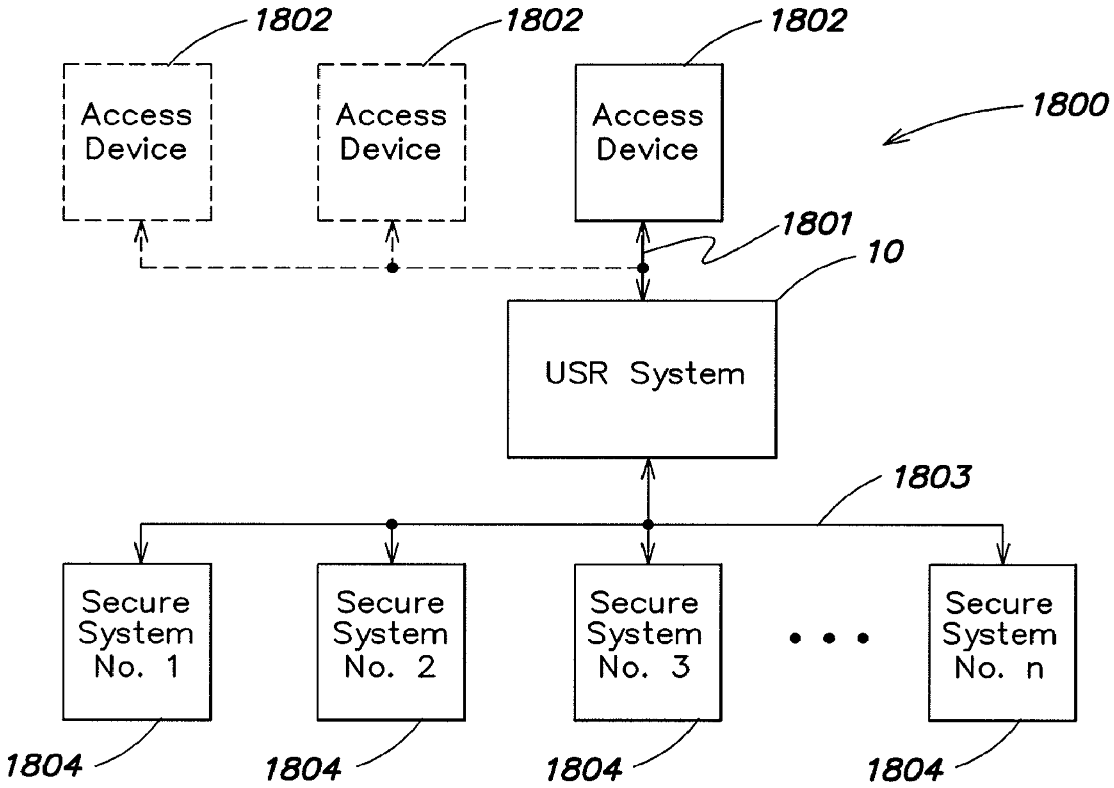

FIG. 18A

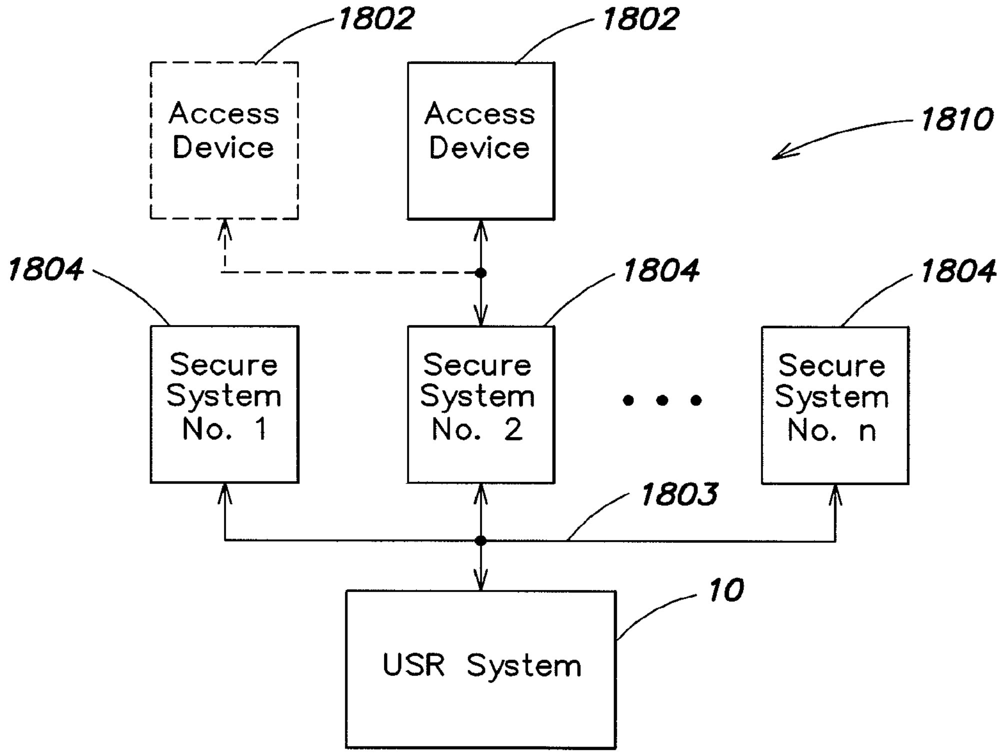

FIG. 18B

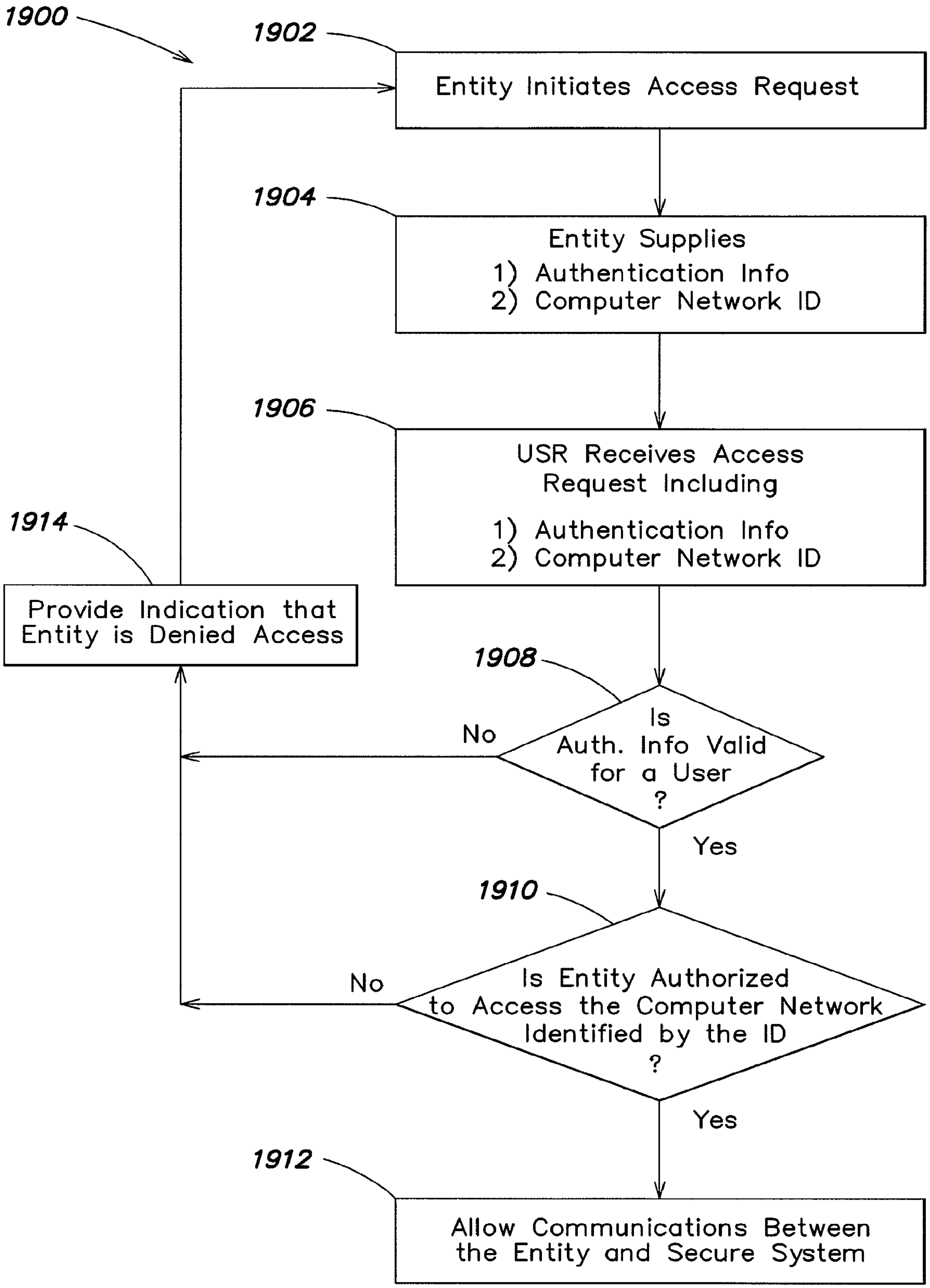
1900
1902
Entity Initiates Access Request
1904
Entity Supplies
1) Authentication Info
2) Computer Network ID
1906
USR Receives Access Request Including
1) Authentication Info
2) Computer Network ID
1914
Provide Indication that Entity is Denied Access
1908
Is Auth. Info Valid for a User ?
No
Yes
1910
Is Entity Authorized to Access the Computer Network Identified by the ID ?
No
Yes
1912
Allow Communications Between the Entity and Secure System

FIG. 19

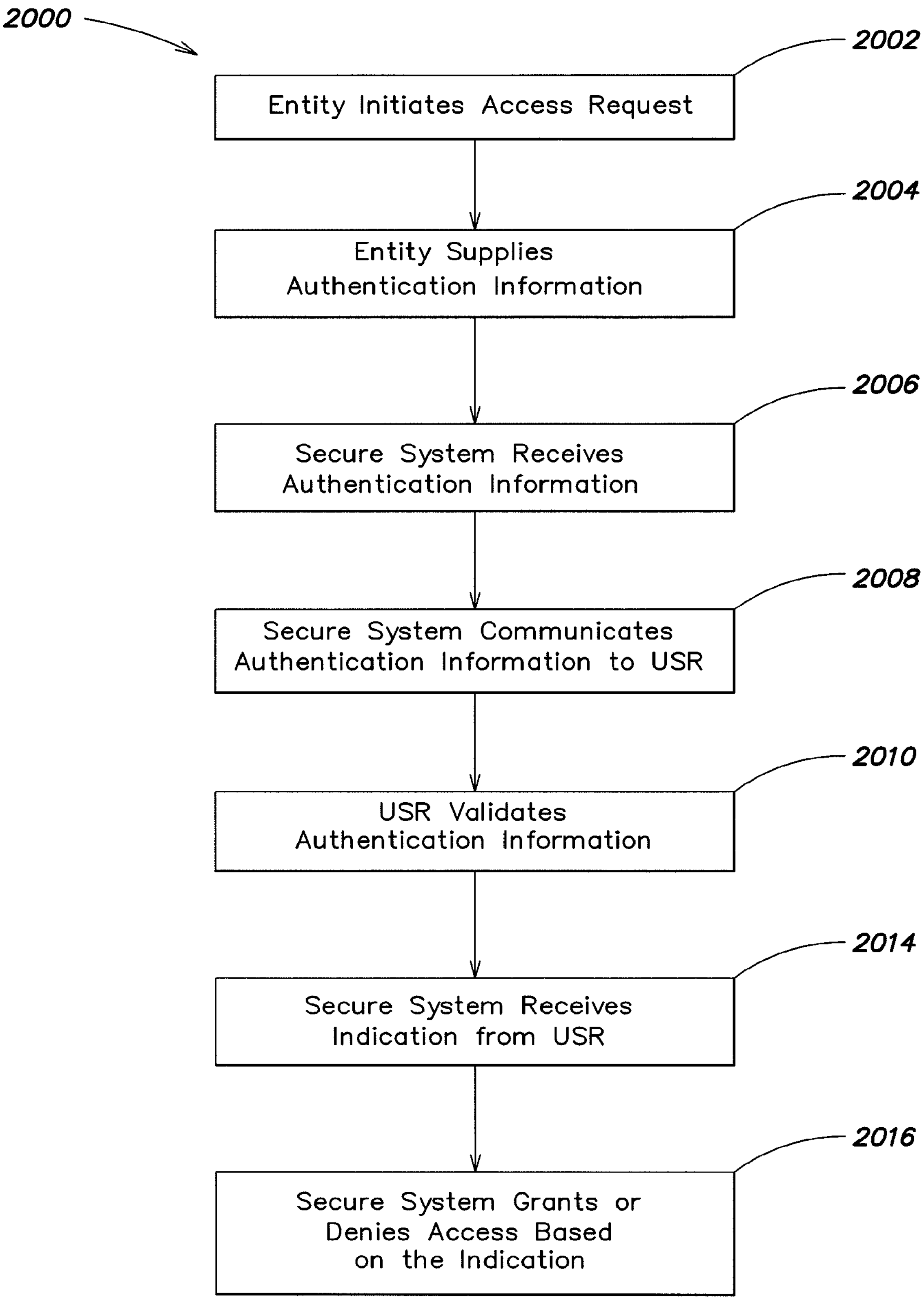
2000
2002
Entity Initiates Access Request
2004
Entity Supplies Authentication Information
2006
Secure System Receives Authentication Information
2008
Secure System Communicates Authentication Information to USR
2010
USR Validates Authentication Information
2014
Secure System Receives Indication from USR
2016
Secure System Grants or Denies Access Based on the Indication

FIG. 20

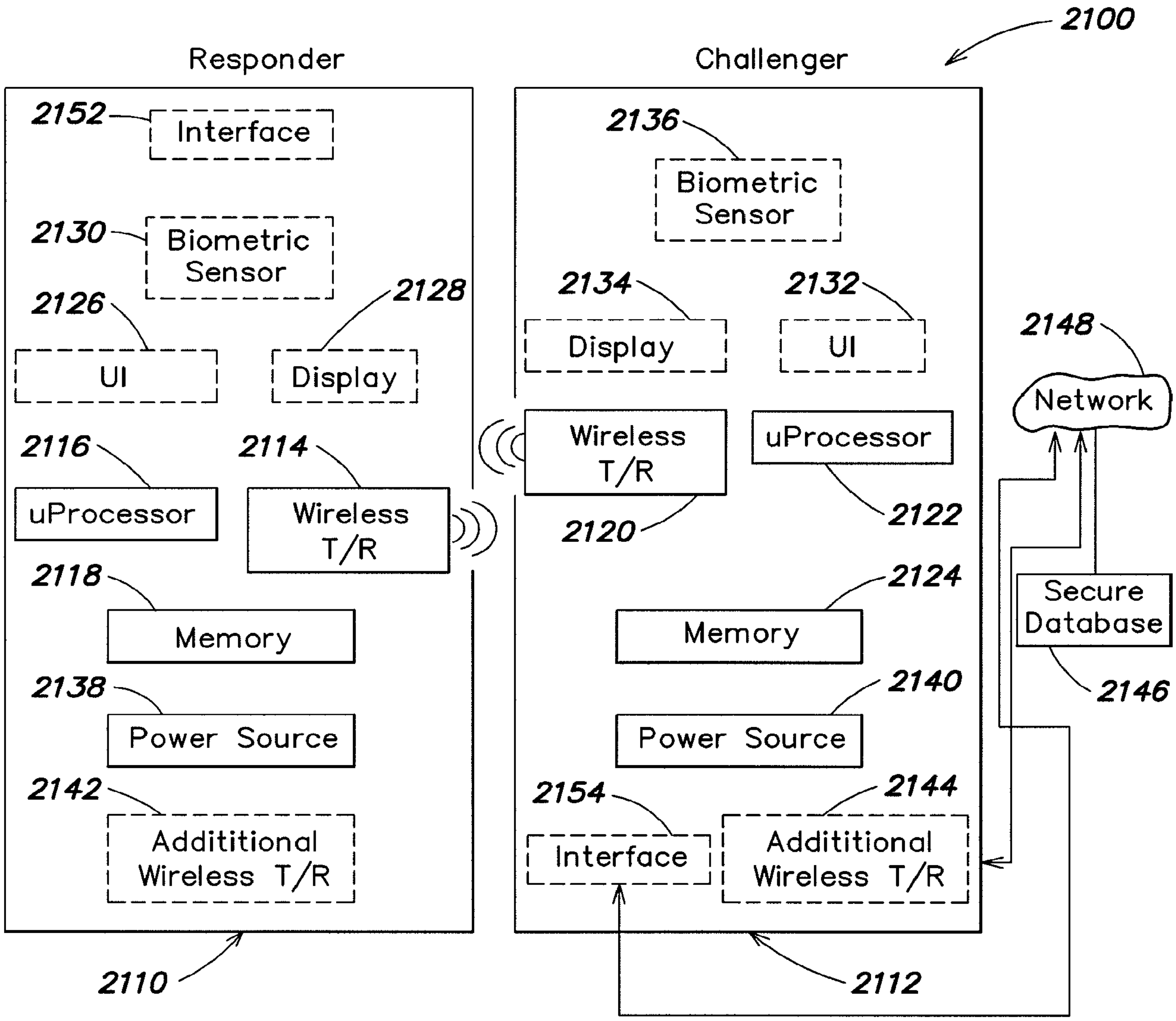
2100
Responder
Challenger
2152
Interface
2130
Biometric Sensor
2126
2128
UI
Display
2116
2114
uProcessor
Wireless T/R
2118
Memory
2138
Power Source
2142
Addititional Wireless T/R
2110
2136
Biometric Sensor
2134
2132
Display
UI
Wireless T/R
uProcessor
2120
2122
2124
Memory
2140
Power Source
2154
2144
Interface
Addititional Wireless T/R
2112
2148
Network
Secure Database
2146

FIG. 21

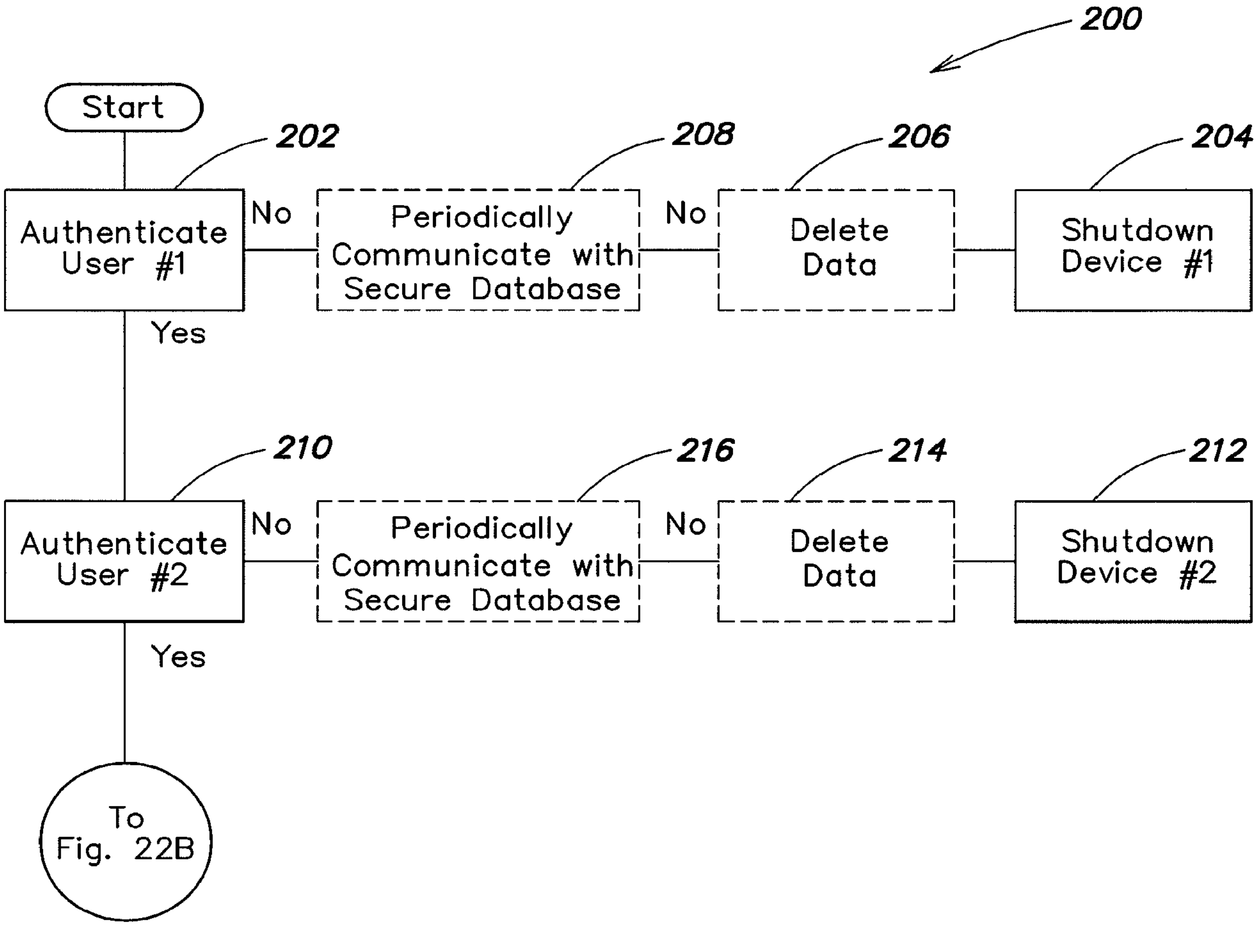
200
Start
202
Authenticate User #1
No
208
Periodically Communicate with Secure Database
No
206
Delete Data
204
Shutdown Device #1
Yes
210
Authenticate User #2
No
216
Periodically Communicate with Secure Database
No
214
Delete Data
212
Shutdown Device #2
Yes
To Fig. 22B

FIG. 22A

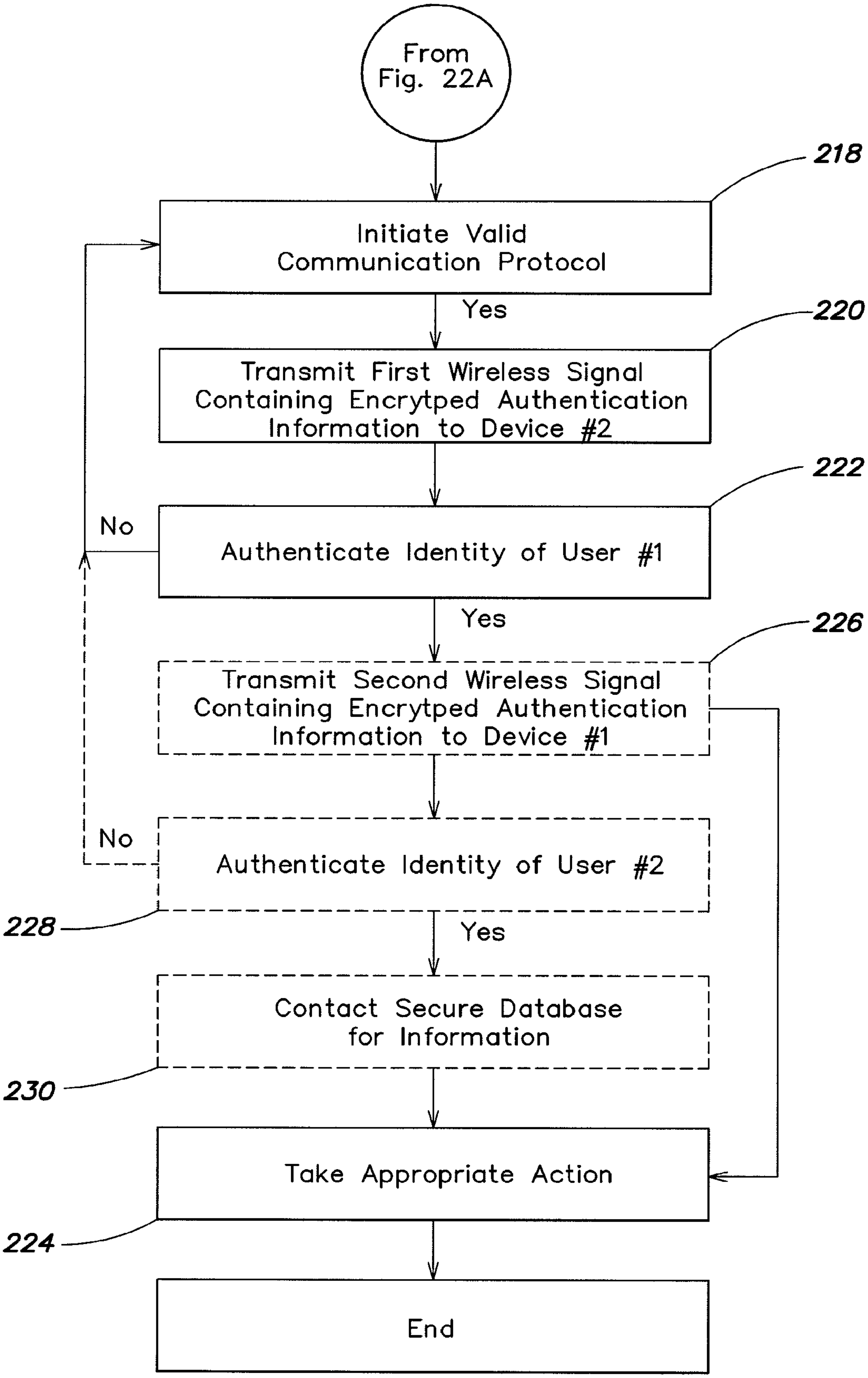
From Fig. 22A
218
Initiate Valid Communication Protocol
Yes
220
Transmit First Wireless Signal Containing Encrytped Authentication Information to Device #2
222
No
Authenticate Identity of User #1
Yes
226
Transmit Second Wireless Signal Containing Encrytped Authentication Information to Device #1
No
Authenticate Identity of User #2
228
Yes
Contact Secure Database for Information
230
Take Appropriate Action
224
End

FIG. 22B

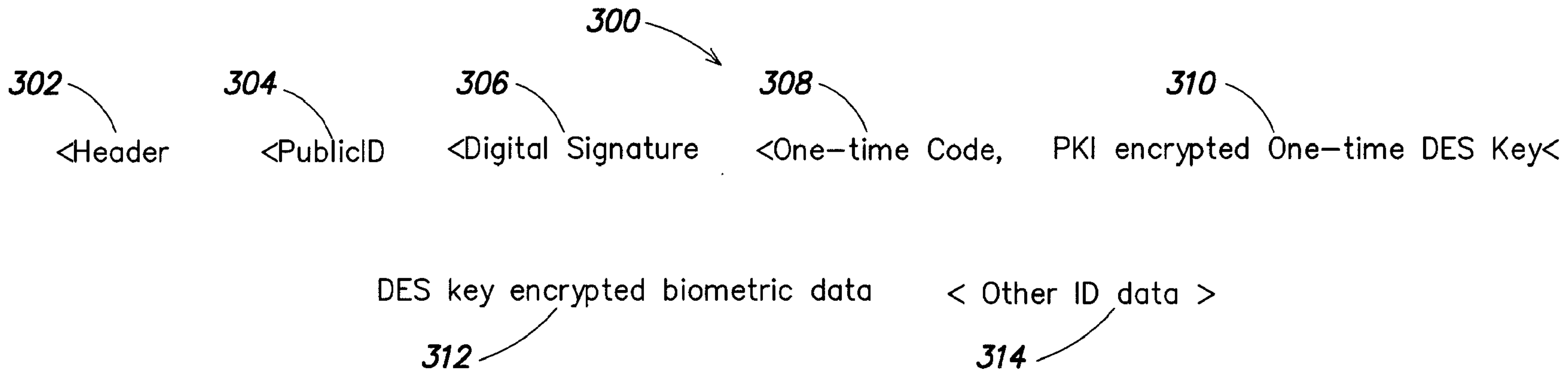
300
302
<Header
304
<PublicID
306
<Digital Signature
308
<One-time Code,
310
PKI encrypted One-time DES Key<
DES key encrypted biometric data
312
< Other ID data >
314

FIG. 23

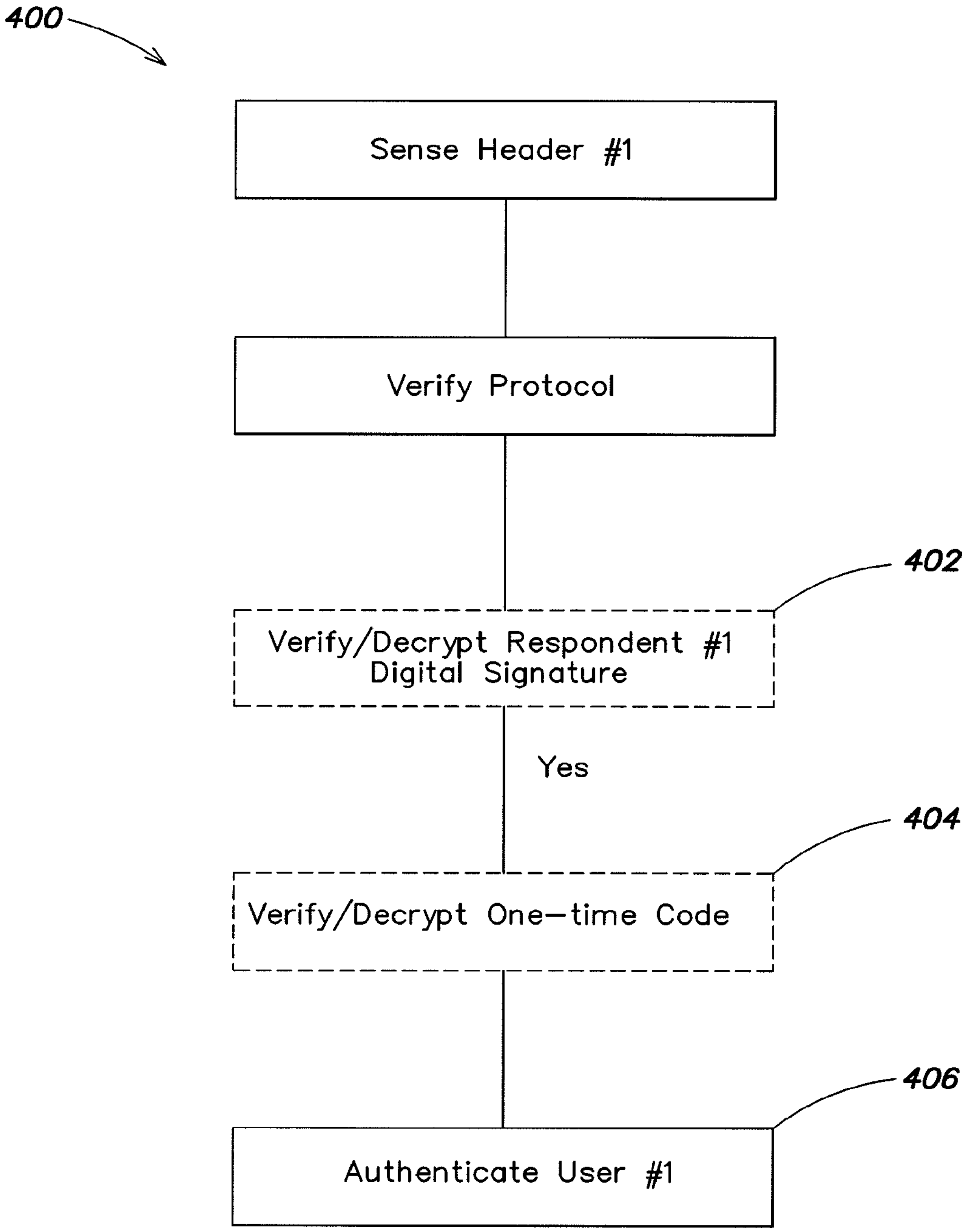
400
Sense Header #1
Verify Protocol
402
Verify/Decrypt Respondent #1 Digital Signature
Yes
404
Verify/Decrypt One–time Code
406
Authenticate User #1

FIG. 24

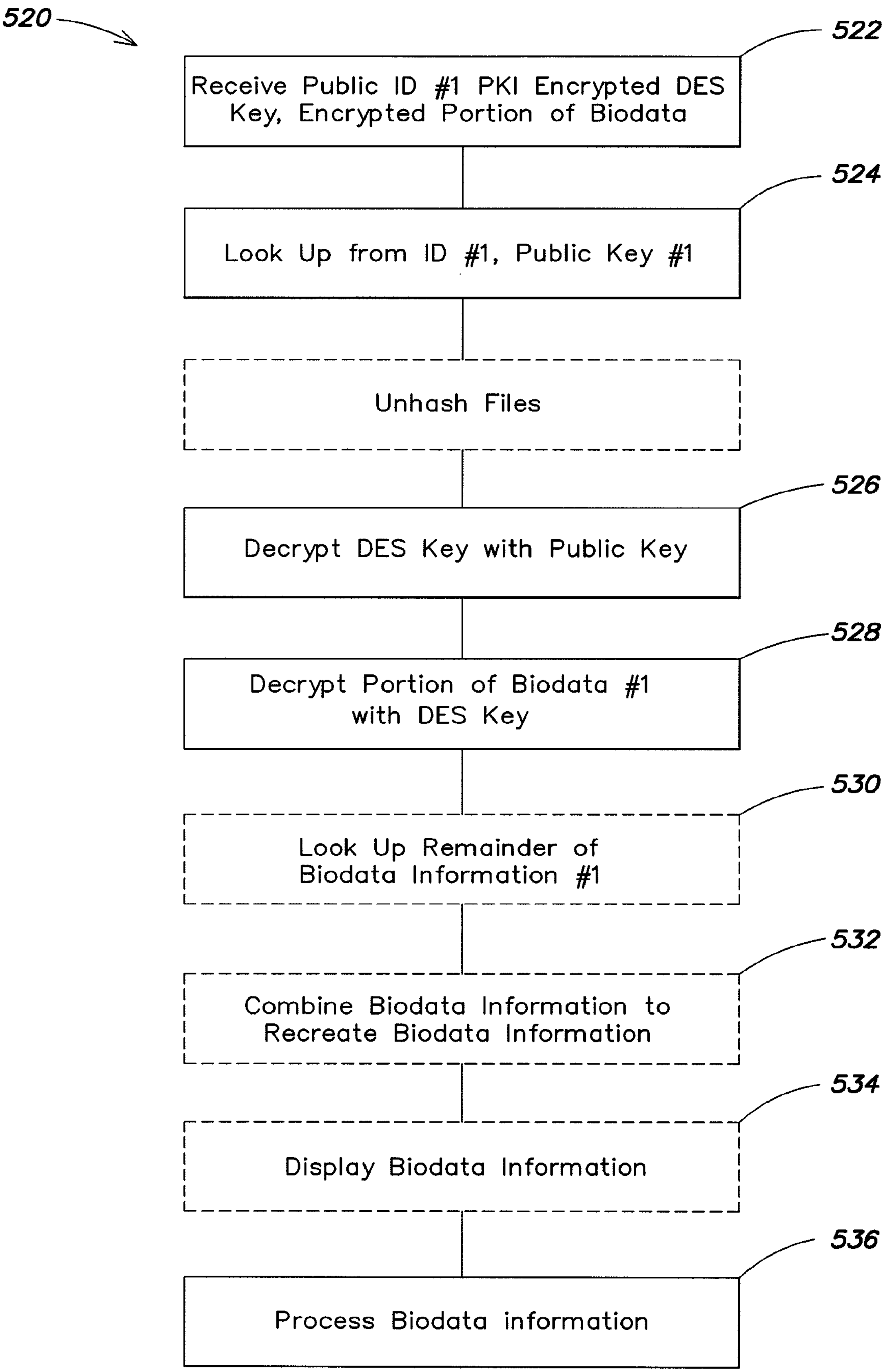
520
522
Receive Public ID #1 PKI Encrypted DES Key, Encrypted Portion of Biodata
524
Look Up from ID #1, Public Key #1
Unhash Files
526
Decrypt DES Key with Public Key
528
Decrypt Portion of Biodata #1 with DES Key
530
Look Up Remainder of Biodata Information #1
532
Combine Biodata Information to Recreate Biodata Information
534
Display Biodata Information
536
Process Biodata information

FIG. 25

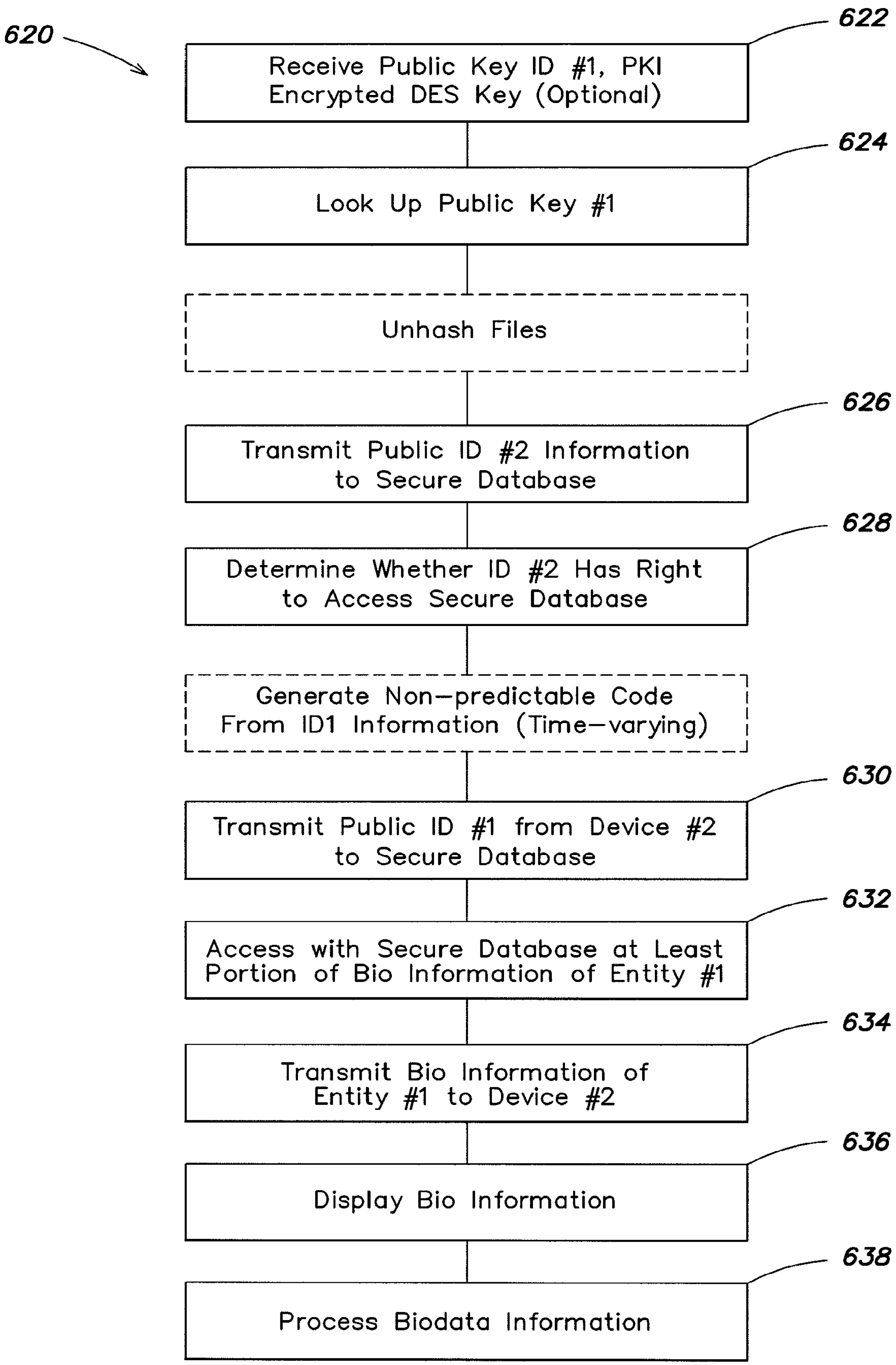
620
622
Receive Public Key ID #1, PKI Encrypted DES Key (Optional)
624
Look Up Public Key #1
Unhash Files
626
Transmit Public ID #2 Information to Secure Database
628
Determine Whether ID #2 Has Right to Access Secure Database
Generate Non–predictable Code From ID1 Information (Time–varying)
630
Transmit Public ID #1 from Device #2 to Secure Database
632
Access with Secure Database at Least Portion of Bio Information of Entity #1
634
Transmit Bio Information of Entity #1 to Device #2
636
Display Bio Information
638
Process Biodata Information

FIG. 26

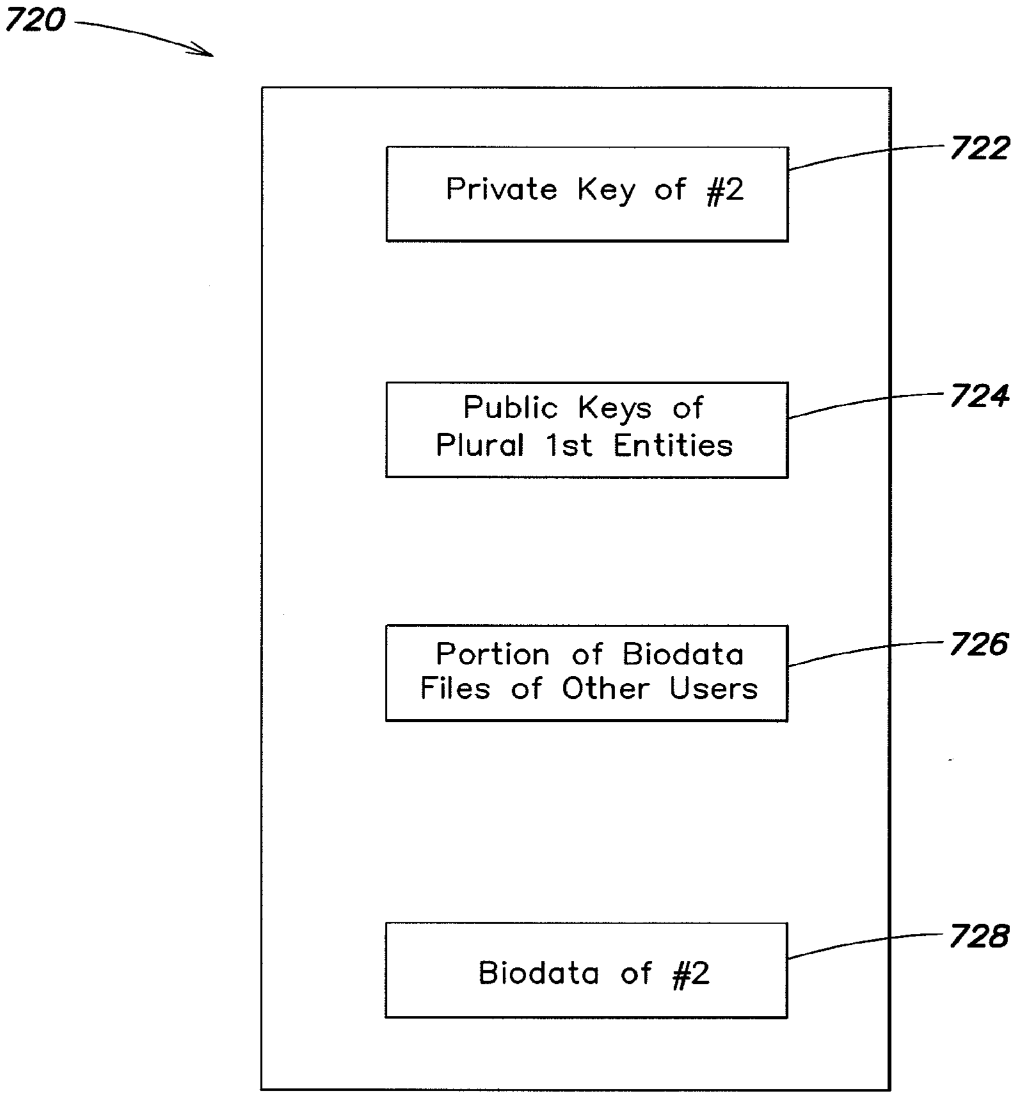
720
Private Key of #2
722
Public Keys of Plural 1st Entities
724
Portion of Biodata Files of Other Users
726
Biodata of #2
728

FIG. 27

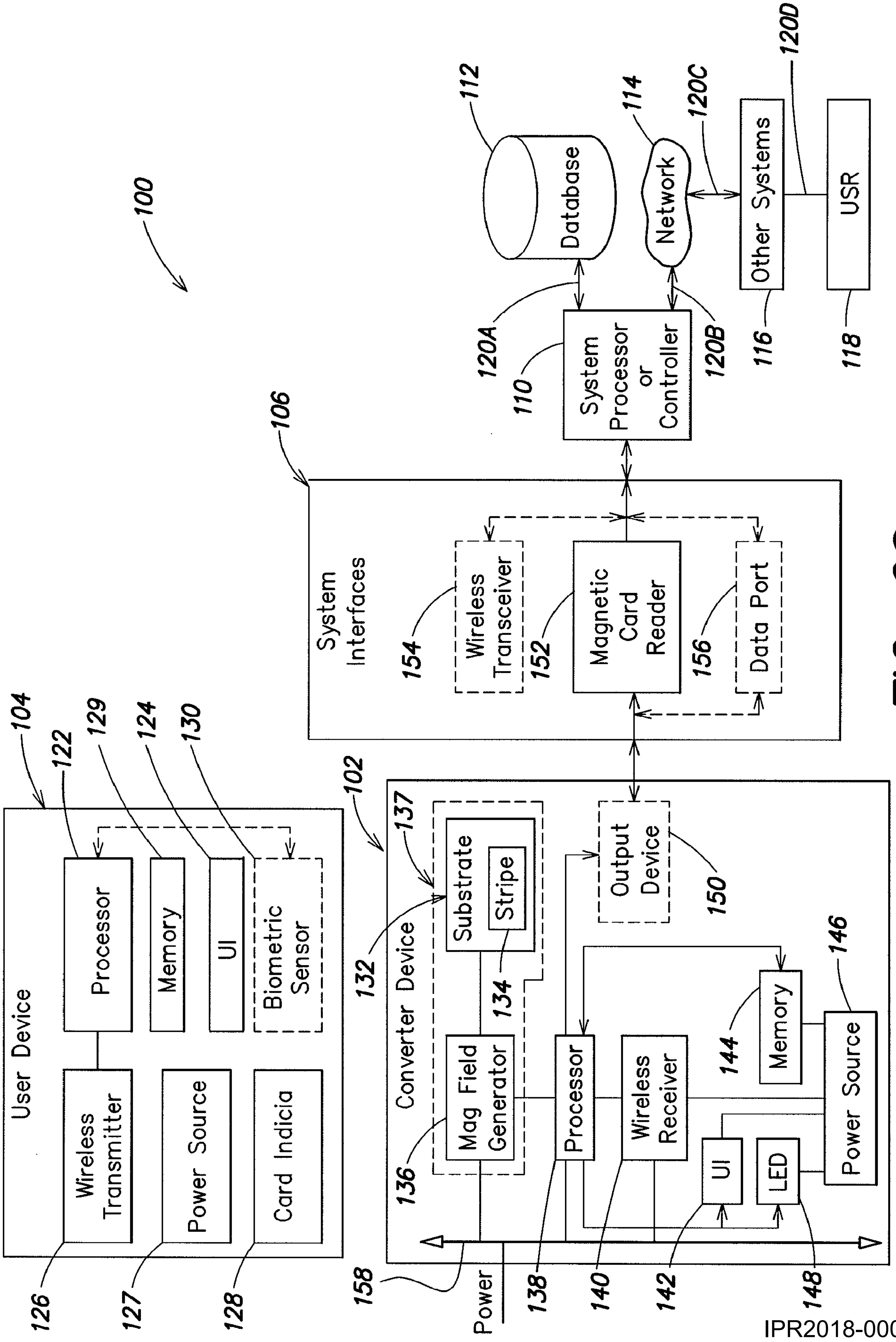
100
User Device
104
Processor
122
Memory
129
UI
124
Biometric Sensor
130
Wireless Transmitter
126
Power Source
127
Card Indicia
128
Converter Device
102
Substrate
Stripe
137
132
134
Mag Field Generator
136
Processor
138
Wireless Receiver
140
UI
142
LED
148
Memory
144
Power Source
146
Output Device
150
Power
158
System Interfaces
106
Wireless Transceiver
154
Magnetic Card Reader
152
Data Port
156
System Processor or Controller
110
Database
112
Network
114
Other Systems
116
USR
118
120A
120B
120C
120D

FIG. 28

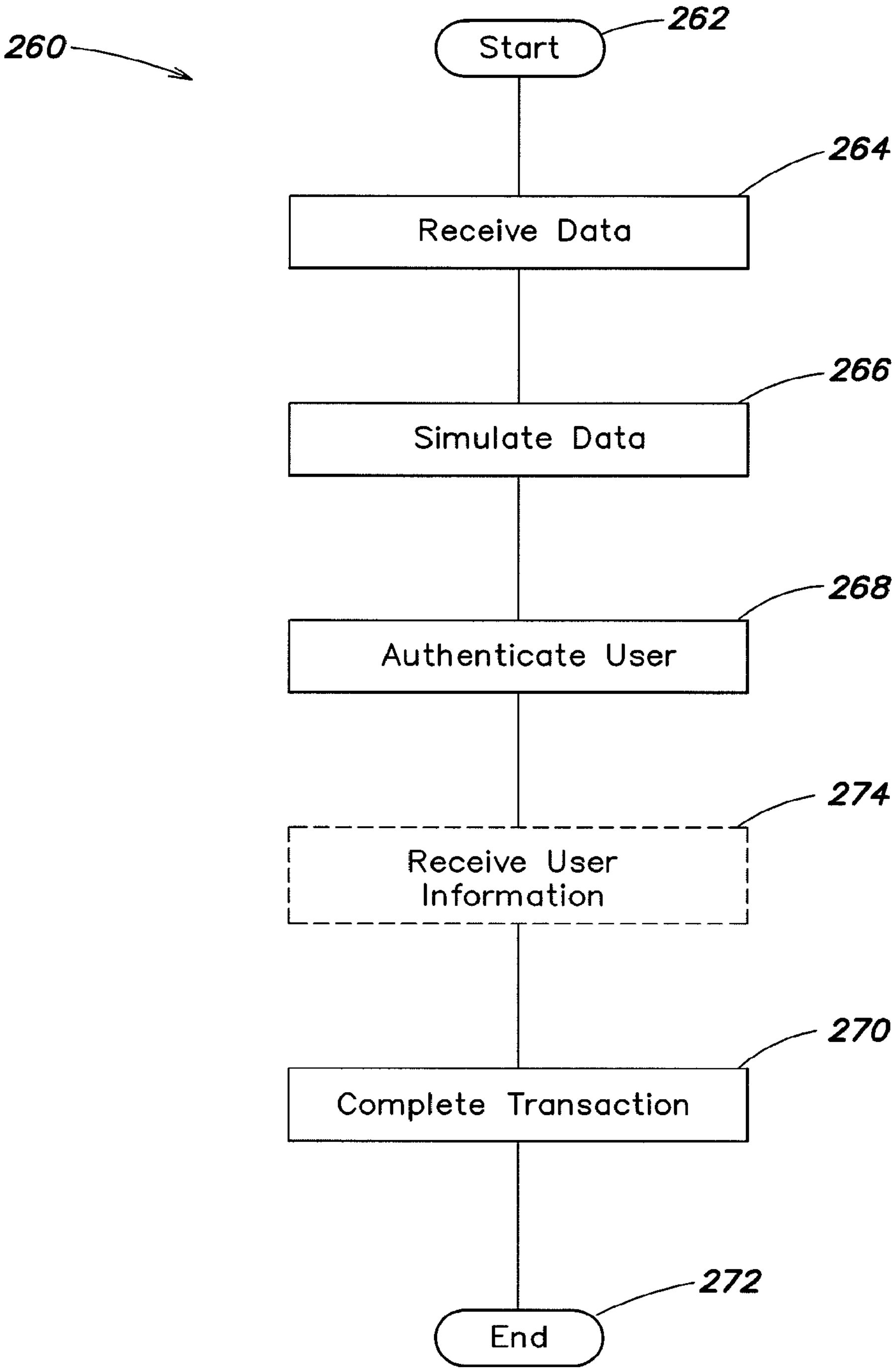
260
262
Start
264
Receive Data
266
Simulate Data
268
Authenticate User
274
Receive User Information
270
Complete Transaction
272
End

FIG. 29

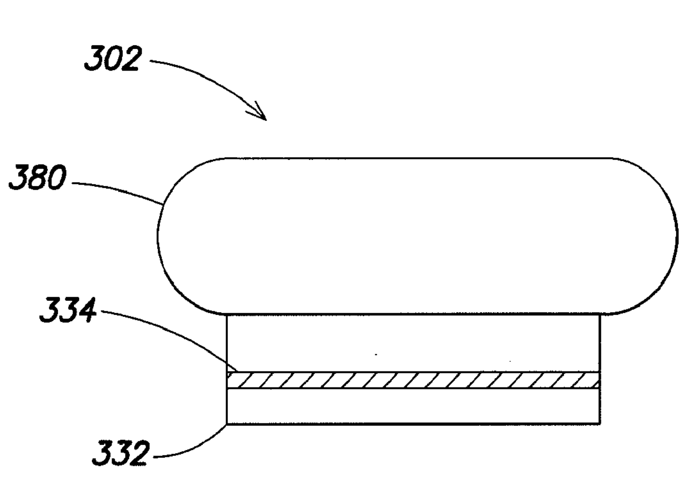

FIG. 30A

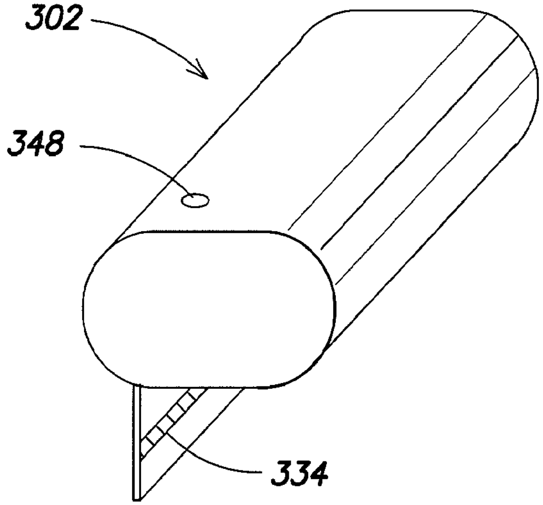

FIG. 30B

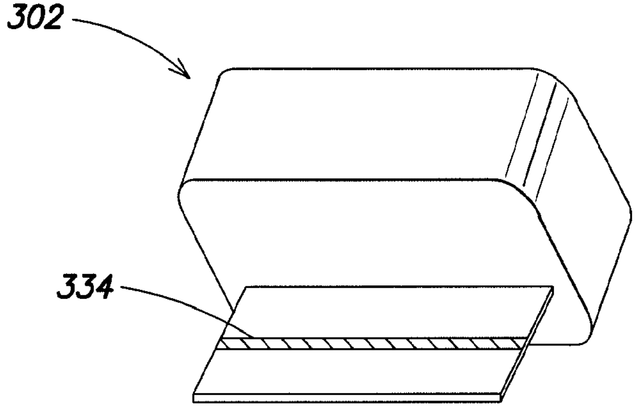

FIG. 30C

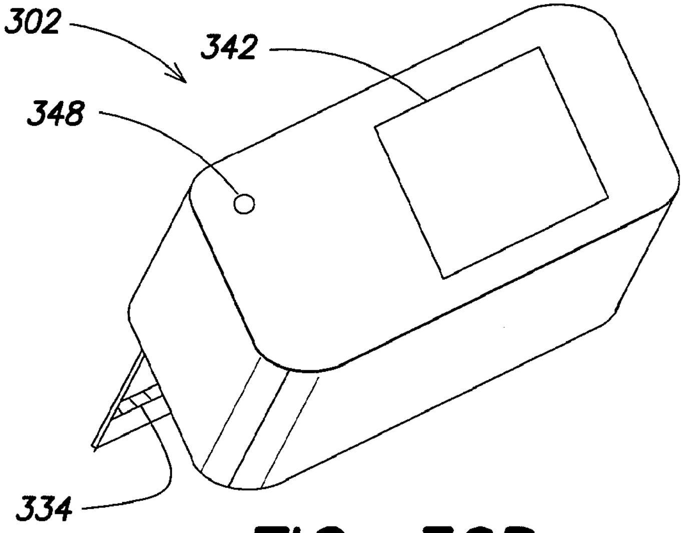

FIG. 30D

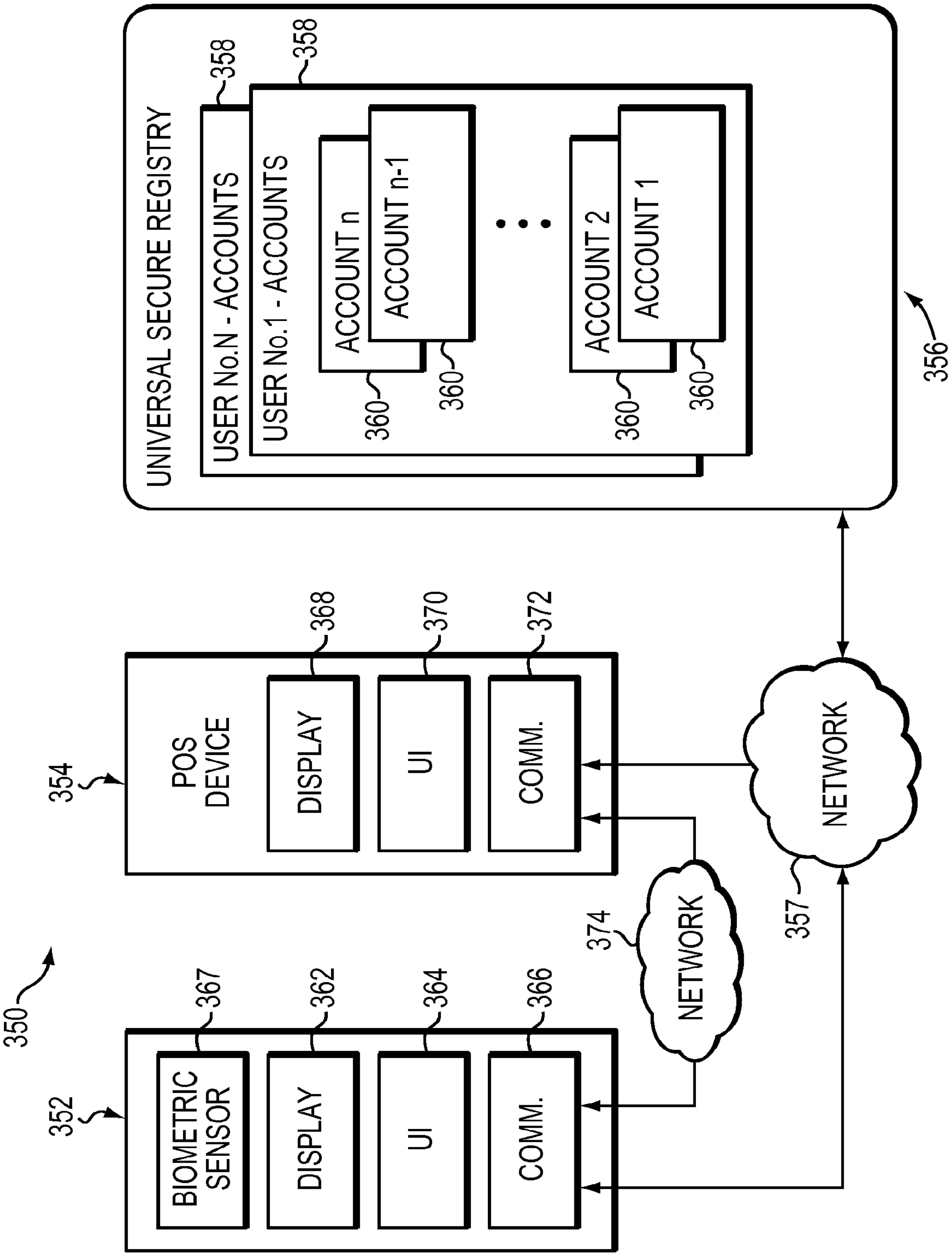
350
352
BIOMETRIC SENSOR
367
DISPLAY
362
UI
364
COMM.
366
374
NETWORK
354
POS DEVICE
DISPLAY
368
UI
370
COMM.
372
NETWORK
357
UNIVERSAL SECURE REGISTRY
USER No.N - ACCOUNTS
358
USER No.1 - ACCOUNTS
358
ACCOUNT n
ACCOUNT n-1
ACCOUNT 2
ACCOUNT 1
360
360
360
360
356

FIG. 31

UNIVERSAL SECURE REGISTRY

CROSS REFERENCE TO RELATED APPLICATIONS

This application claims the benefit under 35 U.S.C. § 120 as a continuation of U.S. patent application No. 13/237,184 filed September 20, 2011, which is a continuation of U.S. patent application No. 12/393,586 filed February 26, 2009, which is a continuation-in-part of each of U.S. patent application serial no. 11/760,732 filed June 8, 2007, now U.S. Patent No. 7,809,651; U.S. patent application serial no. 11/760,729 filed June 8, 2007, now U.S. Patent No. 7,805,372; and U.S. patent application serial no. 11/677,490 filed February 21, 2007, now U.S. Patent No. 8,001,055. This application also claims the benefit under 35 U.S.C. § 120 as a continuation-in-part of U.S. patent application no. 13/168,556 filed on June 24, 2011, which claims the benefit under 35 U.S.C. § 120 as a continuation of U.S. application no. 11/677,490. Each of U.S. application nos. 11/760,732, 11/760,729 and 11/677,490 claim priority under 35 U.S.C. § 119 (e) to U.S. Provisional Application Nos. 60/812,279 filed on June 9, 2006, and 60/859,235 filed on November 15, 2006. U.S. application no. 11/677,490 also claims priority under 35 U.S.C. § 119 (e) to U.S. Provisional Application No. 60/775,046 filed on February 21, 2006. Application serial no. 12/393,586 filed February 26, 2009 claims priority under 35 U.S.C. § 119(e) to U.S. Provisional Application Serial No. 61/031,529, entitled "UNIVERSAL SECURE REGISTRY," filed on February 26, 2008. Each of the above-identified applications is hereby incorporated herein by reference in its entirety.

BACKGROUND OF INVENTION

1. Field of Invention

Embodiments of the invention generally relate to systems, methods, and apparatus for authenticating identity or verifying the identity of individuals and other entities seeking access to certain privileges and for selectively granting privileges and providing other services in response to such identifications/verifications. In addition, embodiments of the invention relate generally to systems and methods for obtaining information from and/or transmitting information to a user device and, in particular, to systems, methods, and apparatus that provide for contactless information transmission.

2. Discussion of Related Art

Control of access to secure systems presents a problem related to the identification of a person. An individual may be provided access to the secure system after their identity is authorized. Generally, access control to secure computer networks is presently provided by an authentication scheme implemented, at least partly, in software located on a device being employed to access the secure computer network and on a server within the secure computer network. For example, if a corporation chooses to provide access control for their computer network, they may purchase authentication software that includes server-side software installed on a server in their computer system and corresponding client-side software that is installed on the devices that are used by employees to access the system. The devices may include desktop computers, laptop computers, and handheld computers (e.g., PDAs and the like).

In practice, the preceding approach has a number of disadvantages including both the difficulty and cost of maintaining the authentication system and the difficulty and cost of maintaining the security of the authentication system. More specifically, the software resides in the corporation's computers where it may be subject to tampering/unauthorized use by company employees. That is, the information technology team that manages the authentication system has access to the private keys associated with each of the authorized users. As a result, these individuals have an opportunity to compromise the security of the system. Further, any modification and/or upgrade to the authentication system software is likely to require an update to at least the server-side software and may also require an update of the software located on each user/client device. In addition, where the company's computer systems are geographically distributed, software upgrades/updates may be required on a plurality of geographically distributed servers.

There is also a need, especially in this post September 11 environment, for secure and valid identification of an individual before allowing the individual access to highly secure areas. For example, an FBI agent or an air marshal may need to identify themselves to airport security or a gate agent, without compromising security. Typically such identification may comprise the air marshal or FBI agent showing identification indicia to appropriate personnel.

However, there are inherent flaws in this process that allow for security to be compromised, including falsification of identification information and failure of the airport security or other personnel to recognize the situation. Of course this process could be automated, for example, by equipping airport personnel or security with access to a database and requiring the FBI agent or air marshal to appropriately identify themselves to the database, for example, by again providing identification which airport personnel can then enter into the database to verify the identity of the person seeking access to a secure area. However, this process also has the inherent flaws in it as described above. In addition, there may be times when airport security or personnel may not be able to communicate with the database to check the identity of the person seeking access, for example, when they are not near a computer terminal with access to a database or are carrying a hand-held device that does not have an appropriate wireless signal to access the database. In addition, there is a need to ensure that if such a hand-held device ends up the wrong hands, that security is not compromised.

Further, both commercial (e.g., banking networks) and non-commercial (e.g., security systems) information systems often rely on magnetic card readers to collect information specific to a user (e.g., a security code, a credit card number, etc.) from a user device (e.g., a transaction card). Credit card purchases made in person provide an example of the most common transaction-type that relies on a user device, the credit or debit card, which is read by a magnetic card reader. User devices that rely on magnetic-stripe based technology magnetically store information (e.g., binary information) in the magnetic stripe. The magnetic stripe reader provides an interface to a larger computerized network that receives the user's information to determine, for example, whether to authorize a transaction, to allow the user access to a secure area, etc.

Recently, such devices have seen technological advances that increase their capabilities and improve their security. For example, such devices may now include embedded processors, integral biometric sensors that sense one or more biometric feature (e.g., a fingerprint) of the user, and magnetic stripe emulators. As one result, such devices may provide greater security by dynamically generating the necessary information, for example, generating the credit card number at the time of a transaction. Improved security can also be provided by such devices because more sophisticated authentication schemes can be implemented with the devices.

In addition, user devices such as transaction cards may now also provide for one or more modes of information transmission other than transmission via a magnetic stripe/card reader combination. For example, user devices that may transmit information optically or via radio frequency ("RF") signal transmission to a compatible system interface are now available. Further, the architecture of a user device that includes a processor is generally compatible with both the improved security features described above and the contactless transmission modes such as optical and RF signal transmission. As a result of the improved security and greater functionality of some current user devices, there is a desire to replace magnetic-stripe based user devices with devices that include forms of information transmission other than the reading of a magnetic-stripe.

There is, however, a substantial installed base of interfaces (for example, at points of sale, at automatic teller machines ("ATM"), and the like) that include magnetic card readers which are not equipped to receive information from a user device in any other format other than from a magnetic stripe. As a result of the cost to replace or retrofit the installed base, efforts to more-widely introduce user devices that do not employ magnetic stripe devices have not been developed. Because of the potential to substantially reduce fraud, however, the further implementation of such devices is of great interest to financial institutions among others. RF devices that transmit information wirelessly are expected to become much more prevalent and at some point, the predominant form of information transmission for user authentication based on a hand-held device, for example, credit card, debit card, drivers license, passport, social security card, personal identification, etc. Thus, new and improved methods for transitioning from a purely magnetic based form of communication to a wireless form of communication are desired.

One current approach that is intended to "transform" a smart card for use with a magnetic stripe card reader employs a "bridge" device. The bridge device requires that the smart card be inserted within it. The bridge device includes a slot for receiving the smart card, a key pad whereby the user may enter information (e.g., a PIN number), and a credit card sized extension member. Operation of the bridge device requires that the smart card be inserted within it and that an electrical contact surface of the smart card engage a similar surface within the bridge device before the bridge device (i.e., the extension member) can be used with a magnetic card reader. Thus, the contactless nature of more advanced information transmission systems is lost with the bridge device because it does not support wireless signal transmission.

Accordingly, there is a desire for one or more devices, systems and methods for accomplishing any of the herein mentioned objectives.

SUMMARY OF INVENTION

There is thus a need for an identification system that will enable a person to be accurately identified ("identification" sometimes being used hereinafter to mean either identified or verified) and/or authenticated without compromising security, to gain access to secure systems and/or areas. Likewise, there is a need for an identification system that will enable a person to be identified universally without requiring the person to carry multiple forms of identification.

Accordingly, this invention relates, in one embodiment, to an information system that may be used as a universal identification system and/or used to selectively provide information about a person to authorized users. Transactions to and from a secure database may take place using a public key/private key security system to enable users of the system and the system itself to encrypt transaction information during the transactions. Additionally, the private key/public key security system may be used to allow users to validate their identity. For example, in one embodiment, a smart card such as the Secure ID^{TM} card from RSI Security, Inc. may be provided with the user's private key and the USR system's public key to enable the card to encrypt messages being sent to the USR system and to decrypt messages from the USR system 10.

The system or database of the invention may be used to identify the person in many situations, and thus may take the place of multiple conventional forms of identification. Additionally, the system may enable the user's identity to be confirmed or verified without providing any identifying information about the person to the entity requiring identification. This can be advantageous where the person suspects that providing identifying information may subject the identifying information to usurpation.

Access to the system may be by smart card, such as a Secure ID^{TM} card, or any other secure access device. The technology enabling the user to present their identity information may be physically embodied as a separate identification device such as a smart ID card, or may be incorporated into another electronic device, such as a cell phone, pager, wrist watch, computer, personal digital assistant such as a Palm Pilot^{TM}, key fob, or other commonly available electronic device. The identity of the user possessing the identifying device may be verified at the point of use via any combination of a memorized PIN number or code, biometric identification such as a fingerprint, voice print, signature, iris or facial scan, or DNA analysis, or any other method of identifying the person possessing the device. If desired, the identifying device may also be provided with a picture of the person authorized to use the device to enhance security.

According to one embodiment of the invention, a method of controlling access to a plurality of secure computer networks using a secure registry system located remotely from the secure computer networks is disclosed. The secure registry system includes a database containing selected data of a plurality of users each authorized to access at least one of the plurality of secure computer networks. The method comprises acts of receiving authentication information from an entity at a secure computer network, communicating the authentication information to the secure registry system, and validating the authentication information at the secure registry system. The method also includes receiving from the secure registry system an indication of whether the entity is authorized to access the secure computer network, granting the entity access to the secure computer network when the authentication information of the entity corresponds to one of the plurality of users, and denying the entity access to the secure computer network when the authentication information of the user does not correspond to one of the plurality of users.

Another embodiment of the invention comprises a method of controlling access to a secure computer network using a secure registry system. The secure registry system includes a database containing selected data of a plurality of users authorized to access the secure computer network and selected data identifying the secure computer network. The method comprises receiving an access request including authentication information and a computer network ID from an entity, determining whether the authentication information is valid for any of the plurality of users, accessing data when the authentication information of the entity is valid for one of the plurality of users to determine whether the entity is authorized to access the computer network identified by the computer network ID, and allowing the entity to access the secure computer network when the authentication information of the entity is valid for one of the plurality of users authorized to access the computer network identified by the computer network ID.

Another embodiment of the invention comprises a method of authenticating an identity of a first entity. The method comprises the acts of wirelessly transmitting from a first device, first encrypted authentication information of the first entity, receiving with a second device the wirelessly transmitted first encrypted authentication information, decrypting with the second device, the first wirelessly encrypted authentication information to provide the first authentication information of the first entity to the second device; and authenticating the identity of the first entity based upon the first authentication information; and acting based on the assessed identity of the first entity.

Another embodiment of the invention comprises a system for authenticating an identity of a first entity, comprising a first wireless device comprising a first wireless transmitter and receiver configured to transmit a first wireless signal including first encrypted authentication information, a first processor configured to compare stored biometric data with detected biometric data of the first entity and configured to enable or disable use of the first device based on a result of the comparison, and configured to encrypt first authentication information with a first private key of the first entity into the first encrypted authentication information, a first biometric detector for detecting biometric data of the first entity, and a first memory for storing biometric data of the first entity, a private key of the first entity authorized to use the first device, and the first authentication information.

According to some embodiments, the system further comprises a second wireless device comprising a second wireless transmitter and receiver configured to receive the first wireless signal and to process the first wireless signal, a second processor configured to compare detected biometric data of a second entity with stored biometric data and configured to enable or disable use of the second device based upon a result of the comparison, and configured to decrypt the first authentication information received in the first wireless signal, a biometric detector for detecting biometric data of a second entity, and a second memory storing biometric data of the second entity and a plurality of public keys of a plurality of first entities.

Another embodiment of the invention provides a first wireless device comprising a processor configured to enable operation of the first wireless device if it receives an enablement signal validating first biometric information of a first entity and configured to generate a non-predictable signal from the biometric information, a first wireless transmitter and receiver configured to transmit a first wireless signal including first encrypted biometric information of the first entity and to receive the enablement signal, and a first biometric detector for detecting the first biometric information of the first entity.

In one aspect of the invention, a device converts a wireless transaction device to a magnetic-stripe emulator device. In one embodiment, the device includes a wireless signal receiver that is configured to receive a wireless signal and provide information from the wireless signal. In addition, the device may include a magnetic-stripe emulator which is communicatively coupled to the wireless signal receiver and adapted to provide a time-varying signal which emulates data provided by a magnetic-stripe card to a magnetic card reader in response to receiving the information from the wireless signal. In one embodiment, the device includes a processor communicatively coupled to the wireless signal receiver and to the magnetic-stripe emulator. The device may also include an LED. In a version of this embodiment, the processor is configured to control the LED to indicate that the device is properly aligned with the magnetic card reader. In another embodiment, the device includes an output device that can provide information to a network or to a network device. In a version of this embodiment, the output device is a wireless transmitter device.

Further embodiments of the invention may include additional features, for example, in one embodiment the output device is a data port to which the device can provide data to a network or to a network device. In a version of this embodiment, the data port is also configured to receive data from the network or the network's device. In a further embodiment, the device is configured to communicate with the magnetic card reader via the data port.

In a further embodiment, the wireless receiver and/or processors configure, decrypt and encrypt the wireless signal. In a further embodiment, the processor is configured to determine whether a user is authorized to provide the information contained within the wireless signal from data within the wireless signal. In a version of this embodiment, the data contained within the wireless signal includes user ID information. In yet another embodiment, the data contained within the wireless signal includes biometric information of the user.

According to another aspect, the invention provides a system for validating an identity of a user to enable or prevent an occurrence of an event. In one embodiment, the system includes a first device including a wireless transmitter which is configured to transmit validation information, a second device including a wireless receiver, where the second device is configured to receive the validation information and further transmit the validation information; and a secure system in communication with the second device. According to one embodiment, the secure system includes a database. In a further embodiment, the secure system is configured to receive the validation information transmitted from the second device, and to transmit additional information to the second device following a receipt of the validation information to assist the second device in either enabling or preventing the occurrence of the event. In various embodiments, the event that is enabled or prevented may be a transaction (e.g., a financial transaction), access control (e.g., physical or electronic access) or other action that is either enabled or prevented.

According to a further aspect, the invention provides a method employing a system to validate an identity of a user to enable or prevent an occurrence of an event. In one embodiment, the system includes a first device, a second device and a secure system including a database. According to one embodiment, the method includes acts of receiving at the second device validation information wirelessly transmitted from the first device, communicating the validation information from the second device to the secure system, and receiving at the second device additional information from the secure system. In a further embodiment, the additional information assists the second device in either enabling or preventing the occurrence of the event. In various embodiments, the event that is enabled or prevented may be a transaction (e.g., a financial transaction), access control (e.g., physical or electronic access) or other action that is either enabled or prevented.

In still another aspect, a user device is configured to allow a user to select any one of a plurality of accounts associated with the user to employ in a financial transaction. In one embodiment, the user device includes a biometric sensor configured to receive a biometric input provided by the user, a user interface configured to receive a user input including secret information known to the user and identifying information concerning an account selected by the user from the plurality of accounts. In a further embodiment, the user device includes a communication link configured to communicate with a secure registry, and a processor coupled to the biometric sensor to receive information concerning the biometric input, the user interface, and the communication link. According to one embodiment, the processor is configured to generate a non-predictable value and to generate encrypted authentication information from the non-predictable value, the identifying information, and at least one of the information concerning the biometric input and the secret information, and to communicate the encrypted authentication information via the communication link to the secure registry.

In accordance with another aspect, a method of generating authentication information includes acts of authenticating an identity of a user to a device based on at least one of biometric data received by the device from the user and secret information known to the user and provided to the device. The method can also include the generation of a non-predictable value with the device. The method can further include acts of receiving identifying information from the user concerning a selected one of a plurality of user accounts and generating encrypted authentication information from the non-predictable value, the identifying information, and at least one of the biometric data and the secret information. In a further embodiment, the device can generate encrypted authentication information from each of the non-predictable value, the biometric data, the secret information, and the identifying information.

According to a still further aspect, a method of controlling access to a plurality of accounts is provided where the method includes acts of generating, with a device, encrypted authentication information from a non-predictable value generated by the device, identifying information concerning an account selected by a user of the device from among a plurality of accounts associated with the user, and at least one of a biometric of the user received by the device and secret information provided to the device by the user, communicating the encrypted authentication information from the device to a secure registry via a point-of-sale (POS) device to authenticate or not authenticate the device with the secure registry, authorizing the POS device to initiate a financial transaction involving a transfer of funds to or from the account selected by the user when the encrypted authentication information is successfully authenticated, and denying the POS device from initiation of the financial transaction involving a transfer of funds to or from the account selected by the user when the encrypted authentication information is not successfully authenticated.

BRIEF DESCRIPTION OF DRAWINGS

This invention is pointed out with particularity in the appended claims. The above and further advantages of this invention may be better understood by referring to the following description when taken in conjunction with the accompanying drawings. The accompanying drawings are not intended to be drawn to scale. In the drawings, each identical or nearly identical component that is illustrated in various figures is represented by a like numeral. For purposes of clarity, not every component may be labeled in every thawing. In the drawings:

FIG. 1 is a functional block diagram of a computer system configured to implement the universal secure registry ("USR"), including a USR database, according to one embodiment of the invention;

FIG. 2 is a functional block diagram of a first embodiment of a networked environment including the computer system of FIG. 1;

FIG. 3 is a functional block diagram of an entry of a database forming the USR database of FIG. 1;

FIG. 4 is a functional block diagram of a second embodiment of a networked environment including the computer system of FIG. 1;

FIG. 5 is a flow chart illustrating steps in a process of inputting data into the USR database;

FIG. 6 is a flow chart illustrating steps in a process of retrieving data from the USR database;

FIG. 7 is a flow chart illustrating a first protocol for purchasing goods from a merchant via the USR database without transmitting credit card information to the merchant;

FIG. 8 is a flow chart illustrating a second protocol for purchasing goods from a merchant via the USR database without transmitting credit card information to the merchant;

FIG. 9 is a flow chart illustrating a protocol for purchasing goods from a merchant via the USR database by validating the user's check;

FIG. 10 is a flow chart illustrating a protocol for purchasing goods from an on-line merchant via the USR database without transmitting credit card information to the on-line merchant, and enabling the on-line merchant to ship the goods to a virtual address;

FIG. 11 is a flow chart illustrating a protocol for shipping goods to a virtual address via the USR database;

FIG. 12 is a flow chart illustrating a protocol for telephoning a virtual phone number via the USR database;

FIG. 13 is a flow chart illustrating a protocol for identifying a person via the USR database;

FIG. 14 is a flow chart illustrating a protocol for identifying a person to a policeman via the USR database;

FIG. 15 is a flow chart illustrating a protocol for providing information to an authorized recipient of the information via the USR database;

FIG. 16 is a flow chart illustrating a protocol for providing application information to an authorized recipient of the information via the USR database;

FIG. 17 is a functional block diagram of an embodiment configured to use information in the USR system to activate or keep active property secured through the USR system; and

FIG. 18A is a functional block diagram of an embodiment configured to use the USR system to control access to a secure computer network;

FIG. 18B is a functional block diagram of another embodiment configured to use the USR system to control access to a secure computer network;

FIG. 19 is a flow diagram of a process for controlling access to a secure computer network with the USR system in accordance with an embodiment of the invention;

FIG. 20 is a flow diagram of a process for controlling access to a secure computer network with the USR system in accordance with another embodiment of the invention;

FIG. 21 illustrates an embodiment of a system for validating the identity of an individual;

FIGS. 22A and 22B illustrate one embodiment of a process for validating the identity of an individual;

FIG. 23 illustrates one embodiment of various fields included within a first wireless signal and a second wireless signal as transmitted by the system of FIG. 21;

FIG. 24 illustrates one embodiment of a process for verifying or authenticating the identity of a first user of a first wireless transmission device;

FIG. 25 illustrates another embodiment of a process for authenticating the identity of a first user of a wireless transmission device;

FIG. 26 illustrates still another embodiment of a process for authenticating the identity of a first user of a wireless transmission device; and

FIG. 27 illustrates one embodiment of a data structure that can be used by any wireless device of the system of FIG. 21;

FIG. 28 illustrates a system in accordance with one embodiment of the invention;

FIG. 29 illustrates a process in accordance with an embodiment of the invention;

FIGS. 30A-30D illustrate a converter device in accordance with one embodiment of the invention; and

FIG. 31 illustrates a further embodiment of a system that employs the USR system.

DETAILED DESCRIPTION

This invention is not limited in its application to the details of construction and the arrangement of components set forth in the following description or illustrated in the drawings. The invention is capable of other embodiments and of being practiced or of being carried out in various ways. Also, the phraseology and terminology used herein is for the purpose of description and should not be regarded as limiting. The use of "including," "comprising," or "having," "containing", "involving", and variations thereof herein, is meant to encompass the items listed thereafter and equivalents thereof as well as additional items.

In one embodiment, an information system is formed as a computer program running on a computer or group of computers configured to provide a universal secure registry (USR) system. The computer, in this instance, may be configured to run autonomously (without the intervention of a human operator), or may require intervention or approval for all, a selected subset, or particular classes of transactions. The invention is not limited to the disclosed embodiments, and may take on many different forms depending on the particular requirements of the information system, the type of information being exchanged, and the type of computer equipment employed. An information system according to this invention, may optionally, but need not necessarily, perform functions additional to those described herein, and the invention is not limited to a computer system performing solely the described functions.

In the embodiment shown in FIG. 1, a computer system 10 for implementing a USR system according to the invention includes at least one main unit 12 connected to a wide area network, such as the Internet, via a communications port 14. The main unit 12 may include one or more processors (CPU 16) running USR software 18 configured to implement the USR system functionality discussed in greater detail below. The CPU 16 may be connected to a memory system including one or more memory devices, such as a random access memory system RAM 20, a read only memory system ROM 22, and one or more databases 24. In the illustrated embodiment, the database 24 contains a universal secure registry database. The invention is not limited to this particular manner of storing the USR database. Rather, the USR database may be included in any aspect of the memory system, such as in RAM 20, ROM 22 or disc, and may also be separately stored on one or more dedicated data servers.

The computer system may be a general purpose computer system which is programmable using a computer programming language, such as C, C++, Java, or other language, such as a scripting language or even assembly language. The computer system may also be specially programmed, special purpose hardware, an application specific integrated circuit (ASIC) or a hybrid system including both special purpose components and programmed general purpose components.

In a general purpose computer system, the processor is typically a commercially available microprocessor, such as Pentium series processor available from Intel, or other similar commercially available device. Such a microprocessor executes a program called an operating system, such as UNIX, Linux, Windows NT, Windows 95, 98, or 2000, or any other commercially available operating system, which controls the execution of other computer programs and provides scheduling, debugging, input/output control, accounting, compilation, storage assignment, data management, memory management, communication control and related services, and many other functions. The processor and operating system defines a computer platform for which application programs in high-level programming languages are written.

The database 24 may be any kind of database, including a relational database, object-oriented database, unstructured database, or other database. Example relational databases include Oracle 81 from Oracle Corporation of Redwood City, California; Informix Dynamic Server from Informix Software, Inc. of Menlo Park, California; DB2 from International Business Machines of Armonk, New York; and Access from Microsoft Corporation of Redmond, Washington. An example object-oriented database is ObjectStore from Object Design of Burlington, Massachusetts. An example of an unstructured database is Notes from the Lotus Corporation, of Cambridge, Massachusetts. A database also may be constructed using a flat file system, for example by using files with character-delimited fields, such as in early versions of dBASE, now known as Visual dBASE from Inprise Corp. of Scotts Valley, California, formerly Borland International Corp.

The main unit 12 may optionally include or be connected to an user interface 26 containing, for example, one or more input and output devices to enable an operator to interface with the USR system 10. Illustrative input devices include a keyboard, keypad, track ball, mouse, pen and tablet, communication device, and data input devices such as voice and other audio and video capture devices. Illustrative output devices include cathode ray tube (CRT) displays, liquid crystal displays (LCD) and other video output devices, printers, communication devices such as modems, storage devices such as a disk or tape, and audio or video output devices. Optionally, the user interface 26 may be omitted, in which case the operator may communicate with the USR system 10 in a networked fashion via the communication port 14. It should be understood that the invention is not limited to any particular manner of interfacing an operator with the USR system.

It also should be understood that the invention is not limited to a particular computer platform, particular processor, or particular high-level programming language. Additionally, the computer system may be a multiprocessor computer system or may include multiple computers connected over a computer network. It further should be understood that each module or step shown in the accompanying figures and the substeps or subparts shown in the remaining figures may correspond to separate modules of a computer program, or may be separate computer programs. Such modules may be operable on separate computers. The data produced by these components may be stored in a memory system or transmitted between computer systems.

Such a system may be implemented in software, hardware, or firmware, or any combination thereof. The various elements of the information system disclosed herein, either individually or in combination, may be implemented as a computer program product, such as USR software 18, tangibly embodied in a machine-readable storage device for execution by the computer processor 16. Various steps of the process may be performed by the computer processor 16 executing the program 18 tangibly embodied on a computer-readable medium to perform functions by operating on input and generating output. Computer programming languages suitable for implementing such a system include procedural programming languages, object-oriented programming languages, and combinations of the two.

As shown in FIG. 2, the computer system 10 may be connected to a plurality of interface centers 27 over a wide area network 28. The wide area network 28 may be formed from a plurality of dedicated connections between the interface centers 27 and the computer system 10, or may take place, in whole or in part, over a public network such as the Internet. Communication between the interface centers 27 and the computer system 10 may take place according to any protocol, such as TCP/IP, ftp, OFX, or XML, and may include any desired level of interaction between the interface centers 27 and the computer system 10. To enhance security, especially where communication takes place over a publicly accessible network such as the Internet, communications facilitating or relating to transmission of data from/to the USR database 24 or the computer system 10 may be encrypted using an encryption algorithm, such as PGP, DES, or other conventional symmetric or asymmetric encryption algorithm.

In one embodiment, the USR system 10 or USR database 24 may be able to authenticate its identity to a user or other entity accessing the system by providing an appropriate code which may be displayed on the user's smart card, for example a SecurID^{TM} card or its equivalent, or other code generator, for example a single use code generator, being employed by the user. A comparison by the user or the code generator between the provided number and an expected number can validate, to the user (or other entity) or the code generator, that communication is with the database and not an imposter. In another embodiment, a challenge-response protocol is employed to authenticate the identity of the USR system and/or the user to the other.

The database 24 shown in FIG. 1 has a USR database containing entries related to persons 1-n. The data in the USR database may also be segregated, as shown in FIG. 4, according to data type to enable individual computer modules to handle discrete applications on discrete data types. Segregating the data, as illustrated in FIG. 4, may make access to the database more robust by enabling portions of the data in the USR database 24 to be accessible even when it is necessary to perform maintenance on a portion of the database. However, storing the data in the USR database 24 according to the scheme illustrated in FIG. 1 may make it easier for a user of the database to make changes to multiple types of data simultaneously or in a single session. There are advantages and disadvantages to each data structure, and the invention is not limited to a particular manner of organizing the data within the database 24, data structures other than the two shown also being possible.

As shown in FIG. 3, each entry 30 in the database 24 may contain multiple types of information. For example, in the embodiment shown in FIG. 3, the entry contains validation information 32, access information 34, publicly available information 36, address information 38, credit card and other financial information 40, medical information 42, job application information 44, and tax information 46. The invention is not limited to a USR containing entries with all of this information or only this particular information, as any information on a person or other entity such as a company, institution, etc. may be stored in USR database 24.

If the database information is split between multiple databases, each database will typically include at least the validation and access information to enable the USR software to correlate a validation attempt with a verified validation, and to enable the USR software to determine access privileges to the requested data. Alternatively, databases may be linked to permit information not in a main USR database to be retrieved, with validation/identification for all databases accessed being done at the USR system.

In FIG. 3, the validation information is information about the user of the database to whom the data pertains and is to be used by the USR software 18 to validate that the person attempting to access the information is the person to whom the data pertains or is otherwise authorized to receive it. The validation information may be any type of information that will reliably authenticate the identity of the individual. For example, in some embodiments, the information may include any of a secret known by the user (e.g., a pin, a phrase, a password, etc.), a token possessed by the user that is difficult to counterfeit (e.g., a secure discrete microchip), and/or a measurement such as a biometric (e.g., a voiceprint, a fingerprint, DNA, a retinal image, a photograph, etc.).

The user's identifying information may be manually entered or scanned at the interface center. However, a variety of types of communication may be employed to communicate the user's identifying information from the identification card or token to the computer system. For example, near field signal may be employed to communicate information between the identification card or token and the computer system 10. According to one embodiment, the user's identifying information is included in (or entered via) the user's cell phone where it is then communicated to the computer system 10. In one embodiment, the cell phone is also configured to receive information from the computer system 10 at the interface center 27.

In one embodiment, the user of the database will carry a SecurID^{TM} card available from RSA Security, formerly Security Dynamics Technologies, Inc., of Cambridge, MA. Use of this card enables secure access to the USR database without requiring the user to transmit any personal information. Specifically, to access the USR database, the card retrieves a secret user code and/or time varying value from memory and obtains from the user a secret personal identification code. The card mathematically combines these three numbers using a predetermined algorithm to generate a one-time nonpredictable code which is transmitted to the computer system 10. The computer system, specifically USR software 18, utilizes the received one-time nonpredictable code to determine if the user is authorized access to the USR database and grants access to the USR database if the user is determined to be authorized. The verification information 32 in the database entry in the embodiment of the invention illustrated in FIG. 3 contains information to enable the USR software 18 to validate the user using such a card in this manner.

Alternative types of identification cards or tokens may likewise be used. For example, other smart cards may be used which generate non-predictable single use codes, which may or may not be time varying, or other access code generators may be used. An algorithm generating such non-predictable codes may also be programmed onto a processor on a smart card or other computing device, such as a cell phone, pager, ID badge, wrist watch, computer, personal digital assistant, key fob, or other commonly available electronic device. For convenience, the term “electronic ID device” will be used generically to refer to any type of electronic device that may be used to obtain access to the USR database.

Likewise, various types of biometric information may be stored in the verification area of the database entry to enable the identity of the user possessing the identifying device to be verified at the point of use. Examples of the type of biometric information that may be used in this situation includes a personal identification number (PIN), fingerprint, voice print, signature, iris or facial scan, or DNA analysis. If desired, the verifying section of the database may contain a picture to be transmitted back to the person seeking to validate the device to ensure the person using the device is the correct person. Optionally, the identifying device itself may also be provided with a picture of the person authorized to use the card to provide a facial confirmation of the person’s right to use the card.

Further, a challenge-response protocol may be employed in combination with or as an alternative to the preceding to validate the person attempting to access the information. Various embodiments may employ a challenge-response protocol with or without an identification card.

In FIG. 3, the Access information 34 is provided to enable different levels of security to attach to different types of information stored in the entry 30 in the USR database 14. For example, the person may desire that their address information be made available only to certain classes of people, for example colleagues, friends, family, Federal Express, U.P.S., and the U.S. mail service. The names or universal identifiers for those selected individuals, companies, organizations and/or agencies may be entered into appropriate fields in the Access information to specify to the USR software 18 those individuals to whom the address information may be released. Likewise, access fields may be specified for the other types of information. For example, the individual may specify that only particular individuals and/or companies have access to the credit card and other financial information 40, medical information 42, job application information 44 and tax information 46. Additionally, the individual may specify that no one have access to that information unless the individual participates in the transaction (see FIG. 6).

As shown in FIG. 1, the USR software 18 contains algorithms for execution by the CPU 16 that enables the CPU 16 to perform the methods and functions of the USR software described below in connection with Figs. 5-16. The USR software 18, in this embodiment, performs all functions associated with validating an electronic ID card. If desired, a separate validation software module may be provided to validate electronic ID devices outside of a firewall segregating the validation information from other user information.

This algorithm comprising the USR software 18 may be used to implement, in one exemplary embodiment, a USR system configured to enable selected information to be disseminated to selected individuals in a secure and dynamic fashion. This information may be used for numerous purposes, several of which are set forth below and discussed in greater detail in connection with Figs. 5-16.

For example, the USR system may be used to identify the person, enable the person to be contacted by telephone or mail anonymously, enable the person to be contacted by telephone or by mail without revealing the person's telephone number or present location, enable the person to purchase items over the Internet or in a store without revealing to the merchant any personal identification information or credit card information, enable the person to complete a job application without completing a job application form, enable the police to discern the person's identity and any outstanding warrants on the individual, and numerous other uses. The invention is not limited to these several enumerated uses, but rather extends to any use of the USR database. The methods of using the USR database 24 will now be discussed in connection with Figs. 5-16.

FIG. 5 illustrates a method of training the USR database 24. As shown in FIG. 5, the USR software 18 first validates the person's identification (500). The initial validation of the person's identification (500) may take place at the point of sale of an electronic ID device (for example, a smart card). This may be done in any conventional manner, such as by requiring the person to show a government issued identification card, passport, birth certificate, etc. Once the person's electronic ID device has been issued and initially validated, the validation process proceeds as discussed above.

After the validation process (500), the USR software 18 determines if the person has rights to enter data into the system (502). This step enables the system to charge persons for maintaining information in the USR database 24. For example, the USR software 18 may poll a database of current accounts or a database of accounts that are currently in default to determine if the person has paid the access fee to enter data into the database. A similar account status inquiry process may be performed by the USR software 18 in connection with each of the other methods set forth in Figs. 6-16. If the person is not authorized to enter data into the USR database 24, the person is notified of the status of their account and the process returns (512) to wait for further input from another person. Alternatively, a person may be permitted to enter some classes of data into the system and update such classes of data at no charge, with a fee possibly being required for other classes of data, for example medical records. This would facilitate a more robust database.

If the person is authorized, the USR software 18 then enables the person to enter basic personal data into the USR database 24 (504). Optionally, personal data may be one class of data the USR software 18 allows the person to enter into the USR database 18 regardless of account status, i.e., for free.

The USR software 18 will then check to see if the person has additional rights to enter additional data (506), such as data to be entered into one of the other categories of data in FIG. 3. Optionally, this step of checking the person's rights to enter data (506) may be combined with the initial check (502). If the person does not have rights to enter any further data, the USR software 18 notifies the user and returns (512).

If the USR software 18 determines that the person has the right to enter additional data into the USR database 24, the person is prompted through the use of appropriate prompts, provided with forms, and otherwise enabled to enter advanced personal data into the USR database 24 (508). For each type of data entered, the person is asked to specify the type of access restrictions and/or whom should be allowed to access the advanced personal data (510). When the person has completed entering data into the database, the process returns (512) and commits the data to the database.

In the situation where only one person has access to enter and/or modify data for a given person in the database, there should be no conflict with committing data to the database. If, however, multiple people have access to a given account to modify data, the database may perform an integrity check to ensure the absence of conflict in the data before committing the new data to the database.

Enabling access to the information in the database will be explained in greater detail in connection with FIG. 6. As shown in FIG. 6, the database will generally allow anyone to access basic personal data on anyone without performing any authorization check (600).

If information beyond that specified in the basic personal information area is requested, the USR software 18 queries whether the requestor has the right to access the type of requested data (602). The process of determining the requestor's rights (602) typically involves validating the requestor's identity and correlating the identity, the requested information and the access information 34 provided by the person to the USR database during the training process described above with respect to FIG. 5.

If the USR software 18 determines that the requestor has rights to access the type of requested data (604), the USR software 18 instructs the USR database 24 to enable access to the type of requested data (606). The actual step of enabling access to the type of requested data may involve multiple steps of formulating a database query, querying the USR database 24, retrieving the results, assembling the results into a user friendly or user readable format, and transmitting the information to the user.

If the USR software 18 determines that the requestor does not have the appropriate rights to access the type of requested data (604), the USR software 18 checks to see if the person is participating in the transaction (608). Checking to see if the person is participating in the transaction enables the user to authorize access to the requested data in real time. For example, a person may wish to participate in a transaction to give a potential employer one-time access to job application information 44 (see FIG. 3). If the person is not participating in the transaction, the USR software 18 determines that the requestor is not authorized to have access to the requested data, notifies the requestor of this determination, and ends (610).

If the person is participating in the transaction (608), however, the USR software 18 validates the person's identity (612) and enables the person to change access rights to the data (614). If the USR software 18 is not able to validate the person's identity, the USR software 18 refuses to allow the person to update the database, notifies the person and/or requestor of this determination, and returns (610).

It is also possible that a person may be required to grant access to certain data, for example financial data such as account numbers, under duress. The system may provide the person with the ability to safely signal this when accessing the system by using a selected access code or by making a known modification to the access code provided by the electronic ID device. On receiving such code, the system would take appropriate steps to protect the person, including for example alerting the police, tracking the person's location to the extent possible, providing traceable data, and the like.

Once the person has had the opportunity to change access rights to the data (614), the USR software 18 again checks to see if the requestor has rights to access the type of requested data (616). Although step 616 may seem redundant, given the fact that the person is participating in the transaction and has just previously changed access rights to the database to enable the requestor to have access to the data, step 616 is actually useful at preventing a different type of fraud. Specifically, the requestor may not be forthright with the person regarding the type of information they are requesting. If step 616 were omitted, the USR software 18 may inadvertently allow access to an unauthorized type of information in the situation where the requestor has surreptitiously requested multiple types of data.

If the USR software 18 determines that the requestor has rights to the type of data requested (616), it causes the USR database to enable access to the type of requested data (606). Otherwise, it notifies the requestor of the decision to deny access to the requested data and returns (610).

Various applications of the USR database 24 and USR software 18 will now be discussed in connection with Figs. 7-16. These applications are merely exemplary of the types of applications enabled by the USR software 18 and USR database 24, and the invention is not limited to these particular applications.

Figure 7 illustrates one embodiment of a method of using the USR software 18 and USR database 24 to purchase goods or services from a merchant without revealing to the merchant account information relating to the person's bank or credit card.

As shown in FIG. 7, when a user initiates a purchase (700), the user enters a secret code in the user's electronic ID device (702) to cause the ID device to generate a onetime code or other appropriate code, and presents the electronic ID device with the code to the merchant or otherwise presents the code to the merchant. The merchant transmits to the credit card company (1) the code from the electronic ID device, (2) the store number, (3) the amount of the purchase (704), and the time of receipt of the code. The credit card company takes this information and passes the code from the electronic ID device to the USR software 18 (706). The USR software 18 determines if the code is valid, or was valid at the time offered, and if valid accesses the user's credit card information and transmits the appropriate credit card number to the credit card company (708). While the link between the USR system and the credit card system is a secure link, there is always a danger that the link may be penetrated and credit card numbers obtained. This may be avoided by instead transmitting, on approval, a multidigit public ID code for the credit card holder which the credit card company can map to the correct credit card number. Even if the link is violated, the public ID code is of no value and the secure link prevents this code from being improperly sent to the credit card company. The credit card company checks the credit worthiness of the user and declines the card or debits the user's account in accordance with its standard transaction processing system (710). The credit card company then notifies the merchant of the result of the transaction (712). In this embodiment, the user has been able to purchase goods or services from a merchant without ever providing to the merchant the credit card number. Since the electronic ID device generates a time variant code or otherwise generates a code that can for example only be used for a single transaction, the merchant retains no information from the transaction that may be fraudulently used in subsequent transactions.

Another embodiment of a system for facilitating purchase of goods or services without providing financial information to the merchant is set forth in FIG. 8. In FIG. 8, like FIG. 7, the user initiates a purchase (800), enters a secret code in the electronic ID device (802) and presents the resultant code to the merchant. The merchant, in this embodiment, transmits to the USR software 18, (1) the code from the electronic ID, (2) the store number, and (3) the amount of the purchase (804). The USR software 18 determines if the code is valid (806) and, if valid, accesses from the USR database 24 the user's credit card information (808). The USR software then transmits to the credit card company (1) the credit card number, (2) the store number, and (3) the amount of purchase (808). The information in this embodiment transmitted to the credit card company is intended to be in a format recognizable to the credit card company. Accordingly, the invention is not limited to transferring from the USR system 10 to the credit card company the enumerated information, but rather encompasses any transfer of information that will enable the use of the USR system 10 to appear transparent to the credit card company.

The credit card company then processes the transaction in a standard fashion, such as by checking the credit worthiness of the person, declining the card or debiting the user's account and transferring money to the merchant's account (810). The credit card company then notifies the USR system 10 the result of the transaction (812) and the USR software 18 in turn notifies the merchant of the result of the transaction (814).

In this embodiment, like the embodiment of FIG. 7, the user can use the USR system 10 to purchase goods or services from a merchant without providing the merchant with the user's credit card number. In the embodiment of FIG. 8, the interposition of the USR system 10 between the merchant and the credit card company is transparent to the credit card company and thus requires no or minimal cooperation from the credit card company to implement.

FIG. 9 illustrates one embodiment of a method of using the USR system 10 to verify funds when using a check to purchase goods or services from a merchant. In the embodiment of FIG. 9, the user initiates a purchase and writes a check to the merchant (900). The check may be a conventional check containing identifying information, or may be a check bearing a unique serial number and no identifying information to enable the check to be used anonymously.

In either situation, the user enters a secret code into the electronic ID card and presents the resulting code to the merchant along with the check (902). The merchant transmits to the USR software 18 (1) the code from the electronic ID card, (2) the store number, and (3) the amount of the purchase (904). Where the check is an anonymous check, the merchant also transmits to the USR software 18 the check number.

The USR software 18 then determines if the code from the electronic ID is valid (906), and if valid accesses the user's bank information and transmits to the bank: (1) the user's bank account number, (2) the store number, and (3) the amount of the purchase (908). Optionally, the USR software 18 may additionally inform the bank of the check number.

The bank polls its own database to determine if there are sufficient funds in the user's account (910) and notifies the USR software 18 of the result (912). The USR software 18 then, in turn, notifies the merchant of the result of the verification (914).

This check verification system may take place over an unsecured connection between the merchant and the USR system 10 since the user's bank account information is not sent over the connection between the merchant and the USR system 10. Moreover, where an anonymous check is used, the merchant is not even provided with the person's name or account information in written form. This provides additional security against unauthorized persons writing subsequent checks.

The check verification system may be conducted over a telephone network, such as by having the merchant call a toll free number or over a network connection such as over the Internet.

FIG. 10 illustrates a method of conducting a transaction with a merchant without requiring the user to provide to the merchant the user's name, address, or other identifying information, while enabling the merchant to ship the goods to the user. This may be beneficially employed, for example, in connection with transactions that take place between remote parties in a networked environment, such as the Internet.

As shown in FIG. 10, the user initiates an anonymous purchase by entering a secret code into the electronic ID device and transmitting the result to the on-line merchant (1000). The merchant transmits this information to the USR software 18, along with the store number and the amount of the purchase (1002). Optionally, the merchant may provide the store number and purchase price to the user and the user may send this information directly to the USR software 18 along with the code from the electronic ID. Where the number from the electronic ID device is a time varying number, the merchant may also need to input the time the number was received. Alternatively, the electronic ID device may encode or encrypt the time with the number, the USR software being able to extract time when receiving the number from the merchant. This may not be required where the time varying number varies slowly, for example changing every hour rather then every minute as with some devices.

In either event, the USR software 18 determines if the code is valid (1004) and, if valid, accesses the user's credit card information from the USR database 24 (1006). The USR software 18 then contacts the user's credit card company, as described above in connection with FIG. 8 (1008) and notifies the USR software 18 of the result (1010).

If the user's credit is declined, the USR software 18 notifies the on-line merchant and the transaction is terminated (1012). If the user's credit is honored, the USR software 18 polls the USR database 24 for the user's address and/or address code (1014). Address codes are discussed below in greater detail with reference to FIG. 11. The merchant then packages the goods into a parcel, labels the parcel with the appropriate address and/or address code and ships the parcel to the user (1016). Having the USR system 10 provide the address and/or address code to the on-line merchant enables the user to purchase items in a networked environment without requiring the user to input address information in connection with every sale.

FIG. 11 illustrates a use of the USR database 24 to deliver mail to a user without requiring the user to provide address information to the sender. This may be useful in many contexts. For example, the user may wish that the address information be known only by the post office. In this instance, using the USR database 24 according to the method of the invention described below will enable the user to receive parcels without requiring the user to provide the merchant with the address information. Additionally, the user's address may change, temporarily, permanently, or frequently. Enabling the sender to send mail by entering a code instead of an address enables the post office to effectively deliver the coded mail to the corresponding address regardless of the frequency with which the address changes or the duration in which the address will remain valid.

In FIG. 11, the user provides an address code on a public area of the USR database 24 that is available to all persons to see (1100). This code may for example be six alpha characters, which should be adequate for currently anticipated system populations. Optionally, the user may provide this code directly to a merchant or other person desirous of sending the person one or more parcels.

The user also provides address information to the address information area 38 of the user's entry in the USR database 24 (1102). Access to the address information 38 is restricted by a rule or other appropriate entry in the access information 34 of the user's entry to only permit mail, parcel or other material delivery services, such as the US mail, UPS and Fed Ex to access the address information.

When someone wishes to have a parcel or other items delivered to the user, the sender retrieves the user's address code from the USR database 24 or otherwise receives the address code from the user, and prints the address code on the parcel (1104).

The delivery service accesses the USR software 18, validates its identity, and queries the USR database 24 for address information corresponding to the address code (1106). The USR database 24 retrieves the appropriate address data and provides the address information to the delivery service. The delivery service then either prints out an address label, prints a machine readable bar code to be attached to the package, or correlates an entry in a delivery database between the address code and the user address (1110). The delivery service then uses this retrieved information to deliver the package to the user while never supplying the merchant with the user's permanent or temporary address. A user may also assure that mail, parcels, etc. are delivered to a current location by providing only a single notice to the USR system, regardless of how frequently the person moves. The person can also automatically provide for address changes where the person moves according to a known schedule. Thus, deliveries to be made on a weekday could be directed to one address and deliveries on a weekend to another address; or deliveries during winter months to one address and during summer months to a different address.

FIG. 12 illustrates a method of enabling a person to telephone a user of the USR system 10 without providing the user's telephone number to the person. In the embodiment illustrated in FIG. 12, the user provides a telephone code on the publicly available area of his entry on the USR database 24 (1200). This code may be assigned by the USR software 18 or made up by the user. The user also provides the USR database 24 with actual telephone information to enable the USR system 10 to connect callers with the user (1202).

The person wishing to telephone the user of the USR system 10 calls a telephone number and enters the telephone code of the user (1204). The USR software 18, optionally, may require the person to identify themselves to see if they are authorized to call the user.

Assuming that the person is authorized to call the person, or if no authorization check is performed, the USR connects the person to the telephone number in the USR database 24 without providing the person with the telephone number.

Enabling the user to specify the telephone number may be advantageous for many reasons. First, the user may frequently be switching between telephone coverage areas and may wish to be reachable at all times. Simply by instructing the USR database 24 to connect incoming telephone calls to one of a myriad of numbers will facilitate connecting the incoming calls to, for example, the user's cell phone, work phone, pager, car phone or home phone, without necessitating the user to provide all these numbers to the caller. A similar system may be implemented for facsimile transmissions, e-mails or other communications.

The user also may have predefined rules to enable telephone calls to follow a set pattern. For example, the user may desire to receive telephone calls only from family members during the night time at home, may wish to have all incoming calls routed to a car phone during commuting hours, and may wish to have all incoming calls routed to a cell phone during lunch. These time dependent rules may and/or caller specific rules may be entered into the USR database to specify accessibility and connectivity of incoming telephone calls.

The publicly available address code and telephone code and any other codes may be the same, or may be different, there being some advantages to having a single code usable for all such applications for each person on the system. The codes could be accessible through a variety of media including telephone and the Internet. Where two or more people on the system have the same name, which will frequently be the case, additional publicly available biographical data may be provided with the name to assure that the right code is selected. The system may similarly be used to provide public keys for use in a public key/private key encryption system, to provide other public codes for an individual or to provide other public information. Access to such information would typically be unrestricted.

Where the system is used to provide public keys, the public code used to obtain the key, or possibly the public key itself, may be used as above to obtain the e-mail address, telephone number or the like for the person to whom the message is being sent, and the USR system may also be used to perform the encryption. When the recipient receives the message, he deencrypts it using the recipient's private key in standard fashion, including deencrypting the name of the sender. However, this does not necessarily verify the sender and such verification may be desirable for important messages, particularly ones involving large financial transactions. The USR system may accomplish such verification by also storing private keys for people in the system. The sender first authenticates himself to the system, and the system then adds a second signature to the message which is encrypted with the sender's private key. The receiving party deencrypts this signature with the sender's public key. Since the system only sends such signatures for authenticated users, the message is thus verified.

FIG. 13 illustrates a general method of using the USR database 24 to authenticate a user's identification. This may be used in connection with any of the other methods disclosed herein to ensure that the electronic ID device has not been stolen and/or hacked by an unauthorized holder.

Specifically, in the embodiment illustrated in FIG. 13, the user attempts to prove identification to a validator, such as to prove that the possessor of the electronic ID device is of sufficient age to purchase alcohol (1300). In connection with this attempt, the user enters a secret code into the electronic ID (1302). The validator transmits to the USR software 18 the code from the electronic ID (1304). If the USR software 18 determines that the code is valid (1306), it accesses the user's photograph, age information, or any other desired information, and transmits that information to the validator (1308). By transmitting back to the validator a picture of the person to whom the electronic ID card was issued, the validator can ensure that the person using the electronic ID card is the proper person. Likewise, the validator can ensure, based on the information provided by the USR system 10, that the person is as old as the person claims to be.

A specific embodiment of this identification validation procedure is illustrated in FIG. 14. In FIG. 14, a policeman takes the place of the validator. In this scenario, however, instead of simply transmitting to the policeman a validation of the user's identity, such as their picture, the policeman may also receive additional information, such as the user's police records, records of any arrests, outstanding warrants, and other similar information that may be of use to the policeman when determining how to handle a particular individual.

FIG. 15 illustrates a process for enabling the user to provide specific information to a party, such as medical staff in an emergency room. As shown in FIG. 15, if the user desires to provide information to a party (1500), the user enters a secret code in the electronic ID device and provides the electronic ID code to the party (1502). The party transmits to the USR software 18 the ID code and the party code (1504). The party code may be a code from for example an electronic device which identifies the party, may be a status code which identifies the class of users to which the party belongs, for example policeman, emergency room personnel, doctor, etc. or may be a combination of both, the status code for example being encrypted into the ID code. The USR software 18 determines if the code is valid (1506), accesses the user's information in the USR database 24 and transmits available information to the party (1508). In this scenario, the user may be provided with a plurality of different codes to enter into the electronic ID device depending on the type of information to be released to the party. For example, the user's basic code may be 1234. The fifth digit of the electronic code may specify the type of information to be provided, i.e., 1 = address information, 2 = medical information; 3 = telephone information, 4 = job application information, etc. Using multiple codes eliminates any ambiguity about the authority provided by the user to the party, but requires the user to remember additional information.

The above assumes the user is able to provide an ID code when the information is required. However, in for example an emergency room situation, the user may not be in a position to provide the ID code, but would still want medical records provided. The release authorization for certain portions of the user's database could therefore specify that the information be released to certain class or classes of individuals and the USR system would release such information to individuals or organizations based only on status code. Thus, the status code of an emergency room could alone trigger release of medical data.

FIG. 16 illustrates one embodiment of a method of using the USR database 24 to complete a standard application, such as a job application or an application to rent an apartment. This embodiment is a specific example of the more generic method of enabling a party to retrieve information discussed above with respect to FIG. 15. In FIG. 16, however, the party may be provided with the opportunity to provide a form to the USR software 18, the fields of which may be automatically completed with information from the job application information section of the USR database 24.

As can be seen from the above, many of the users of the USR system are organizations or agencies such as carriers (post office, UPS, FedEx), communication companies, law enforcement organizations, hospitals and other medical facilities and the like. Each of these organizations can be provided with specialized software either on a disc or other suitable media or electronically, for example over the Internet, which performs a number of functions, for example automatically generating status codes for data access requests, controlling information received, and formatting data received in response to a request in a desired way. This can result in an access request from such organization for a given user causing all data on the user required to complete the form being retrieved and presented to the organization in the format of their form. A user may also authorize an organization for which a form has been completed using the USR system to receive updates, either in response to a request from the organization or at selected intervals, for example once a year, so as to maintain information in the forms current. Since the user will be providing information to the system on a regular basis, this is a relatively easy and painless way for the user to maintain current information with many organizations the user deals with.

Another potential use of the system is to permit a person to be located where only limited biographical information on the person is known. Users of the USR system wishing to participate in this feature could be cued to provide non-confidential biographical data when they come on the system or at any time thereafter when they decide to participate. They can also indicate whether they wish their name given out in response to such an inquiry or to merely be alerted to an inquiry which might involve them and information on the requester. A person seeking to find another person or group of people can input appropriate biographical data, for example members of 1975 Harvard University hockey team, or information of a person's last known address plus school information, etc. The system will then provide a list of persons who meet the listed criteria from which the person making the inquiry can hopefully find the person they are looking for.

In the above application and others, when a person is located, the person may request that only the person's address code or general access code (i.e. a single code which is used to get current address, telephone, e-mail, etc. information) be provided when the person is located. This can further protect the individual from undesired contacts.

Further, although each of FIGS. 13-16 refer to the entry of a secret code for validation by the USR system, the processes illustrated for each of FIGS. 13-16 may include a challenge-response protocol by which the user's identity is authenticated.

FIG. 17 illustrates another embodiment of the invention. As shown in FIG. 17, the USR system 10 may be used to secure expensive personal equipment, such as stereos, televisions, laptop computers, cellular telephones, cars, boats, and other items of value to a person. In this embodiment, each item to be secured using the USR system is provided with a USR timer chip imbedded in the electronics. If the USR timer chip is not provided with a code within a predefined period of time, for example every 30 days, the equipment is deactivated. Thus, for example, a television, mobile phone, laptop computer, automobile, heavy equipment, weapon or facility may be provided with a security chip having an internal timer that must be reset before expiration by provision of a particular code. When reset does not occur, the timer will disable the electronic device or other device using any one of a number of known disablement methods. Exemplary codes may be transmitted in the same manner as beeper signals are conventionally transmitted or may be transmitted to wired devices over the Internet or other public network.

The USR system 10 may be advantageously employed to automatically provide the secured property with the necessary codes at appropriate intervals, unless instructed by the user of the USR system 10 to cease doing so. Alternatively, the USR system 10 may require participation by the user prior to sending out the activation codes.

In this embodiment, the user may provide to the USR system 10, information indicative of the codes to be transmitted, timing information, and automation information -- i.e., whether the codes should be sent automatically or should require user intervention. Optionally, where the user opts to require user intervention, the USR system 10 may notify the user of the upcoming deadline via e-mail or another method.

This system may be useful to secure sensitive equipment other than personal equipment as well, such as military equipment, public equipment, school equipment and any other equipment that is subject to theft.

FIG. 18A illustrates another embodiment of the invention that can provide a centralized system to control access to a plurality of secure networks. As shown in FIG. 18A, for example, a system 1800 may employ the USR 10 to control access to a plurality of secure systems 1804 (e.g., a plurality of secure computer networks). The system 1800 may include one or more access devices 1802 that can be employed by a user to access a secure computer network included in the plurality of secure systems. In addition, the system 1800 may be employed to protect other secure systems such as secure communication networks and/or other resources that are accessed electronically. According to one embodiment, the system 1800 includes a first communication link 1801 that provides a communication path between the access device 1802 and the USR 10, and a second communication link 1803 that provides a communication path between the USR 10 and the plurality of secure system 1804. In one embodiment, each of the first communication link 1801 and the second communication link 1803 are wide area networks, for example, the Internet.

Each of the secure systems 1804 can be associated with an organization. An organization is any entity that employs a secure (e.g., restricted access) host system to provide resources to a plurality of users. For example, an organization may be a corporation (including a non-profit corporation), partnership, other business entity, an affiliation or individual that employs a secure host system to provide resources to a plurality of authorized users. As should be apparent to those of ordinary skill in the art, an organization is not restricted to any particular size, for example, as measured by the number of members or employees.

More specifically, each of the secure systems No. 1, No. 2, No. 3, etc. may be associated with a different organization and the USR 10 may control access to each of the secure systems. That is, the USR 10 can provide access control for a plurality of secure computer networks each associated with a different and unrelated organization. Further, each of the secure computer networks may have a different plurality of users who are authorized to access the network.

The access device may include any of a desktop computer, a laptop computer, and a handheld computer (e.g., a PDA, call phone and the like). Further, as shown in phantom, a plurality of access devices may communicate with the USR 10. Where a web-based system is employed, for example, each of a plurality of computers connected to the Internet may be individually employed as a separate access device to communicate (e.g., independently communicate) with the USR 10 to gain access to one or more of the secure systems 1804.

For example, the access device 1802 may be a computer employed with a client-server network. In this example, to access resources provided by one of the secure system 1804, the user initiates an access request for a secure system 1804 selected by the user. That is, the user may supply authentication information and a computer network ID to the USR. As is described in further detail below, the authentication information and the computer network ID are processed by the USR to authenticate the user and determine whether the user is authorized to access the secure system 1804 that is identified by the computer network ID. The USR then routes communications between the user and the secure system provided that the user authentication is successfully completed.

According to one embodiment, the USR 10 connects the access device 1802 to one of the secure systems 1804 via a communication path that does not include the USR 10. In an alternate embodiment, the USR 10 connects the access device 1802 to one of the secure system 1804 via a communication path that does include the USR.

Referring now to FIG. 18B, a system 1810 employs a USR 10 to control access to a secure system (e.g., a secure computer network) according to another embodiment. In one embodiment, the system 1810 includes the USR 10, an access device 1802, and a plurality of secure system 1804. According to this embodiment, the user selects from the plurality of secure systems 1804 a secure system that the user would like to access. With the access device 1802, the user communicates authentication information directly to the selected secure system 1804, e.g., without gaining access to the system. The secure system then communicates the authentication information and/or information corresponding to the authentication information to the USR 10. The USR 10 processes the information received from the secure system and then communicates an indication of whether the authentication information corresponds to one of the plurality of users authorized to access the secure system. The secure system grants or denies access to the secure system (and the associated resources) based on the indication received from the USR 10.

As illustrated in Figs. 18A and 18B, the USR 10 can provide a centralized access control system (e.g., an authentication system) for a plurality of secure systems 1804 that are associated with independent organizations that may have no affiliation with one another. Referring to Figs. 18A and 18B, a first organization may be associated with (have resources located on and/or accessed by) the secure system no. 1, a second organization may be associated with the secure system no. 2, and so on. In addition, a single organization may also be associated with a plurality of the secure systems 1804. Thus, in one embodiment, the USR 10 provides access control to a plurality of secure systems for a single organization.

The systems 1800 and 1810 allow an organization to operate a secure system without hosting the authentication system software or at least without the need to host a substantial part of authentication system software. Thus, in one embodiment, software upgrades/maintenance can be implemented at the USR 10 (e.g., centrally) for the plurality of secure systems 1804 and specialized authentication software is not required at the access device. In a further embodiment, specialized authentication software is also not required at the secure system. In versions of these embodiments, the USR 10 provides a web-based system in which the user employs a web-browser when communicating with the USR 10 and the secure system.

The USR 10 can also provide centralized administration and management for the plurality of secure systems 1804. The centralized administration can include routine tasks such as adding or removing authorized users for each of the plurality of secure systems 1804, for example, based on the hiring or resignation, respectively, of an employee. Additional administrative functions such as maintaining a secure database of private keys associated with each user, generating time varying codes, maintaining encryption software, maintaining audit trails and other functions may also be accomplished in a centralized fashion with the USR 10 for a plurality of organizations.

In one embodiment, following the connection of the access device 1802 to the secure system 1804, the USR 10 develops an audit trail by monitoring the communication path to capture information concerning the use of the secure system. For example, the USR 10 may collect and store information concerning the length of time during which the access device remains connected to the secure system, the type of resources accessed by the user, the type of data transmitted (including the identification of specific documents) during a login period and the volume of data transmitted.

According to one embodiment, the USR continuously monitors the communication between a plurality of access devices 1802 and a secure computer network and collects information to generate an audit trail for each device. According to another embodiment, the USR does not continuously monitor communications. Instead, the secure computer network intermittently (e.g., periodically) transmits audit information to the USR 10 where the audit information may concern one or a plurality of users connected to the network during a specific time period.

In each of the embodiments, described with reference to FIGS. 18A and 18B, the USR 10 may be located in an ultra-secure facility that employs heightened security relative to the security provided by the organizations that it serves. The physical facility where the USR is located may meet requirements generally associated with critical military installations. For example, the USR 10 may be housed in a facility that is hardened against radiation, shielded against electromagnetic interference, and/or protected against earthquakes, hurricanes, etc. to allow operation of the USR during times of general emergency. Further, the personnel and hiring policies of the facility operating the USR 10 may also be more secure relative to the security measures taken by the organizations associated with the secure systems 1804. That is, the individuals operating the USR 10 may undergo more rigorous background checks that include a detailed investigation of their personal and employment histories.

The centralized approach described above can provide increased security because the administration of the access control system (e.g., authentication software) is in the hands of a highly trusted third party who has taken heightened security measures regarding the hiring of the administrative personnel, in particular, the personnel who have access to authentication data (e.g., private encryption keys, etc.).

In any of the preceding embodiments, the USR 10 may be geographically remote from the secure systems.

Further, in any of the preceding embodiments, there may be situations where a user employs the access device 1802 to connect to more than one of the plurality of secure systems 1804. In one embodiment, the user is independently authorized to access separate secure systems 1804 associated with independent organizations. In another embodiment, the user is authorized to access separate secure systems 1804 each associated with the same organization. In either situation, the user may employ one or more of the authentication procedures described herein before being allowed access to any one of the secure systems 1804.

Referring now to FIG. 19, a process 1900 that employs a USR to control access to a secure computer network is illustrated. In one embodiment, the process 1900 is employed with the system 1800 illustrated in FIG. 18A. At step 1902 an entity initiates an access request. In general, the access request will be initiated when the user or entity inputs information into an access device such as a computer. At stage 1904, the entity supplies authentication information and a computer network ID to the USR (e.g., the information is electronically transmitted from the access device to the USR). According to one embodiment, the information is transmitted via the Internet from the access device to the USR. At stage 1906, the USR receives the access request which includes the authentication information and the computer network ID. At stage 1908, the USR determines whether the authentication information is valid for a user. According to one embodiment, the USR includes a database containing selected data of a plurality of users authorized to access a secure computer network, and may compare the authentication information supplied by the entity with authentication information included in the database to determine whether the authentication information corresponds or is valid for a user. If the authentication information is valid, the process 1900 moves to stage 1910 where the USR determines whether the entity is authorized to access the computer network identified by the computer network ID. If the entity is authorized to access the computer network then the USR may allow communication between the entity and the secure computer network at stage 1912. As previously indicated, the USR may route communications between the entity and the secure computer network and remain in the communication path employed by the access device to communicate with the secure computer network. Alternatively, the USR may simply provide a connection between the access device and the secure computer network where the communication path provided by the connection does not involve the USR.

Returning to stage 1908 if the authentication information supplied by the entity is not valid for any of the plurality of users then the process 1900 moves to stage 1914 where an indication is provided to the entity that access is denied. Similarly, if at stage 1910 the entity is not authorized to access the computer network identified by the computer network ID, an indication is provided that the entity is denied access at stage 1914. In various embodiments, the entity may be allowed additional opportunities to successfully access the system.

Referring now to FIG. 20, a process 2000 for controlling access to a secure computer network is illustrated in accordance with one embodiment. In one embodiment, the process 2000 is employed with the system 1810 illustrated in FIG. 18B.

In one embodiment the entity initiates an access request at stage 2002. As described above, the access request can be initiated using an access device and each secure computer network may communicate with a plurality of access devices. At stage 2004, the entity supplies authentication information to the secure computer network, for example, by entering the information in a web browser and transmitting the authentication information over the Internet to the secure computer network. At stage 2006, the secure computer network receives the authentication information. At stage 2008, the secure computer network communicates authentication information to the USR (or information corresponding to the authentication information) to allow the USR to authenticate the access request. At stage 2010, the USR validates the authentication information to determine whether the entity is authorized to access the secure system, and at stage 2014, the secure system receives an indication from the USR concerning whether the entity is authorized to access the system. In one embodiment, the indication is transmitted from the USR to the secure system via the Internet. At stage 2016, the secure system grants or denies the entity access to the secure system based on the indication received from the USR.

As should be recognized by those of ordinary skill, the processes 1900 and 2000 can be accomplished in a variety of stages that may include any of the stages described above in various combinations and sequences including one or more of the stages described above in combination with one or more additional stages.

Various embodiments can be employed to control access to a physical facility. That is, an electronic device (e.g., a keypad, a card reader, a biometric scanner, etc.) or combination of electronic devices can be located at an access point to a secure area (e.g., a door, a gate, etc.). The entity initiates the request using the electronic device. In one embodiment, the physical facility includes all or a portion of the secure computer network. Thus, in one embodiment, the secure system receives an indication of whether an entity is authorized to access a physical facility. The secure system communicates authentication information to the USR. The USR validates the authentication information and communicates an indication of whether the entity is authorized to access the physical facility. The secure system receives the indication and grants or denies the entity access to the physical facility.

Each of the embodiments described with reference to any FIGS. 18-20, may include a challenge-response protocol, for example, to authenticate the identity of the entity and/or the USR system to the other.

FIG. 21 illustrates an embodiment of a system 2100 for validating the identity of an individual or an entity. The system includes a first wireless device 2110 and a second wireless device 2112. The first wireless device 2110 comprises a first wireless transmitter and receiver 2114, a first processor 2116 and a first memory 2118. Similarly, the second wireless device 2112 comprises a second wireless transmitter and receiver 2120, a second processor 2122 and a second memory 2124. According to aspects of the invention, the first wireless device and the second wireless device are configured to wirelessly communicate with each other so that the entity associated with the first wireless device can communicate his identity to the entity associated with the second wireless device. It is to be appreciated that the first wireless transmitter and the second wireless transmitter can be configured to communicate by any form of a wireless signal such as low power Bluetooth signal, infrared signals, RF signals and electromagnetic signals in general. In accordance with one embodiment, the first wireless device and the second wireless device communicate via near field signal.

The first wireless device can also comprise user interface 2126 that allows the first entity to interact with the first wireless device and can also comprise a display, such as a LCD display, 2118 that allows the first entity to further interact with the first wireless device. In accordance with some embodiments the invention, the first wireless device can be configured so that the first entity must enter a PIN identification number, for example, via the user interface to gain access to the wireless device. Alternatively, or in addition, the first wireless device may comprise a biometric sensor or detector 2130 that enable the first entity to present biometric data to the first wireless device to gain access to the first wireless device. For example, the biometric sensor can be configured to detect a fingerprint of the first entity. For such embodiment, the memory 2128 also comprises stored biometric data of the first entity, which is compared, for example, by the processor 2116 with the detected biometric data to determine whether the first entity is enabled or should be disabled from using the first wireless device. It is also to be appreciated that the biometric data need not be fingerprint data and can be any biometric data known to those of skill in the art, and that the biometric sensor need not be a fingerprint sensor and can be any biometric sensor known to those of skill in the art.

Similarly, the second wireless device 2112 can also be configured as discussed above with respect to the first wireless device, namely with any or all of a user interface 2132, a display 2134 and a biometric sensor 2136 and can be configured to require any and/or all of a second entity to provide a PIN number, or the second wireless device to match biometric information of the second entity with stored biometric information to enable or disable the second entity to gain access to the second wireless device. Each of the first wireless device 2110 and the second wireless device 2112 comprise a power source or a power source interface 2138, 2140 that can be coupled to a power source that provides power to respective devices. It is to be appreciated that the power source can be any power source, such as, alkaline batteries, rechargeable batteries, proprietary power sources, and interfaces to power sources such as standard 120 VAC, or an AC to DC conversion device, as well as any other type of power source known to those of skilled in the art. In addition, it is to be appreciated that each of the first wireless device 2110 and the second wireless device 2112 can also comprise an additional wireless transmitter and receiver device 2142, 2144, respectively, which enable each of these devices to communicate wirelessly via other wireless communication systems such as, via any cell phone standard, via satellite communications, over wireless area networks, local area networks, wide area networks, as well as any other wireless communication standard know to those of skill in the art.

According to some embodiments of the system 2100 of FIG. 21, either or both of the first wireless device 2110 and the second wireless device 2112 can be configured to communicate with a secure database 2146, as will be discussed in further detail herein. According to some embodiments, either of the first or second wireless devices may communicate with the secure database on a periodic basis to update it's corresponding data, or to stay alive as will be discussed herein, or to retrieve information in the secure database that is used in the communication protocol between the first and second wireless devices to verify the identity of at least the first entity. Accordingly, it is to be appreciated that communication with a secure database can be, for example, via the additional respective wireless transmitters and receivers 2142, 2144 of the first and second wireless devices, or can be via a network interface 2152, 2154 of the respective devices, that communicate with a network 2148 and to the secure database 2146.

Referring now to FIG. 22, there is illustrated one embodiment of an overall communication process that occurs with the system 2100 of FIG. 21. In particular, the process is effected by the system of FIG. 1 so as to identify and authenticate the identity of the first user associated with the first wireless device 2110 to the second user associated with the second wireless device 2112. For example, consider the situation where an air marshal or an FBI agent is carrying the first wireless device 2110 and airport security or security personnel generally want to ensure the identity of the user of the device 2110. The communication protocol 200 illustrated in FIG. 22 is one embodiment of a protocol that enables secure authentication of the first user of the wireless device 2110.

According to one embodiment of the process, the first user of the first wireless device 2110 first authenticates his or herself to the wireless device 2110, for example as has been discussed above, by either entering a PIN via the user interface 2126 of the first wireless device or by interacting with the biometric sensor of the first wireless device at step 202. In various embodiments, a challenge-response protocol is employed in which the first user supplies information (a biometric, a PIN or other information) to authenticate his or herself to the wireless device 2110. If the user of the device does not enter the correct PIN number or does not match the biometric data stored in memory 2118 of the first authorized user of the device, then the device at a minimum shuts down at step 204. However, according to some embodiments, the device 2110 can also be configured to automatically delete any portion of or all of the data stored in memory 2118 at step 206. In addition, as will be discussed in further detail herein, according to some aspects of the invention, the first wireless device can be configured to periodically communicate with the secure database 2146 to remain alive, for example, after the first user of the first device authenticates itself to the first device. If the first device does not communicate with the secure database at such periodic intervals at step 208, then the first device can be configured to delete any or a portion of the data stored in memory at step 206.

The communication protocol also comprises a second user of the second device to authenticate his or herself to the second device at step 210. It is to be appreciated that the authentication by the second device of the second user by any of the mechanisms discussed herein and above with respect to the first wireless device, including entering a PIN number to the user interface 2132 of the second wireless device or by interacting with the biometric sensor 2136 of the second wireless device. In addition, it is to be appreciated that as discussed above with respect to the first wireless device, if such identification is not successful, the second wireless device will at a minimum shut itself down at step 212. However, it is also to be appreciated that the second wireless device can be configured to automatically delete a portion of or all of the data stored in the memory 2124 of the second wireless device, should such authentication not be successful at step 214. In addition, it is to be appreciated that the second wireless device can also be configured at step 216 to communicate with the secure database 2146 within defined periods of time, or even a periodic interval once the second user authenticates himself to the second wireless device, and to delete a portion of or all of the data in memory 2124 should such periodic communication not occur.

If both the first user and the second user are successful in authenticating themselves to the first and second wireless devices respectively, then a communication protocol is initiated between the first wireless device 2110 and the second wireless device 2112 at step 218. If the communication protocol is not a valid communication protocol between the devices, the devices wait until there is a valid communication protocol. If the communication protocol is a valid protocol (218 yes), then the first wireless device transmits a first wireless signal containing encrypted authentication information of the first user to the second wireless device 2112 at step 220. The details of the communication protocol and the encrypted authentication information will be discussed further herein.

The second wireless device 2112 receives the first wireless signal and processes the wireless signal to determine the identity of the first user. In particular, as will be discussed herein, according to some aspects of the invention, the authentication of the first user includes displaying a picture of the first user to the second user on the display 2134 of the second wireless device as a result of the communication from the first wireless device to the second wireless device. The user of the second wireless device can view the picture on the display and ascertain whether the first user of the first wireless device is who he or she purports to be. However, as will also be discussed herein, it is to be appreciated that the second wireless device need not be a device that requires a user to interact with it and can be, for example, an unmanned detection system that receives the first encrypted authentication information and determines from the first authenticated encrypted information whether the first user is authorized to gain access to a secured place, a secure network, or a secure computer, to do whatever the first person is seeking to do. If the first user is not who they purport to be, the communication process goes back to look for a valid communication protocol. In addition, the process allows the second user or the system associated with the second wireless device to take an appropriate action such as denying access to the secure site at step 224.

If the user of the first wireless device is authenticated (at step 222 yes), then according to some aspects of the invention, the communication process allows for the second wireless device to transmit a second wireless signal comprising encrypted authentication information of the second user to the first wireless device at step 226. In addition, according to such aspects, the communication protocol and the first wireless device are configured to authenticate the identity of the second user to the first user at step 228. It is to be appreciated that the authentication of the second user to the first user can be in any of the manners discussed above with respect to the authentication of the first user of the first device, such as by viewing a picture of the second user as provided on the display 2128 of the first wireless device, by matching one-time information contained in the encrypted authentication information or via a challenge-response protocol.

In addition, according to some embodiments of the protocol, either or both of the first wireless device 2110 and the second wireless device 2112 may communicate with the secure database 2146 to retrieve additional information at step 230. Such information, as will be discussed herein, can include for example, a portion of the biographic data of the first user of the first wireless device or of the second user of the second wireless device, or full biometric information of the first user or the second user, which can be communicated back to the respective device and used by the respective device to authenticate the user. In addition, the information can be periodic updates as provided the secure database to the respective device, such as will be described herein, including periodic updates of public keys of a plurality of first users as stored in memory on the second wireless device, or updates to public keys of a plurality of second users as stored in memory on the first wireless device. In addition, such information may include periodic updates of the biometric information of a plurality of first users as stored on the second wireless device or a plurality of second users as stored on the first wireless device, which can comprise for example a portion of the biometric information or all of the biometric information.

Referring now to FIG. 23, there is illustrated one embodiment of various fields included within the first wireless signal and the second wireless signal as transmitted between the first wireless device and the second wireless device. According to some embodiments, the signal comprises a header field 302. The header field can be any header field known to those of skill in the art. In addition, the signal comprises a public ID field 304, which can comprise, for example, any of name information, a badge number, an employee number, an e-mail address, a social security number, and the like, of the first user. In addition, the first wireless signal may also include a digital signature field 306 containing a digital signature of the first user. For example, the digital signature may be generated with the user's private PKI key. Further, the first wireless signal may comprise a one-time time varying code field 308 that includes a random code as generated by the first wireless device. According to some embodiments, the digital signature field and the one-time code field can be used, for example by the second wireless device, to allow access to a secure place without the need for a user of the second wireless device to interact with the second wireless device to authenticate the first user. As an example, referring to FIG. 24, the digital signature and one time code can be encrypted with the private key of the first user and transmitted to the second wireless device. The second wireless device can decrypt the digital signature and one time code with the public key of the first user at steps 402-404 to authenticate or not the first user at step 406.

In addition, referring back to FIG. 23, the first wireless signal also comprises a PKI encrypted one-time DES key field 310 comprising a PKI encrypted one-time DES key. Further, the first wireless signal comprises a DES key encrypted biometric data field 312, which includes at least a portion of biometric data of the first user encrypted with the DES key. As will be discussed in further detail herein, according to some aspects of the invention, the public key of a first user, for example, stored in memory 24 of the second wireless device can be used to decrypt the DES key, and the DES key can be used to decrypt at least a portion of the biometric data of the first user to use in the authentication of the identity of the first user. According to some embodiments, the first wireless signal can also comprise another ID data field 314, which can contain other information such as name, height, weight, eye color or anything else.

It is to be appreciated that although the embodiment of the wireless signal discussed in FIG. 23 has been discussed with reference to the first wireless signal transmitted from the first wireless device 2110 of FIG. 21 to the second wireless 2112, that the same protocol can be used when transmitting a second wireless signal from the second wireless device 2112 to the first wireless device 2110 to authenticate the identity of the user of the second wireless device to the user of the first wireless device. It is to be further appreciated that various fields of the signal can be used and not all of the fields of the wireless signal are needed to authenticate identity of the user.

Referring now to FIG. 24, there is illustrated one embodiment of a process 400 as identified by act 222 in FIG. 22 for verifying or authenticating the identity of the first user of the first device. According to this embodiment, which has been briefly discussed herein with respect to FIG. 23, the second wireless device can verify the identity of the respondent without necessarily interacting with a second user by decrypting the first user's digital signature from the digital signature field 306 at step 402 and verifying that it is the digital signature of the first user, decrypting the one-time code from the one-time code field 308 at step 404, and using this information at step 406 to authenticate the first user. If the first user is authenticated at 406, an appropriate action such as allowing access to the secure site, or computer, or network can be granted.

Referring now to FIG. 25 there is illustrated another embodiment of a process 520 for authenticating the identity of the first user at step 222 of the communication process of FIG. 22. According to aspects of the invention, the second wireless device at step 522 receives the first wireless signal and extracts the PKI encrypted DES key from field 310. The wireless device looks up the public key of the first user from memory 2124 [See FIG. 21] or from a secure server based on the information provided in the public ID field 304 at step 524. The second wireless device uses the first public key to decrypt the PKI encrypted DES key at step 526. The second wireless device acts on the DES key encrypted biometric information from the field 312 and uses the decrypted DES key to decrypt the at least a portion of the biometric information of the first user as included in the first wireless signal at step 528.

According to some embodiments, the biometric information included in the first wireless signal is a portion of the biometric information of the first user and the second wireless device is configured to store a remainder of the biometric information of the first user in memory. According to such embodiments, the process 520 also comprises looking up the remainder of the biometric information stored in the memory at step 530 and combining the remainder of the biometric information with the decrypted and extracted biometric information to provide complete biometric information of the first user at step 532. According to some aspects of the invention, the biometric information can comprise a digital image of the first user and for such aspects, the digital image can be displayed on display 2134 of the second wireless device so that the second user can ascertain whether the first user associated with the first device is who he or she purports to be. However, it is to also be appreciated that the biometric information can be fingerprint information, a voiceprint, DNA codes of the first user, or any other biometric information known and used by those of skill in the art. Accordingly, the processor 2122 of device 2112 can also be configured to process the combined biometric information to authenticate the first user at step 536.

Referring now to FIG. 26, there is illustrated another embodiment of a process 620 that can be used to authenticate the identity of the first user at step 222 of the process 200 of FIG. 22. According to this embodiment, some of the steps are similar to the steps of the process 520 illustrated in FIG. 25 and accordingly a full description of these steps will not be herein duplicated. It is to be appreciated that this embodiment can be used for example, where the biometric information of the plurality of first users is not stored on the second wireless device 2112 but is instead stored at the secure database 2146 as illustrated in FIG. 21. In particular, for highly secure applications, where there is a worry that the second wireless device can be compromised (even with the necessity to authenticate the second user to the second wireless device), the second wireless device can be configured to interact with the secure database to obtain at least a portion of the biometric information of the first user, rather than storing at least a portion of the biometric information of the first user in memory on the second wireless device.

According to such embodiments, the second wireless device can receive the first wireless signal including the fields discussed above in respect to FIG. 23, in particular, the public ID field 304 and optionally the PKI encrypted DES key. According to some embodiments, the PKI encrypted DES key may be used by this process. At step 624, the second wireless device accesses public key information of the first user from the public keys stored in memory on the second wireless device. However, it is to be appreciated that in some embodiments, the public keys may not be stored on the second wireless device. For such embodiments, the second wireless device will communicate with the secure database to obtain the public key of the first user also at step 624. According to some embodiments, at step 626 the second wireless device transmits a signal to the secure database comprising public identification number to identify the second device to the secure database, presumably after the second user of the second device has authenticated his or herself to the second device. For such embodiments, at step 628, the secure database determines whether the second device is authorized to access the secure database at step 628. It is to be appreciated that according to some embodiments, this communication between the second wireless device and the secure database can be accomplished with encrypted signals and in some embodiments the encrypted signals can include using time varying one time codes to further secure the communication. If the second device is authorized to interact with the secure database, the process also comprises transmitting the first public ID from the second wireless device 2112 to the secure database at step 630, and with this information, the secure database accesses the biometric or identification information of the first user at step 632. The biometric or the at least a portion of the biometric information can then be transmitted by the secure database to the second wireless device at step 634. Again, this transmission can be encrypted and further include time varying or one time codes to further secure the communication. The second wireless device can use the received portion of the first biometric information and combine it with portion of the first biometric information provided in the first wireless signal, or can receive all of the first biometric information as provided by the secure database and, for example, display it on the display 2134 of the second wireless device 2112 at step 636, or can process the biometric or identification information at step 638 to determine whether the first user is authenticated.

Referring now to FIG. 27 there is illustrated one embodiment of a data structure 720 that can comprise memory 2124 of the second wireless device 2112. It is to be appreciated that any or all of the various portions of this data structure can be present in the memory 2124. According to some aspects of the invention, the memory will include the private key of the second user at field 722. The private key can be used, for example, when communicating by the second wireless device to the first wireless device to provide a digital signature of the second entity encrypted with the second user's private PKI key to the first user. In addition, the memory can also comprise a plurality of public keys of a plurality of first users at area 724. Such public keys of a plurality of first users can be used as has been discussed herein in combination with the private key of the first user to decrypt information of the first user. For example, the public and private key can be used to decrypt the DES key of the first user. In addition, the memory can also comprise at least a portion of biometric data of a plurality of first users, at area 726. As been discussed herein, the at least a portion of the biometric data of the plurality of first users can be combined with the portion of the biometric data provided in the first wireless signal or from the secure database, to create the complete biometric data of the first user for ascertaining or authenticating the identity of the first user as has been described herein. In addition, the memory can also comprise biometric data of the second user at field 728. The biometric information of the second user can be used, for example, as has been discussed herein to compare the biometric data detected by the biometric sensor 2136 of the second wireless device to determine whether the second user is authorized to have access to the second wireless device. It is to be appreciated that the data structure 720 of FIG. 27 can also comprise the memory 2118 of the first wireless device 2110, and that any or all of the fields of the data structure 720 can exist in the memory 2118 in the first wireless device. It is also to be appreciated that the first wireless device can access the data structure 720 and the various fields for the same purposes as discussed above with respect to the second wireless device, namely, to provide the first digital signature of the first entity encrypted with the first private key in the first wireless signal, to access the public keys of a plurality of second users for the purpose of decrypting information provided in the second wireless signal, to access at least a portion of biometric information of the second user stored in the field 726, as well as to compare biometric information of the first user with sensed biometric data provided by the biometric sensor 2130 of the first wireless device.

In one embodiment, the method comprises acts of receiving first authentication information about the first entity with the first device, transmitting the authentication information about the first entity to a secure database, determining whether or not the first entity is allowed to access the first device based on the first authentication information, and transmitting an enablement signal to the first device indicating to enable nor not enable the first entity to access the first device. According to a further embodiment, the method also includes an act of allowing or not allowing operation of the first device based on the enablement signal. In another embodiment, the act of receiving the first authentication information of the first entity comprises receiving biometric information of the first entity by detecting the biometric information with the first device.

In yet another embodiment, the act of transmitting the first authentication information about the first entity to a secure database comprises generating a non-predictable signal from the biometric information. In a further embodiment, the act of generating the non-predictable signal from the biometric information comprises generating a time varying non-predictable signal from the biometric information. In a still further embodiment, the act of receiving biometric information of the first entity comprises receiving a voice signature of the first entity with the first device and the act of generating the non-predictable signal from the biometric information comprises mixing the voice signature of the first entity with a random code to generate the non-predictable signal. In yet a further embodiment, the act of transmitting the enablement signal to the first device comprises sending the random code to the first device. In a still further embodiment, the act of receiving biometric information of the first entity comprises receiving fingerprint data of the first entity with the first device and the act of generating the non-predictable signal from the biometric information comprises mixing the fingerprint data of the first entity with a random code to generate the non-predictable signal. In another embodiment, the act of transmitting the enablement signal to the first device comprises sending the random code to the first device.

In a further embodiment, the act of authenticating the biometric of the first entity comprises authenticating a voice signature of the first entity. In another embodiment, the act of authenticating the biometric information of the first entity comprises authenticating a finger print of the first entity.

In one embodiment, a first wireless device includes a biometric detector comprising a fingerprint detector that detects a fingerprint of the first entity. In an alternate embodiment, the biometric detector comprises a voice signature that detects a voice signature of the first entity.

According to one embodiment, the system comprises a first wireless device including a processor configured to enable operation of the first wireless device if it receives an enablement signal validating first biometric information of a first entity and configured to generate a non-predictable signal from the biometric information, a first wireless transmitter and receiver configured to transmit a first wireless signal including first encrypted biometric information of the first entity and to receive the enablement signal, a first biometric detector for detecting the first biometric information of the first entity and a secure database configured receive the first wireless signal, to authenticate or not authenticate the first biometric information of the first entity, and to provide the enablement signal validating or not validating the first biometric data of the first entity.

In a further embodiment, the secure database further comprises biometric data of a plurality of first entities. In another embodiment, the processor is configured to generate the non-predictable signal from the biometric information by generating a time varying non-predictable signal from the biometric information. In a still further embodiment, the processor is configured to generate the non-predictable signal from the biometric information by mixing the biometric information of the first entity with a random code to generate the non-predictable signal. In yet another embodiment, the secure database is configured to transmit the enablement signal to the first device including the random code so as to authenticate the secure database to the first device. In still another embodiment, the system includes a memory for storing a private key of the first entity authorized to use the first device.

It should be understood that various changes and modifications of the embodiments shown in the drawings and described in the specification may be made within the spirit and scope of the present invention. Accordingly, it is intended that all matter contained in the above description and shown in the accompanying drawings be interpreted in an illustrative and not in a limiting sense. The invention is limited only as defined in the following claims and the equivalents thereto.

FIG. 28 illustrates an embodiment of a system 100 that employs a converter device 102 to provide an interface between a user device 104 (e.g., a transaction card, a cell phone, etc.) and a system interface 106 where, for example, the system interface 106 employs a magnetic card reader and the user device 104 is not equipped with a magnetic stripe. That is, in one embodiment, the converter device 102 provides a mode of information transmission between the user device 102 and the system interface 106 which would otherwise be unavailable to the user device 102. The converter device 102 provides a modified system 100 that provides compatibility with a greater variety of user devices, for example, user devices such as transaction cards, cell phones or PDAs that are not equipped with a magnetic stripe. For example, in one embodiment, the converter device 102 includes a magnetic stripe emulator 137 communicatively coupled to a wireless signal receiver 140 and adapted to provide a time-varying signal emulating data provided by a magnetic stripe card to a magnetic card reader 152.

The user device need not be a "card" and may, for example, take the form of a fob used as a key ring, a cell phone, a watch, a personal digital assistant or any device that can include a wireless transmitter, or a magnetic stripe emulator.

In various embodiments, the user device 104 employs near field signal to communicate with the converter device 102. In one embodiment, the near field communication is bi-directional such that the user device 104 may both send and receive wireless communication. That is, the user device includes a transceiver.

In general, the system interface 106 provides an interface to a larger information system (e.g., a financial system, an access control system, a medical records system, and the like) that in one embodiment includes a system processor or controller 110, a database 112, a network 114, other systems 116, such as a universal secure registry 118 as will be described further herein. Each of the preceding system elements may be placed in communication with any one or any combination of the system elements, for example, over communication links 120A, 120B, 120C, 120D. It should be recognized that the communication links 120 need not provide the communication paths shown in FIG. 28 and that other communication paths may be employed. For example, the database 112 may be connected to the network 114 via the communication link 120A and to the system processor 110 via the communication link 120B instead of being connected as shown in FIG. 28.

The communication link may be a wireless communication link, a hardwired communication link, a fiber optic communication link, any communication link used in the art, as well as a combination of any of the preceding or any other any communication link capable of transmitting signals between the elements of the system 100. The system processor 110 allows information transfer of both data and instructions, for example, between the interface 106 and one or more databases which may be connected to the system or other network elements.

In general, the operation of the converter device 102 allows a user in possession of the user device 104 to wirelessly communicate information to the device so that the device can be employed to interface with a network system. For example, in one embodiment, the network system may provide a magnetic card reader interface and the converter device 102 provides a magnetic stripe emulator that can interface with the system. In general, the overall operation of the system 100 includes the communication of information between the user device 104 and the converter device 102, for example, RF communication. In one embodiment, the communication is bi-directional such that information can be communicated both to and from the user device 104. The converter device 102 provides an interface by which information derived from the information being transmitted to or from the user device 104 is transmitted between the converter device and the system interface 106. The system interface 106 provides the communication interface between it and the remainder of the system 100 (e.g., processor 110, database 112, network 114, etc.).

According to one embodiment, the user device 104 includes a processor 122, a user interface 124, a wireless transmitter 126 and device indicia 128. In another embodiment, the user device 104 includes a biometric sensor 130. In various embodiments, the processor 122 is communicatively coupled to each of the wireless transmitter 126, the user interface 124 and the biometric sensor 130.

The processor 122 may include a chip such as a general purpose processor, an application specific integrated circuit ("ASIC"), or a field programmable gate array ("FPGA") and the like that may execute various programs and/or provide logic inputs and outputs. For example, the processor 122 may process biometric information received from the biometric sensor 130 to verify the identity of the user before the user can employ the user device 104. Exemplary details of a processor and biometric sensor which are configured to authenticate a fingerprint of a user are disclosed in U.S. published application 2004/0133787, published on July 8, 2004, which is herein incorporated by reference in its entirety. The processor 122 may also include or be coupled to driver circuitry to drive a display included in the user interface 124 and can be configured to process user input data entered via the user interface 124. In one embodiment, the user interface 124 includes one or more control inputs (for example, control buttons).

The wireless transmitter 126 can process information provided by the processor and convert the information to an RF signal and can also include an RF antenna that transmits the RF information wirelessly. In another embodiment, the user device may also include an RF receiver that receives a wireless RF signal from the RF antenna and converts the RF signal to an information signal provided to the processor. It is to be appreciated that the wireless transmitter and/or receiver need not be an RF device; it can also be any of an IR device, an optical device, a Bluetooth signal or any other wireless signal transmitter or receiver used in the art.

The user device may also include a power source such as a battery that fits within the device. In one alternative embodiment, the user device remains in a sleep mode until it is placed in the vicinity of an RF transmitter at which time the user device 104 converts received RF energy into electrical energy used to provide power to the processor 122 and the other components included in the user device 104.

According to one embodiment, the user device 104 can be a smart card configured for wireless signal transmission using RF signals. For example, the wireless transmitter 126 may be an RF transmitter device or any other wireless transmitter device configured to transmit the smart card information of the card. Alternatively, it is to be appreciated that the card can be many cards such as a debit card, a plurality of credit cards such as VISA, MasterCard, American Express, or any other card with the card indicia and relevant information being stored in card memory 129 and read out by processor 122 and provided to the wireless transmitter 126. However, the user device 104 need not be in the form of a card and may instead include a cell phone or PDA.

In the embodiment illustrated in FIG. 28, the converter device 102 includes a substrate 132 which may include a stripe 134 and a magnetic field generator 136 which together comprise the magnetic stripe emulator 137, a processor 138, a wireless receiver 140, a user interface 142, a memory 144, and a power source 146. In a further embodiment, the converter device 102 includes an indicating light 148 (e.g., an LED) and an output device 150.

According to one embodiment, the system interface 106 with which the converter device 132 is employed includes any of or all of a magnetic card reader 152, a wireless transceiver 154 and a data port 156.

In general, according to one embodiment, the converter device 102 receives a wireless signal from the user device 104, processes the information that is received and provides an output in the form of a time-varying signal provided to the stripe 134 (e.g., a magnetic stripe). The signal provided to the stripe 134 can then be provided to the system processor 110 by inserting the stripe and the associated substrate 132 or portion thereof in the magnetic card reader of the system interface 106. That is, in one embodiment, the stripe 134 and at least a portion of the substrate 132 can be either slid by the magnetic card reader 152 or inserted to sit statically in front of the read head of the card reader.

The processor 138 may be a general purpose processor, an application specific integrated circuit ("ASIC"), or a field programmable gate array ("FPGA") and may be implemented in hardware, software, firmware or any combination of the preceding. The processor 138 may be communicatively coupled with any of the magnetic field generator 136 the wireless receiver 140, the memory 144, the user interface 142, the light source 148, the power source 146 and the output device 150. In general, the processor can be configured to receive inputs from one or more of the preceding elements and may provide outputs to each of the elements included in converter device 138.

For example, according to one embodiment, the magnetic stripe 134 is a programmable magnetic stripe and the magnetic field generator 136 generates a magnetic signal that controls the information provided by the magnetic stripe 134. The U.S. Patent Application No. 10/680,050, filed October 7, 2003, entitled "System Method and Apparatus for Enabling

Transactions Using a Biometrically Enabled Programmable Magnetic Stripe which was published on July 8, 2004 as US2004/0133787 (the ‘050 application), provides further details concerning embodiments of the user device that emulates a magnetic stripe and may also include, for example, a biometric sensor. The ‘050 application is incorporated herein by reference in its entirety. In this embodiment, the processor 138 may control the operation of the magnetic field generator 136 to provide the desired information to the stripe 134. For example, the processor 138 may provide an output to the stripe 134 in response to receiving information from the wireless receiver 140, where the information from the wireless receiver is information transmitted from the user device 104.

Further, the processor 138 may be configured to provide signals to drive a display included in the user interface 142 and process user input data entered with the user interface 142. In one embodiment, the user interface 142 includes a display screen that can be used to display an image of the user to whom the user device 104 belongs, for security purposes. The image to be displayed by the UI can either be part of the information transmitted by the user device 104, for example, where the user device 104 also requires some authentication by the user before transmitting the device information and image, or can be provided, for example, by the USR system 118 through the system interface 106 as part of the user authentication process, as will be described in more detail herein. In further embodiments, the user interface 142 may include a plurality of control elements that allow the user and/or the transaction processor (e.g., store clerk, security guard, medical service provider, etc.) to enter information into the converter device 102. According to one embodiment, the user interface 142 includes an LCD display.

The processor 138 may also be configured to provide signals to operate the indicating light 148. The indicating light 148 may provide an indication of the operational status of the converter device 102, for example, the indicating light 148 may indicate any of the following: that the converter device 102 is receiving a transmission from a user device 104; that the converter device 102 has generated output data to the stripe 134; the status of the power source 146 is normal or conversely that the power source has a low power level; that the converter device 102 is transmitting information via the output device 150; that the converter device 102 is properly aligned with the magnetic card reader 152; that the converter device 102 has received authorization for a transaction; and the like. It should be apparent to one of skill in the art that the indicating light may be a single lamp or a plurality of lamps and that the lamp or lamps may be a single color including white or may included a plurality of colors. Further, it should also be apparent that the lights may provide a plurality of status indications based on their color, intensity, rate of change of the preceding characteristics or any combination of these and other features.

The power source 146 may include a battery power source or other energy sources suitable for the form factor of the converter device 102. For example, in a form factor where the converter device 102 is a hand-held device the power source 146 may be any one of a standard size battery (e.g., a AA battery). In a further embodiment, the power source is a lithium battery. Alternatively, the power source can be any of an AC power source, an AC to DC converter device, or any other DC power source known to those skilled in the art.

According to one embodiment, the converter device 102 includes a power bus 158 that provides a path for the transmission of power to the various components included in the converter device 102.

In accordance with one embodiment, the converter device 102 includes the output device 150. It is to be appreciated that the output device can be any standard interface device to be coupled to a data bus such as a USB device, or the output device can be configured for contactless communication with the system interface 106. For example, in one embodiment, the output device is an optical transmitter device. In general, the communication between the converter device 102 and the system interface 106 is bi-directional such that information (e.g., information associated with the user's identity) may be transmitted to the system interface 106, the system processor 110 may generate a response (e.g., a transaction approval), and the response may transmitted to the converter device 102 via the system interface 106.

In one embodiment, the processor 138 is configured in combination with the output device 150 to provide an encrypted output signal. In a further embodiment, the processor 138 is configured in combination with the output device 150 to provide a time-varying encrypted output signal. In yet another embodiment, the processor 138 is configured in combination with the output device 150 to provide a time-varying encrypted (or not) public and private key output signal. In addition, the processor can also be configured in combination with the wireless receiver to receive and decrypt any and all of an encrypted signal, a time-varying encrypted signal and a signal encrypted with a private key as provided by the user device 104.

A challenge-response protocol may also be employed alternatively or in addition to any of the preceding.

For example, embodiments of the invention may employ a protocol that does not require synchronized clocks in each of the user device 104 and the converter device and/or elsewhere in the system 100 to complete a validation and/or authentication process. That is, according to one embodiment, an information exchange between the user device 104 and the converter device 102 includes a first piece of information transmitted from the user device 104 to the converter device 102 and a subsequent challenge (e.g., an encrypted challenge) generated by the converter device and transmitted from the converter device to the user device 104. According to one embodiment, the user employs the user device to respond to the challenge. In one embodiment, the user's response is at least in part based on information included in the challenge. An identity of a user who responds accurately to the challenge can be successfully validated. In various embodiments, a challenge-response protocol includes an information exchange whereby the identity of the converter 102 is also authenticated by the user with the user device 104.

In various embodiments, the above-described challenge-response protocol may not require any further action by the user than is required under current approaches that require synchronized clocks in disparate devices.

In some embodiments, the output device 150 need not transmit any personal information associated with the user. For example, commonly owned U.S. Patent Application No. 09/810,703, filed March 16, 2001, entitled "Universal Secure Registry" ("the '703 application") describes an approach that can improve security and reduce the need for multiple forms of identification. The '703 application is incorporated herein by reference in its entirety. The universal secure registry 118 included in the system 100 provides one example of the integration of such a registry into a system that employs a converter device 102. With the USR system, for example, the user device 104 can provide some information, e.g., such as a public code of the user, which can be authenticated by the user, for example by providing an ID through the user interface 124 or through biometric sensor 130. The public code can be provided to the USR via the converter 102, system interface 104, and network 114. The USR can then provide back to any of the system interface and the converter device any or all of device information (e.g., transaction card information), authorization for a transaction, e.g., where the network or the USR also communicates with the relevant authority, and indicia about the holder of the user device.

The system 100 may include a variety of system interfaces 106 of different types such as the wireless transceiver 154 and the data port 156 in addition to the magnetic card reader 152. Although not illustrated, other system interfaces such as an optical interface, a smart card reader interface or any other system interface known to those of skill in the art can also be included. Further, the system interfaces may be either commonly located or may be geographically distributed such that some locations include a wireless transceiver 154, some locations include a data port 156, some locations include a magnetic card reader 152, and some locations include a plurality of types of system interfaces.

Thus, in some embodiments the output device 150 of the converter device 102 may include a data port via which the converter device 102 can provide data to a network or a networked device. In one embodiment, the data port is also configured to receive data from the network or a networked device.

Embodiments of the converter device 102 can be configured to provide communication to the system interface 106 via any of the preceding approaches including wireless signal transmission. In a version of this embodiment, the converter device 102 may receive wireless signals from the user device and transmit wireless signals to the system interface 106. Further, the converter device may include a transmitter that allows it to transmit information back to the user device.

Referring now to FIG. 29, a process 260 employing the converter device 102 is illustrated in accordance with one embodiment. The process begins at Stage 262 –START. Here, the converter device 102 is in a steady state in which it awaits receipt of a signal from a user device 104. At Stage 264, the converter device 102 receives data, for example, a wireless signal transmitted from the user device 104. At Stage 266, the converter device 266 extracts information from the wireless signal for processing. As one example, the converter device 102 may extract information corresponding to the user's identity and/or the identity of the individual to whom the user device was issued. The extracted information is then provided to the system interface, for example, it is simulated as magnetic striped data to the magnetic card reader. At Stage 268, the system 100 authenticates the user. In one embodiment, if the authentication is successful, the process continues at Stage 270. In this embodiment, if the authentication is unsuccessful, the process returns to Stage 262 where, for example, the user may be prompted to attempt to authenticate again.

Various user authentication approaches may be implemented using the converter device 102. For example, the authentication may be performed locally, that is, without the need for communication between the converter device 102 and the system interface 106 and system processor 110. In one embodiment, the authentication process employs the universal secure registry 118. In further embodiments, the authentication process employs one or more authentication protocols such as public-key cryptography, key exchange protocols, protocols employing one-way functions, and the like that are well known by those of ordinary skill in the art. In other embodiments, however, the authentication may require an exchange of information between the converter device 102 and any of the system interface 106, the network 114, the USR 118 and another database 112. A challenge-response protocol may also be employed alternatively or in combination with any of the preceding authentication approaches.

At Stage 270, the completion of the transaction may be involve any of a wide variety of acts including: authorizing a withdrawal of money from a user's account, permitting the user access to a secure area, permitting a user to view medical information concerning themselves or a third party, or permitting the user to access other confidential information.

In addition, in some embodiments, the process 260 includes Stage 274 where following authentication the converter device 102 receives information associated with the user. The information may, for example, be necessary for the completion of the transaction. For example, where the system 100 is employed in conjunction with a check-authorization process, the converter device 102 may receive an indication that the user has sufficient funds to cover the amount of the check that is presented at a point of sale. Alternatively, or in addition, the information may include indicia related to the authorized holder of the user device 104, such as a picture ID. The process 260 is completed at Stage 272 – END.

An embodiment, of the converter device 302 is illustrated in FIGS. 30A through 30D. As illustrated in the front view of FIG. 30A, in one embodiment, the converter device 302 includes a housing 380, a substrate 332, and a magnetic stripe 334. In one embodiment, the housing 380 is manufactured from a rigid material, for example, metal or plastic and the converter device 302 is designed to be a hand-held device. FIG. 30B illustrates a side view perspective of an embodiment of the converter device 302, showing an indicating light 348 (e.g., an LED). As described in greater detail above, the indicating light 348 can include a single indicating light or a plurality of indicating lights.

FIGS. 30A-30D illustrate an embodiment where the substrate extends substantially perpendicular from a side of the housing 380, however, the specific angle at which the substrate extends from the housing may vary so long as the housing does not interfere with the insertion of the substrate into, for example, the magnetic card reader 152.

FIG. 30D illustrates a top view of an embodiment of the converter device 302 which includes a display screen (e.g., an LCD display screen) that may provide the user interface 342 or a portion of the user interface of the converter device 302. In one embodiment, the user interface 342 includes a display screen that displays either a black and white or a color image of the individual to whom the user device 104 was issued. It should be recognized that the display screen may provide a wide range of functionality, for example, the display screen may display a variety of data received by the converter device 302 including data represented in alpha numeric format.

The magnetic stripe 334 may be a programmable magnetic stripe such that the converter device 302 provides a magnetic stripe emulator. In one embodiment, as has been described herein, the converter device 302 receives a wireless signal from a user device 104 and provides a time varying signal which emulates data provided by a magnetic-stripe card to a magnetic card reader in response to receiving the information from the wireless signal. In a further embodiment, the information is provided to the magnetic card reader by inserting the magnetic stripe 334 into the magnetic card reader.

The various embodiments of a system and method for converting a wireless transaction device to a magnetic stripe emulator device may include any of the following or any combination of the following: a converter device with a processor communicatively coupled to a wireless signal receiver and to a magnetic stripe emulator. The converter device may optionally include an LED. Further the processor may be configured for any combination of the following: control of the LED to indicate that the device is properly aligned with the magnetic card reader, control of the LED to indicate that the device has received authorization for a transaction, and where the converter device includes a power supply, a processor configured to control the LED to indicate that the device has power.

In one embodiment, the information received from the wireless signal by the converter device may include any of a name, a card number, user identification, a device code, amount of credit available, and an expiration date of the card for a transaction.

Further, in various embodiments, the converter device may include an output device that can provide information to a network or to a networked device. In various embodiments, the output device can be configured as a wireless transmitter device, such as an optical transmitter device.

In various embodiments the wireless transmitter device where the wireless transmitter may generally be configured as an RF transmitter device, and in particular, as a Bluetooth transmitter device.

In addition, in various embodiments, the processor can be configured in combination with the output device to provide any of an encrypted output signal, a time-varying encrypted output signal, and in particular, a time-varying public and private key output signal.

In further embodiments, the converter device may include an output device configured as a data port via which the converter device can provide data to a network or a networked device and to receive data from the network or a networked device.

In one embodiment, the converter device may also include an LCD screen for displaying at least some of the data received by the converter device, and a processor configured in combination with the LCD device to display indicia corresponding to the authorization of a transaction, and in particular, indicia that includes picture information of the cardholder.

In addition to the above described features, the various embodiments of a system and method for converting a wireless transaction device to a magnetic stripe emulator device may include any combination of the following or any combination of the following and the above listed features: the converter device can be configured to communicate with the magnetic card reader via the data port; the wireless receiver and/or processor is configured to decrypt an encrypted wireless signal; the converter device is configured to decrypt a time-varying encrypted wireless signal; the converter device configured to decrypt time-varying public and private key information contained within the wireless signal; the converter device includes a user interface communicatively coupled to the processor; the converter device processor is configured to determine whether the user is authorized to provide the information contained within the wireless signal from data provided through the user interface.

In addition, the following further additional features may be combined alone or in combination with the preceding: the data contained within the wireless signal received by the converter device may include any combination of the following: user I.D. information, biometric information of the user, secret information, (for example, a PIN, a password, or a passcode of the user), or information about an uncounterfeitable token of the user.

In various embodiments, the converter device may include a substrate housing the magnetic stripe emulator, and the substrate may include a programmable magnetic stripe.

In various embodiments, the system employed with the converter device may also include a system interface coupled to a network where the system interface includes a magnetic stripe reading device configured to read a time-varying signal. In a further embodiments, the system interface may be configured to transmit data received from the wireless transaction device to a networked credit card authentication entity also coupled to the network. The system may also include any of a keyboard, a printer, an (LCD) display, and an audio signal transducer.

Although the preceding description is primarily directed to an embodiment of the user device 104 that does not include a magnetic stripe, it should be recognized that some embodiments of the user device 104 may include a magnetic stripe. In these various embodiments, the converter device 102 may be employed to convert information coded on the magnetic stripe for transmission via another mode of information transmission.

As described above, various embodiments allow a user to employ a mobile phone or other device as a token to assist the user in securely accomplishing a variety of operations. Some embodiments also allow the user to employ the token in combination with a USR system to increase the utility of the token and the functionality and security of the various operations. That is, the token may be employed to assist the user in conducting operations that access data concerning commercial transactions (for example, retail purchases), finance and banking operations, medical records and medical information systems, physical security and access control, and identification and authentication of the parties involved in any of the preceding, etc.

Referring now to FIG. 31, a system 350 is illustrated for use in facilitating financial transactions in accordance with some embodiments. As used herein with reference to Fig. 31, the term “financial transaction” can include any of sales transactions including transactions conducted on-line or at a point of sale using credit or debit accounts, banking transactions, purchases or sales of investments and financial instruments or generally the transfer of funds from a first account to a second account. The system includes a user device 352, a point-of-sale (“POS”) device 354 and a universal secure registry 356 which can communicate with one another wirelessly, and/or over a network 357.

According to one embodiment, the user device 352 includes a display 362, a user interface 364, a communication link 366 and a biometric sensor 367. In various embodiments, the user device 352 may be any of a mobile phone, a personnel digital assistant or other handheld device.

In various embodiments, the communication link 366 may include any of a receiver and a transmitter suitable for wireless communication such as via RF and/or optical signals. Accordingly, in some embodiments, the communication link 366 includes an antenna and/or an optical signal source such as a LED alone or in combination with an optical receiver. In accordance with one embodiment, the user device 352 can employ an optical signal in the infrared spectrum. In various embodiments, the user device 352 can be configured to communicate by any form of a wireless signal such as a Bluetooth signal, WiFi, near field communication, ultra-wideband communication, RF signals and electromagnetic signals in general.

In some embodiments, the biometric sensor 367 may be employed to receive and process biometric inputs such as any of or any combination of a fingerprint, a speech/voice input, an iris scan, a retina scan, a facial scan, a written input, the user’s fingerprint and DNA. In a further embodiment, the biometric sensor can be employed to process a written input that includes a signature.

In addition, various embodiments of the user device 352 may be in the form of a smart card or other type of credit card as described previously. Further, in some embodiments, the user device 352 may include an embodiment of the first wireless device 2110 illustrated in FIG. 21. Accordingly, in various embodiments, the user device 352 can include all or some of the features and functionality found in the first wireless device 2110. That is, the user device

352 can include features that may not be illustrated in FIG. 31, for example, a microprocessor, memory, a power source, etc. In yet another embodiment, the first wireless device 2110 can be employed to conduct transactions in accordance with the embodiment illustrated in FIG. 31 and described below.

In general, the POS device 354 may be any type of POS device as known to those of ordinary skill in the art. In accordance with some embodiments, the POS device 354 includes a display 368, a user interface 370 and a communication link 372. Further, in some embodiments, the user device may include an embodiment of the second wireless device 2112 illustrated in FIG. 21. Accordingly, in various embodiments, the POS device 354 can include all or some of the features and functionality found in the second wireless device 2112. That is, the POS device 354 can include features that may not be illustrated in FIG. 31, for example, a microprocessor, memory, a power source, a biometric sensor, etc. In yet another embodiment, the second wireless device 2112 can be employed to conduct transactions in accordance with the embodiment illustrated in FIG. 31 and described below. Further, it should be apparent to those of skill in the art that the POS device may be a handheld device or a larger "countertop" device. It should also be apparent to those of skill in the art that the POS device may communicate wirelessly with the network or may be coupled to the network 357 via a hardwired connection.

In accordance with one embodiment, the network 357 includes a plurality of networks that may allow communication between any of the user device 352, the POS device 354 and the USR 356 over any communication medium including wired networks (including fiber optic networks) or wireless networks. Further, the network may include one or more of either or both of local area networks and wide area networks including the Internet. In general, the network 357 can be employed for communication between the user device 352 and the USR 356, communication between the user device 352 and the POS device 354, communication between the POS device 354 and the USR 356, and communication between the user device 352 and the USR 356 via the POS device 354. According to the illustrated embodiment, the system 350 may also include a network 374 that allows communication between the user device 352 and the POS device 354 but does not provide communication with the USR. A wireless personal area network such as Bluetooth provides one example, while a local WiFi network, near field communication and ultra-wideband communication provide further examples of various embodiments of the network 374. As should be apparent to those of ordinary skill in the art, however, the network 357 may include any of the preceding in accordance with some embodiments.

Further, in accordance with some embodiments, the user device 352 may wirelessly communicate with a converter device, for example, the converter device 102 described with reference to FIG. 28. According to this embodiment, the converter device is used to communicate with the POS device 354, for example, where the POS includes a mag-stripe reader.

According to one embodiment, the USR 356 includes a secure database that stores account information for a plurality of users 358. In a further embodiment, the USR 356 retains records concerning one or more accounts 360 for each of the plurality users so that in effect the USR 356 in the system creates a secure wallet that allows a user of the device 352 to select a particular account from among a plurality of accounts associated with the user for use in a selected transaction. The type of account can vary in accordance with various embodiments. In accordance with one embodiment, the accounts 360 are credit card accounts, for example, any of those serviced by VISA, MasterCard, Discover and American Express. Alternatively or in combination with the preceding, the accounts 360 may be debit accounts associated with the various bank accounts held by the user 358.

In accordance with various embodiments, the user device 352 includes software that allows the user device 352 to operate in combination with the USR 356. In accordance with one embodiment, the user device 352 can initially be provided with the software or it can be retrofitted by downloading software for operation with the USR via the network 357. In one embodiment, the software is loaded via a cellular network. In another embodiment, the software is loaded via any wireless network such as a WiFi network. In a further embodiment, the software is included in a Subscriber Identity Module ("SIM") that can be removably installed in the user device 352. In yet another embodiment, the software is loaded over a hardwired communication link between the user device 352 and an access point to the network 357. Accordingly, various embodiments can allow a user to download the software for operation with the USR (including the initial receipt of the software, later updates, security patches, etc.).

In general and in accordance with one embodiment, the system 350 allows each user to employ their respective user device 352 to purchase goods or services at a wide variety of points-of-sale, and further, to make such purchases from one or more accounts selected from a plurality of accounts 360. Accordingly, the system 350 allows users to employ a mobile phone as an "electronic wallet" to select, at the point-of-sale, a particular account from among a plurality of available accounts, for example, a plurality of credit card accounts. Further, in some embodiments, the system 350 allows users to employ the approach for purchases that are made using the Internet. As mentioned above, the system 350 can also be employed in other forms of financial transactions including banking transactions and investment transactions.

In accordance with some embodiments, the user device 352 is activated for a transaction when the user satisfactorily completes an authentication process with the device. In some embodiments, the entry of a PIN number known to the user is employed to activate the device. In some embodiments, the software included in the user device 352 and employed in conducting transactions using the system 350 remains inoperative until the entry of the correct PIN. In a further embodiment, the data (for example, contact lists and associated information) stored in the user device 352 is unavailable or unintelligible until the entry of the correct PIN. In accordance with one embodiment, the data in the user device 352 is stored following a mathematical operation that acts to modify the data such that it is unintelligible. In this example, the user device 352 employs the PIN supplied by the user to reverse the mathematical operation, for example, by performing an exclusive or operation ("XOR") on the data using the PIN to render the data legible. In other words, this embodiment provides a secure embodiment of the user device that is useless in the hands of a user without knowledge of the PIN information, as without the entry of the PIN, the data stored on the device is useless.

In a further embodiment, the above approach is used to disable the software employed by the user device 352. That is, a mathematical operation is performed on software stored in the user device 352 with the PIN. Once the mathematical operation is performed the modified software is unusable and the software remains inoperative until the PIN is supplied by the user. Here too, an XOR operation may be employed to recover the software, which allows the software to operate.

In accordance with one embodiment, the preceding approaches provide an increased level of security because the theft of the user device 352 (for example, the mobile phone) is not enough for the thief to employ the user device 352. Instead, a third party in possession of the user device 352 cannot employ the device to conduct a transaction without knowledge of the PIN.

Some embodiments can employ a multi-factor authentication process before allowing a user to employ the user device 352 to conduct a transaction. That is, the system 350 can authenticate a user based on something the user knows, something the user is, and something that the user has. According to one embodiment, the user device 352 is included in the last element of the three factors. For example, many electronic devices, including mobile phones, include an electronic serial number. Thus, in one embodiment, the user is authenticated and allowed to conduct a transaction with the USR 356 by providing something the user knows (for example, a PIN), something the user is (for example, a biometric measurement as detected by the biometric sensor 367) and something the user possesses (for example, the mobile phone as evidenced by the correct electronic serial number). In accordance with this embodiment, the PIN, the biometric information and the electronic serial number are communicated to the USR 356 where the user is authenticated. In various embodiments, the multiple pieces of data can be combined (for example, cryptographically combined through known encryption techniques) before being communicated. The transaction and/or access to the user's account info are permitted when an authentication is successful. Conversely, a transaction can be denied/refused where the authentication is unsuccessful, for example, where one or more of the PIN, the biometric information and the electronic serial number are incorrect.

According further embodiments, the multi-factor authentication process can also employ the identification of the account selected by the user for the current transaction. That is, the system 350 can authenticate the user based on a combination of two or more of something the user knows, something the user is, something that the user has and an account selected by the user for the current transaction (i.e., the transaction for which the authentication is being completed). For example, in one embodiment, encrypted authentication information is generated from a non-predictable value generated by the user device 352, identifying information for the selected user account 360, and at least one of the biometric information and secret information the user knows (for example, a PIN). According to one embodiment, the authentication information (for example, encrypted authentication information) is communicated to the secure registry for authentication and approval of the requested account access and/or financial transaction. In a further embodiment, one or more aspects of the authentication and approval are completed at the POS, for example, using the POS device 354, while in another embodiment, the POS provides a conduit or communication path from the user device 352 to the secure registry 356.

According to another embodiment, the user device 352 is secured such that authentication information cannot be generated by the user device 352 prior to an authentication of the user based on the biometric input provided to the user device 352. In one embodiment, the user device 352 performs the authentication. In another embodiment, the POS device 354 authenticates the biometric information provided by the user. In yet another embodiment, the biometric information is authenticated by the secure registry 356.

According to one embodiment, any two of the PIN, the biometric information, the electronic serial number, a discrete code associated with the device and the identifying information concerning the selected account are employed to generate a seed from which further authentication information is generated, for example, to generate a seed from which a non-predictable value can be generated by the user device 352. For example, in one embodiment, the seed is employed in an algorithm that also employs a temporal value to generate the authentication information. In one embodiment, the seed and the further authentication information are generated at the user device 352 and are provided to either or both of the second device 354 and the USR 356. Either or both of the second device and the USR can use the authentication information to authenticate or validate the identity of the user of the device 352, as has been described herein. In accordance with another embodiment, all four of the PIN, the biometric information, the electronic serial number and the identifying information concerning the selected account are employed to generate the seed. In one embodiment, the discrete code that is associated with the device is also used in combination with each of the preceding to generate the seed.

In some embodiments, the discrete code that is associated with the device is provided in lieu of the electronic serial number while in other embodiments the unique code is employed with the electronic serial number to generate the seed. In one embodiment, the discrete code is unique to the user device 352. In accordance with one embodiment, the discrete code is inaccessible to an individual in possession of the device. Further, the discrete code may be maintained by the user device 352 such that any indication that the security of the device is compromised results in the discrete code being set to a default value (for example, zero) which effectively prevents valid authentication information from being generated by the user device 352. As just one example, the preceding security measure can be taken when the device receive an indication that it is being used under duress.

In another embodiment, a challenge/response protocol is employed, for example, where the USR 356 communicates a challenge to the user device 352 and access to the USR is only granted where the user's response is correct. In accordance with one embodiment, a correct response is generated using any of the PIN, the biometric information and the electronic serial number in combination with the information provided as the challenge. As has been discussed herein, the challenge/response protocol can be invisible and seamless to the user of the device 352, since other than the user providing any of PIN and/or biometric information, the communication protocol of the challenge/response protocol can be done in the background without active participation from the user.

According to some embodiments, the validation of the biometric information provided by the user can be performed on a character by character basis. For example, where the biometric information includes a spoken word or phrase, each spoken character (whether alpha or numeric) can be individually evaluated to determine whether it was provided by a user authorized to employ the user device 352. In various embodiments, the authentication of the biometric occurs at the user device 352, at the POS device 354, at the USR 356 or at a combination of the preceding.

In accordance with some embodiments, the security of the system may be further increased where the system 350 allows for one or more approaches to limit the use of the user device 352. For example, according to one embodiment, the system allows a user to establish limitations on the use of the user device 352. For example, a user may establish an active period or periods as the only period(s) that the user device 352 can be used in combination with the USR 356. Accordingly, the active period may include a temporal element. For example, the active period may be so many consecutive hours or days beginning from the start of the activation period, a fixed period of time during every day, certain days of the week, etc. As should be apparent to those of skill in the art, in one embodiment, operation of the user device 352 may be completely disabled outside of the designated active period(s). In the embodiment illustrated in FIG. 31 where the system 350 is employed for financial transactions including credit card purchases, the user may limit the use of the user device 352 to conduct such transactions to a maximum amount of a single transaction, a maximum cumulative amount of all transactions, a maximum quantity of transactions and/or a predetermined monetary amount. According to some embodiments, each of the preceding can be employed alone or in combination with a temporal element such that, for example, the maximums are determined for an active period of time having a known length. Further, the values may be set by the user, or for example, by an issuer of the user device 352. Alternatively, the maximum values may be provided by an issuer of one or more of the plurality of user accounts 360.

As a further security enhancement, the user device 352 can be configured to cease operating when an unauthorized use of the device is detected. The unauthorized use may be detected where the user 352 provides an indication that the device is being used under duress as described above. In one embodiment, a transaction in which a user signals the use under duress proceeds but the user device 352 becomes inoperative for one or more subsequent transactions. In a further embodiment, the system 350 communicates information concerning the situation to local law enforcement, for example, the location of the user device and the identity and/or appearance of the user. According to one embodiment, a constant is added to the value of the PIN when the user device 352 is being used under duress. For example, the user can enter a value which corresponds to the PIN plus one.

In some embodiments, the USR 356 provides consolidated security for the plurality of user accounts associated with a plurality of individual service companies (i.e., VISA MasterCard, etc.) who employ USR. In some embodiments, this avoids the need for the individual service companies to separately monitor the security of transactions for each of their respective accounts even where the service companies are not be affiliated with one another.

In a further embodiment, the user device 352 may destroy data/information present in the user device based on the occurrence of an event or multiple events. In one embodiment, this action is the result of evidence of tampering with the user device 352, for example, the repeated entry of an incorrect PIN. In another embodiment, the user device 352 destroys sensitive information (or a subset of information included in the user device 352) following the passage of a predetermined period of time of, for example, inactivity. It is also to be appreciated that, in an embodiment, the underlying data and/or software need not be destroyed in the above events, but instead there may be a lockout period as a result of the above events for which the device is rendered unusable. This lockout period may be extended and/or increased for repeated events discussed above.

It is to be appreciated, as has been discussed herein, that according to some embodiments, biometric information of a user of the first device or authentication of biometric information of the user of the first device can be provided to the second device 354 for any of the purposes described herein in any of the following ways: at least in part from the first device 352, at least in part from the USR 356, and at least in part from reading the biometric data stored on the second device.

In accordance with one embodiment where wireless communication is employed to communicate information between the user device 352 and the POS device 354 (for example, communication via Bluetooth protocol), the POS device may receive signals from a plurality of user devices 352 in the vicinity of the POS device 354. Accordingly, the POS device 354 may be employed to select from a plurality of users to conduct a transaction. For example, where an image of each of the users in the vicinity is displayed at the POS device 354, the individual operating the POS device 354 may select the user (and associated accounts) by selecting the photo of the user who is employing the user device 352 for the current transaction.

It is to be appreciated, as has been discussed herein, that according to some embodiments the system 350 including the USR 356 is used to provide authorization for an occurrence of an event, such as a credit or debit transaction, without providing secure information such as the credit or debit card number. In particular, for such embodiments, the USR either by itself or in combination with credit or banking authority, authenticates the user of the first device and the selected account information and either provides a one time code for authorizing the transaction or a denial to the second device, which can be displayed on the second device to indicate the approval or denial of the transaction to the POS operator. It also to be appreciated that the system can also be employed, for example, for internet purchase through a web site where the USR can alone or in combination approves or denies the transaction and provides the approval or denial to the operator of the web site, for example, where the user of the first device 352 either manually logs into a web site and provides account information, or where the user of the first device communicates via the first device 352 and the token provided by the first device with the web site. It is also to be appreciated that the code or information displayed at the second device 354 can enable many forms of a transaction not just limited to a credit or debit transaction. It can include approval for enablement of any of the events that have been described herein. In addition, the code or information can, for example, provide authorization or security that funds exist in the account to cover a check written by the user of the first device, in effect providing a code that turns the personal check into a certified check, without the need for the user of the first device having to obtain a bank check.

In various embodiments of the preceding system, the system 350 can be employed as a peer to peer network. For example, the first device and the second device are configured as peer to peer devices, in combination with the USR 356 or in some embodiments without the needs for information in the USR 356, as has been discussed herein, to authenticate and/or validate an identity of a user of the first device to the second device and in addition to authenticate and/or validate an identity of a user of the second device to the first device, to allow an occurrence of an event, such as a credit or debit transaction, access to a secure location, passport identification information and the like.

Although the above-described system 350 employs the USR 356 to facilitate the preceding operations, the above approach may be employed with alternative systems that include a secure database with the user's account information. Further, although the preceding description concerning FIG. 31 primarily discusses sales transactions, the system 350 may be employed in a variety of fields to allow only authorized access by authenticated users to secure data, for example, as illustrated in FIG. 4, and the like as has been described herein.

Further, the user device can in some embodiments be used to authenticate identity in a variety of applications. That is, an authentication code can be generated by the user device 352 as described above where the authentication code is used to determine whether the user is authorized to take one or more actions. According to one embodiment, the authentication code is provided to a security system to determine whether the user is permitted to access a physical facility, for example, to determine whether the user is permitted to access a residence or a place of business. In a further embodiment, the user device 352 wirelessly communicates an authentication code to a home security system as part of an access request. The authentication code generated by the user device 352 can be used in a similar manner to determine whether an individual can access a computer network, for example, log in. According to additional embodiments, such an authentication code can also be used to provide positive identification of an individual in possession of the user device 352 in the manner of a passport, driver's license or other form of identification issued by the government or another third party such as an employer.

In one embodiment, a user device is configured to allow a user to select any one of a plurality of accounts associated with the user to employ in a financial transaction. In one embodiment, the user device includes a biometric sensor configured to receive a biometric input provided by the user, a user interface configured to receive a user input including secret information known to the user and identifying information concerning an account selected by the user from the plurality of accounts. In a further embodiment, the user device includes a communication link configured to communicate with a secure registry, and a processor coupled to the biometric sensor to receive information concerning the biometric input, the user interface, and the communication link. According to one embodiment, the processor is configured to generate a non-predictable value and to generate encrypted authentication information from the non-predictable value, the identifying information, and at least one of the information concerning the biometric input and the secret information, and to communicate the encrypted authentication information via the communication link to the secure registry. According to another embodiment, the secret information includes the identifying information.

In a further embodiment, the communication link wirelessly transmits the encrypted authentication information to a point-of-sale (POS) device, and the POS device is configured to transmit at least a portion of the encrypted authentication information to the secure registry. Further, the POS device can include a magnetic stripe reader.

In yet another embodiment, the communication link wirelessly transmits the encrypted authentication information to a converter device configured to generate an emulated magnetic stripe output for use with the POS device.

In still another embodiment, the user device includes a memory coupled to the processor where the memory stores information employed by the device to authenticate the biometric received by the biometric sensor. In one embodiment, the device does not permit the entry of the user input if the biometric input received by the biometric sensor is determined to not belong to an authorized user of the device.

According to a further embodiment, the secret information known to the user includes a PIN, and the authentication of the secret information and the biometric input activate the device for the financial transaction. In one embodiment, the user device includes a memory coupled to the processor and the data stored in the memory is unavailable to an individual in possession of the device until the device is activated. According to his embodiment, the data can be subject to a mathematical operation that acts to modify the data such that it is unintelligible until the device is activated.

In accordance with some embodiments, a method of generating authentication information includes acts of authenticating an identity of a user to a device based on at least one of biometric data received by the device from the user and secret information known to the user and provided to the device. The method can also include the generation of a non-predictable value with the device. The method can further include acts of receiving identifying information from the user concerning a selected one of a plurality of user accounts and generating encrypted authentication information from the non-predictable value, the identifying information, and at least one of the biometric data and the secret information. In a further embodiment, the device can generate encrypted authentication information from each of the non-predictable value, the biometric data, the secret information, and the identifying information.

In accordance with another embodiment, the method includes an act of de-activating the device without generating the encrypted authentication information if the identity of the user is not successfully authenticated to the device. Embodiments may also include an act of generating encrypted authentication information in a manner that allows the identification of the user and the selected one of the plurality of user accounts by a secure registry.

According to a still further embodiment, a method of controlling access to a plurality of accounts is provided where the method includes acts of generating, with a device, encrypted authentication information from a non-predictable value generated by the device, identifying information concerning an account selected by a user of the device from among a plurality of accounts associated with the user, and at least one of a biometric of the user received by the device and secret information provided to the device by the user, communicating the encrypted authentication information from the device to a secure registry via a point-of-sale (POS) device to authenticate or not authenticate the device with the secure registry, authorizing the POS device to initiate a financial transaction involving a transfer of funds to or from the account selected by the user when the encrypted authentication information is successfully authenticated, and denying the POS device from initiation of the financial transaction involving a transfer of funds to or from the account selected by the user when the encrypted authentication information is not successfully authenticated.

According to a further embodiment, the method includes an act of authenticating an identity of the user by validating the biometric with one of the device and the secure registry. In some embodiments, the biometric can be validated on a character-by-character basis.

According to yet another embodiment, the method includes an act of transmitting image data from the secure registry to the POS device along with an authorization authorizing the POS device to initiate the financial transaction provided that the image data when processed at the POS device authenticates an identity of the user. In a further embodiment, the method also includes an act of authenticating the identity of the user at the POS device by any of displaying an image of the user at the POS device for visual confirmation by an operator of the POS device and processing biometric data provided by the image data. The operator may be a store clerk, bank clerk, security personnel or an individual in any other capacity in which they are tasked with a responsibility to verify an identity of an individual in possession of the user device.

In accordance with one embodiment, the secure registry includes a database containing information concerning a plurality of accounts associated with a different one of a plurality of users, respectively. Further, the plurality of accounts can include accounts associated with a plurality of different financial service providers. According to some embodiments, the method can include an act of transmitting information including at least a portion of the encrypted authentication information to the secure registry from the POS device.

Having thus described several aspects of at least one embodiment of this invention, it is to be appreciated various alterations, modifications, and improvements will readily occur to those skilled in the art. Such alterations, modifications, and improvements are intended to be part of this disclosure, and are intended to be within the spirit and scope of the invention. Accordingly, the foregoing description and drawings are by way of example only.

What is claimed is:

CLAIMS

1. A device configured to allow a user to select any one of a plurality of accounts associated with the user to employ in a financial transaction, comprising:

a biometric sensor configured to receive a biometric input provided by the user;

a user interface configured to receive a user input including secret information known to the user and identifying information concerning an account selected by the user from the plurality of accounts;

a communication link configured to communicate with a secure registry; and

a processor coupled to the biometric sensor to receive information concerning the biometric input, the user interface and the communication link, the processor configured to generate a non-predictable value and to generate encrypted authentication information from the non-predictable value, the identifying information, and at least one of the information concerning the biometric input and the secret information, and to communicate the encrypted authentication information via the communication link to the secure registry.

2. The device of claim 1, wherein the communication link is configured to wirelessly transmit the encrypted authentication information to a point-of-sale (POS) device, and wherein the POS device is configured to transmit at least a portion of the encrypted authentication information to the secure registry.

3. The device of claim 2, wherein the POS device includes a magnetic stripe reader, and wherein the communication link is configured to wirelessly transmit the encrypted authentication information to a converter device configured to generate an emulated magnetic stripe output for use with the POS device.

4. The device of claim 2, wherein the processor is configured to generate the encrypted authentication information from each of the non-predictable value, the identifying information, the information concerning the biometric input and the secret information.

5. The device of claim 1, wherein the biometric received by the biometric sensor is communicated to the secure registry for authentication prior to generation of the encrypted authentication information.

6. The device of claim 1, wherein the secret information includes the identifying information.

7. The device of claim 1, further comprising a memory coupled to the processor, wherein the memory stores information employed by the device to authenticate the biometric received by the biometric sensor.

8. The device of claim 7, wherein the device does not permit the entry of the user input if the biometric input received by the biometric sensor is determined to not belong to an authorized user of the device.

9. The device of claim 8, wherein the secret information known to the user includes a PIN, and wherein the authentication of the secret information and the biometric input activate the device for the financial transaction.

10. The device of claim 9, further comprising a memory coupled to the processor, wherein data stored in the memory is unavailable to an individual in possession of the device until the device is activated.

11. The device of claim 10, wherein the data is subject to a mathematical operation that acts to modify the data such that it is unintelligible until the device is activated.

12. The device of claim 9, further comprising a memory coupled to the processor and configured to store an electronic serial number of the device, wherein the processor is configured to generate a seed using at least two of the electronic serial number, a discrete code associated with the device, the PIN and the biometric input to generate the encrypted

authentication information, and wherein the seed is employed by the processor to generate the non-predictable value.

13. The device of claim 1, wherein the biometric sensor is configured to receive and process at least one of a fingerprint, a speech/voice input, an iris scan, a retina scan, a facial scan, a fingerprint, written information and a DNA input.

14. The device of claim 1, further comprising a handheld device including each of the biometric sensor, the user interface, the communication link and the processor.

15. A method of generating authentication information comprising acts of:

authenticating an identity of a user to a device based on at least one of biometric data received by the device from the user and secret information known to the user and provided to the device;

generating a non-predictable value with the device;

receiving identifying information from the user concerning a selected one of a plurality of user accounts; and

generating encrypted authentication information from the non-predictable value, the identifying information, and at least one of the biometric data and the secret information.

16. The method of claim 15, further comprising an act of generating encrypted authentication information from each of the non-predictable value, the biometric data, the secret information, and the identifying information.

17. The method of claim 15, further comprising an act of de-activating the device without generating the encrypted authentication information if the identity of the user is not successfully authenticated to the device.

18. The method of claim 15, further comprising an act of generating a seed from which the authentication information is generated by employing at least two of the biometric data, the secret information known to the user, and an electronic serial number of the device.

19. The method of claim 15, further comprising an act of generating encrypted authentication information in a manner that allows the identification of the user and the selected one of the plurality of user accounts by a secure registry.

20. A method of controlling access to a plurality of accounts, the method comprising acts of:

generating, with a device, encrypted authentication information from a non-predictable value generated by the device, identifying information concerning an account selected by a user of the device from among a plurality of accounts associated with the user, and at least one of a biometric of the user received by the device and secret information provided to the device by the user;

communicating the encrypted authentication information from the device to a secure registry via a point-of-sale (POS) device to authenticate or not authenticate the device with the secure registry;

authorizing the POS device to initiate a financial transaction involving a transfer of funds to or from the account selected by the user when the encrypted authentication information is successfully authenticated; and

denying the POS device from initiation of the financial transaction involving a transfer of funds to or from the account selected by the user when the encrypted authentication information is not successfully authenticated.

ABSTRACT

In one embodiment, a user device is configured to allow a user to select any one of a plurality of accounts associated with the user to employ in a financial transaction. In one embodiment, the user device includes a biometric sensor configured to receive a biometric input provided by the user, a user interface configured to receive a user input including secret information known to the user and identifying information concerning an account selected by the user from the plurality of accounts. In a further embodiment, the user device includes a communication link configured to communicate with a secure registry, and a processor coupled to the biometric sensor to receive information concerning the biometric input, the user interface, and the communication link. According to one embodiment, the processor is configured to generate a non-predictable value and to generate encrypted authentication information from the non-predictable value, the identifying information, and at least one of the information concerning the biometric input and the secret information, and to communicate the encrypted authentication information via the communication link to the secure registry.

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
14/071,126	11/04/2013	Kenneth P. Weiss	W0537-701321

CONFIRMATION NO. 3814

37462
LANDO & ANASTASI, LLP
ONE MAIN STREET, SUITE 1100
CAMBRIDGE, MA 02142

FORMALITIES LETTER

OC000000065050285

Date Mailed: 11/22/2013

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.
  *Applicant must submit $***280** *to complete the basic filing fee for an undiscounted entity. If appropriate, applicant may make a written assertion of entitlement to small entity status and pay the small entity filing fee (37 CFR 1.27) or make a certification of entitlement to micro entity status and pay the micro entity filing fee (37 CFR 1.29).*

The applicant needs to satisfy supplemental fees problems indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

- A surcharge (for late submission of the basic filing fee, search fee, examination fee or inventor's oath or declaration) as set forth in 37 CFR 1.16(f) of $ **140** for an undiscounted entity, must be submitted.

SUMMARY OF FEES DUE:

Total fee(s) required within **TWO MONTHS** from the date of this Notice is $ **1740** for an undiscounted entity
- $ **280** Statutory basic filing fee.
- $ **140** Surcharge.
- The application search fee has not been paid. Applicant must submit $ **600** to complete the search fee.
- The application examination fee has not been paid. Applicant must submit $ **720** to complete the examination fee for an undiscounted entity.

Items Required To Avoid Processing Delays:

Applicant is notified that the above-identified application contains the deficiencies noted below. No period for reply is set forth in this notice for correction of these deficiencies. However, if a deficiency relates to the inventor's oath or declaration, the applicant must file an oath or declaration in compliance with 37 CFR 1.63, or a substitute statement in compliance with 37 CFR 1.64, executed by or with respect to each actual inventor no later than the expiration of the time period set in the "Notice of Allowability" to avoid abandonment. See 37 CFR 1.53(f).

- A properly executed inventor's oath or declaration has not been received for the following inventor(s):
  Kenneth P. Weiss
  Applicant may submit the inventor's oath or declaration at any time before the Notice of Allowance and Fee(s) Due, PTOL-85, is mailed.

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.
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.

/kgebremichael/

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
14/071,126

APPLICATION AS FILED - PART I

	(Column 1)	(Column 2)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE($)	FEE($)		RATE($)	FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	280
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	600
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	720
TOTAL CLAIMS (37 CFR 1.16(i))	20 minus 20 =	*			OR	x 80 =	0.00
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*				x 420 =	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			TOTAL	1600

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
AMENDMENT A		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
	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)		(Column 2)	(Column 3)					
AMENDMENT B		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
	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	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
14/071,126	11/04/2013		0.00	W0537-701321	20	3

CONFIRMATION NO. 3814

37462
LANDO & ANASTASI, LLP
ONE MAIN STREET, SUITE 1100
CAMBRIDGE, MA 02142

FILING RECEIPT

OC000000065050284

Date Mailed: 11/22/2013

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)

Kenneth P. Weiss, Newton, MA;

Applicant(s)

Kenneth P. Weiss, Newton, MA;

Assignment For Published Patent Application

UNIVERSAL SECURE REGISTRY, LLC, Newton, MA

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CON of 13/237,184 09/20/2011 PAT 8577813
which is a CIP of 13/168,556 06/24/2011 PAT 8271397
which is a CON of 11/677,490 02/21/2007 PAT 8001055
which claims benefit of 60/859,235 11/15/2006
and claims benefit of 60/812,279 06/09/2006
and claims benefit of 60/775,046 02/21/2006
and said 13/237,184 09/20/2011
is a CON of 12/393,586 02/26/2009 PAT 8234220
which claims benefit of 61/031,529 02/26/2008
and is a CIP of 11/760,732 06/08/2007 PAT 7809651
which is a CON of 11/677,490 02/21/2007 PAT 8001055
and said 12/393,586 02/26/2009
is a CIP of 11/760,729 06/08/2007 PAT 7805372
which is a CON of 11/677,490 02/21/2007 PAT 8001055
and said 12/393,586 02/26/2009
is a CIP of 11/677,490 02/21/2007 PAT 8001055

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: 11/18/2013

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/071,126**

Projected Publication Date: To Be Determined - pending completion of Missing Parts

Non-Publication Request: No

Early Publication Request: No

Title

UNIVERSAL SECURE REGISTRY

Preliminary Class

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.

SUPPLEMENTAL ADS

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	W0537-701321
	Application Number	14/071,126
Title of Invention	UNIVERSAL SECURE REGISTRY	

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
	Kenneth	P.	Weiss	

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

City	Newton	**State/Province**	MA	**Country of Residence**	US

Mailing Address of Inventor:

Address 1	59 Sargent Street		
Address 2			
City	Newton	**State/Province**	MA
Postal Code	02458	**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	37462	
Email Address		Add Email Remove Email

Application Information:

Title of the Invention	UNIVERSAL SECURE REGISTRY		
Attorney Docket Number	W0537-701321	**Small Entity Status Claimed**	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	29	Suggested Figure for Publication (if any)	31

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	W0537-701321
	Application Number	14/071,126
Title of Invention	UNIVERSAL SECURE REGISTRY	

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	37462		

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.

Prior Application Status	Patented			Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13237184	Continuation in part of	13168556	2011-06-24	8271397	2012-09-18
Prior Application Status	Patented			Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13168556	Continuation of	11677490	2007-02-21	8001055B	2011-08-16

Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
11677490	non provisional of	60859235	2006-11-15
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
11677490	non provisional of	60812279	2006-06-09
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
11677490	non provisional of	60775046	2006-02-21

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	W0537-701321
	Application Number	14/071,126
Title of Invention	UNIVERSAL SECURE REGISTRY	

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13237184	Continuation of	12393586	2009-02-26	8234220	2012-07-31

Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
12393586	non provisional of	61031529	2008-02-26

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
12393586	Continuation in part of	11760732	2007-06-08	7809651B	2010-10-05

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
11760732	Continuation of	11677490	2007-02-21	8001055B	2011-08-16

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
12393586	Continuation in part of	11760729	2007-06-08	7805372B	2010-09-28

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
11760729	Continuation of	11677490	2007-02-21	8001055B	2011-08-16

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
12393586	Continuation in part of	11677490	2007-02-21	8001055B	2011-08-16

Prior Application Status			Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation of	13237184	2011-09-20

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).

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	W0537-701321
	Application Number	14/071,126
Title of Invention	UNIVERSAL SECURE REGISTRY	

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

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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	W0537-701321
	Application Number	14/071,126
Title of Invention	UNIVERSAL SECURE REGISTRY	

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. □

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

Mailing Address Information For Applicant:

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

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	W0537-701321
	Application Number	14/071,126
Title of Invention	UNIVERSAL SECURE REGISTRY	

If the Assignee is an Organization check here.	☒
Organization Name	UNIVERSAL SECURE REGISTRY, LLC

Mailing Address Information For Non-Applicant Assignee:

Address 1	59 Sargent Street		
Address 2			
City	Newton	**State/Province**	MA
Country i	US	Postal Code	02458
Phone Number		Fax Number	
Email Address			

Additional 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	/Matthew H. Grady/			Date (YYYY-MM-DD)	~~2013-11-04~~ 2014-01-22
First Name	Matthew	Last Name	Grady	Registration Number	52957

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

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.

Docket No.: W0537-7013/21
Declaration – Page 1 of 1

DECLARATION FOR PATENT APPLICATION

As the below named inventor, I hereby declare that:

This declaration is directed to:

□ The attached application, titled UNIVERSAL SECURE REGISTRY , or

☒ United States application number 14/071,126
filed on 11/04/2013 .

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 state that I have reviewed and understand the contents of the application, including the claims.

I acknowledge the duty to disclose all information which is known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that any willful false statements made in this declaration are punishable under 18 U.S.C. § 1001 by fine or imprisonment of not more than five (5) years, or both, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

12-11-13

Inventor's signature **Date**
Full legal name of original or original joint inventor: Kenneth P. Weiss

Electronic Patent Application Fee Transmittal

Application Number:	14071126
Filing Date:	04-Nov-2013
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Filer:	Matthew H. Grady/Paula Sullivan
Attorney Docket Number:	W0537-701321

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

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:	17981382
Application Number:	14071126
International Application Number:	
Confirmation Number:	3814
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Customer Number:	37462
Filer:	Matthew H. Grady
Filer Authorized By:	
Attorney Docket Number:	W0537-701321
Receipt Date:	22-JAN-2014
Filing Date:	04-NOV-2013
Time Stamp:	17:21:27
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$800
RAM confirmation Number	4183
Deposit Account	502762
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet	-Suppl-ADS-Small-Entity.PDF	1031229 d2234f6d5f1357206c1f2e0c3f0b756c13231f12	no	7
Warnings:					
Information:					
This is not an USPTO supplied ADS fillable form					
2	Oath or Declaration filed	-Declaration.PDF	41732 a728b476e8fb9b788230c06a55a35afdfbdcb26c	no	1
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	36925 b87d1208573a6da06db666c363dfb773795942ad	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1109886		

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.

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted via the Office electronic filing system in accordance with 37 CFR § 1.6(a)(4).

Dated: February 12, 2014
Electronic Signature for Matthew H. Grady: /Matthew H. Grady/

Docket No.: W0537-701321
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Kenneth P. Weiss

Application No.: 14/071,126

Confirmation No.: 3814

Filed: November 4, 2013

Art Unit: N/A

For: UNIVERSAL SECURE REGISTRY

Examiner: Not Yet Assigned

FIRST PRELIMINARY AMENDMENT UNDER 37 C.F.R. 1.115

MS Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Madam:

INTRODUCTORY COMMENTS

Prior to examination on the merits, please amend the above-identified U.S. patent application as follows:

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks/Arguments begin on page 7 of this paper.

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1-20 (Cancelled)

21. (New) An electronic ID device configured to provide encrypted authentication information to execute a secure operation, comprising:

a biometric sensor configured to receive a biometric input provided by the user;

a user interface configured to receive a user input including secret information known to the user and information concerning a secure operation to be executed;

a communication interface configured to communicate with a system configured to execute the secure operation;

a processor coupled to the biometric sensor, the user interface, and the communication interface, the processor being programmed to activate the electronic ID device based on successful authentication by the electronic ID device of at least the biometric input or the secret information, the processor also being programmed such that once the electronic ID device is activated the processor is configured to generate a non-predictable value and to generate encrypted authentication information from the non-predictable value, from information derived from at least a portion of the biometric input, and from information derived from at least a portion of the secret information, and to communicate the encrypted authentication information via the communication interface to the system configured to execute the secure operation.

22. (New) The electronic ID device of claim 21, wherein the communication interface comprises a transmitter configured to wirelessly transmit the encrypted authentication information to the system configured to execute the secure operation.

23. (New) The electronic ID device of claim 21, wherein the system providing the secure operation is configured to transmit the encrypted authentication information to a secure registry

software and to receive authorization to perform the secure operation from the secure registry software.

24. (New) The electronic ID device of claim 21, wherein the secure operation includes a secure transaction, and the system configured to perform the secure operation comprises a point-of-sale (POS) device.

25. (New) The electronic ID device of claim 24, wherein the user interface is configured to display options for purchase.

26. (New) The electronic ID device of claim 24, wherein the user interface is configured to accept user selection of at least one product or service for purchase.

27. (New) The electronic ID device of claim 21, wherein execution of the secure operation permits access to a secure location, and the system configured to execute the secure operation is further configured to manage access to the secure location.

28. (New) The electronic ID device of claim 21, wherein the electronic ID device comprises a discrete code associated with the electronic ID device.

29. (New) The electronic ID device of claim 21, wherein the user interface is configured to initiate authentication with the system configured to execute the secure operation responsive to the user manually entering a secret code.

30. (New) The electronic ID device of claim 21, wherein the user initiates authentication with the system configured to execute the secure operation.

31. (New) The electronic ID device of claim 21, wherein at least a portion of the biometric input received by the biometric sensor is communicated to secure registry software for authentication by the electronic device prior to generation of the encrypted authentication information.

32. (New) The electronic ID device of claim 21, wherein the secret information includes the identifying information.

33. (New) The electronic ID device of claim 21, further comprising a memory coupled to the processor, wherein the memory stores information employed by the electronic ID device to authenticate the biometric received by the biometric sensor.

34. (New) The electronic ID device of claim 31, wherein the electronic ID device does not permit the entry of the user input if the biometric input received by the biometric sensor is determined to not belong to an authorized user of the electronic ID device.

35. (New) The electronic ID device of claim 32, wherein the secret information known to the user includes a PIN, and wherein the authentication of both the secret information and the biometric input activate the electronic ID device for the secure operation.

36. (New) The electronic ID device of claim 32, wherein data stored in the memory is unavailable to an individual in possession of the electronic ID device until the electronic ID device is activated.

37. (New) The electronic ID device of claim 34, wherein the data stored in the memory is subject to a mathematical operation that acts to modify the data such that it is unintelligible until the electronic ID device is activated.

38. (New) The electronic ID device of claim 33, wherein the memory is configured to store an electronic code unique to the electronic ID device, wherein the processor is configured to generate

a seed using at least two of the electronic serial number, a discrete code associated with the electronic ID device, the PIN, a time value, and information derived from the biometric input to generate the encrypted authentication information, and wherein the seed is employed by the processor to generate the non-predictable value.

39. (New) The electronic ID device of claim 21, wherein the electronic ID device and the system configured to execute the secure operation execute a challenge-response protocol as part of authentication.

40. (New) A method of controlling execution of a secure operation, the method comprising acts of:

authenticating an identity of a user to an electronic ID device based on at least biometric data received by the electronic ID device from the user or secret information known to the user and provided to the electronic ID device;

activating the electronic ID device based on successful authentication;

generating, with the electronic ID device, a non-predictable value;

generating, with the electronic ID device, encrypted authentication information from the non-predictable value, from information derived from at least a portion of the biometric input, and from information derived from at least a portion of the secret information;

communicating the encrypted authentication information from the electronic ID device to the system configured to execute the secure operation.

41. (New) The method of claim 40, further comprising an act of receiving at least a portion of a users secret information manually within a user interfaces.

42. (New) The method of claim 40, further comprising an act of displaying, on a user interface indicators for the plurality of user accounts stored in a memory of the electronic ID device.

43. (New) The method of claim 40, further comprising an act of de-activating the electronic ID device without generating the encrypted authentication information if the identity of the user is not successfully authenticated to the electronic ID device.

44. (New) The method of claim 40, further comprising an act of generating a seed from which the authentication information is generated by employing at least two of the biometric data, the secret information known to the user, and a discrete code unique to the electronic ID device.

45. (New) The method of claim 40, further comprising an act of generating encrypted authentication information in a manner that allows the identification of the user and the selected one of the plurality of user accounts by secure registry software.

46. (New) The method of claim 40, further comprising displaying options for selection of the system configured to execute the secure operation on a user interface.

47. (New) The method of claim 46, further comprising selecting with the user interface at least one product, service, or secure operation.

48. (New) The method of claim 46, further comprising maintaining an audit trail of purchases made.

49. (New) The method of claim 40, where the user initiates an authentication request on the electronic ID device triggering communication of the encrypted authentication information from the electronic ID device to the system configured to execute the secure operation.

REMARKS

Prior to Examination on the merits, Applicant respectfully requests entry of this Preliminary Amendment. No new matter has been added.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicant hereby requests any necessary extension of time. If there is a fee occasioned by this response, including an extension fee that is not covered by an accompanying payment, please charge any deficiency to Deposit Account No. 50/2762 (W0537-701321)

Dated: February 12, 2014

Respectfully submitted,

Electronic signature: /Matthew H. Grady/
Matthew H. Grady
Registration No.: 52,957
John N. Anastasi
Registration No.: 37,765
Lando & Anastasi
Riverfront Office Park
One Main Street
Suite 1100
Cambridge, Massachusetts 02142
(617) 395-7000
Attorney for Applicant

Electronic Patent Application Fee Transmittal

Application Number:	14071126
Filing Date:	04-Nov-2013
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Filer:	Matthew H. Grady
Attorney Docket Number:	W0537-701321

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Claims in excess of 20	2202	9	40	360
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
	Total in USD ($)			**360**

Electronic Acknowledgement Receipt

EFS ID:	18183153
Application Number:	14071126
International Application Number:	
Confirmation Number:	3814
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Customer Number:	37462
Filer:	Matthew H. Grady
Filer Authorized By:	
Attorney Docket Number:	W0537-701321
Receipt Date:	12-FEB-2014
Filing Date:	04-NOV-2013
Time Stamp:	13:46:55
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$360
RAM confirmation Number	4
Deposit Account	502762
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		_PRELIM_AMEND_TO_FILE_WITH_KENS_COMMENTS.pdf	34588 8af6027f20ae58e759ceae8a8c67ed228b78db13	yes	7

Multipart Description/PDF files in .zip description

Document Description	Start	End
Preliminary Amendment	1	1
Claims	2	6
Applicant Arguments/Remarks Made in an Amendment	7	7

Warnings:

Information:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
2	Fee Worksheet (SB06)	fee-info.pdf	30084 fe18e59963ee8cc9fd97f90caea419600079a45d	no	2

Warnings:

Information:

Total Files Size (in bytes):	64672

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.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/071,126

APPLICATION AS FILED - PART I

	(Column 1)		(Column 2)	SMALL ENTITY			OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED		NUMBER EXTRA	RATE($)	FEE($)	OR	RATE($)	FEE($)
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))	29	minus 20 =	* 9	x 40 =	360	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	2	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	1090		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
AMENDMENT A		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
	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)		(Column 2)	(Column 3)					
AMENDMENT B		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
	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	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
14/071,126	11/04/2013		1160	W0537-701321	29	2

CONFIRMATION NO. 3814

37462
LANDO & ANASTASI, LLP
ONE MAIN STREET, SUITE 1100
CAMBRIDGE, MA 02142

UPDATED FILING RECEIPT

OC000000066667697

Date Mailed: 02/21/2014

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)

Kenneth P. Weiss, Newton, MA;

Applicant(s)

Kenneth P. Weiss, Newton, MA;

Assignment For Published Patent Application

UNIVERSAL SECURE REGISTRY, LLC, Newton, MA

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CON of 13/237,184 09/20/2011 PAT 8577813
which is a CIP of 13/168,556 06/24/2011 PAT 8271397
which is a CON of 11/677,490 02/21/2007 PAT 8001055
which claims benefit of 60/859,235 11/15/2006
and claims benefit of 60/812,279 06/09/2006
and claims benefit of 60/775,046 02/21/2006
and said 13/237,184 09/20/2011
is a CON of 12/393,586 02/26/2009 PAT 8234220
which claims benefit of 61/031,529 02/26/2008
and is a CIP of 11/760,732 06/08/2007 PAT 7809651
which is a CON of 11/677,490 02/21/2007 PAT 8001055
and said 12/393,586 02/26/2009
is a CIP of 11/760,729 06/08/2007 PAT 7805372
which is a CON of 11/677,490 02/21/2007 PAT 8001055
and said 12/393,586 02/26/2009
is a CIP of 11/677,490 02/21/2007 PAT 8001055

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: 11/18/2013

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/071,126**

Projected Publication Date: 05/29/2014

Non-Publication Request: No

Early Publication Request: No

**** SMALL ENTITY ****

Title

UNIVERSAL SECURE REGISTRY

Preliminary Class

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.

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
14/071,126	11/04/2013	Kenneth P. Weiss	W0537-701321

CONFIRMATION NO. 3814

PUBLICATION NOTICE

OC000000068705299

37462
LANDO & ANASTASI, LLP
ONE MAIN STREET, SUITE 1100
CAMBRIDGE, MA 02142

Title:UNIVERSAL SECURE REGISTRY

Publication No.US-2014-0149295-A1
Publication Date:05/29/2014

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

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

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted via the Office electronic filing system in accordance with 37 CFR § 1.6(a)(4).

Dated: May 23, 2016
Electronic Signature for John N. Anastasi: /John N. Anastasi/

Docket No.: W0537-701321
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Kenneth P. Weiss

Application No.: 14/071,126	Confirmation No.: 3814
Filed: November 4, 2013	Art Unit: 3685
For: UNIVERSAL SECURE REGISTRY	Examiner: T. J. Huang

SECOND PRELIMINARY AMENDMENT UNDER 37 C.F.R. § 1.115

MS Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

INTRODUCTORY COMMENTS

Prior to examination on the merits, please amend the above-identified U.S. patent application as follows:

Amendments to the Specification begin on page 2 of this paper.

Remarks/Arguments begin on page 3 of this paper.

AMENDMENTS TO THE SPECIFICATION

Please replace the paragraph beginning at page 1, line 3 with the following:

CROSS REFERENCE TO RELATED APPLICATIONS

This application claims the benefit under 35 U.S.C. § 120 as a continuation of U.S. patent application No. 13/237,184 filed September 20, 2011, which is a continuation of U.S. patent application No. 12/393,586 filed February 26, 2009, which is a continuation-in-part of each of U.S. patent application serial no. 11/760,732 filed June 8, 2007, now U.S. Patent No. 7,809,651; U.S. patent application serial no. 11/760,729 filed June 8, 2007, now U.S. Patent No. 7,805,372; and U.S. patent application serial no. 11/677,490 filed February 21, 2007, now U.S. Patent No. 8,001,055. ~~This application~~ U.S. patent application No. 13/237,184 also claims the benefit under 35 U.S.C. § 120 as a continuation-in-part of U.S. patent application no. 13/168,556 filed on June 24, 2011, which claims the benefit under 35 U.S.C. § 120 as a continuation of U.S. application no. 11/677,490. Each of U.S. application nos. 11/760,732, 11/760,729 and 11/677,490 claim priority under 35 U.S.C. § 119 (e) to U.S. Provisional Application Nos. 60/812,279 filed on June 9, 2006, and 60/859,235 filed on November 15, 2006. U.S. application no. 11/677,490 also claims priority under 35 U.S.C. § 119 (e) to U.S. Provisional Application No. 60/775,046 filed on February 21, 2006. Application serial no. 12/393,586 filed February 26, 2009 claims priority under 35 U.S.C. § 119(e) to U.S. Provisional Application Serial No. 61/031,529, entitled "UNIVERSAL SECURE REGISTRY," filed on February 26, 2008. Each of the above-identified applications is hereby incorporated herein by reference in its entirety.

REMARKS

Prior to examination on the merits, Applicants respectfully request consideration and entry of this Preliminary Amendment and submit the following remarks.

The specification is amended to include the correct priority designation.

CONCLUSION

In view of the foregoing, consideration and favorable action are respectfully requested. If the Examiner believes, after this Preliminary Amendment, that the application is not in condition for allowance, or otherwise has any questions regarding the application, the Examiner is invited to contact the Applicant's Attorney at the telephone number provided below.

In view of the above amendment, applicant believes the pending application is in condition for allowance.

Dated: May 23, 2016

Respectfully submitted,

Electronic signature: /John N. Anastasi/
John N. Anastasi
Registration No.: 37,765
LANDO & ANASTASI, LLP
Riverfront Office Park
One Main Street, Suite 1100
Cambridge, Massachusetts 02142
(617) 395-7000
Attorney for Applicant

Corrected Application Data Sheet

Inventor Information

Inventor Number::	1
Given Name::	Kenneth
Middle Name::	P.
Family Name::	Weiss
City of Residence::	Newton
State or Province of Residence::	MA
Country of Residence::	US
Street of mailing address::	59 Sargent Street
City of mailing address::	Newton
State or Province of mailing address::	MA
Postal or Zip Code of mailing address::	02458

Correspondence Information

Correspondence Customer Number::	37462

Application Information

Application Number::	14/071,126
Filing Date::	11/04/13
Application Type::	Regular
Subject Matter::	Utility
CD-ROM or CD-R?::	None
Sequence submission?::	None

Computer Readable Form (CRF)?::	No
Title::	UNIVERSAL SECURE REGISTRY
Attorney Docket Number::	W0537-701321
Request for Early Publication?::	No
Request for Non-Publication?::	No
Small Entity?::	Yes
Petition included?::	No
Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2::	No
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::	No

Representative Information

Representative Customer Number::	37462

Domestic Priority Information

Application::	Continuity Type::	Parent Application::	Parent Filing Date::
This Application	Continuation of	13/237184	09/20/11
13/237184	Continuation-in-part of	13/168556	06/24/11
13/168556	Continuation of	11/677490	02/21/07
11/677490	An application claiming the benefit under 35 USC 119(e)	60/859235	11/15/06
11/677490	An application claiming the benefit under 35 USC 119(e)	60/812279	06/09/06
11/677490	An application claiming the benefit under 35 USC 119(e)	60/775046	02/21/06
13/237184	Continuation of	12/393586	02/26/09
12/393586	An application claiming the benefit under 35 USC 119(e)	61/031529	02/26/08
12/393586	Continuation-in-part of	11/760732	06/08/07
11/760732	Continuation of	11/677490	02/21/07
11/760732	An application claiming the benefit under 35 USC 119(e)	60/859235	11/15/06
11/760732	An application claiming the benefit under 35 USC 119(e)	60/812279	06/09/06
12/393586	Continuation-in-part of	11/760729	06/08/07
11/760729	Continuation of	11/677490	02/21/07
11/760729	An application claiming the benefit	60/859235	11/15/06

	under 35 USC 119(e)		
11/760729	An application claiming the benefit under 35 USC 119(e)	60/812279	06/09/06
12/393586	Continuation-in-part of	11/677490	02/21/07

Foreign Priority Information

Applicant Information

Applicant Number::	1
Applicant Type::	Assignee
Organization Name::	UNIVERSAL SECURE REGISTRY, LLC
Street of mailing address::	59 Sargent Street
City of mailing address::	Newton
State or Province of mailing address::	MA
Postal or Zip Code of mailing address::	02458

Assignee Information Including Non-Applicant Assignee Information

Signature:

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). **However, if this Application Data Sheet is submitted with the INITIAL filing of the application and either box A or B is not checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).**

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	/John N. Anastasi/	Date (YYYY-MM-DD)	
Name	John N. Anastasi	Registration Number	37,765

Electronic Acknowledgement Receipt

EFS ID:	25852281
Application Number:	14071126
International Application Number:	
Confirmation Number:	3814
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Customer Number:	37462
Filer:	John N Anastasi
Filer Authorized By:	
Attorney Docket Number:	W0537-701321
Receipt Date:	23-MAY-2016
Filing Date:	04-NOV-2013
Time Stamp:	16:04:31
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		Second_Preliminary_Amendment.pdf	31642 e74abcf132515e960ad7795031b86c35727e8ba4	yes	3

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Preliminary Amendment	1	1
	Specification	2	2
	Applicant Arguments/Remarks Made in an Amendment	3	3

Warnings:

Information:

2	Application Data Sheet	Supplemental_Application_Data_Sheet_ADS_-_PTO_AIA-14.pdf	23706 18980ba36f312e4be5dc0dd0793457891246d7e0	no	5

Warnings:

Information:

This is not an USPTO supplied ADS fillable form

Total Files Size (in bytes):	55348

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 NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/071,126	11/04/2013	Kenneth P. Weiss	W0537-701321	3814

37462 7590 08/31/2016
LANDO & ANASTASI, LLP
ONE MAIN STREET, SUITE 1100
CAMBRIDGE, MA 02142

EXAMINER	
IMMANUEL, ISIDORA I	

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
08/31/2016	ELECTRONIC

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

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

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@LALaw.com
gengelson@LALaw.com

Office Action Summary	**Application No.** 14/071,126	**Applicant(s)** WEISS, KENNETH P.	
	Examiner ISIDORA IMMANUEL	**Art Unit** 3685	**AIA (First Inventor to File) Status** No

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02/12/2014*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *21-49* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *21-49* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

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

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b)
Paper No(s)/Mail Date *02/04/2014, 02/26/2015, 04/17/2015, 10/09/2015*.

3) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

Acknowledgements

1. This office action is in response to the claims filed 02/12/2014.

2. Claims 1-20 are cancelled.

3. Claims 21-49 are new.

4. Claims 21-49 are pending.

5. Claims 21-49 have been examined.

Notice of Pre-AIA or AIA Status

6. The present application is being examined under the pre-AIA first to invent provisions.

Examiner's Comments

7. Regarding claim 21, with respect to claim language "sensor configured to receive...", "interface configured to receive...", "operation to be executed...", "interface configured to communicate...", "processor being programmed to activate...", "processor configured to generate… to generate … to communicate...", claim 22, "transmitter configured to wirelessly transmit ...", claim 23, "the system…configured to transmit… to receive … to perform...", claim 24, "system configured to perform...", claim 25, "interface configured to display options for purchase", claim 26, "interface configured to accept...for purchase", claim 27, "system configured to execute...", "operation is further configured to manage...", claim 29, "interface configured to initiate...", "system configured to execute...", claim 30, "system configured to execute...", claim 31,

"software for authentication…", claim 33, "device to authenticate…", claim 37, "operation that acts to modify…", claim 38, "memory is configured to store...", "processor is configured to generate...", "processor to generate…", and claims 39, 40, 46 and 49, "system configured to execute...", recites intended use and therefore does not have patentable weight. See MPEP 2114.

8. Regarding claim 21, with respect to claim language "sensor configured to receive...", "interface configured to receive...", "interface configured to communicate...", "processor being programmed to activate...", "processor configured to generate… to generate … to communicate...", claim 22, "transmitter configured to wirelessly transmit ...", claim 23, "the system…configured to transmit… to receive … to perform...", claim 24, "system configured to perform...", claim 25, "interface configured to display options for purchase", claim 26, "interface configured to accept...for purchase", claim 27, "system configured to execute...", claim 29, "interface configured to initiate...", "system configured to execute...", claim 30, "system configured to execute...", claim 33, "device to authenticate…", claim 38, "memory is configured to store...", "processor is configured to generate...", "processor to generate…", and claims 39, 40, 46 and 49, "system configured to execute...", recites functional language, and therefore does not have patentable weight. (In re Schreiber, 128 F.3d 1473, 1478, 44 USPQ2d 1429, 1432 (Fed. Cir. 1997).

9. Regarding claim 24, "wherein the secure operation comprises…", claim 28, "device comprises a discrete code…", claim 32, " information includes the identifying…", and claim 35, "secret information… includes a PIN…", are nonfunctional descriptive

material and therefore do not have patentable weight. See *In re Gulack*, 217 USPQ 401 (Fed. Cir. 1983), *In re Ngai,* 70 USPQ2d (Fed. Cir. 2004), *In re Lowry*, 32 USPQ2d 1031 (Fed. Cir. 1994); MPEP 2111.05. MPEP 2111.05 III.

10. Regarding claim 40, the language "data received… provided to...", and claim 49, "user initiates…" does not disclose a positively recited step and therefore does not patentable weight. See MPEP 2111.04.

11. Regarding claim 41, "de-activating the electronic ID device … if the identity…", similarly, claim 45, "the selected one..." is optional and conditional language and therefore does not have patentable weight. See MPEP 2103(I)(c).

Claim Rejections - 35 USC § 101

12. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

13. Claims 21-49 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Subject Matter Eligibility Standard

14. When considering subject matter eligibility under 35 U.S.C. 101, it must be determined whether the claim is directed to one of the four statutory categories of invention, i.e., process, machine, manufacture, or composition of matter. If the claim does fall within one of the statutory categories, it must then be determined whether the claim is directed to a judicial exception (i.e., law of nature, natural phenomenon, and

abstract idea), and if so, it must additionally be determined whether the claim is a patent-eligible application of the exception. If an abstract idea is present in the claim, any element or combination of elements in the claim must be sufficient to ensure that the claim amounts to significantly more than the abstract idea itself. Examples of abstract ideas include fundamental economic practices; certain methods of organizing human activities; an idea itself; and mathematical relationships/formulas. (*Alice Corporation Pty. Ltd. v. CLS Bank International, et al. US Supreme Court, No. 13-298, June 19, 2014*).

Analysis

15. In the instant case, claim 40 is directed to a method and claim 21 is directed to a device.

16. Additionally, the claim is directed towards receiving, and processing data and automating mental tasks, which is similar to Alice which dealt with receiving, processing, and storing data (*Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 573 U.S. __, 134 S. Ct. 2347, 2356 (2014)), Classen which dealt with automating mental tasks and SmartGene which dealt with comparing new and stored information and using rules to identify options SmartGene, Inc. v. Advanced Biological Labs., SA (Fed. Cir. 2014)). Therefore, based on case law precedent, the claims are claiming subject matter similar to concepts already identified by the courts as dealing with abstract ideas. See Alice Corp. Pty. Ltd., 134 S.Ct. at 2356 (citing Bilski v. Kappos, 561, U.S. 593, 611 (2010)). Claim 21 is directed towards the generic computer used to implement the method of claim 40 and is therefore also directed towards a judicial exception regarding an abstract idea involving

the receiving and processing data, based on case law precedent, is claiming subject matter similar to concepts identified by the courts as dealing with abstract ideas.

17. Taking the claim elements separately, the functions performed by the machine at each step of the process are purely conventional. Using a processor, using a device, receiving and processing data. All of these functions are well-understood, routine, conventional activities previously known to the industry. In short, each step does no more than require a generic computer to perform generic computer functions.

18. The claims do not include additional elements that are sufficient to amount to significantly more than the judicial exception because the elements of “authenticating an identity” are drawn to data comparisons in SmartGene and “activating the electronic device…” as explained by Applicant’s specification (PGPub¶ 255) is “the user device **352** is activated for a transaction when the user satisfactorily completes an authentication process with the device”, as the device is already in use, “activating” is drawn to the using of the device for transactions as in automation of tasks in Classen and receiving and processing data in Alice (Alice Corp. Pty. Ltd. v. CLS Bank Int’l, 573 U.S. __, 134 S. Ct. 2347, 2356 (2014)), electronic recordkeeping (Alice Corp. Pty. Ltd. v. CLS Bank Int’l, 573 U.S. __, 134 S. Ct. 2347, 2356 (2014)), automating mental tasks (Bancorp Services LLC v. Sun Life Assurance Co. of Canada (U.S.), 103 USPQ2d 1425 (Fed. Cir. 2012), (Cybersource Corp. v. Retail Decisions, Inc., 654 F.3d 1366, 1372 (Fed. Cir. 2011)) and receiving or transmitting data over a network, e.g., using the Internet to gather data (Ultramercial, Inc. v. Hulu, LLC, 772 F.3d 709, 714-15 (Fed. Cir. 2014), (buySAFE, Inc. v. Google, Inc., 765 F.3d 1350, 1355 (Fed. Cir. 2014),

(Cyberfone Systems, LLC v. CNN Interactive Group, Inc., 558 Fed. Appx. 988, 993 (Fed. Cir. 2014)).

19. Viewed as a whole, instructions/method claims simply recite the concept of receiving and processing data as performed by a generic computer. The method claims do not, for example, purport to improve the functioning of the computer itself. Nor do they effect an improvement in any other technology or technical field. Instead, the claims at issue amount to nothing significantly more than an instruction to apply the abstract idea of receiving and processing data using some unspecified, generic computer. See Alice Corp. Pty. Ltd., 134 S.Ct. at 2360.

20. The use of a device implementing the abstract idea does not render the claim patent eligible because it does not provide meaningful limitations beyond generally linking the use of an abstract idea to a particular technology environment and requires no more than a generic computer to perform generic computer functions.

Conclusion

21. The claim as a whole, does not amount to significantly more than the abstract idea itself. This is because the claim does not affect an improvement to another technology or technical filed; the claim does not amount to an improvement to the functioning of a computer system itself; and the claim does not move beyond a general link of the use of an abstract idea to a particular technological environment.

22. Accordingly, the Examiner concludes that there are no meaningful limitations in the claim that transform the judicial exception into a patent eligible application such that the claim amounts to significantly more than the judicial exception itself.

23. Dependent claims do not resolve the deficiency of independent claims and accordingly stand rejected under 35 USC 101 based on the same rationale.

24. Dependent claims 22-39 and 41-49 are also rejected.

Claim Rejections - 35 USC § 112

25. The following is a quotation of the first paragraph of 35 U.S.C. 112(a):

> (a) IN GENERAL.—The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor or joint inventor of carrying out the invention.

The following is a quotation of the first paragraph of pre-AIA 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor of carrying out his invention.

26. Claims 21-49 are rejected under 35 U.S.C. 112(a) or 35 U.S.C. 112 (pre-AIA), first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor or a joint inventor, or for pre-AIA the inventor(s), at the time the application was filed, had possession of the claimed invention.

27. Claims 21 and 40 recite executing a “secure operation”. The recitation of electronic ID device and the system both executing the "secure operation" calls to question the scope of the claims, whether the claim actually encompasses the “secure

operation and the claim being directed to a genus of secure operations because there is no limitation on what falls under the banner of “secure operation”. Additionally, disclosure doesn’t provide sufficient teaching to claim a genus. Dependent claims 22-39 and 41-49 are also rejected.

28. Claim 21 recites “a processor coupled to the biometric sensor, the user interface, and the communication interface, the processor being programmed to activate the electronic ID device based on successful authentication by the electronic ID device of at least the biometric input or the information”, claim 35 recites “wherein the authentication of both the secret information and the biometric input activate the electronic ID device for the secure operation…”, and claim 40 recites "activating the electronic ID device based on successful authentication...." “When examining computer-implemented functional claims, examiners should determine whether the specification discloses the computer and the algorithm (e.g., the necessary steps and/or flowcharts) that perform the claimed function in sufficient detail such that one of ordinary skill in the art can reasonably conclude that the inventor invented the claimed subject matter”. See MPEP 2161.01. The specification (PGpub ¶ 255) says “in some embodiments, the software included in the user device 352 and employed in conducting transactions using the system 350 remains inoperative until the entry of the correct PIN” but the secret information and biometric input and subsequent authentication are all transactions performed by the device before it’s “activation”. The specification does not provide sufficient teaching for an “active state” device or what state the device was in prior to “activation”, the algorithms used or sufficient detail of how the device operates,

especially since Applicant is claiming an additional level of activation and function for an already functioning device.

29. Claim 37 recites “memory is subject to a mathematical operation…”. “When examining computer-implemented functional claims, examiners should determine whether the specification discloses the computer and the algorithm (e.g., the necessary steps and/or flowcharts) that perform the claimed function in sufficient detail such that one of ordinary skill in the art can reasonably conclude that the inventor invented the claimed subject matter”. See MPEP 2161.01. In this case, the specification (¶ 255, 256, 279) recites “that is, a mathematical operation is performed on software stored in the user device 352 with the PIN. Once the mathematical operation is performed the modified software is unusable and the software remains inoperative until the PIN is supplied by the user”. The specification does not provide sufficient detail as to what “mathematical operation" or algorithm is used.

30. The following is a quotation of 35 U.S.C. 112(b):

> (b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

31. Claims 21-49 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

32. Regarding claim 21, the claim recites “an electronic device configured to provide encrypted authentication information to execute a secure operation… the system configured to execute the secure operation.” However, claim 21 is directed to an electronic ID device of which the system is not a part of. The claim concludes, the system, not the electronic ID device, executes a secure operation. Similarly, claim 40 recites “a method of controlling execution of a secure operation… the system configured to execute the secure operation.” However, claim 40, directed to method step performed the electronic ID device of which the system is not a part of. The claims are hybrid claims as the cited language is not directed to the device but to external use of claimed structural elements. Therefore, it would be unclear whether infringement of claim 21 and 40 occurs based on possession of the device. *In re Katz Interactive Call Processing Patent Litigation*, 639 F.3d 1303 (Fed. Cir. 2011). *IPXL Holdings v. Amazon.com, Inc.*, 430 F.2d 1377, 1384, 77 USPQ2d 1140, 1145 (Fed. Cir. 2005). *Ex parte Lyell*, 17 USPQ2d 1548 (Bd. Pat. App. & Inter. 1990). Dependent claims 22-39 and 41-49 are also rejected.

33. Claim 21 recites “a processor coupled to the biometric sensor, the user interface, and the communication interface, the processor being programmed to activate the electronic ID device based on successful authentication by the electronic ID device of at least the biometric input or the information”, claim 35 recites “wherein the authentication of both the secret information and the biometric input activate the electronic ID device for the secure operation…”, and claim 40 recites "activating the electronic ID device based on successful authentication..." From Applicant's limitations, it is unclear how an

electronic ID device that received information and conducted an authentication transaction is not an already activated electronic ID device or whether the processor of the electronic ID device that activates the electronic ID device was somehow dormant prior to input of information and authentication by the electronic ID device. Dependent claims 22-39 and 41-49 are also rejected.

34. Claim 21 recites the limitation "provided by the user…" Claim 31 recites "the electronic device…" Claim 42 recites "the plurality of user accounts…", claim 45 recites "the selected one…" There is insufficient antecedent basis for this limitation in the claim. Dependent claims 22-39 are rejected.

35. Regarding claim 23, the claim recites "the system providing the secure operation is configured to transmit…" However, claim 21, from which claim 23 depends, is directed to an electronic ID device of which the system is not a part of. Similarly, claim 30 recites "wherein the user initiates authentication…." However, claim 21, from which claim 30 depends, is directed to an electronic ID device of which the user is not a part of. The claim is a hybrid claim as the cited language is not directed to the device but to external use of claimed structural elements. Therefore, it would be unclear whether infringement of claim 23 occurs based on possession of the device. *In re Katz Interactive Call Processing Patent Litigation*, 639 F.3d 1303 (Fed. Cir. 2011). *IPXL Holdings v. Amazon.com, Inc.*, 430 F.2d 1377, 1384, 77 USPQ2d 1140, 1145 (Fed. Cir. 2005). *Ex parte Lyell*, 17 USPQ2d 1548 (Bd. Pat. App. & Inter. 1990).

36. Claim 40 recites "data received by the electronic ID device from the user or secret information known to the user and provided to the electronic ID … generating, …

from information derived from at least a portion of the biometric input, and from information derived from at least a portion of the secret information" but the electronic ID device was provided either biometric input or secret information. It is unclear how the generated information uses both sets of information. Dependent claims 41-49 are rejected.

37. Claim 40 recites "activating the electronic ID device based on successful authentication…", but a successful authentication has not been achieved, therefore it is unclear how the device can be subsequently activated. Dependent claims 41-49 are rejected.

38. Claim 43 recites " an act of de-activating the electronic ID device without generating the encrypted authentication information if the identity of the user is not successfully authenticated…". Claim 40, from which claim 43 depends, recites "activating the electronic ID device based on successful authentication…". Claim 43 calls for de-activation when "the user is not successfully authenticated…". This claim is indefinite and unclear because it operates on the premise that the device is already "activated" prior to authentication, which is in direct opposition to independent claim 40, which only activates after successful authentication.

Claim Rejections - 35 USC § 103

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

> (a) A patent may not be obtained through the invention is not identically disclosed or described as set forth in section 102, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been

> obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

40. Claims 21-49 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Gullman et al (5,280,527) ("Gullman"), and further in view of Maritzen et al. (2002/0184500) ("Maritzen").

41. Regarding claims 21 and 40, Gullman teaches a biometric sensor configured to receive a biometric input provided by the user (column 4, line 39-49, column 5, line 42-54); a user interface configured to receive a user input information concerning a secure operation to be executed (column 4, line 3-8, 39-64); a communication interface configured to communicate with a system configured to execute the secure operation (column3, line 50-55, column 4, line 13-20, 29-36, column 6, line 35-40); a processor coupled to the biometric sensor, the user interface, and the communication interface, the processor being programmed to activate the electronic ID device based on successful authentication by the electronic ID device of at least the biometric input or the information (column 3, line 19-55, column 4, line 3-61, column 6, line 8-20), the processor also being programmed such that once the electronic ID device is activated the processor is configured to generate a non-predictable value and to generate encrypted authentication information from the non-predictable value (column 3, line 37-46, column 5, line 15-33; claim 1), from information derived from at least a portion of the biometric input, and from information derived from at least a portion of the secret information, and to communicate the encrypted authentication information via the communication interface to the system configured to execute the secure operation (Abstract; column 4, line 29-36; column 6, line 35-61; claim 1). Gullman does not teach

including secret information known to the user. Maritzen teaches including secret information known to the user (¶ 57, 70, 77). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Gullman and Maritzen in order to provide secure authentication of a user to prevent unauthorized access (Maritzen; ¶ 2-4).

42. Regarding claim 22, Maritzen teaches wherein the communication interface comprises a transmitter configured to wirelessly transmit the encrypted authentication information to the system configured to execute the secure operation (¶ 23, 27, 35, 39, 42).

43. Regarding claim 23, Maritzen teaches wherein the system providing the secure operation is configured to transmit the encrypted authentication information to a secure registry software and to receive authorization to perform the secure operation from the secure registry software (¶ 28-31).

44. Regarding claim 24, Maritzen teaches wherein the secure operation includes a secure transaction, and the system configured to perform the secure operation comprises a point-of-sale (POS) device (¶ 28, 34, 57, 61).

45. Regarding claim 25, Maritzen teaches wherein the user interface is configured to display options for purchase (¶ 18, 30, 33, 74, 81).

46. Regarding claim 26, Maritzen teaches wherein the user interface is configured to accept user selection of at least one product or service for purchase (¶ 30, 33, 69, 74, 81).

47. Regarding claim 27, Gullman teaches wherein execution of the secure operation permits access to a secure location, and the system configured to execute the secure operation is further configured to manage access to the secure location (column 4, line 29-36, column 6, line 35-45).

48. Regarding claim 28, Maritzen teaches wherein the electronic ID device comprises a discrete code associated with the electronic ID device (¶ 37).

49. Regarding claim 29, Gullman teaches wherein the user interface is configured to initiate authentication with the system configured to execute the secure operation responsive to the user manually entering a secret code (column 3, line 56-68, column 6, line 9-16).

50. Regarding claim 30, Gullman teaches wherein the user initiates authentication with the system configured to execute the secure operation (column 3, line 56-64, column 6, line 9-16).

51. Regarding claim 31, Gullman teaches wherein at least a portion of the biometric input received by the biometric sensor is communicated to secure registry software for authentication by the electronic device prior to generation of the encrypted authentication information (column 3, line 44-48, column 5, line 57-65).

52. Regarding claim 32, Maritzen teaches wherein the secret information includes the identifying information (¶ 57, 61, 62, 77).

53. Regarding claim 33, Gullman teaches further comprising a memory coupled to the processor, wherein the memory stores information employed by the electronic ID

device to authenticate the biometric received by the biometric sensor (column 3, line 44-48, column 5, line 57-65).

54. Regarding claim 34, Gullman teaches wherein the electronic ID device does not permit the entry of the user input if the biometric input received by the biometric sensor is determined to not belong to an authorized user of the electronic ID device (column 3, line 37-55).

55. Regarding claim 35, Gullman teaches wherein the secret information known to the user includes a PIN, and wherein the authentication of both the secret information and the biometric input activate the electronic ID device for the secure operation (column 3, line 37-68, column 4, line 3-36).

56. Regarding claim 36, Gullman teaches wherein data stored in the memory is unavailable to an individual in possession of the electronic ID device until the electronic ID device is activated (column 4, line 29-36, column 5, line 64-68, column 6, line 1-5).

57. Regarding claim 37, Maritzen teaches wherein the data stored in the memory is subject to a mathematical operation that acts to modify the data such that it is unintelligible until the electronic ID device is activated (¶ 55, 56).

58. Regarding claim 38, Gullman teaches wherein the processor is configured to generate a seed using at least two of the electronic serial number, a discrete code associated with the electronic ID device, the PIN, a time value, and information derived from the biometric input to generate the encrypted authentication information, and wherein the seed is employed by the processor to generate the non-predictable value (column 3, line 37-68, column 4, line 3-22). Gullman does not teach wherein the

memory is configured to store an electronic code unique to the electronic ID device. Maritzen teaches wherein the memory is configured to store an electronic code unique to the electronic ID device (¶ 37). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Gullman and Maritzen in order to provide secure authentication of a user to prevent unauthorized access (Maritzen; ¶ 2-4).

59. Regarding claim 39, Gullman teaches wherein the electronic ID device and the system configured to execute the secure operation execute a challenge-response protocol as part of authentication (column 3, line 37-68, column 4, line 8-11).

60. Regarding claim 41, Maritzen teaches an act of receiving at least a portion of a users secret information manually within a user interfaces (¶ 22, 57).

61. Regarding claim 42, Gullman teaches further comprising an act of displaying, on a user interface indicators for the plurality of user accounts stored in a memory of the electronic ID device (column 5, line 57-65).

62. Regarding claim 43, Maritzen teaches further comprising an act of de-activating the electronic ID device without generating the encrypted authentication information if the identity of the user is not successfully authenticated to the electronic ID device (¶ 57).

63. Regarding claim 44, Gullman teaches further comprising an act of generating a seed from which the authentication information is generated by employing at least two of the biometric data, the secret information known to the user, and a discrete code unique to the electronic ID device (column 3, line 37-68, column 4, line 3-22).

64. Regarding claim 45, Gullman teaches further comprising an act of generating encrypted authentication information in a manner that allows the identification of the user and the selected one of the plurality of user accounts by secure registry software (column 4, line 23-36, column 5, line 57-65).

65. Regarding claim 46, Maritzen teaches further comprising displaying options for selection of the system configured to execute the secure operation on a user interface (¶ 33, 69, 74).

66. Regarding claim 47, Gullman teaches further comprising selecting with the user interface at least one product, service, or secure operation (Abstract; column 3, line 50-55, column 4, line 59-62; claim 2, 3).

67. Regarding claim 48, Maritzen teaches further comprising maintaining an audit trail of purchases made (¶ 32, 42, 82).

68. Regarding claim 49, Gullman teaches where the user initiates an authentication request on the electronic ID device triggering communication of the encrypted authentication information from the electronic ID device to the system configured to execute the secure operation (column 3, line 56-68, column 4, line 50-64).

Conclusion

69. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ISIDORA IMMANUEL whose telephone number is (571)272-9862. The examiner can normally be reached on Monday-Thursday 8am-5pm EDT.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Calvin Hewitt can be reached on 571-272-6709. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/I. I./
Examiner, Art Unit 3685

/JAMES D NIGH/
Primary Examiner, Art Unit 3685

Notice of References Cited	Application/Control No. 14/071,126	Applicant(s)/Patent Under Reexamination WEISS, KENNETH P.	
	Examiner ISIDORA IMMANUEL	Art Unit 3685	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-5,280,527 A	01-1994	Gullman; Lawrence S.	G06K19/0718	713/184
*	B	US-2002/0184500 A1	12-2002	Maritzen, Michael	G06Q20/18	713/170
	C	US-				
	D	US-				
	E	US-				
	F	US-				
	G	US-				
	H	US-				
	I	US-				
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

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

BIB DATA SHEET

CONFIRMATION NO. 3814

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
14/071,126	11/04/2013 **RULE**	705	3685	W0537-701321

APPLICANTS

INVENTORS

Kenneth P. Weiss, Newton, MA;

** **CONTINUING DATA** *************************

This application is a CON of 13/237,184 09/20/2011 PAT 8577813
which is a CIP of 13/168,556 06/24/2011 PAT 8271397
which is a CON of 11/677,490 02/21/2007 PAT 8001055
which claims benefit of 60/859,235 11/15/2006
and claims benefit of 60/812,279 06/09/2006
and claims benefit of 60/775,046 02/21/2006
and said 13/237,184 09/20/2011
is a CON of 12/393,586 02/26/2009 PAT 8234220
which claims benefit of 61/031,529 02/26/2008
and is a CIP of 11/760,732 06/08/2007 PAT 7809651
which is a CON of 11/677,490 02/21/2007 PAT 8001055
and said 12/393,586 02/26/2009
is a CIP of 11/760,729 06/08/2007 PAT 7805372
which is a CON of 11/677,490 02/21/2007 PAT 8001055
and said 12/393,586 02/26/2009
is a CIP of 11/677,490 02/21/2007 PAT 8001055

** **FOREIGN APPLICATIONS** *************************

** **IF REQUIRED, FOREIGN FILING LICENSE GRANTED** ** ** SMALL ENTITY **
11/18/2013

		STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
Foreign Priority claimed □ Yes ☑ No 35 USC 119(a-d) conditions met □ Yes ☑ No Verified and Acknowledged /ISIDORA I IMMANUEL/ Examiner's Signature	□ Met after Allowance Initials	MA	29	29	2

ADDRESS

LANDO & ANASTASI, LLP
ONE MAIN STREET, SUITE 1100
CAMBRIDGE, MA 02142
UNITED STATES

TITLE

UNIVERSAL SECURE REGISTRY

FILING FEE RECEIVED	FEES: Authority has been given in Paper No.___________ to charge/credit DEPOSIT ACCOUNT	□ All Fees □ 1.16 Fees (Filing) □ 1.17 Fees (Processing Ext. of time) □ 1.18 Fees (Issue)

Index of Claims	**Application/Control No.** 14071126	**Applicant(s)/Patent Under Reexamination** WEISS, KENNETH P.
	Examiner ISIDORA IMMANUEL	**Art Unit** 3685

✓	**Rejected**	**-**	**Cancelled**	**N**	**Non-Elected**	**A**	**Appeal**
=	**Allowed**	**÷**	**Restricted**	**I**	**Interference**	**O**	**Objected**

□ **Claims renumbered in the same order as presented by applicant** □ **CPA** □ **T.D.** □ **R.1.47**

CLAIM		**DATE**								
Final	Original	08/22/2016								
	1	-								
	2	-								
	3	-								
	4	-								
	5	-								
	6	-								
	7	-								
	8	-								
	9	-								
	10	-								
	11	-								
	12	-								
	13	-								
	14	-								
	15	-								
	16	-								
	17	-								
	18	-								
	19	-								
	20	-								
	21	✓								
	22	✓								
	23	✓								
	24	✓								
	25	✓								
	26	✓								
	27	✓								
	28	✓								
	29	✓								
	30	✓								
	31	✓								
	32	✓								
	33	✓								
	34	✓								
	35	✓								
	36	✓								

Index of Claims	**Application/Control No.** 14071126	**Applicant(s)/Patent Under Reexamination** WEISS, KENNETH P.
	Examiner ISIDORA IMMANUEL	**Art Unit** 3685

✓	**Rejected**	-	**Cancelled**	N	**Non-Elected**	A	**Appeal**
=	**Allowed**	÷	**Restricted**	I	**Interference**	O	**Objected**

□ **Claims renumbered in the same order as presented by applicant** □ **CPA** □ **T.D.** □ **R.1.47**

CLAIM		**DATE**								
Final	Original	08/22/2016								
	37	✓								
	38	✓								
	39	✓								
	40	✓								
	41	✓								
	42	✓								
	43	✓								
	44	✓								
	45	✓								
	46	✓								
	47	✓								
	48	✓								
	49	✓								

Search Notes	**Application/Control No.** 14071126	**Applicant(s)/Patent Under Reexamination** WEISS, KENNETH P.
	Examiner ISIDORA IMMANUEL	**Art Unit** 3685

CPC- SEARCHED

Symbol	Date	Examiner
G06Q	8/22/2016	II

CPC COMBINATION SETS - SEARCHED

Symbol	Date	Examiner

US CLASSIFICATION SEARCHED

Class	Subclass	Date	Examiner

SEARCH NOTES

Search Notes	Date	Examiner
See attached notes	8/22/2016	II

INTERFERENCE SEARCH

US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

/I.I./ Examiner.Art Unit 3685	

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14071126
Filing Date	2013-11-04
First Named Inventor	Kenneth P. Weiss
Art Unit	3685
Examiner Name	T. J. Huang /ISIDORA I IMMANUEL/
Attorney Docket Number	W0537-701321

U.S.PATENTS

Remove

Examiner Initial*	Cite No	Patent Number	Kind Code1	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/I.I.I./	1	7552467		2009-06-23	Lindsay	
/I.I.I./	2	8380637		2013-02-19	Levovitz	
/I.I.I./	3	8423466		2013-04-16	Lanc	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS

Remove

Examiner Initial*	Cite No	Publication Number	Kind Code1	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/I.I.I./	1	20020194499		2002-12-19	Audebert et al.	
/I.I.I./	2	20040014423		2004-01-22	Croome et al.	
/I.I.I./	3	20120150750		2012-06-14	Law et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.I./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14071126
	Filing Date	2013-11-04
	First Named Inventor	Kenneth P. Weiss
	Art Unit	3685
	Examiner Name	T. J. Huang
	Attorney Docket Number	W0537-701321

/I.I.I./	4	20120230555		2012-09-13	Miura et al.	
/I.I.I./	5	20130318581		2013-11-28	COUNTERMAN	
/I.I.I./	6	20150046340		2015-02-12	Dimmick	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							□

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		□

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/ISIDORA I IMMANUEL/	Date Considered	08/22/2016

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.I./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number		14071126
	Filing Date		2013-11-04
	First Named Inventor	Kenneth P. Weiss	
	Art Unit		3685
	Examiner Name	T. J. Huang	
	Attorney Docket Number		W0537-701321

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.J.H./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	14071126
	Filing Date	2013-11-04
	First Named Inventor	Kenneth P. Weiss
	Art Unit	3685
	Examiner Name	T. J. Huang
	Attorney Docket Number	W0537-701321

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

□ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

□ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

□ See attached certification statement.

□ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Matthew H. Grady/	Date (YYYY-MM-DD)	2015-04-17
Name/Print	Matthew H. Grady	Registration Number	52957

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1 hour 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.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.J.H./

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 record s.

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.

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14071126
Filing Date	2013-11-04
First Named Inventor	Kenneth P. Weiss
Art Unit	3685
Examiner Name	T. J. Huang /ISIDORA I IMMANUEL/
Attorney Docket Number	W0537-701321

U.S.PATENTS

Remove

Examiner Initial*	Cite No	Patent Number	Kind Code1	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/I.I.I./	1	8271397		2012-09-18	Weiss	
/I.I.I./	2	8538881		2013-09-17	Weiss	
/I.I.I./	3	8577813		2013-11-05	Weiss	
/I.I.I./	4	8594632		2013-11-26	Azizi et al.	
/I.I.I./	5	8613052		2013-12-17	Weiss	
/I.I.I./	6	8856539		2014-10-07	Weiss	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS

Remove

Examiner Initial*	Cite No	Publication Number	Kind Code1	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.I./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14071126
Filing Date	2013-11-04
First Named Inventor	Kenneth P. Weiss
Art Unit	3685
Examiner Name	T. J. Huang
Attorney Docket Number	W0537-701321

/I.I.I./	1	20030037233		2003-02-20	Pearson	
/I.I.I./	2	20040088369		2004-05-06	Yeager et al.	
/I.I.I./	3	20050097362		2005-05-05	Winget et al.	
/I.I.I./	4	20060087999		2006-04-27	Gustave et al.	
/I.I.I./	5	20060276226		2006-12-07	Jiang	
/I.I.I./	6	20070118758		2007-05-24	Takahashi et al.	
/I.I.I./	7	20070265984		2007-11-15	Santhana	
/I.I.I./	8	20090097661		2009-04-16	Orsini et al.	
/I.I.I./	9	20110283337		2011-11-17	Schatzmayr	
/I.I.I./	10	20130307670		2013-11-21	Ramaci	
	11	20140096216		2014-04-03	Weiss	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.I./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	14071126
	Filing Date	2013-11-04
	First Named Inventor	Kenneth P. Weiss
	Art Unit	3685
	Examiner Name	T. J. Huang
	Attorney Docket Number	W0537-701321

/I.I.I/	12	20140101049		2014-04-10	Fernandes et al.	
/I.I.I/	13	20140196118		2014-07-10	Weiss	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number3	Country Code2 i	Kind Code4	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T5
	1							□

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1		□

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/ISIDORA I IMMANUEL/	Date Considered	08/22/2016

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.I/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14071126
Filing Date	2013-11-04
First Named Inventor	Kenneth P. Weiss
Art Unit	3685
Examiner Name	T. J. Huang
Attorney Docket Number	W0537-701321

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

□ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

□ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

□ See attached certification statement.

□ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Matthew H. Grady/	Date (YYYY-MM-DD)	2015-02-26
Name/Print	Matthew H. Grady	Registration Number	52957

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1 hour 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.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.J.H./

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 record s.

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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.T.J./

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14071126
Filing Date	2013-11-04
First Named Inventor	Kenneth P. Weiss
Art Unit	N/A
Examiner Name	Not Yet Assigned /ISIDORA I IMMANUEL/
Attorney Docket Number	W0537-701321

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code1	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/I.I.I./	1	4720860		1988-01-19	Weiss	
/I.I.I./	2	4856062		1989-08-08	Weiss	
/I.I.I./	3	4885778		1989-12-05	Weiss	
/I.I.I./	4	4998279		1991-03-05	Weiss	
/I.I.I./	5	5023908		1991-06-11	Weiss	
/I.I.I./	6	5058161		1991-10-15	Weiss	
/I.I.I./	7	5097505		1992-03-17	Weiss	
/I.I.I./	8	5168520		1992-12-01	Weiss	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.I./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	14071126
	Filing Date	2013-11-04
	First Named Inventor	Kenneth P. Weiss
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	W0537-701321

/I.I.I./	9	5237614		1993-08-17	Weiss	
/I.I.I./	10	5361062		1994-11-01	Weiss et al.	
/I.I.I./	11	5367572		1994-11-22	Weiss	
/I.I.I./	12	5398285		1995-03-14	Borgelt et al.	
/I.I.I./	13	5479512		1995-12-26	Weiss	
/I.I.I./	14	5485519		1996-01-16	Weiss	
/I.I.I./	15	5657388		1997-08-12	Weiss	
/I.I.I./	16	5664109		1997-09-02	Johnson et al.	
/I.I.I./	17	5813006		1998-09-22	Polnerow et al.	
/I.I.I./	18	5915023		1999-06-22	Bernstein	
/I.I.I./	19	6073106		2000-06-06	Rozen et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.I./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	14071126
	Filing Date	2013-11-04
	First Named Inventor	Kenneth P. Weiss
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	W0537-701321

/I.I.I./	20	6130621		2000-10-10	Weiss	
/I.I.I./	21	6253202		2001-06-26	Gilmour	
/I.I.I./	22	6253203		2001-06-26	O'Flaherty et al.	
/I.I.I./	23	6260039		2001-07-10	Schneck et al.	
/I.I.I./	24	6308203		2001-10-23	Itabashi et al.	
/I.I.I./	25	6309342		2001-10-30	Blazey et al.	
/I.I.I./	26	6393421		2002-05-21	Paglin	
/I.I.I./	27	6516315		2003-02-04	Gupta	
/I.I.I./	28	6546005		2003-04-08	Berkley et al.	
/I.I.I./	29	6581059		2003-06-17	Barrett et al.	
/I.I.I./	30	6640211		2003-10-28	Holden	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.I./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14071126
Filing Date	2013-11-04
First Named Inventor	Kenneth P. Weiss
Art Unit	N/A
Examiner Name	Not Yet Assigned
Attorney Docket Number	W0537-701321

/I.I.I./	31	6658400		2003-12-02	Perell et al.	
/I.I.I./	32	6819219		2004-11-16	Bolle et al.	
/I.I.I./	33	6845448		2005-01-18	Chaganti et al.	
/I.I.I./	34	6941271		2005-09-06	Soong	
/I.I.I./	35	7237117		2007-06-26	Weiss	
/I.I.I./	36	7249112		2007-07-24	Berardi et al.	
/I.I.I./	37	7278026		2007-10-02	McGowan	
/I.I.I./	38	7489781		2009-02-10	Klassen et al.	
/I.I.I./	39	7502459		2009-03-10	Moseley	
/I.I.I./	40	7548981		2009-06-16	Taylor et al.	
/I.I.I./	41	7571139		2009-08-04	Giordano et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.I./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14071126
Filing Date	2013-11-04
First Named Inventor	Kenneth P. Weiss
Art Unit	N/A
Examiner Name	Not Yet Assigned
Attorney Docket Number	W0537-701321

/I.I.I./	42	7657639		2010-02-02	Hinton	
/I.I.I./	43	7705732		2010-04-27	Bishop et al.	
/I.I.I./	44	7412604		2008-08-12	Doyle	
/I.I.I./	45	7007298		2006-02-28	Shinzaki et al.	
/I.I.I./	46	6202055		2001-03-13	Houvener et al.	
/I.I.I./	47	6088450		2000-07-11	Davis et al.	
/I.I.I./	48	8079079		2011-12-13	Zhang et al.	
/I.I.I./	49	5870723		1999-02-09	Pare, Jr. et al.	
/I.I.I./	50	7809651		2010-10-05	Weiss	
/I.I.I./	51	6498861		2002-12-24	Hamid et al.	
/I.I.I./	52	7805372		2010-09-28	Weiss	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.I./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	14071126
	Filing Date	2013-11-04
	First Named Inventor	Kenneth P. Weiss
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	W0537-701321

/I.I.I./	53	8234220		2012-07-31	Weiss	
/I.I.I./	54	5457747		1995-10-10	Drexler et al.	
/I.I.I./	55	6950521		2005-09-27	Marcovici et al.	
/I.I.I./	56	8001055		2011-08-16	Weiss	
/I.I.I./	57	5971272		1999-10-26	Hsiao	
/I.I.I./	58	7766223		2010-08-03	Mello et al.	
/I.I.I./	59	7552333		2009-06-23	Wheeler et al.	
/I.I.I./	60	7742967		2010-06-22	Keresman, III et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/I.I.I./	1	20010032100		2001-10-18	Mahmud et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.I./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14071126
Filing Date	2013-11-04
First Named Inventor	Kenneth P. Weiss
Art Unit	N/A
Examiner Name	Not Yet Assigned
Attorney Docket Number	W0537-701321

/I.I.I./	2	20010044900		2001-11-22	Uchida	
/I.I.I./	3	20020046061		2002-04-18	Wright et al.	
/I.I.I./	4	20020090930		2002-07-11	Fujiwara et al.	
/I.I.I./	5	20020176610		2002-11-28	Okazaki et al.	
/I.I.I./	6	20020178364		2002-11-28	Weiss	
/I.I.I./	7	20030115490		2003-06-19	Russo et al.	
/I.I.I./	8	20030123713		2003-07-03	Geng	
/I.I.I./	9	20030129965		2003-07-10	Siegel	
/I.I.I./	10	20030163710		2003-08-28	Ortiz et al.	
/I.I.I./	11	20030226041		2003-12-04	Palmer et al.	
/I.I.I./	12	20040017934		2004-01-29	Kocher	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.I./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14071126
Filing Date	2013-11-04
First Named Inventor	Kenneth P. Weiss
Art Unit	N/A
Examiner Name	Not Yet Assigned
Attorney Docket Number	W0537-701321

/I.I.I./	13	20040034771		2004-02-19	Edgett et al.	
/I.I.I./	14	20040059923		2004-03-25	ShamRao	
/I.I.I./	15	20040111625		2004-06-10	Duffy et al.	
/I.I.I./	16	20040117215		2004-06-17	Marchosky	
/I.I.I./	17	20040117302		2004-06-17	Weichert et al.	
/I.I.I./	18	20040133787		2004-07-08	Doughty et al.	
/I.I.I./	19	20040151351		2004-08-05	Ito	
/I.I.I./	20	20040188519		2004-09-30	Cassone	
/I.I.I./	21	20040236699		2004-11-25	Beenau et al.	
/I.I.I./	22	20050001711		2005-01-06	Doughty et al.	
/I.I.I./	23	20050039027		2005-02-17	Shapiro	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.I./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	14071126
	Filing Date	2013-11-04
	First Named Inventor	Kenneth P. Weiss
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	W0537-701321

/I.I.I./	24	20050187843		2005-08-25	Lapsley et al.	
/I.I.I./	25	20050210270		2005-09-22	Rohatgi et al.	
/I.I.I./	26	20050235148		2005-10-20	Scheidt et al.	
/I.I.I./	27	20050238208		2005-10-27	Sim	
/I.I.I./	28	20060016884		2006-01-26	Block et al.	
/I.I.I./	29	20060104486		2006-05-18	Le Saint et al.	
/I.I.I./	30	20060122939		2006-06-08	Cohen et al.	
/I.I.I./	31	20060165060		2006-07-27	Dua	
/I.I.I./	32	20060256961		2006-11-16	Brainard et al.	
/I.I.I./	33	20070040017		2007-02-22	Kozlay	
/I.I.I./	34	20070079136		2007-04-05	Vishik et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.I./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14071126
Filing Date	2013-11-04
First Named Inventor	Kenneth P. Weiss
Art Unit	N/A
Examiner Name	Not Yet Assigned
Attorney Docket Number	W0537-701321

/I.I.I./	35	20070124697		2007-05-31	Dongelmans	
/I.I.I./	36	20070186105		2007-08-09	Bailey et al.	
/I.I.I./	37	20070198436		2007-08-23	Weiss	
/I.I.I./	38	20080021997		2008-01-24	HINTON	
/I.I.I./	39	20080212848		2008-09-04	Doyle	
/I.I.I./	40	20080275819		2008-11-06	Rifai	
/I.I.I./	41	20090144814		2009-06-04	Sacco	
/I.I.I./	42	20090175507		2009-07-09	Schaffner	
/I.I.I./	43	20060206724		2006-09-14	Schaufele et al.	
/I.I.I./	44	20020184538		2002-12-05	Sugimura et al.	
/I.I.I./	45	20070140145		2007-06-21	Kumar et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.I./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14071126
Filing Date	2013-11-04
First Named Inventor	Kenneth P. Weiss
Art Unit	N/A
Examiner Name	Not Yet Assigned
Attorney Docket Number	W0537-701321

/I.I.I./	46	20050187873		2005-08-25	Labrou et al.	
/I.I.I./	47	20070005988		2007-01-04	Zhang et al.	
/I.I.I./	48	20060000900		2006-01-05	Fernandes et al.	
/I.I.I./	49	20070124597		2007-05-31	Bedingfield	
/I.I.I./	50	20070186115		2007-08-09	GAO et al.	
/I.I.I./	51	20090203355		2009-08-13	Clark	
/I.I.I./	52	20070245152		2007-10-18	Pizano et al.	
/I.I.I./	53	20100046443		2010-02-25	Jia et al.	
/I.I.I./	54	20090083544		2009-03-26	Scholnick et al.	
/I.I.I./	55	20030014372		2003-01-16	Wheeler et al.	
/I.I.I./	56	20030046540	A1	2003-03-06	Nakamura et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.I./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	14071126
	Filing Date	2013-11-04
	First Named Inventor	Kenneth P. Weiss
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	W0537-701321

/I.I.I./	57	20030229637	A1	2003-12-11	Baxter et al.	
/I.I.I./	58	20120240195		2012-09-20	Weiss	
/I.I.I./	59	20120130904		2012-05-24	Weiss	
/I.I.I./	60	20030028481		2003-02-06	Flitcroft et al.	
/I.I.I./	61	20030084332		2003-05-01	Krasinski et al.	
/I.I.I./	62	20080127311		2008-05-29	Yasaki et al.	
/I.I.I./	63	20050113070		2005-05-26	Okabe	
/I.I.I./	64	20030085808		2003-05-08	Goldberg	
/I.I.I./	65	20050238147		2005-10-27	Carro	
/I.I.I./	66	20130024374		2013-01-24	Weiss	
/I.I.I./	67	20110258120		2011-10-20	Weiss	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.I./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number		14071126
	Filing Date		2013-11-04
	First Named Inventor	Kenneth P. Weiss	
	Art Unit		N/A
	Examiner Name	Not Yet Assigned	
	Attorney Docket Number		W0537-701321

/I.I.I./	68	20090292641		2009-11-26	Weiss	
/I.I.I./	69	20080005576		2008-01-03	Weiss	
/I.I.I./	70	20070256120		2007-11-01	Shatzkamer et al.	
/I.I.I./	71	20080040274		2008-02-14	UZO	
/I.I.I./	72	20100000455		2010-01-07	Harper	
/I.I.I./	73	20120037479		2012-02-16	Lucchi et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number3	Country Code2 i	Kind Code4	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T5
/I.I.I./	1	0986209	EP	A2	2000-03-15	Mitsubishi Electric Corp		□
/I.I.I./	2	1081632	EP	A1	2001-03-07	Keyware, Technologies		□
/I.I.I./	3	2382006	GB	A	2003-05-14	Ibm		□

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.I./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	14071126
	Filing Date	2013-11-04
	First Named Inventor	Kenneth P. Weiss
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	W0537-701321

/I.I.I./	4	1992007436	WO	A1	1992-04-30	Security Dynamics Techn		□
/I.I.I./	5	1996036934	WO	A1	1996-11-21	Smart Touch L L C		□
/I.I.I./	6	2002014985	WO	A2	2002-02-21	Kern, Daniel A		□
/I.I.I./	7	2010000455	WO	A1	2010-01-07	Vodafone Holding Gmbh et al.		□
/I.I.I./	8	9207436	WO	A1	1992-04-30	Security Dynamics Technologies, Inc		□
/I.I.I./	9	9636934	WO	A1	1996-11-21	Smart Touch, L.l.c		□
/I.I.I./	10	0214985	WO	A2	2002-02-21	Kern, Daniel		□
/I.I.I./	11	2012/037479	WO	A9	2012-07-26	Universal Secure Registry, Llc		□
/I.I.I./	12	2012037479	WO	A1	2012-03-22	Universal Secure Registry, Llc		□

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.I./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14071126
Filing Date	2013-11-04
First Named Inventor	Kenneth P. Weiss
Art Unit	N/A
Examiner Name	Not Yet Assigned
Attorney Docket Number	W0537-701321

/I.I.I./	1	"Biometrics: Who's Watching You?", Electronic Frontier Foundation (EFF), September 2003, all pages, http://www.eff.org/wp/biometrics-whos-watching-you.	□
/I.I.I./	2	"FIPS PUB 46-3", National Institute of Science and Technology (NIST), October 25, 1999, all pages.	□
/I.I.I./	3	"Information Security: Challenges in using biometrics", September 9, 2003, all pages, <http://www.gao.gov/news.items/d031137t.pdf>.	□
/I.I.I./	4	"PGP: An introduction to cryptography", 2000, all pages.	□
/I.I.I./	5	"Single Sign On Authentication", Authentication World, March 13, 2007, all pages, retrieved July 9, 2010 via Wayback Machine, <http://web.archive.org/web/20070313200434/http://www.authenticationworld.com/Single-Sign-On-Authentication/>.	□
/I.I.I./	6	HUNGTINGTON, "101 Things to know about single sign on", Authentication World, 2006, all pages, <http://www.authenticationworld.com/Single-Sign-On-Authentication/101ThingsToKnowAboutSingleSignOn.pdf>.	□
/I.I.I./	7	International Search Report from PCT Application No. PCT/US2007/004646 mailed November 27, 2007.	□
/I.I.I./	8	International Search Report from PCT Application No. PCT/US2007/070701 mailed March 11, 2008.	□
/I.I.I./	9	International Search Report from PCT Application No. PCT/US2009/035282 mailed July 10, 2009.	□
/I.I.I./	10	KESSLER, "An overview of cryptography", August 22, 2002, all pages, retrieved via Wayback Machine on January 19, 2010, http://www.garykessler.net/library/crypto.html.	□
/I.I.I./	11	PABRAI, "Biometrics for PC-user authentication: a primer", Access Controls & Security Systems, February 1, 2001, all pages, <http://www.securitysolutions.com/mag/securit_biometrics_pcuser_authentication/index.html>.	□

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.I./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14071126
Filing Date	2013-11-04
First Named Inventor	Kenneth P. Weiss
Art Unit	N/A
Examiner Name	Not Yet Assigned
Attorney Docket Number	W0537-701321

/I.I.I./	12	Pabrai, U. "Biometrics for PC-User Authentication: A Primer" 1 February 2001. Access Controls & Security Systems. All pages. <http://www.securitysolutions.com/mag/security_biometrics_pcuser_authentication/index.html>	□
/I.I.I./	13	"Information Security: Challenges in Using Biometrics" 9 September 2003. All pages. <http://www.gao.gov/new.items/d031137t.pdf>	□
/I.I.I./	14	Huntington, G. "101 Things to Know About Single Sign On." 2006. Authentication World. All pages. <http://www.authenticationworld.com/Single-Sign-On-Authentication/101ThingsToKnowAboutSingleSignOn.pdf>	□
/I.I.I./	15	"Single Sign on Authentication" 13 March 2007. Authentication World. All pages. Retrieved 9 July 2010 via Wayback Machine. <http://web.archive.org/web/20070313200434/http://www.authenticationworld.com/Single-Sign-On-Authentication/>	□
/I.I.I./	16	Kessler, G. "An Overview of Cryptography." 22 August 22, 2002. All pages. Retrived via Wayback Machine on 19 January 2010. http://www.garykessler.net/library/crypto.html	□
/I.I.I./	17	Treasury Board of Canada Secretariat, PKI for Beginners Glossary, http://www.tbs-sct.gc.ca/pki-icp/beginners/glossary-eng.asp	□
/I.I.I./	18	"FIPS PUB 46-3." 25 October 1999. National Institute of Science and Technology (NIST). All pages.	□
/I.I.I./	19	International Search Report from PCT/US2007/004646 mailed November 27, 2007.	□
/I.I.I./	20	International Search Report from corresponding PCT/US2007/070701 mailed March 11, 2008.	□
/I.I.I./	21	International Search Report from PCT/US2009/035282 mailed July 10, 2009.	□
/I.I.I./	22	"Bluetooth Technology FAQ", Mobileinfo.com, 21 January 2001, all pages, http://www.web.archive.org/web/200101211551/http://www.mobileinfo.com/Bluetooth/FAQ.htm	□

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.I./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	14071126
	Filing Date	2013-11-04
	First Named Inventor	Kenneth P. Weiss
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	W0537-701321

/I.I.I./	23	International Search Report and Written Opinion for International Application No. PCT/US2011/051966, 49 pages.	□
/I.I.I./	24	International Search Report from PCT/US2007/070701 mailed March 11, 2008.	□

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/ISIDORA I IMMANUEL/	Date Considered	08/22/2016

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.I./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	14071126
	Filing Date	2013-11-04
	First Named Inventor	Kenneth P. Weiss
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	W0537-701321

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

□ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

□ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

□ See attached certification statement.

□ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Matthew H. Grady/	Date (YYYY-MM-DD)	2014-02-04
Name/Print	Matthew H. Grady	Registration Number	52957

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1 hour 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.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.T./

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 record s.

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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.T.J./

EAST Search History

EAST Search History (Prior Art)

<table>
<tr><th>Ref #</th><th>Hits</th><th>Search Query</th><th>DBs</th><th>Default Operator</th><th>Plurals</th><th>Time Stamp</th></tr>
<tr><td>L1</td><td>4</td><td>("5,280,527").PN.</td><td>US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT</td><td>OR</td><td>OFF</td><td>2016/08/22 09:20</td></tr>
<tr><td>L2</td><td>2</td><td>("20020184500").PN.</td><td>US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT</td><td>OR</td><td>OFF</td><td>2016/08/22 09:20</td></tr>
<tr><td>S1</td><td>163</td><td>("20060205388" | "20090287921" | "20020194499" | "20040014423" | "20120150750" | "20120230555" | "20130318581" | "20150046340" | "7552467" | "8380637" | "8423466" | "20030037233" | "20040088369" | "20050097362" | "20060087999" | "20060276226" | "20070118758" | "20070265984" | "20090097661" | "20110283337" | "20130307670" | "20140096216" | "20140101049" | "20140196118" | "8271397" | "8538881" | "8577813" | "8594632" | "8613052" | "8856539" | "20010032100" | "20010044900" | "20020046061" | "20020090930" | "20020176610" | "20020178364" | "20020184538" | "20030014372" | "20030028481" | "20030046540" | "20030084332" | "20030085808" | "20030115490" | "20030123713" | "20030129965" | "20030163710" | "20030226041" | "20030229637" | "20040017934" | "20040034771" | "20040059923" | "20040111625" | "20040117215" | "20040117302" | "20040133787" | "20040151351" | "20040188519" | "20040236699" | "20050001711" | "20050039027" | "20050113070" | "20050187843" | "20050187873" | "20050210270" | "20050235148" | "20050238147" | "20050238208" | "20060000900" | "20060016884" | "20060104486" | "20060122939" | "20060165060" | "20060206724" | "20060256961" | "20070005988" | "20070040017" | "20070079136" | "20070124597" | "20070124697" |</td><td>US-PGPUB; USPAT</td><td>OR</td><td>ON</td><td>2016/08/21 23:52</td></tr>
</table>

		"20070140145" | "20070186105" | "20070186115" | "20070198436" | "20070245152" | "20070256120" | "20080005576" | "20080021997" | "20080040274" | "20080127311" | "20080212848" | "20080275819" | "20090083544" | "20090144814" | "20090175507" | "20090203355" | "20090292641" | "20100000455" | "20100046443" | "20110258120" | "20120037479" | "20120130904" | "20120240195" | "20130024374" | "4720860" | "4856062" | "4885778" | "4998279" | "5023908" | "5058161" | "5097505" | "5168520" | "5237614" | "5361062" | "5367572" | "5398285" | "5457747" | "5479512" | "5485519" | "5657388" | "5664109" | "5813006" | "5870723" | "5915023" | "5971272" | "6073106" | "6088450" | "6130621" | "6202055" | "6253202" | "6253203" | "6260039" | "6308203" | "6309342" | "6393421" | "6498861" | "6516315" | "6546005" | "6581059" | "6640211" | "6658400" | "6819219" | "6845448" | "6941271" | "6950521" | "7007298" | "7237117" | "7249112" | "7278026" | "7412604" | "7489781" | "7502459" | "7548981" | "7552333" | "7571139" | "7657639" | "7705732" | "7742967" | "7766223" | "7805372" | "7809651" | "8001055" | "8079079" | "8234220").PN.				

8/22/2016 9:21:12 AM
C:\ Users\ iiluonakhamhe\ Documents\ EAST\ Workspaces\ 14071126.wsp

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. OMB 0651-0031
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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(**Not for submission under 37 CFR 1.99)**

Application Number	14071126
Filing Date	2013-11-04
First Named Inventor	Kenneth P. Weiss
Art Unit	3685
Examiner Name	T. J. Huang /ISIDORA I IMMANUEL/
Attorney Docket Number	W0537-701321

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code1	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code1	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/I.I.I/	1	20060205388		2006-09-14	Semple et al.	
/I.I.I/	2	20090287921		2009-11-19	Zhu et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number3	Country Code2 i	Kind Code4	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T5
	1							□

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.I/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	14071126
	Filing Date	2013-11-04
	First Named Inventor	Kenneth P. Weiss
	Art Unit	3685
	Examiner Name	T. J. Huang
	Attorney Docket Number	W0537-701321

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1		□

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/ISIDORA I IMMANUEL/	Date Considered	08/22/2016

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.I./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(**Not for submission under 37 CFR 1.99)**

Application Number	14071126
Filing Date	2013-11-04
First Named Inventor	Kenneth P. Weiss
Art Unit	3685
Examiner Name	T. J. Huang
Attorney Docket Number	W0537-701321

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Matthew H. Grady/	Date (YYYY-MM-DD)	2015-10-09
Name/Print	Matthew H. Grady	Registration Number	52957

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1 hour 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.**

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 record s.

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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.T.J./

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted via the Office electronic filing system in accordance with 37 CFR § 1.6(a)(4).

Dated: November 30th, 2016
Electronic Signature for John N. Anastasi: /John N. Anastasi/

Docket No.: W0537-701321
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Kenneth P. Weiss

Application No.: 14/071,126

Confirmation No.: 3814

Filed: November 4, 2013

Art Unit: 3685

For: UNIVERSAL SECURE REGISTRY

Examiner: I. I. Immanuel

AMENDMENT IN RESPONSE TO NON-FINAL OFFICE ACTION UNDER 37 C.F.R. § 1.111

MS Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

INTRODUCTORY COMMENTS

In response to the Non-Final Office Action dated August 31, 2016, please amend the above-identified U.S. patent application as follows:

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks/Arguments begin on page 8 of this paper.

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1-20 (Cancelled)

21. (Currently Amended) An electronic ID device configured to provide encrypted authentication information to enable execution of ~~execute~~ a secure operation, comprising:

a biometric sensor configured to receive a biometric input provided by [[the]] a user;

a user interface configured to receive a user input including secret information known to the user and information indicative of ~~concerning~~ a secure operation to be executed;

a communication interface configured to communicate with a system configured to execute the secure operation;

a processor coupled to the biometric sensor, the user interface, and the communication interface, the processor being programmed ~~to activate the electronic ID device based on successful authentication by the electronic ID device of at least the biometric input or the secret information, the processor also being programmed~~ such that once the electronic ID device successfully authenticates at least one of the biometric input and the secret information, ~~is activated~~ the processor is configured to generate a non-predictable value and to generate encrypted authentication information from the non-predictable value, from information derived from at least a portion of the biometric input, and from information derived from at least a portion of the secret information, and to communicate the encrypted authentication information via the communication interface to the system configured to execute the secure operation.

22. (Previously Presented) The electronic ID device of claim 21, wherein the communication interface comprises a transmitter configured to wirelessly transmit the encrypted authentication information to the system configured to execute the secure operation.

23. (Currently Amended) The electronic ID device of claim 21, further comprising the system configured to execute the secure operation, wherein the system ~~providing the secure operation~~ is configured to transmit the encrypted authentication information to a secure registry

software and to receive authorization to perform the secure operation from the secure registry software.

24. (Currently Amended) The electronic ID device of claim 21, further comprising the system configured to execute the secure operation, wherein the secure operation includes a secure transaction, and wherein the system configured to perform the secure operation comprises a point-of-sale (POS) device.

25. (Previously Presented) The electronic ID device of claim 24, wherein the user interface is configured to display options for purchase.

26. (Previously Presented) The electronic ID device of claim 24, wherein the user interface is configured to accept user selection of at least one product or service for purchase.

27. (Currently Amended) The electronic ID device of claim 21, further comprising the system configured to execute the secure operation, wherein execution of the secure operation permits access to a secure location, and the system configured to execute the secure operation is further configured to manage access to the secure location.

28. (Previously Presented) The electronic ID device of claim 21, wherein the electronic ID device comprises a discrete code associated with the electronic ID device.

29. (Previously Presented) The electronic ID device of claim 21, wherein the user interface is configured to initiate authentication with the system configured to execute the secure operation responsive to the user manually entering a secret code.

30. (Currently Amended) The electronic ID device of claim 21, wherein the user ~~initiates~~ initiates, via the electronic ID device, authentication with the system configured to execute the secure operation.

31. (Currently Amended) The electronic ID device of claim 21, wherein at least a portion of the biometric input received by the biometric sensor is communicated to a secure registry software for authentication by the electronic ID device prior to generation of the encrypted authentication information.

32. (Currently Amended) The electronic ID device of claim 21, wherein the user interface is configured to receive the secret information ~~includes~~ including the identifying information.

33. (Currently Amended) The electronic ID device of claim 21, further comprising a memory coupled to the processor, wherein the memory stores information employed by the electronic ID device to authenticate the biometric input received by the biometric sensor.

34. (Currently Amended) The electronic ID device of claim 31, wherein the electronic ID device is configured to [[does]] not permit the entry of the user input if the biometric input received by the biometric sensor is determined to not belong to an authorized user of the electronic ID device.

35. (Currently Amended) The electronic ID device of claim 32, wherein the secret information known to the user includes a [[PIN,]] Personal Identification Number (PIN), and wherein the processor is configured to generate the non-predictable value and the encrypted authentication information responsive to authentication of both the secret information and the biometric input ~~activate the electronic ID device for the secure operation~~.

36. (Currently Amended) The electronic ID device of claim 32, wherein data stored in [[the]] a memory is unavailable to an individual in possession of the electronic ID device until the electronic ID device ~~is activated~~ successfully authenticates at least one of the biometric input and the secret information.

37. (Currently Amended) The electronic ID device of claim 34, wherein [[the]] data stored in [[the]] a memory is subject to ~~a mathematical operation~~ encryption that acts to modify the data

such that it is unintelligible until the electronic ID device successfully authenticates at least one of the biometric input and the secret information ~~is activated~~.

38. (Currently Amended) The electronic ID device of claim 33, wherein the memory is configured to store an electronic code unique to the electronic ID device, wherein the processor is configured to generate a seed using at least two of the electronic serial number, a discrete code associated with the electronic ID device, ~~the PIN,~~ a Personal Identification Number (PIN), a time value, and information derived from the biometric input to generate the encrypted authentication information, and wherein the seed is employed by the processor to generate the non-predictable value.

39. (Currently Amended) The electronic ID device of claim 21, wherein the electronic ID device executes a challenge-response protocol as part of authentication with [[and]] the system configured to execute the secure operation ~~execute a challenge-response protocol as part of authentication~~.

40. (Currently Amended) A method of controlling execution of a secure operation, the method comprising acts of:

receiving, from a user by an electronic ID device, information indicative of the secure operation to be executed;

authenticating an identity of [[a]] the user to [[an]] the electronic ID device based on at least one of biometric data received by the electronic ID device from the user [[or]] and secret information known to the user and provided to the electronic ID device; and

~~activating the electronic ID device based on successful authentication;~~

responsive to successful authentication of the identity of the user to the electronic ID device:

generating, with the electronic ID device, a non-predictable value;

generating, with the electronic ID device, encrypted authentication information from the non-predictable value, from information derived from at least a portion of the biometric input, and from information derived from at least a portion of the secret information; and communicating the encrypted authentication information from the electronic ID device to [[the]] a system configured to execute the secure operation.

41. (Currently Amended) The method of claim 40, further comprising an act of receiving at least a portion of a [[users]] user's secret information manually within a user interface ~~interfaces~~.

42. (Currently Amended) The method of claim 40, further comprising an act of displaying, on a user interface, ~~interface~~ indicators for [[the]] a plurality of user accounts stored in a memory of the electronic ID device.

43. (Currently Amended) The method of claim 40, further comprising an act of ~~de-activating~~ entering, by the electronic ID ~~device~~ device, a de-active state without generating the encrypted authentication information if the identity of the user is not successfully authenticated to the electronic ID device.

44. (Previously Presented) The method of claim 40, further comprising an act of generating a seed from which the authentication information is generated by employing at least two of the biometric data, the secret information known to the user, and a discrete code unique to the electronic ID device.

45. (Currently Amended) The method of claim 40, further comprising an act of generating encrypted authentication information in a manner that allows [[the]] identification of the user and [[the]] a selected one of [[the]] a plurality of user accounts by secure registry software.

46. (Previously Presented) The method of claim 40, further comprising displaying options for selection of the system configured to execute the secure operation on a user interface.

47. (Previously Presented) The method of claim 46, further comprising selecting with the user interface at least one product, service, or secure operation.

48. (Previously Presented) The method of claim 46, further comprising maintaining an audit trail of purchases made.

49. (Currently Amended) The method of claim 40, [[where]] wherein the user initiates an authentication request on the electronic ID device triggering communication of the encrypted authentication information from the electronic ID device to the system configured to execute the secure operation.

REMARKS

In response to the Non-Final Office Action mailed August 31, 2016, Applicant respectfully requests reconsideration in view of the amendments and the following remarks.

Claims 21-49 were pending in this application. Claims 21, 23, 24, 27, 30, 31-43, 45, and 49 have been amended herein. As a result, claims 21-49 are pending for examination, with claims 21 and 40 being in independent form. No new matter has been added. The application as presented is believed to be in condition for allowance.

EXAMINER COMMENTS

The Examiner alleges that numerous elements of the claims recite intended use and therefore do not have patentable weight pursuant to MPEP 2114. The Examiner also alleges that numerous elements of the claims recite functional language and therefore lack patentable weight, with reference to *In re Schreiber*. However, MPEP §2114 also acknowledges that features of an apparatus "may be recited either structurally or functionally." Further, MPEP §2173.05(g) describes the use of functional limitations in detail and notes with reference to *In re Schreiber,* 128 F.3d 1473, 1478 (Fed. Cir. 1997) that a patent applicant is free to recite features of an apparatus either structurally or functionally.

Claim 21 of the present application, prior to the functional language recited in the Office Action, recites an electronic ID device that is "configured to" perform the functional limitations. The limitations of claim 21 are met by an electronic ID device that is structurally configured to perform the recited functions.

With regard to claims 24, 32, and 35, the Office Action states that these claims are nonfunctional descriptive material and therefore do not have patentable weight pursuant to MPEP 2111.05 III. Applicant notes that MPEP 2111.05 III is directed to "a claim directed to a computer-readable medium containing certain programming." Claims 24, 32, and 34 are not "claim[s] directed to a computer-readable medium." Accordingly, the Examiner's assertion that these claims lack patentable weight is improper and incorrect. Nevertheless, Applicant has amended these claims to recite that the device is configured to accomplish the function and therefore the rejection is now moot. Withdrawal of this rejection is therefore requested.

The Examiner alleges that claims 40 and 49 do not have patentable weight pursuant to MPEP 2111.04, and that claims 41 and 45 do not have patentable weight pursuant to MPEP

2103(I)(c). Each of claims 40, 41, 45 and 49 have been amended to remedy the issue, and the Examiner's remarks with respect thereto are moot. Withdrawal of this rejection is therefore requested.

REJECTIONS UNDER 35 U.S.C. § 101

Claims 21-49 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Applicant respectfully traverses the rejection. The rejection of claims 21-49 under 35 U.S.C. §101 is improper and should be withdrawn.

As set forth by the USPTO in both the *2014 Interim Guidance on Patent Subject Matter Eligibility* and in the *July 2015 Update: Subject Matter Eligibility* (the "July 2015 Update") and as reiterated in the *May 2016 Update: Memorandum - Formulating a Subject Matter Eligibility Rejection and Evaluating the Applicant's Response to a Subject Matter Eligibility Rejection* (the "May 2016 Memo") "[w]hen the examiner has determined the claim recites an abstract idea, the rejection should identify the abstract idea as it is recited (i.e., set forth or described) in the claim, ***and explain why it corresponds to a concept that the courts have identified as an abstract idea***. Citing to an appropriate court decision that supports the identification of the subject matter recited in the claim language as an abstract idea is a best practice that will advance prosecution. Examiners should be familiar with any cited decision relied upon in making or maintaining a rejection to ensure that the rejection is reasonably tied to the facts of the case and to avoid relying upon language taken out of context. ***Examiners should not go beyond those concepts that are similar to what the courts have identified as abstract ideas***." (Emphasis added.)

The USPTO also instructs Examiners in the May 2016 Memo that "when an examiner determines that a claim is directed to an abstract idea . . . the rejection should identify the abstract idea ***as it is recited (i.e., set forth or described) in the claim***." (Emphasis added.) In the *May 2016 Update: Memorandum - Recent Subject Matter Eligibility Decisions (Enfish, LLC v. Microsoft Corp. and TLI Communications LLC v. A.V. Automative, LLC)* the USPTO further warns Examiners ***"against describing a claim at a high level of abstraction untethered from the language of the claim when determining the focus of the claimed invention."***

In the current application, the Examiner asserts that claims 21-49 are directed to the allegedly abstract ideas of "authenticating an identity" and "activating the electronic device." The latter limitation is not recited by any of the claims as amended, and the rejection thereof is therefore moot. The former limitation is merely a single element of a single limitation of a single independent claim, and is not exclusively representative of the complete scope of the claims. Furthermore, the alleged abstract ideas identified by the Examiner are divorced from the language of the claims as amended and overgeneralizes what is recited in independent claims 21 and 40.

Further, none of the Supreme Court and CAFC cases of *Alice*, *Classen*, and *SmartGene* identified in the Office Action are cases in which the Supreme Court or CAFC held patent claims subject matter ineligible for patentability for being directed to a concept similar to either of the alleged abstract idea of "authenticating an identity." The Examiner improperly overgeneralizes the characterization of the abstract idea identified in the cases cited above and overgeneralizes the subject matter of the claims of the present application.

The Examiner asserts that "the claim is directed towards receiving, and processing data and automating mental tasks, which is similar to Alice which dealt with receiving, processing and storing data…, Classen which dealt with automating mental tasks and SmartGene which dealt with comparing new and stored information and using rules to identify options," (Office Action, Page 5), but in making this assertion, has failed to acknowledge several claim limitations.

For example, with regards to *Alice*, the Court evaluated claims directed to "the abstract idea of intermediated settlement." *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 134 S. Ct. at 2350 (2014). The Court found that "the method claims… merely require generic computer implementation," and therefore "fail to transform [the] abstract idea into a patent-eligible invention." Id.

Accordingly, *Alice* holds that claims directed to intermediated settlements, and which require no more than a generic computer implementation, are patent-ineligible. However, the claims as presented herein are not directed to intermediated settlements and require more than a generic computer implementation. For example, claim 21 recites "[a]n electronic ID device… comprising: a biometric sensor configured to receive a biometric input." Applicant respectfully requests that, if the rejection is to be maintained, the Examiner explain exactly how "a biometric sensor," as recited by claim 21, is equivalent to a computer program which may be implemented on a generic computer.

Furthermore, with regards to *Classen*, the Court notes that "precedent has recognized that the presence of a mental step is not of itself fatal to §101 eligibility." *Classen Immunotherapies, Inc. v. Biogen Idec*, 659 F.3d at 1065 (Fed. Cir. 2011). *Classen* notes that "***claims [that] are directed to a specific, tangible application… traverse[] the coarse eligibility filter of §101***." Id. at 1066.

Accordingly, *Classen* holds that a claim including mental steps is nonetheless valid if the claim is directed to a specific, tangible application. Although one part of one limitation of one claim recites "authenticating an identity," as the Examiner has incorrectly identified as an allegedly abstract idea, the claims are directed to a specific, tangible device. For example, claims 21 and 40 are directed at least in part to "[a]n electronic ID device… comprising: a biometric sensor configured to receive a biometric input," as recited by claim 21, which is a specific, tangible application. Applicant respectfully requests that, if the rejection is to be maintained, the Examiner explain how "a biometric sensor configured to receive a biometric input" is a mental step that can be performed entirely in the human mind.

With regards to *SmartGene*, the Court held the claim at issue invalid because "[c]laim 1 does no more than call on a 'computing device,' with basic functionality for comparing stored and input data and rules, to do what doctors do routinely." *SmartGene, Inc. v. Advanced Biological Labs., SA*, 555 Fed. Appx. at 954 (Fed. Cir. 2014). The Court further held that "[t]he claim does not purport… to identify any steps beyond those which doctors routinely and consciously perform." Id. at 955.

SmartGene holds that a claim or set of claims are invalid if they fail to "identify any steps beyond those which doctors routinely and consciously perform," as discussed above. Applicant respectfully requests that the Examiner explain how "a biometric sensor configured to receive a biometric input," as recited by claim 21, is equivalent to steps which doctors routinely and consciously perform.

Again, it is the burden of the Examiner to specifically set forth the case law that corresponds to the abstract idea ***as it is recited (i.e., set forth or described) in the claim***." If the rejection is to be maintained, Applicant respectfully requests that the Examiner set forth the case law that states that "a biometric sensor configured to receive a biometric input" is directed to patent-ineligible subject matter.

In addition, the USPTO guidance in the May 2016 Memo states that "The explanation should address the additional elements both individually and as a combination when determining whether the claim as whole recites eligible subject matter. It is important to remember that a new combination of steps in a process may be patent eligible even though all the steps of the combination were individually well known and in common use before the combination was made (*Diehr*). Thus, it is particularly critical to address the combination of additional elements, because while individually-viewed elements may not appear to add significantly more, those additional elements when viewed in combination may amount to significantly more than the exception by meaningfully limiting the judicial exception." *See also Bascom Global Internet Services, Inc., v. AT&T Mobility LLC*, No. 2015-1763 (Fed. Cir. June 27, 2016) (holding that an analysis of a claim for subject matter eligibility under §101 requires consideration of the claim elements as an ordered combination, not analysis of each claim element individually: "[t]he inventive concept inquiry requires more than recognizing that each claim element, by itself, was known in the art. As is the case here, an inventive concept can be found in the non-conventional and non-generic arrangement of known, conventional pieces.")

The Examiner has not addressed each separate claim element of the claims of the present application and certainly hasn't addressed the combination of the recited elements. The Examiner merely states the claims are directed to authenticating an identity and activating an electronic device, neither of which appear verbatim in claim 21. This approach to analysis of the claims ignores (overgeneralizes) the recited elements of the claims of the present application and is improper in light of the USPTO guidance and legal precedent holding that the claim elements must be considered as an ordered combination, not individually.

The USPTO guidance in the May 2016 Memo states that a claim should not be rejected under 35 U.S.C §101 if the claim elements, either individually or as an ordered combination recite something more than what is "well-understood, routine and conventional" and that "when the examiner has concluded that certain claim elements recite well-understood, routine, conventional activities in the relevant field of art, the rejection should explain why the courts have recognized, or those in the field would recognize, the additional elements when taken both individually and as a combination to be well-understood, routine, conventional activities." The test for what is "well-understood, routine and conventional" is more strict that the test for novelty or obviousness. As clarified by the USPTO in the May 2016 Memo:

> [L]ack of novelty (i.e., finding the element in the prior art) does not necessarily show that an element is well-understood, routine, conventional activity previously engaged in by those in the relevant field. For example, even if a particular laboratory technique was discussed in several widely-read scientific journals or used by a few scientists, mere knowledge of the particular laboratory technique or use of the particular laboratory technique by a few scientists is not sufficient to make the use of the particular laboratory technique routine or conventional in the relevant field. Instead, the evaluation turns on whether the use of the particular laboratory technique was well-understood, routine, conventional activity previously engaged in by scientists in the field. If it is determined that the additional element ***is widely prevalent and its combination with any other additional elements is well-understood, routine, conventional activity***, the examiner should provide a reasoned explanation that supports that conclusion. (Emphasis Added.)

The rule that claims should not be rejected under §101 if they recite non-conventional methods or if they recite a specific method for achieving a result rather than the result itself was re-emphasized by the CAFC in the recent decision in *McRO Inc. v. Bandai Namco Games America* (Appeal No. 2015-1080, September 13, 2016). The CAFC further held in *McRO* that "[w]hile the result may not be tangible, there is nothing that requires a method "be tied to a machine or transform an article" to be patentable. *Bilski*, 561 U.S. at 603 (discussing 35 U.S.C. § 100(b)). The concern underlying the exceptions to § 101 is not tangibility, but preemption. *Mayo*, 132 S. Ct. at 1301." Finding the claims at issue to be limited to a specific process that does not preempt alternative rule-based approaches using different structures or techniques, the court therefore held that the claims are not directed to ineligible subject matter. The *McRO* decision re-emphasizes that so long as the scope of a claimed method does not preempt all other methods to achieve the same result, the claimed method should be eligible for patentability under §101.

The Examiner has not provided any "reasoned explanation that supports" that the ordered combination of elements in the claims of the present application constitute no more than a recitation of well-understood, routine, and conventional activities or "why the courts have recognized, or those in the field would recognize, the additional elements when taken both individually and as a combination to be well-understood, routine, conventional activities." The Examiner has not provided any reasoning or evidence showing that the claims are directed to a result itself rather than a specific device or method of achieving a result. Nor has the Examiner provided any reasoning or evidence showing that the claims of the present application would preempt all applications of the alleged abstract idea. For the reasons discussed below, each of the claims of the present application is both novel and non-obvious over the prior art. It is not logical that the claims are novel and non-obvious yet recite no more than "well-understood, routine, and conventional activities" and that they broadly preempt any methods of "showing content in others shopping carts."

The dependent claims of the present application recite further technical implementation details that render these claims subject-matter eligible either on their own or as part of the ordered combination of the elements of independent claims 21 and 40. An analysis under 35 U.S.C. §101 must proceed claim-by-claim, yet the Examiner addresses all claims of the application as a group in a general, conclusory way, and engages in no analysis of the dependent claims. *See* 2014 Guidance Quick Reference Sheet, at 1 (instructing that one must "consider each claim separately based on the particular elements recited therein – claims do not automatically rise or fall with similar claims in an application." (emphasis in original)).

Each of the dependent claims adds additional technical features and is entitled to review as an ordered combination of elements— "because even if an element does not amount to significantly more on its own (e.g., because it is merely a generic computer component performing generic computer functions) it can still amount to significantly more when considered in combination with the other elements of the claim." (July 2015 Update, p. 2.) "This instruction is vital to ensuring the eligibility of many claims." *Id.* The Examiner appears to be of the opinion that the claims recite no more than computer code which can be executed on a generic computer system. However, the claims are directed to significantly more than the concepts enumerated by the Examiner at least because, amongst other reasons, a generic computer system is not analogous to "[a]n electronic [ID] device… comprising: a biometric sensor configured to receive a biometric input provided by a user," as recited, in part, by claim 21. Conversely, claim 21 recites specific structural limitations that fundamentally distinguish claim 21 from the claims found to be directed to ineligible subject matter in each of the preceding cases cited by the Examiner.

The Examiner has therefore failed to make a *prima facie* showing that any of the dependent claims are subject-matter ineligible, and the rejection of these claims, in addition to that of independent claims 21 and 40 under 35 U.S.C. § 101 should be withdrawn.

REJECTIONS UNDER 35 U.S.C. § 112

Claims 21-49 are rejected under 35 U.S. C. 112(a) or 35 U.S.C. 112 (pre-AIA), first paragraph, as failing to comply with the written description requirement. Without acceding to the correctness of these rejections, Applicant has amended the claims to address these rejections and to further the prosecution of the application.

Claims 21-49 are rejected under 35 U.S. C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention. Without acceding to the correctness of these rejections, Applicant has amended the claims to address these rejections and to further the prosecution of the application.

With regards to claim 40, the Examiner alleges that "…the electronic ID device was provided either biometric input or secret information," (Office Action, Page 13, Lines 2-3). Applicant traverses this rejection. Claim 40 recites, as amended, "authenticating an identity of the user to the electronic ID device based on at least one of biometric data received by the electronic ID device from the user and secret information known to the user and provided to the electronic ID device." Thus claim 40 recites that the ID device **authenticates** a user based on at least one of biometric data and secret information, not that the electronic ID device only **receives** one or the other. Applicant requests withdrawal of this rejection or respectfully requests that the Examiner indicate specifically what element of claim 40 stipulates that "the electronic ID device was ***provided either*** biometric input or secret information," as alleged in the Office Action.

REJECTIONS UNDER 35 U.S.C. § 103

Claims 21-49 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Gullman et al (5,280,527) ("Gullman"), and further in view of Maritzen et al. (2002/0184500) ("Maritzen"). Without acceding to the correctness of the rejection, Applicant has amended the claims to further the prosecution of the application.

Gullman discloses that, "[c]ommon security mechanisms include use of a personal identification number (PIN)… A problem with [PINs] and tokens is that the legitimate user must remember the number or password. For users having many numbers or passwords, the task of remembering can be burdensome… Accordingly, there is a need for an improved security mechanism enabling convenient use," (Column 1, Lines 28-55).

Maritzen discloses "[a] system and method for providing a secure transaction and authentication system through a gaming console," (Abstract). Maritzen further discloses, "[t]he use of the biometric pad 625 allows for authentication of the consumer's identity through a convenient and unobtrusive source. In another embodiment, the consumer may also be requested to enter a PIN through the control pad 630 to further authenticate the identity of the consumer," (Paragraph [0070]).

The Examiner admits that "Gullman does not teach including secret information known to the user," and relies on Maritzen to cure the deficiencies of Gullman (Office Action, Pages 14-15). Specifically, the Examiner alleges that "Maritzen teaches including secret information known to the user (¶ 57, 70, 77)," (Office Action, Page 15). Maritzen is generally directed, in each of the indicated sections, to embodiments wherein "the consumer may also be requested to enter a PIN through the control pad 630 to further authenticate the identity of the consumer," (Paragraph [0070]).

As a threshold matter, the Examiner's proposed combination of Gullman and Maritzen is improper. Gullman explicitly indicates that "the task of remembering [PINs] can be burdensome," and is in fact teaches away from the use of PINs (Gullman, Column 1, Lines 28-55) and thus teaches away from the asserted combination of references. It is unclear why or how one would combine Gullman, the inventive features of which are directed to alleviating the deficiencies of PINs, with Maritzen, which indicates the implementation of PINs (Maritzen, Paragraph [0070]). Accordingly, the asserted combination is improper and should be withdrawn.

Even assuming, *arguendo*, that the combination is proper, which it is not, the combination still fails to teach or suggest at least some of the elements of claim 21. Claim 21, as amended, recites in part, "[a]n electronic ID device… comprising… a user interface configured to receive… information ***indicative of a secure operation to be executed***."

Gullman is directed to "[a] security apparatus [that] receives a biometric input from a user, which then is compared to a template to determine a correlation factor. The correlation factor, a fixed code and either a time-varying code or a challenge code then are combined to generate a token. The token is displayed to the user, who then enters the token at an access device," (Abstract).

Maritzen, as discussed above, discloses that "the consumer may also be requested to enter a PIN… to further authenticate the identity of the consumer," (Paragraph [0070]).

Gullman and Maritzen, whether taken alone or in combination, fail to teach or suggest at least some of the elements of claim 21. Gullman discloses the receipt of a biometric input and the generation of a token using the biometric input and a plurality of other parameters, none of which are "information indicative of a secure operation to be executed." Similarly, Maritzen discloses receiving a PIN for authenticating the consumer, but fails to disclose "receiv[ing]… information indicative of a secure operation to be executed," as recited by claim 21. Accordingly, Gullman and Maritzen, whether taken alone or in combination, fail to teach or suggest at least some of the elements of independent claim 21.

In light of the foregoing, claim 21 is believed to be in allowable condition. Independent claim 40 recites similar limitations, and is allowable for similar reasons. Claims 22-39 and 41-49 depend from claims 21 and 40, respectively, and are allowable for at least the same reasons. Accordingly, withdrawal of the rejection of claims 21-49 under 35 U.S.C. §103 is respectfully requested.

CONCLUSION

In view of the foregoing amendments and remarks, reconsideration is respectfully requested. This application should now be in condition for allowance; a notice to this effect is respectfully requested. If the Examiner believes, after this amendment, that the application is not in condition for allowance, the Examiner is requested to call the Applicants' attorney at the telephone number listed below.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicants hereby request any necessary extension of time. If there is a fee occasioned by this response, including an extension fee that is not covered by an accompanying payment, please charge any deficiency to Deposit Account No. 50/2762, Ref. No. W0537-701321.

Dated: November 30th, 2016

Respectfully submitted,

Electronic signature: /John N. Anastasi/
John N. Anastasi
Registration No.: 37,765
LANDO & ANASTASI, LLP
Riverfront Office Park
One Main Street, Suite 1100
Cambridge, Massachusetts 02142
(617) 395-7000

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted via the Office electronic filing system in accordance with 37 CFR § 1.6(a)(4).

Dated: November 30, 2016
Electronic Signature for John N. Anastasi: /John N. Anastasi/

Docket No.: W0537-701321
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Kenneth P. Weiss

Application No.: 14/071,126 Confirmation No.: 3814

Filed: November 4, 2013 Art Unit: 3685

For: UNIVERSAL SECURE REGISTRY Examiner: I. I. Immanuel

INFORMATION DISCLOSURE STATEMENT (IDS)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Pursuant to 37 C.F.R. § 1.56, 1.97 and 1.98, the attention of the United States Patent and Trademark Office is hereby directed to the references listed on the attached PTO/SB/08. It is respectfully requested that the information be expressly considered during the prosecution of the above-identified application, and that the references be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

This Information Disclosure Statement is filed more than three months after the filing date of this application, OR more than three months after the date of entry of the national stage in the international application, AND after the mailing date of a first Office Action on the merits, but before the mailing date of any of a Final Action under 37 C.F.R.§ 1.113, a Notice of Allowance under 37 C.F.R. § 1.311 or an action that otherwise closes prosecution in this application (37 C.F.R. § 1.97(c)).

In accordance with 37 C.F.R. § 1.98(a)(2)(ii), copies of the U.S. patent and U.S. patent application publications are not submitted.

In accordance with 37 C.F.R. § 1.97(g), the filing of this Information Disclosure Statement shall not be construed as a representation that a search has been made. In accordance with 37 C.F.R. § 1.97(h), the filing of this Information Disclosure Statement shall not be construed to be an admission that the information cited in this Information Disclosure Statement is, or is considered to be, material to the patentability as defined in 37 C.F.R. § 1.56(b).

It is submitted that the Information Disclosure Statement is in compliance with 37 C.F.R. § 1.98, and the Examiner is respectfully requested to consider the listed references.

Please charge our Deposit Account No. 50/2762 in the amount of $90.00 covering the fee set forth in 37 C.F.R. § 1.17(p). The Director is hereby authorized to charge any deficiency in the fees filed, asserted to be filed or which should have been filed herewith to our Deposit Account No. 50/2762, under Order No. W0537-701321.

Dated: November 30, 2016

Respectfully submitted,

Electronic signature: /John N. Anastasi/
John N. Anastasi
Registration No.: 37,765
LANDO & ANASTASI, LLP
Riverfront Office Park
One Main Street, Suite 1100
Cambridge, Massachusetts 02142
(617) 395-7000

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(**Not for submission under 37 CFR 1.99)**

Application Number	14071126
Filing Date	2013-11-04
First Named Inventor	Kenneth P. Weiss
Art Unit	3685
Examiner Name	I. I. Immanuel
Attorney Docket Number	W0537-701321

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code1	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6678821		2004-01-13	Waugh et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code1	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20030061171	A1	2003-03-27	Gilbert et al.	
	2	20040019564	A1	2004-01-29	Goldthwaite et al.	
	3	20040083170	A1	2004-04-29	Bam et al.	
	4	20040230536	A1	2004-11-18	Fung et al.	
	5	20050035847	A1	2005-02-17	Bonalle et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number		14071126
Filing Date		2013-11-04
First Named Inventor	Kenneth P. Weiss	
Art Unit		3685
Examiner Name	I. I. Immanuel	
Attorney Docket Number		W0537-701321

	6	20060180660	A1	2006-08-17	Gray	
	7	20060191995	A1	2006-08-31	Stewart et al.	
	8	20100241570	A1	2010-09-23	Keresman, III et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	14071126
	Filing Date	2013-11-04
	First Named Inventor	Kenneth P. Weiss
	Art Unit	3685
	Examiner Name	I. I. Immanuel
	Attorney Docket Number	W0537-701321

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14071126
Filing Date	2013-11-04
First Named Inventor	Kenneth P. Weiss
Art Unit	3685
Examiner Name	I. I. Immanuel
Attorney Docket Number	W0537-701321

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

□ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/John N. Anastasi/	Date (YYYY-MM-DD)	2016-11-30
Name/Print	John N. Anastasi	Registration Number	37,765

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1 hour 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.**

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 record s.

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.

Electronic Patent Application Fee Transmittal

Application Number:	14071126
Filing Date:	04-Nov-2013
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Filer:	John N Anastasi/Benjamin Binder
Attorney Docket Number:	W0537-701321

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
SUBMISSION- INFORMATION DISCLOSURE STMT	2806	1	90	90
		Total in USD ($)		**90**

Electronic Acknowledgement Receipt

EFS ID:	27647615
Application Number:	14071126
International Application Number:	
Confirmation Number:	3814
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Customer Number:	37462
Filer:	John N Anastasi
Filer Authorized By:	
Attorney Docket Number:	W0537-701321
Receipt Date:	30-NOV-2016
Filing Date:	04-NOV-2013
Time Stamp:	12:33:41
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$90
RAM confirmation Number	113016INTEFSW00010994502762
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		Response_to_NFOA_mailed_8-31-16.pdf	130476 9cedc573e13e9fb76dc90a704bb3b299340bcce5	yes	18

Multipart Description/PDF files in .zip description

Document Description	Start	End
Amendment/Req. Reconsideration-After Non-Final Reject	1	1
Claims	2	7
Applicant Arguments/Remarks Made in an Amendment	8	18

Warnings:

Information:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
2	Transmittal Letter	Information_Disclosure_Statement_IDS.pdf	26422 53d3740a2e7063090ead0444422936638e3e59c1	no	2

Warnings:

Information:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
3	Information Disclosure Statement (IDS) Form (SB08)	Information_Disclosure_Statement_Fillable_PDF.pdf	1035267 348faa32baeaf6df814483abd1e233069a5e8b0c	no	5

Warnings:

Information:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
4	Fee Worksheet (SB06)	fee-info.pdf	30583 3eeb94299ad88c95b54fac386dd26b6fac70ddda	no	2

Warnings:

Information:

Total Files Size (in bytes): 1222748

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 14/071,126	Filing Date 11/04/2013	□ To be Mailed

ENTITY: □ LARGE ☒ SMALL □ MICRO

APPLICATION AS FILED – PART I

FOR	NUMBER FILED (Column 1)	NUMBER EXTRA (Column 2)	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

AMENDMENT	11/30/2016	CLAIMS REMAINING AFTER AMENDMENT (Column 1)		HIGHEST NUMBER PREVIOUSLY PAID FOR (Column 2)	PRESENT EXTRA (Column 3)	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 29	Minus	** 29	= 0	x $40 =	0
	Independent (37 CFR 1.16(h))	* 2	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**

AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT (Column 1)		HIGHEST NUMBER PREVIOUSLY PAID FOR (Column 2)	PRESENT EXTRA (Column 3)	RATE ($)	ADDITIONAL FEE ($)
	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.

LIE
ANNETTE COWAN

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 NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/071,126	11/04/2013	Kenneth P. Weiss	W0537-701321	3814

37462 7590 04/06/2017
LANDO & ANASTASI, LLP
ONE MAIN STREET, SUITE 1100
CAMBRIDGE, MA 02142

EXAMINER	
IMMANUEL, ISIDORA I	

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
04/06/2017	ELECTRONIC

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

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

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@LALaw.com
CKent@LALaw.com

Office Action Summary	**Application No.** 14/071,126	**Applicant(s)** WEISS, KENNETH P.	
	Examiner ISIDORA IMMANUEL	**Art Unit** 3685	**AIA (First Inventor to File) Status** No

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11/30/2016*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *21-49* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *21-49* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

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

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b)
Paper No(s)/Mail Date *11/30/2016, 02/27/2017*.

3) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

Acknowledgements

1. This office action is in response to the claims filed 11/30/2016.

2. Claims 1-20 are cancelled.

3. Claims 21, 23, 24, 27, 30-43, 45 and 49 are amendment.

4. Claims 21-49 are pending.

5. Claims 21-49 have been examined.

Notice of Pre-AIA or AIA Status

6. The present application is being examined under the pre-AIA first to invent provisions.

Response to Amendment/Arguments

7. Applicant's arguments filed 11/30/2016 have been fully considered but they are not persuasive.

8. 101

9. Applicant’s claims recite “receiving… information... authenticating an identity… generating…a non-predictable value and encrypted authentication information and ... communicating the encrypted authentication information …." First, the limitations of the method claims do not require a computer to execute them, a person can carry out the steps, for example a person can verify a user’s biometric identity, provide an unpredictable value and an encryption is a mathematical operation that can be performed by a person. Secondly, even with a computer, the computer would be

performing conventional functions of a computer such as sending, receiving, comparing and calculating information. There is no demonstration of an improvement or enhancement to the particular technological environment.

10. <u>103</u>

11. In response to applicant's argument that there is no teaching, suggestion, or motivation to combine the references, the examiner recognizes that obviousness may be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988), *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992), and *KSR International Co. v. Teleflex, Inc.*, 550 U.S. 398, 82 USPQ2d 1385 (2007). In this case, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Gullman to Maritzen. Applicant's proposed invention teaches a user device is configured to allow a user to select any one of a plurality of accounts associated with the user to employ in a financial transaction. In one embodiment, the user device includes a biometric sensor configured to receive a biometric input provided by the user, for authenticating identity or verifying the identity of individuals and other entities seeking access to certain privileges and for selectively granting privileges. Gullman teaches a security apparatus receives a biometric input from a user, if access to such system is permitted the user is allowed to perform an electronic funds transfer. Maritzen teaches that the invention allows a consumer to

utilize a game console to conduct secure transactions and authenticate the identity of the consumer using the game console. Both art utilize PINs, and Gullman does not teach away from the use of PINs as Applicant claims. Gullman says "in an exemplary embodiment of the invention, the biometric security mechanism is an integrated circuit card including a processing unit, memory and a biometric sensor. The memory stores a template of the authorized user's biometric information, along with a verification algorithm. Upon entry of the cardholder's biometric information, the processor executes the verification algorithm. The verification algorithm uses the template data, the biometric input, a fixed code (i.e., PIN, embedded serial number, account number)" and also "for a successful biometric entry or where the user is not informed of a failed biometric entry, the correlation factor is combined with a fixed code (i.e., PIN, embedded serial number, account number)" (column 2, line 48-65, column 4, line 3-11)

12. Applicant argues that the combination of Gullman and Maritzen does not teach "an electronic ID device... comprising... a user interface configured to receive... information ***indicative of a secure operation to be executed***." As explained in what Gullman and Maritzen teach and imported from their abstracts and fields of invention, Gullman's user inputs information gain to access so the user is allowed to perform an electronic funds transfer. Maritzen's secure operation to be executed is for a consumer to utilize a game console to conduct secure transactions.

Examiner's Comments

13. Regarding claim 21, with respect to claim language “sensor configured to receive...”, “interface configured to receive...”, “operation to be executed...”, “interface configured to communicate...”, “processor configured to generate… to generate … to communicate...”, claim 22, “transmitter configured to wirelessly transmit ...”, claim 23, “the system…configured to transmit… to receive … to perform...”, claim 24, “system configured to perform...”, claim 25, “interface configured to display options for purchase”, claim 26, “interface configured to accept...for purchase”, claim 27, “system configured to execute...”, “operation is further configured to manage...”, claim 29, “interface configured to initiate...”, “system configured to execute...”, claim 30, “system configured to execute...”, claim 31, “software for authentication…”, claim 33, “device to authenticate…”, claim 37, “operation that acts to modify…”, claim 38, “memory is configured to store...”, “processor is configured to generate...”, “processor to generate…”, and claims 39, 40, 46 and 49, “system configured to execute...”, recites intended use and therefore does not have patentable weight. See MPEP 2114.

14. Regarding claim 21, with respect to claim language “sensor configured to receive...”, “interface configured to receive...”, “interface configured to communicate...”, “processor configured to generate… to generate … to communicate...”, claim 22, “transmitter configured to wirelessly transmit ...”, claim 23, “the system…configured to transmit… to receive … to perform...”, claim 24, “system configured to perform...”, claim 25, “interface configured to display options for purchase”, claim 26, “interface configured to accept...for purchase”, claim 27, “system configured to execute...”, claim 29, “interface configured to initiate...”, “system configured to execute...”, claim 30, “system

configured to execute...", claim 33, "device to authenticate…", claim 38, "memory is configured to store...", "processor is configured to generate...", "processor to generate…", and claims 39, 40, 46 and 49, "system configured to execute...", recites functional language, and therefore does not have patentable weight. (In re Schreiber, 128 F.3d 1473, 1478, 44 USPQ2d 1429, 1432 (Fed. Cir. 1997).

15. Regarding claim 28, "device comprises a discrete code…", claim 32, " information including the identifying…", and claim 35, "secret information… includes a …", are nonfunctional descriptive material and therefore do not have patentable weight. See *In re Gulack*, 217 USPQ 401 (Fed. Cir. 1983), *In re Ngai,* 70 USPQ2d (Fed. Cir. 2004), *In re Lowry*, 32 USPQ2d 1031 (Fed. Cir. 1994); MPEP 2111.05. MPEP 2111.05 III.

16. Regarding claim 40, the language "data received… provided to...", and claim 49, "user initiates…" does not disclose a positively recited step and therefore does not patentable weight. See MPEP 2111.04.

17. Regarding claim 43, "entering, via the electronic ID device … if the identity…", similarly, claim 45, "a selected one..." is optional and conditional language and therefore does not have patentable weight. See MPEP 2103(I)(c).

Claim Rejections - 35 USC § 101

18. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

19. Claims 21-49 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Subject Matter Eligibility Standard

20. When considering subject matter eligibility under 35 U.S.C. 101, it must be determined whether the claim is directed to one of the four statutory categories of invention, i.e., process, machine, manufacture, or composition of matter. If the claim does fall within one of the statutory categories, it must then be determined whether the claim is directed to a judicial exception (i.e., law of nature, natural phenomenon, and abstract idea), and if so, it must additionally be determined whether the claim is a patent-eligible application of the exception. If an abstract idea is present in the claim, any element or combination of elements in the claim must be sufficient to ensure that the claim amounts to significantly more than the abstract idea itself. Examples of abstract ideas include fundamental economic practices; certain methods of organizing human activities; an idea itself; and mathematical relationships/formulas. (*Alice Corporation Pty. Ltd. v. CLS Bank International, et al. US Supreme Court, No. 13-298, June 19, 2014*).

Analysis

21. In the instant case, claim 40 is directed to a method and claim 21 is directed to a device.

22. Additionally, the claim is directed towards receiving, and processing data and automating mental tasks, in this case an electronic device is used, which is similar to Alice which dealt with receiving, processing, and storing data (*Alice Corp. Pty. Ltd. v.*

CLS Bank Int'l, 573 U.S. __, 134 S. Ct. 2347, 2356 (2014)), and Classen which dealt with automating mental tasks. Therefore, based on case law precedent, the claims are claiming subject matter similar to concepts already identified by the courts as dealing with abstract ideas. See Alice Corp. Pty. Ltd., 134 S.Ct. at 2356 (citing Bilski v. Kappos, 561, U.S. 593, 611 (2010)). Claim 21 is directed towards the generic computer used to implement the method of claim 40 and is therefore also directed towards a judicial exception regarding an abstract idea involving the receiving and processing data, based on case law precedent, is claiming subject matter similar to concepts identified by the courts as dealing with abstract ideas.

23. Taking the claim elements separately, the functions performed by the machine at each step of the process are purely conventional. Using a processor, using a device, receiving and processing data. All of these functions are well-understood, routine, conventional activities previously known to the industry. In short, each step does no more than require a generic computer to perform generic computer functions.

24. The claims do not include additional elements that are sufficient to amount to significantly more than the judicial exception because the elements of "authenticating an identity" are drawn to data comparisons in SmartGene and "activating the electronic device…" as explained by Applicant's specification (PGPub¶ 255) is "the user device **352** is activated for a transaction when the user satisfactorily completes an authentication process with the device", as the device is already in use, "activating" is drawn to the using of the device for transactions as in automation of tasks in Classen and receiving and processing data in Alice (Alice Corp. Pty. Ltd. v. CLS Bank Int'l, 573

U.S. __, 134 S. Ct. 2347, 2356 (2014)), electronic recordkeeping (Alice Corp. Pty. Ltd. v. CLS Bank Int'l, 573 U.S. __, 134 S. Ct. 2347, 2356 (2014)), automating mental tasks (Bancorp Services LLC v. Sun Life Assurance Co. of Canada (U.S.), 103 USPQ2d 1425 (Fed. Cir. 2012), (Cybersource Corp. v. Retail Decisions, Inc., 654 F.3d 1366, 1372 (Fed. Cir. 2011)) and receiving or transmitting data over a network, e.g., using the Internet to gather data (Ultramercial, Inc. v. Hulu, LLC, 772 F.3d 709, 714-15 (Fed. Cir. 2014), (buySAFE, Inc. v. Google, Inc., 765 F.3d 1350, 1355 (Fed. Cir. 2014), (Cyberfone Systems, LLC v. CNN Interactive Group, Inc., 558 Fed. Appx. 988, 993 (Fed. Cir. 2014)).

25. Viewed as a whole, instructions/method claims simply recite the concept of receiving and processing data as performed by a generic computer. The method claims do not, for example, purport to improve the functioning of the computer itself. Nor do they effect an improvement in any other technology or technical field. Instead, the claims at issue amount to nothing significantly more than an instruction to apply the abstract idea of receiving and processing data using some unspecified, generic computer. See Alice Corp. Pty. Ltd., 134 S.Ct. at 2360.

26. The use of a device implementing the abstract idea does not render the claim patent eligible because it does not provide meaningful limitations beyond generally linking the use of an abstract idea to a particular technology environment and requires no more than a generic computer to perform generic computer functions.

Conclusion

27. The claim as a whole, does not amount to significantly more than the abstract idea itself. This is because the claim does not affect an improvement to another technology or technical filed; the claim does not amount to an improvement to the functioning of a computer system itself; and the claim does not move beyond a general link of the use of an abstract idea to a particular technological environment.

28. Accordingly, the Examiner concludes that there are no meaningful limitations in the claim that transform the judicial exception into a patent eligible application such that the claim amounts to significantly more than the judicial exception itself.

29. Dependent claims do not resolve the deficiency of independent claims and accordingly stand rejected under 35 USC 101 based on the same rationale.

30. Dependent claims 22-39 and 41-49 are also rejected.

Claim Rejections - 35 USC § 112

31. The following is a quotation of the first paragraph of 35 U.S.C. 112(a):

> (a) IN GENERAL.—The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor or joint inventor of carrying out the invention.

The following is a quotation of the first paragraph of pre-AIA 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor of carrying out his invention.

32. Claims 21-49 are rejected under 35 U.S.C. 112(a) or 35 U.S.C. 112 (pre-AIA), first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor or a joint inventor, or for pre-AIA the inventor(s), at the time the application was filed, had possession of the claimed invention.

33. Claims 21 and 40 recite executing a “secure operation”. The recitation of electronic ID device and the system both executing the "secure operation" calls to question the scope of the claims, whether the claim actually encompasses the “secure operation and the claim being directed to a genus of secure operations because there is no limitation on what falls under the banner of “secure operation”. Additionally, disclosure doesn’t provide sufficient teaching to claim a genus. Dependent claims 22-39 and 41-49 are also rejected.

34. The following is a quotation of 35 U.S.C. 112(b):

> (b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

35. Claims 21-49 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

36. Regarding claim 21, the claim recites “an electronic device configured to provide encrypted authentication information to enable execution of a secure operation… the system configured to execute the secure operation.” However, claim 21 is directed to an electronic ID device of which the system is not a part of. The claim concludes, the system, not the electronic ID device, executes a secure operation. Therefore, it would be unclear whether infringement of claim 21 occurs based on possession of the device. *In re Katz Interactive Call Processing Patent Litigation*, 639 F.3d 1303 (Fed. Cir. 2011). *IPXL Holdings v. Amazon.com, Inc.*, 430 F.2d 1377, 1384, 77 USPQ2d 1140, 1145 (Fed. Cir. 2005). *Ex parte Lyell*, 17 USPQ2d 1548 (Bd. Pat. App. & Inter. 1990). Dependent claims 22-39 are also rejected.

37. Claim 21 is directed towards “an electronic device…”, dependent claims for example, Claim 34 is directed towards “an electronic device…” but recites “the electronic ID device is configured to not….” The claim recites entry of the user input is not permitted while simultaneously reciting that the biometric input has been received. It is therefore unclear as to whether the “entry” is to be viewed as the receiving of the biometric input or a different operation not present in the claim. Similarly, claim 37 recites “until the electronic ID device successfully authenticates….”, claim 39 recites “device executes a challenge..."

38. Regarding claim 30, the claim recites “wherein the user initiates, via the electronic ID device….” However, claim 21, from which claim 30 depends, is directed to an electronic ID device of which the user is not a part of. The claim is a hybrid claim as the cited language is not directed to the device but to external use of claimed structural

elements. Therefore, it would be unclear whether infringement of claim 30 occurs based on possession of the device. *In re Katz Interactive Call Processing Patent Litigation*, 639 F.3d 1303 (Fed. Cir. 2011). *IPXL Holdings v. Amazon.com, Inc.*, 430 F.2d 1377, 1384, 77 USPQ2d 1140, 1145 (Fed. Cir. 2005). *Ex parte Lyell*, 17 USPQ2d 1548 (Bd. Pat. App. & Inter. 1990).

39. Claim 34 recites "wherein the electronic ID device is configured to not permit the entry of the user input if the biometric input received…." The claim makes a distinction between an "entry of the user" and a "biometric input", but the input received in the sensor was entered by the user, it is therefore unclear where else the entry would occur; the sensor, system, interface or somewhere else.

40. Claim 37 recites "an encryption that acts to modify the data such that it is unintelligible **until** the electronic ID device successfully authenticates at least one of the biometric…." It is unclear how successful authentication would make previously unintelligible data "intelligible".

41. Claim 40 recites "at least one of biometric data received by the electronic ID device from the user and secret information known to the user and provided to the electronic ID … generating, … from information derived from at least a portion of the biometric input, and from information derived from at least a portion of the secret information" but the electronic ID device was provided either biometric input or secret information. It is unclear how the generated information now uses a portion of both sets of information. Dependent claims 41-49 are rejected.

Claim Rejections - 35 USC § 103

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

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

43. Claims 21-49 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Gullman et al (5,280,527) ("Gullman"), and further in view of Maritzen et al. (2002/0184500) ("Maritzen").

44. Regarding claims 21 and 40, Gullman teaches a biometric sensor configured to receive a biometric input provided by a user (column 4, line 39-49, column 5, line 42-54); a user interface configured to receive a user input information indicative of a secure operation to be executed (column 4, line 3-8, 39-64); a communication interface configured to communicate with a system configured to execute the secure operation (column3, line 50-55, column 4, line 13-20, 29-36, column 6, line 35-40); a processor coupled to the biometric sensor, the user interface, and the communication interface, the processor being programmed such that once the electronic ID device successful authenticates at least the biometric input or the information (column 3, line 19-55, column 4, line 3-61, column 6, line 8-20), the processor is configured to generate a non-predictable value and to generate encrypted authentication information from the non-predictable value (column 3, line 37-46, column 5, line 15-33; claim 1), from information derived from at least a portion of the biometric input, and from information derived from

at least a portion of the secret information, and to communicate the encrypted authentication information via the communication interface to the system configured to execute the secure operation (Abstract; column 4, line 29-36; column 6, line 35-61; claim 1). Gullman does not teach including secret information known to the user. Maritzen teaches including secret information known to the user (¶ 57, 70, 77). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Gullman and Maritzen in order to provide secure authentication of a user to prevent unauthorized access (Maritzen; ¶ 2-4).

45. Regarding claim 22, Maritzen teaches wherein the communication interface comprises a transmitter configured to wirelessly transmit the encrypted authentication information to the system configured to execute the secure operation (¶ 23, 27, 35, 39, 42).

46. Regarding claim 23, Maritzen teaches wherein the system is configured to transmit the encrypted authentication information to a secure registry software and to receive authorization to perform the secure operation from the secure registry software (¶ 28-31).

47. Regarding claim 24, Maritzen teaches wherein the secure operation includes a secure transaction, and wherein the system configured to perform the secure operation comprises a point-of-sale (POS) device (¶ 28, 34, 57, 61).

48. Regarding claim 25, Maritzen teaches wherein the user interface is configured to display options for purchase (¶ 18, 30, 33, 74, 81).

49. Regarding claim 26, Maritzen teaches wherein the user interface is configured to accept user selection of at least one product or service for purchase (¶ 30, 33, 69, 74, 81).

50. Regarding claim 27, Gullman teaches wherein execution of the secure operation permits access to a secure location, and the system configured to execute the secure operation is further configured to manage access to the secure location (column 4, line 29-36, column 6, line 35-45).

51. Regarding claim 28, Maritzen teaches wherein the electronic ID device comprises a discrete code associated with the electronic ID device (¶ 37).

52. Regarding claim 29, Gullman teaches wherein the user interface is configured to initiate authentication with the system configured to execute the secure operation responsive to the user manually entering a secret code (column 3, line 56-68, column 6, line 9-16).

53. Regarding claim 30, Gullman teaches wherein the user initiates, via the electronic, authentication with the system configured to execute the secure operation (column 3, line 56-64, column 6, line 9-16).

54. Regarding claim 31, Gullman teaches wherein at least a portion of the biometric input received by the biometric sensor is communicated to a secure registry software for authentication by the electronic ID device prior to generation of the encrypted authentication information (column 3, line 44-48, column 5, line 57-65).

55. Regarding claim 32, Maritzen teaches wherein the user interface is configured to receive the secret information including the identifying information (¶ 57, 61, 62, 77).

56. Regarding claim 33, Gullman teaches further comprising a memory coupled to the processor, wherein the memory stores information employed by the electronic ID device to authenticate the biometric input received by the biometric sensor (column 3, line 44-48, column 5, line 57-65).

57. Regarding claim 34, Gullman teaches wherein the electronic ID device is configured to not permit the entry of the user input if the biometric input received by the biometric sensor is determined to not belong to an authorized user of the electronic ID device (column 3, line 37-55).

58. Regarding claim 35, Gullman teaches wherein the secret information known to the user includes a Personal Identification Number (PIN), and wherein the processor is configured to generate the non-predictable value and the encrypted authentication information responsive to authentication of both the secret information and the biometric input (column 3, line 37-68, column 4, line 3-36, column 5, line 15-33; claim 1).

59. Regarding claim 36, Gullman teaches wherein data stored in the memory is unavailable to an individual in possession of the electronic ID device until the electronic ID device successfully authenticates at least one of the biometric input and the information (column 3, line 19-55, column 4, line 3-61, column 5, line 64-68, column 6, line 8-20).

60. Regarding claim 37, Maritzen teaches wherein data stored in a memory is subject to an encryption that acts to modify the data such that it is unintelligible until the electronic ID device successfully authenticates at least one of the biometric input and the information (¶ 55-57, 70, 77).

61. Regarding claim 38, Gullman teaches wherein the processor is configured to generate a seed using at least two of the electronic serial number, a discrete code associated with the electronic ID device, a Personal Identification Number (PIN), a time value, and information derived from the biometric input to generate the encrypted authentication information, and wherein the seed is employed by the processor to generate the non-predictable value (column 3, line 37-68, column 4, line 3-22). Gullman does not teach wherein the memory is configured to store an electronic code unique to the electronic ID device. Maritzen teaches wherein the memory is configured to store an electronic code unique to the electronic ID device (¶ 37). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Gullman and Maritzen in order to provide secure authentication of a user to prevent unauthorized access (Maritzen; ¶ 2-4).

62. Regarding claim 39, Gullman teaches wherein the electronic ID device executes a challenge-response protocol as part of authentication with the system configured to execute the secure operation (column 3, line 37-68, column 4, line 8-11).

63. Regarding claim 41, Maritzen teaches an act of receiving at least a portion of a user's secret information manually within a user interface (¶ 22, 57).

64. Regarding claim 42, Gullman teaches further comprising an act of displaying, on a user interface, indicators for a plurality of user accounts stored in a memory of the electronic ID device (column 5, line 57-65).

65. Regarding claim 43, Maritzen teaches further comprising an act of entering, by the electronic ID device, de-active state without generating the encrypted authentication

information if the identity of the user is not successfully authenticated to the electronic ID device (¶ 57).

66. Regarding claim 44, Gullman teaches further comprising an act of generating a seed from which the authentication information is generated by employing at least two of the biometric data, the secret information known to the user, and a discrete code unique to the electronic ID device (column 3, line 37-68, column 4, line 3-22).

67. Regarding claim 45, Gullman teaches further comprising an act of generating encrypted authentication information in a manner that allows identification of the user and a selected one of a plurality of user accounts by secure registry software (column 4, line 23-36, column 5, line 57-65).

68. Regarding claim 46, Maritzen teaches further comprising displaying options for selection of the system configured to execute the secure operation on a user interface (¶ 33, 69, 74).

69. Regarding claim 47, Gullman teaches further comprising selecting with the user interface at least one product, service, or secure operation (Abstract; column 3, line 50-55, column 4, line 59-62; claim 2, 3).

70. Regarding claim 48, Maritzen teaches further comprising maintaining an audit trail of purchases made (¶ 32, 42, 82).

71. Regarding claim 49, Gullman teaches wherein the user initiates an authentication request on the electronic ID device triggering communication of the encrypted authentication information from the electronic ID device to the system configured to execute the secure operation (column 3, line 56-68, column 4, line 50-64).

Conclusion

72. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

73. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ISIDORA IMMANUEL whose telephone number is (571)272-9862. The examiner can normally be reached on Monday-Thursday 8am-5pm EDT.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Calvin Hewitt can be reached on 571-272-6709. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/I. I./
Examiner, Art Unit 3685

/JAMES D NIGH/
Primary Examiner, Art Unit 3685

Notice of References Cited	Application/Control No. 14/071,126	Applicant(s)/Patent Under Reexamination WEISS, KENNETH P.	
	Examiner ISIDORA IMMANUEL	Art Unit 3685	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-5,280,527 A	01-1994	Gullman; Lawrence S.	G06K19/0718	713/184
*	B	US-2002/0184500 A1	12-2002	Maritzen, Michael	G06Q20/18	713/170
	C	US-				
	D	US-				
	E	US-				
	F	US-				
	G	US-				
	H	US-				
	I	US-				
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. OMB 0651-0031
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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14071126
Filing Date	2013-11-04
First Named Inventor	Kenneth P. Weiss
Art Unit	3685
Examiner Name	I. I. Immanuel
Attorney Docket Number	W0537-701321

U.S.PATENTS

Remove

Examiner Initial*	Cite No	Patent Number	Kind Code1	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS

Remove

Examiner Initial*	Cite No	Publication Number	Kind Code1	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/I.I.I./	1	20070288758		2007-12-13	WEISS	
/I.I.I./	2	20070289000		2007-12-13	WEISS	
/I.I.I./	3	20140149295		2014-05-29	Weiss	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS

Remove

Examiner Initial*	Cite No	Foreign Document Number3	Country Code2 i	Kind Code4	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T5
	1							

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	14071126
	Filing Date	2013-11-04
	First Named Inventor	Kenneth P. Weiss
	Art Unit	3685
	Examiner Name	I. I. Immanuel
	Attorney Docket Number	W0537-701321

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1		

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/ISIDORA I IMMANUEL/	Date Considered	03/19/2017

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14071126
Filing Date	2013-11-04
First Named Inventor	Kenneth P. Weiss
Art Unit	3685
Examiner Name	I. I. Immanuel
Attorney Docket Number	W0537-701321

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

□ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/John N. Anastasi/	Date (YYYY-MM-DD)	2017-02-27
Name/Print	John N. Anastasi	Registration Number	37,765

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1 hour 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.**

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 record s.

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.

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. OMB 0651-0031
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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14071126
Filing Date	2013-11-04
First Named Inventor	Kenneth P. Weiss
Art Unit	3685
Examiner Name	I. I. Immanuel
Attorney Docket Number	W0537-701321

U.S.PATENTS

Remove

Examiner Initial*	Cite No	Patent Number	Kind Code1	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/I.I.I./	1	6678821		2004-01-13	Waugh et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS

Remove

Examiner Initial*	Cite No	Publication Number	Kind Code1	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/I.I.I./	1	20030061171	A1	2003-03-27	Gilbert et al.	
/I.I.I./	2	20040019564	A1	2004-01-29	Goldthwaite et al.	
/I.I.I./	3	20040083170	A1	2004-04-29	Bam et al.	
/I.I.I./	4	20040230536	A1	2004-11-18	Fung et al.	
/I.I.I./	5	20050035847	A1	2005-02-17	Bonalle et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	14071126
	Filing Date	2013-11-04
	First Named Inventor	Kenneth P. Weiss
	Art Unit	3685
	Examiner Name	I. I. Immanuel
	Attorney Docket Number	W0537-701321

/I.I.I./	6	20060180660	A1	2006-08-17	Gray	
/I.I.I./	7	20060191995	A1	2006-08-31	Stewart et al.	
/I.I.I./	8	20100241570	A1	2010-09-23	Keresman, III et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number3	Country Code2 i	Kind Code4	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T5
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1		

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/ISIDORA I IMMANUEL/	Date Considered	03/19/2017

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**		
	Application Number	14071126
	Filing Date	2013-11-04
	First Named Inventor	Kenneth P. Weiss
	Art Unit	3685
	Examiner Name	I. I. Immanuel
	Attorney Docket Number	W0537-701321

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14071126
Filing Date	2013-11-04
First Named Inventor	Kenneth P. Weiss
Art Unit	3685
Examiner Name	I. I. Immanuel
Attorney Docket Number	W0537-701321

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

□ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/John N. Anastasi/	Date (YYYY-MM-DD)	2016-11-30
Name/Print	John N. Anastasi	Registration Number	37,765

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1 hour 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.**

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 record s.

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.

Index of Claims	**Application/Control No.** 14071126	**Applicant(s)/Patent Under Reexamination** WEISS, KENNETH P.
	Examiner ISIDORA IMMANUEL	**Art Unit** 3685

✓	**Rejected**	-	**Cancelled**	N	**Non-Elected**	A	**Appeal**
=	**Allowed**	÷	**Restricted**	I	**Interference**	O	**Objected**

□ **Claims renumbered in the same order as presented by applicant** □ **CPA** □ **T.D.** □ **R.1.47**

CLAIM		**DATE**								
Final	Original	08/22/2016	03/19/2017							
	1	-	-							
	2	-	-							
	3	-	-							
	4	-	-							
	5	-	-							
	6	-	-							
	7	-	-							
	8	-	-							
	9	-	-							
	10	-	-							
	11	-	-							
	12	-	-							
	13	-	-							
	14	-	-							
	15	-	-							
	16	-	-							
	17	-	-							
	18	-	-							
	19	-	-							
	20	-	-							
	21	✓	✓							
	22	✓	✓							
	23	✓	✓							
	24	✓	✓							
	25	✓	✓							
	26	✓	✓							
	27	✓	✓							
	28	✓	✓							
	29	✓	✓							
	30	✓	✓							
	31	✓	✓							
	32	✓	✓							
	33	✓	✓							
	34	✓	✓							
	35	✓	✓							
	36	✓	✓							

Index of Claims	**Application/Control No.** 14071126	**Applicant(s)/Patent Under Reexamination** WEISS, KENNETH P.
	Examiner ISIDORA IMMANUEL	**Art Unit** 3685

✓	**Rejected**	-	**Cancelled**	N	**Non-Elected**	A	**Appeal**
=	**Allowed**	÷	**Restricted**	I	**Interference**	O	**Objected**

□ **Claims renumbered in the same order as presented by applicant** □ **CPA** □ **T.D.** □ **R.1.47**

CLAIM		DATE								
Final	Original	08/22/2016	03/19/2017							
	37	✓	✓							
	38	✓	✓							
	39	✓	✓							
	40	✓	✓							
	41	✓	✓							
	42	✓	✓							
	43	✓	✓							
	44	✓	✓							
	45	✓	✓							
	46	✓	✓							
	47	✓	✓							
	48	✓	✓							
	49	✓	✓							

Search Notes	**Application/Control No.** 14071126	**Applicant(s)/Patent Under Reexamination** WEISS, KENNETH P.
	Examiner ISIDORA IMMANUEL	**Art Unit** 3685

CPC- SEARCHED

Symbol	Date	Examiner
G06Q	8/22/2016	II

CPC COMBINATION SETS - SEARCHED

Symbol	Date	Examiner

US CLASSIFICATION SEARCHED

Class	Subclass	Date	Examiner

SEARCH NOTES

Search Notes	Date	Examiner
See attached notes	8/22/2016	II
See attached notes	3/19/2017	II

INTERFERENCE SEARCH

US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

/I.I./ Examiner.Art Unit 3685	

Doc code: RCEX
Doc description: Request for Continued Examination (RCE)

PTO/SB/30EFS (07-14)
Approved for use through 07/31/2016. OMB 0651-0031
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.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	14071126	Filing Date	2013-11-04	Docket Number (if applicable)	W0537-701321	Art Unit	3685
First Named Inventor	Kenneth P. Weiss			Examiner Name	I. I. Immanuel		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, to any international application that does not comply with the requirements of 35 U.S.C. 371, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV.

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

□ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

- □ Consider the arguments in the Appeal Brief or Reply Brief previously filed on ____________
- □ Other ____________

☒ Enclosed

- ☒ Amendment/Reply
- □ Information Disclosure Statement (IDS)
- □ Affidavit(s)/ Declaration(s)
- □ Other ____________

MISCELLANEOUS

□ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months ____________
(Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

□ Other ____________

FEES

☒ **The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**
The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No 50/2762

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature
Applicant Signature

Signature of Registered U.S. Patent Practitioner

Signature	/John N. Anastasi/	Date (YYYY-MM-DD)	2017-07-06
Name	John N. Anastasi	Registration Number	37765

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.

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted via the Office electronic filing system in accordance with 37 CFR § 1.6(a)(4).

Dated: July 6, 2017
Electronic Signature for John N. Anastasi: /John N. Anastasi/

Docket No.: W0537-701321
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Kenneth P. Weiss

Application No.: 14/071,126 | Confirmation No.: 3814

Filed: November 4, 2013 | Art Unit: 3685

For: UNIVERSAL SECURE REGISTRY | Examiner: I. I. Immanuel

AMENDMENT AFTER FINAL ACTION UNDER 37 C.F.R. § 1.116

MS AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

INTRODUCTORY COMMENTS

In response to the Final Office Action dated April 6, 2017, please amend the above-identified U.S. patent application as follows:

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks/Arguments begin on page 8 of this paper.

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1-20 (Cancelled)

21. (Currently Amended) An electronic ID device configured to encrypt ~~provide encrypted authentication~~ information to enable execution of a secure operation, comprising:

a biometric sensor configured to receive a biometric input provided by a user;

a user interface configured to receive a user input including secret authentication information known to the user and information indicative of a secure operation to be executed;

a communication interface configured to communicate with a system configured to execute the secure operation;

a processor coupled to the biometric sensor, the user interface, and the communication interface, the processor being programmed such that [[once]] after the electronic ID device receives ~~successfully authenticates~~ at least one of the biometric input and the secret authentication information, the processor is configured to generate a non-predictable value and to encrypt ~~generate encrypted authentication information from~~ the non-predictable value, [[from]] information derived from at least a portion of the biometric input, and [[from]] information derived from at least a portion of the secret authentication information to generate encrypted authentication information, and to communicate the encrypted authentication information via the communication interface to the system configured to execute the secure operation.

22. (Previously Presented) The electronic ID device of claim 21, wherein the communication interface comprises a transmitter configured to wirelessly transmit the encrypted authentication information to the system configured to execute the secure operation.

23. (Previously Presented) The electronic ID device of claim 21, further comprising the system configured to execute the secure operation, wherein the system is configured to transmit the encrypted authentication information to a secure registry software and to receive authorization to perform the secure operation from the secure registry software.

24. (Previously Presented) The electronic ID device of claim 21, further comprising the system configured to execute the secure operation, wherein the secure operation includes a secure transaction, and wherein the system configured to perform the secure operation comprises a point-of-sale (POS) device.

25. (Previously Presented) The electronic ID device of claim 24, wherein the user interface is configured to display options for purchase.

26. (Previously Presented) The electronic ID device of claim 24, wherein the user interface is configured to accept user selection of at least one product or service for purchase.

27. (Previously Presented) The electronic ID device of claim 21, further comprising the system configured to execute the secure operation, wherein execution of the secure operation permits access to a secure location, and the system configured to execute the secure operation is further configured to manage access to the secure location.

28. (Previously Presented) The electronic ID device of claim 21, wherein the electronic ID device comprises a discrete code associated with the electronic ID device.

29. (Previously Presented) The electronic ID device of claim 21, wherein the user interface is configured to initiate authentication with the system configured to execute the secure operation responsive to the user manually entering a secret code.

30. (Currently Amended) The electronic ID device of claim 21, wherein the ~~user initiates, via the~~ electronic ID device[[,]] initiates, responsive to receiving an authentication

initiation input from the user, authentication with the system configured to execute the secure operation.

31. (Previously Presented) The electronic ID device of claim 21, wherein at least a portion of the biometric input received by the biometric sensor is communicated to a secure registry software for authentication by the electronic ID device prior to generation of the encrypted authentication information.

32. (Currently Amended) The electronic ID device of claim 21, wherein the user interface is configured to receive the secret authentication information including [[the]] identifying information.

33. (Previously Presented) The electronic ID device of claim 21, further comprising a memory coupled to the processor, wherein the memory stores information employed by the electronic ID device to authenticate the biometric input received by the biometric sensor.

34. (Currently Amended) The electronic ID device of claim [[31]] 33, wherein the electronic ID device is configured to not permit the entry of the user input if the biometric input received by the biometric sensor is determined to not belong to an authorized user of the electronic ID device.

35. (Currently Amended) The electronic ID device of claim 32, wherein the secret authentication information known to the user includes a Personal Identification Number (PIN), and wherein the processor is configured to generate the non-predictable value and the encrypted authentication information responsive to authentication of both the secret authentication information and the biometric input.

36. (Currently Amended) The electronic ID device of claim 32, wherein data stored in a memory is unavailable to an individual in possession of the electronic ID device until the electronic ID device successfully authenticates at least one of the biometric input and the secret authentication information.

37. (Currently Amended) The electronic ID device of claim 34, wherein data stored in a memory is subject to encryption that acts to modify the data such that it is unintelligible until the data is subjected to decryption that acts to modify the data such that it is intelligible responsive to the electronic ID device successfully authenticating ~~authenticates~~ at least one of the biometric input and the secret authentication information.

38. (Previously Presented) The electronic ID device of claim 33, wherein the memory is configured to store an electronic code unique to the electronic ID device, wherein the processor is configured to generate a seed using at least two of the electronic serial number, a discrete code associated with the electronic ID device, a Personal Identification Number (PIN), a time value, and information derived from the biometric input to generate the encrypted authentication information, and wherein the seed is employed by the processor to generate the non-predictable value.

39. (Previously Presented) The electronic ID device of claim 21, wherein the electronic ID device executes a challenge-response protocol as part of authentication with the system configured to execute the secure operation.

40. (Currently Amended) A method of controlling execution of a secure operation, the method comprising acts of:

receiving, from a user by an electronic ID device, information indicative of the secure operation to be executed;

receiving, by the electronic ID device from the user, biometric data and secret authentication information known to the user;

authenticating an identity of the user to the electronic ID device based on at least one of the biometric data received by the electronic ID device from the user and the secret authentication information known to the user and provided to the electronic ID device; and

subsequent ~~responsive~~ to successful authentication of the identity of the user to the electronic ID device:

generating, with the electronic ID device, a non-predictable value;

encrypting, by ~~generating, with~~ the electronic ID device, ~~encrypted authentication information from~~ the non-predictable value, [[from]] information derived from at least a portion of the biometric input, and [[from]] information derived from at least a portion of the secret authentication information to generate encrypted authentication information; and

communicating the encrypted authentication information from the electronic ID device to a system configured to execute the secure operation.

41. (Currently Amended) The method of claim 40, further comprising an act of receiving at least a portion of a user's secret authentication information manually within a user interface.

42. (Previously Presented) The method of claim 40, further comprising an act of displaying, on a user interface, indicators for a plurality of user accounts stored in a memory of the electronic ID device.

43. (Previously Presented) The method of claim 40, further comprising an act of entering, by the electronic ID device, a de-active state without generating the encrypted authentication information if the identity of the user is not successfully authenticated to the electronic ID device.

44. (Currently Amended) The method of claim 40, further comprising an act of generating a seed from which the encrypted authentication information is generated by employing at least two of the biometric data, the secret authentication information known to the user, and a discrete code unique to the electronic ID device.

45. (Previously Presented) The method of claim 40, further comprising an act of generating encrypted authentication information in a manner that allows identification of the user and a selected one of a plurality of user accounts by secure registry software.

46. (Previously Presented) The method of claim 40, further comprising displaying options for selection of the system configured to execute the secure operation on a user interface.

47. (Previously Presented) The method of claim 46, further comprising selecting with the user interface at least one product, service, or secure operation.

48. (Previously Presented) The method of claim 46, further comprising maintaining an audit trail of purchases made.

49. (Previously Presented) The method of claim 40, wherein the user initiates an authentication request on the electronic ID device triggering communication of the encrypted authentication information from the electronic ID device to the system configured to execute the secure operation.

REMARKS

In response to the Final Office Action mailed April 6, 2017, Applicant respectfully requests reconsideration in view of the amendments and the following remarks. Claims 21-49 were previously pending in this application. By this amendment, Applicant is not adding or canceling any claims. Claims 21, 30, 32, 34-37, 40, 41, and 44 have been amended. As a result claims 21-49 are pending for examination with claims 21 and 40 being independent claims. No new matter has been added.

Applicant's Comments

The Examiner has made assertions pertaining to the patentable weight of the claims which were already addressed in Applicant's previous response. The Examiner has not acknowledged any of Applicant's comments made in Applicant's most recent response and therefore this Office Action has not met the obligations of the Examiner. Accordingly, Applicant disagrees with the Examiner's assertions for all of the reasons already presented in the most recent response, which have not been addressed, and submits the following additional remarks with respect to the Examiner's Comments.

The Examiner's current comments with respect to MPEP 2114 differ from the Examiner's previous comments with respect to MPEP 2114 in that the Examiner asserts "[r]egarding claim 21, with respect to claim language… 'processor configured to generate'… recites intended use and therefore does not have patentable weight," (Office Action, Page 5). The language provided by the Examiner is not recited in claim 21, and the Examiner's assertions are therefore moot. To the extent that the Examiner's assertions apply to language recited by claim 21, Applicant refers to the comments made in the most recent Office Action response which were not addressed by the Examiner.

The Examiner further alleges that "[r]egarding claim 43, 'entering, via the electronic ID device… if the identity…', similarly, claim 45, 'a selected one…' is optional and conditional language and therefore does not have patentable weight. See MPEP 2103(I)(c)," (Office Action, Page 6). Claim 43 does not recite "entering, via the electronic ID device… if the identity…" and the Examiner's assertions are therefore moot. To the extent that the Examiner's assertions apply to language recited by claim 43, Applicant notes that MPEP 2103(I)(c) does not mention the patentable weight of "conditional" language. MPEP 2103(I)(c) refers to language which is purely optional, but says nothing about conditional language. Applicant requests that, if the Examiner's assertions are to be maintained, the Examiner point out with specificity where MPEP 2103(I)(c) mentions the patentable weight of conditional language.

With respect to the Examiner's allegations pertaining to claim 45, "a selected one" is not conditional or optional language. Notwithstanding the fact that MPEP 2103(I)(c) does not apply to conditional language, Applicant requests that, if the Examiner's assertions are to be maintained, the Examiner explain how "a selected one" is either conditional or optional language.

Rejections Under 35 U.S.C. § 101

Claims 21-49 stand rejected under 35 U.S.C. § 101 because the claimed invention is allegedly directed to non-statutory subject matter. Without acceding to the correctness of the rejection, Applicant has amended the claims to further the prosecution of the application. The claims as currently presented are directed to statutory subject matter, are in condition for allowance, and withdrawal of the rejection of claims 21-49 under 35 U.S.C. §101 is therefore respectfully requested.

The Examiner has repeated many of the same arguments from the most recent rejection, some of which refer to claim language which was previously deleted and no longer appears in any of the claims. The Applicant has already addressed all of the Examiner's arguments in the most recent response. However, the Examiner has not acknowledged most of Applicant's arguments presented in the most recent response. The Examiner has failed to address the Applicants prior response and this Office Action, per se, does not meet the obligation of the Examiner. Accordingly, Applicant maintains that the Examiner cannot choose to ignore and not address the Applicant's prior response, that the rejection under 35 U.S.C. §101 is still improper for at least for the reasons previously presented but not acknowledged in the most recent response and submits the following additional remarks.

As set forth by the USPTO in the *May 2016 Update: Memorandum – Formulating a Subject Matter Eligibility Rejection and Evaluating the Applicant's Response to a Subject Matter Eligibility Rejection* (the "May 2016 Memo") Examiners are advised that "the rejection should identify the abstract idea ***as it is recited (i.e., set forth or described)*** in the claim." (Emphasis added.) In the *May 2016 Update: Memorandum – Recent Subject Matter Eligibility*

Decisions (Enfish, LLC v. Microsoft Corp. and TLI Communications LLC v. A.V. Automotive, LLC) the USPTO further advises Examiners "***against describing a claim at a high level of abstraction untethered from the language of the claim when determining the focus of the claimed invention.***" (Emphasis added.) "The explanation should address the additional elements both individually and as a combination when determining whether the claim as a whole recites eligible subject matter."

Nonetheless, the Examiner has described the claims at a high level of abstraction untethered from the language of the claims. For example, the Examiner invents language not recited by any claim in asserting that "the limitations of the method claims do not require a computer to execute them, a person can carry out the steps, for example a person can verify a user's biometric entity," (Office Action, Page 3; Emphasis added).

Applicant notes that "verify[ing] a user's biometric entity" is the Examiner's overly-abstract fabrication and does not appear in any claim previously or currently presented. Claim 21 recites, in part, "**a biometric sensor configured to receive a biometric input provided by a user**," and "**encrypt[ing] the non-predictable value**, **information derived from at least a portion of the biometric input**, **and information derived from at least a portion of the secret authentication information to generate encrypted authentication information**." The Examiner's characterization of the foregoing limitations as "verify[ing] a user's biometric entity" is the "high level of abstraction untethered from the language of the claim" that the May 2016 Memo is directed to eradicating.

Applicant once again notes that the limitations of claim 21 **cannot be performed entirely in the human mind**. Holding a claim ineligible despite the impossibility of performing the claim entirely in the human mind is inconsistent with *SmartGene*, cited by the Examiner, which held that "[t]his conclusion [of claim 1's ineligibility] follows from *CyberSource Corp. v. Retail Decisions, Inc.,* where, based on earlier precedents, this court held that section 101 did not embrace a process **defined simply as using a computer to perform a series of mental steps that people, aware of each step, can and regularly do perform in their heads**," (*SmartGene*, Pages 7-8).

The Examiner has re-characterized the limitations of claim 21 into an overly-abstract form bearing no resemblance to the actual language of the claim so that the fabricated language can be performed in the human mind. This **directly contravenes the explicit guidelines** of the

May 2016 Memo. Accordingly, Applicant requests that the Examiner withdraw the rejection or provide relevant authority supporting the position that the foregoing recited limitations of claim 21 – not "verifying a user's biometric identity," which is not recited by any claim – are patent-ineligible.

In addition, the Examiner again misrepresents the claims at a high level of abstraction in asserting that "[t]aking the claim elements separately, the functions performed by the machine at each step of the process are purely conventional. Using a processor, using a device, receiving and processing data. All of these functions are well-understood, routine, conventional activities previously known to the industry," (Office Action, Page 8; Emphasis added). The language used by the Examiner is again a high level of abstraction not tethered to the actual claim language and is not recited by any claim, and the Examiner has not provided any reasoning to explain how the claims can be reduced to no more than using a processor, using a device, and receiving and processing data.

The Examiner has simply attempted to describe the combination of the claim elements at an extremely high level of abstraction by fabricating language that is untethered from the claim language, and then attempts to make a broad assertion about this fabricated language – which does not actually appear in the claim and which has no authoritative support – in direct contravention to the guidelines of the May 2016 Memo. Applicant requests that the Examiner comply with the obligations of the guidelines and explain how the claims recite no more than "[u]sing a processor, using a device, [and] receiving and processing data," and how such a characterization is not an highly-abstract over-generalization advised against by the May 2016 Memo.

In the Examiner's rejection of the individual claim elements, the Examiner asserts that "'activating the electronic device'… is drawn to the using of the device for transactions as in automation of tasks in Classen and receiving and processing data in Alice," (Office Action, Page 8). Applicant notes that the language referenced by the Examiner is not recited in any claim. The Examiner appears to be repeating arguments from the most recent Office Action without acknowledging that the recited language was deleted in the most recent Office Action response. Accordingly, Applicant requests that the Examiner's arguments be withdrawn because they do not apply to any of the claims under examination.

The Examiner also asserts that "the elements of 'authenticating an identity' are drawn to data comparisons in SmartGene," (Office Action, Page 8), the subject matter of which is directed to selection of a therapeutic treatment regimen for a patient with a known disease or medical condition. Applicant is unaware of any holding in *SmartGene* which held all claims involving "data comparisons" patent-ineligible, and the Examiner has not provided any citation to support this assertion. Not only does *SmartGene* not make this statement, *SmartGene* explicitly specified that "[o]ur ruling is **limited to the circumstances presented here**, in which **every step** is a familiar part of the conscious process that **doctors can and do perform in their heads**," (*SmartGene,* Page 9). The Examiner's overly-broad reading of *SmartGene* to render all claims including "data comparisons" – even those outside the bounds established by *SmartGene* – is inconsistent with and unsupported by the clear and explicit language of *SmartGene*.

Even if *SmartGene* had provided such a broad and universally-applicable holding – which it did not – Applicant respectfully disagrees with the Examiner's characterization of "authenticating an identity" as being "drawn to data comparisons," on the grounds that the characterization is an overly-broad abstraction advised against by the May 2016 Memo. The Examiner has not provided any reasoning to support the contention that these disparate concepts are analogous to one another. Applicant requests that the Examiner comply with the published USPTO guidelines, and that if the characterization is to be maintained by the Examiner, the Examiner provide reasoning as to how "authenticating an identity" is drawn to "data comparisons."

The Examiner only identifies a single element of a single claim limitation abstracted at a high level – specifically "authenticating an identity" – in the rejection of the individual elements of the claims, not including the previously-deleted claim limitation that the Examiner erroneously asserts was recited by claim 21, yet has failed to identify any relevant court decision in support of the rejection. Furthermore, claim 21 is not limited nor fully characterized by the only claim language identified by the Examiner. Claim 21 contains additional limitations containing subject matter that courts have found patent-eligible, including "generat[ing] encrypted authentication information" as recited by amended claim 21.

For example, the Court in Paone v. Broadcom Corp. held that "it would require an overly broad view of the Supreme Court's § 101 jurisprudence to find that a patent directed at a method of encryption does not claim eligible subject matter *per se*, as long as it is specific enough… [I]n

TQP, Judge Bryson ***rejected the notion that the claimed encryption method was a 'mental process' ineligible under [Gottschalk]***, because 'the invention involves a several-step manipulation of data that, except perhaps in its most simplistic form, ***could not conceivably be performed in the human mind or with pencil and paper***." Paone v. Broadcom Corp., 2015 U.S. Dist. LEXIS 109725 (2015), citing TQP Dev., LLC v. Intuit Inc., 2014 U.S. Dist. LEXIS 20077 (2014).

The Court in TQP noted that "[t]ypically, transforming data from one form to another does not qualify as the kind of transformation that the Supreme Court in Bilski regarded as an important indicator of patent eligibility… ***In the case of an invention in the field of encryption, however, the entire object of the invention is to transform data from one form into another*** that will be recognizable by the intended recipient but secure against decryption by unintended recipients. In that setting***, it does not make sense to say that the transformation of data from one form to another cannot qualify as a patent-eligible invention, because that is what the field of cryptology is all about***." TQP Dev., LLC v. Intuit Inc., 2014 U.S. Dist. LEXIS 20077 (2014).

In view of the foregoing, it is apparent that the Examiner's assertion that the claims merely recite using a processor, using a device, and receiving and processing data or are "drawn to data comparisons" is an overly-abstract, high-level generalization unsupported by relevant precedent. Decisions pertinent to the field of encryption cited herein make clear that it is inappropriate to hold claims involving encryption subject matter-ineligible *per se*. The rejection should be withdrawn in view of these holdings.

Moreover, the Examiner's allegation that the claims "do [not] effect an improvement in any other technology or technical field," (Office Action, Page 9) is plainly false and is not supported by any argument or authority. Claim 21, which recites, in part, "encrypt[ing] information to enable execution of a secure operation," provides improvement at least to the technical fields of encryption and executing secure operations.

Despite the foregoing deficiencies discussed with respect to the Examiner's assertions, and without acceding to the correctness of the rejection, Applicant has amended claim 21 to recite, in part, "[a]n electronic IDentification (ID) device configured to encrypt information… comprising… [a] processor being programmed… to encrypt the non-predictable value, information derived from at least a portion of the biometric input, and information derived from at least a portion of the secret authentication information to generate encrypted authentication information, and to communicate the encrypted authentication information… to execute the secure operation."

Claim 21 as amended is in condition for allowance for the reasons discussed herein. Claim 40 recites similar limitations, and is allowable for similar reasons. Claims 22-39 and 41-49 depend from claims 21 and 40, respectively, and are allowable for at least the same reasons. Accordingly, withdrawal of the rejection of claims 21-49 under 35 U.S.C. §101 is respectfully requested.

Rejections Under 35 U.S.C. § 112

Claims 21-49 are rejected under 35 U.S.C. § 112 as allegedly failing to comply with the written description requirement and for allegedly being indefinite for failing to particularly point out and distinctly claim the subject matter regarded as the invention. Without acceding to the correctness of these rejections, Applicant has amended the claims to address these rejections and to further the prosecution of the application.

Claims 21-39 are rejected under 35 U.S.C. § 112 because "the claim recites 'an electronic device configured to provide encrypted authentication information to enable execution of a secure operation… the system configured to execute the secure operation.' However, claim 21 is directed to an electronic ID device of which the system is not a part of. The claim concludes, the system, not the electronic ID device, executes a secure operation. Therefore, it would be unclear whether infringement of claim 21 occurs based on possession of the device," (Office Action, Page 12).

Applicant notes that the language used by the Examiner is not an accurate quotation of the limitations of previously-presented claim 21, and the rejection is therefore moot. Additionally, the above-recited limitations of claim 21 have been amended, and the rejection thereof is therefore moot.

To the extent that the rejection applies to the amended claim language, Applicant notes that the claim is clear as written. Claim 21 is directed to an electronic ID device that generates and communicates encrypted authentication information to a system that is configured to execute a secure operation. The system is not positively recited in the claim. Therefore, the limitations of claim 21 reciting, in part, "[a]n electronic ID device configured to encrypt information to enable execution of a secure operation," and "a system configured to execute the secure operation" are consistent with one another.

The Office Action recites that "[c]laim 21 is directed towards 'an electronic device…', dependent claims for example, Claim 34 is directed towards 'an electronic device…' but recites 'the electronic ID device is configured to not…' The claim recites entry of the user input is not permitted while simultaneously reciting that the biometric input has been received. It is therefore unclear as to whether the 'entry' is to be viewed as the receiving of the biometric input or a different operation not present in the claim. Similarly, claim 37 recites 'until the electronic ID device successfully authenticates…', claim 39 recites 'device executes a challenge…'," (Office Action, Page 12).

Applicant notes that the language used by the Examiner is not an accurate quotation of the limitations of previously-presented claim 21, and the Examiner's comments are therefore moot. To the extent that the Examiner's comments apply to the limitations of the claims, Applicant notes that each claim introduces an additional feature of the electronic device and should be examined accordingly.

Claim 37 recites an additional aspect of the device that is subject to the electronic ID device successfully authenticating at least one of the biometric input and the secret authentication information, and claim 39 recites additional challenge response features. Both are consistent with claim 21 and definite.

The Office Action recites that "[c]laim 34 recites 'wherein the electronic ID device is configured to not permit the entry of the user input if the biometric input received…' The claim makes a distinction between an 'entry of the user' and a 'biometric input', but the input received in the sensor was entered by the user, it is therefore unclear where else the entry would occur; the sensor, system, interface or somewhere else," (Office Action, Page 13).

Applicant notes that it is unclear what the Examiner is attempting to convey and what the Examiner finds objectionable. To the extent that the Applicant has attempted to construe the Examiner's comments, Applicant notes that the claims are clear and accurate as written. For example, claim 21 recites, in part, "[a]n electronic ID device… comprising[] a biometric sensor configured to receive a biometric input…[and] a user interface configured to receive a user input." Claim 34 recites a feature of not permitting entry of a user input if the biometric input received by the biometric sensor is determined to not belong to an authorized user. Claim 34 still allows for receipt of a biometric input, but prevents a user input of further information if the biometric input is not authorized.

Claims 41-49 are rejected under 35 U.S.C. § 112 because "[c]laim 40 recites 'at least one of biometric data received by the electronic ID device from the user and secret information known to the user and provided to the electronic ID… generating, … from information derived from at least a portion of the biometric input, and from information derived from at least a portion of the secret information' but the electronic ID device was provided either biometric input or secret information. It is unclear how the generated information now uses a portion of both sets of information. Dependent claims 41-49 are rejected," (Office Action, Page 13).

Claim 40 has been amended and no longer recites the limitations identified by the Examiner, and the rejection of claim 40 is therefore moot. To the extent that the rejection applies to amended claim 40, Applicant has already explained to the Examiner in the most recent Office Action response that the allegation that "the electronic ID device was provided either biometric input or secret information" is neither accurate nor recited anywhere in the claims. As the Examiner has not acknowledged Applicant's explanation pertaining to the above, Applicant again refers the Examiner to the most recent Office Action response.

Rejections Under 35 U.S.C. § 103

Claims 21-49 are rejected under pre-AIA 35 U.S.C. § 103(a) as being unpatentable over Gullman et al (5,280,527) ("Gullman"), and further in view of Maritzen et al. (2002/0184500) ("Maritzen"). Without acceding to the correctness of the rejection, Applicant has amended the claims to further the prosecution of the application.

Claim 21 recites, in part, "a user interface configured to receive a user input including secret authentication information known to the user and information indicative of a secure operation to be executed."

Gullman discloses that, "[c]ommon security mechanisms include use of a personal identification number (PIN)… A problem with [PINs] and tokens is that the legitimate user must remember the number or password. For users having many numbers or passwords, the task of remembering can be burdensome… Accordingly, there is a need for an improved security mechanism enabling convenient use," (Column 1, Lines 28-55).

Maritzen discloses "[a] system and method for providing a secure transaction and authentication system through a gaming console," (Abstract). Maritzen further discloses, "the **consumer may also be requested to enter a PIN** through the control pad 630 to further authenticate the identity of the consumer," (Paragraph [0070]).

The Examiner asserts that "[r]egarding claims 21 and 40, Gullman teaches… a user interface configured to receive a user input information [*sic*] indicative of a secure operation to be executed (column 4, line 3-8, 39-64)," (Office Action, Page 14).

The Examiner has omitted limitations of claim 21 in the rejection thereof, and it is therefore unclear what limitations the Examiner believes are taught by Gullman and which the Examiner believes are not. For the purposes of this response, Applicant has interpreted the Examiner's statements to be an admission that Gullman does not teach "a user interface configured to receive a user input including secret authentication information known to the user," as recited in part by claim 21, and an assertion that Gullman teaches or suggests "a user interface configured to receive a user input including… information indicative of a secure operation to be executed," as recited in part by claim 21.

Nonetheless, Gullman also fails to teach or suggest a user interface configured to receive a user input including information indicative of a secure operation to be executed. The Examiner has not pointed out with particularity how or where Gullman teaches such a "user interface," and indeed, Applicant has not identified any teaching or suggestion of such a "user interface" by Gullman.

To the extent that Applicant has attempted to interpret the Examiner's comments, it is assumed for the purposes of this response that the Examiner believes that the security apparatus 14 of Gullman includes a user interface configured to receive information indicative of a secure operation to be executed. However, the security apparatus 14 does not include any such user interface and does not receive any such information.

The security apparatus 14 receives a biometric – which is not itself information indicative of a secure operation to be executed – sensed by a biometric sensor, which is not a user interface. The security apparatus 14 is completely agnostic of any operation to be executed because it does not receive information indicative of the operation to be executed, and is completely ignorant of what operation is executed using the token. The apparatus 14 generates a token based on a received biometric, but the biometric does not provide any indication of what secure operation is executed. Accordingly, Gullman fails to teach or suggest "a user interface configured to receive a user input including… information indicative of a secure operation to be executed," as recited, in part, by claim 21.

Moreover, Applicant previously noted that the Examiner's proposed combination of Gullman and Maritzen is improper and should be withdrawn. Applicant maintains the position that the Examiner's proposed combination of Gullman and Maritzen is improper and should be withdrawn. Accordingly, claim 21 is also in allowable condition because the Examiner admits that Gullman fails to teach "a user interface configured to receive a user input including secret authentication information known to the user," as recited in part by claim 21, and Maritzen cannot be combined with Gullman and therefore fails to cure this deficiency.

Gullman explicitly indicates that "the task of remembering [PINs] can be burdensome," and in fact teaches away from ***requesting*** **PINs from users** (Gullman, Column 1, Lines 28-55) and thus teaches away from the asserted combination of references. As recited above, Gullman discusses the deficiencies of requesting PINs from a user to give background as to why an alleged necessity exists for an authentication system that obviates the need to request PINs from a user. It is therefore unclear why or how one would combine Gullman, the inventive features of which are directed to alleviating the deficiencies of users remembering PINs and requesting those PINs from users, with Maritzen, which indicates that PINs are requested from users who are forced to remember and provide the PINs (Maritzen, Paragraph [0070]).

The Examiner correctly points out that Gullman recites "[t]he verification algorithm uses the template data, the biometric input**, a fixed code (i.e., PIN, embedded serial number, account number)**," (Office Action, Page 4; Emphasis added). However, although Gullman recites the **use** of PINs, Gullman **does not recite receiving or requesting a PIN from a user**. The "fixed code" of Gullman is known to the "verification algorithm" **without requesting it from the user**, i.e., it is stored in a memory accessible to the verification algorithm without requesting the PIN from the user. For example, Gullman notes that "[e]ach security apparatus 14 comes with an embedded 'fixed' code stored in PROM 24. Such fixed code is used to form a token…" (Column 4, Lines 58-60). Requesting a PIN from the user would directly contravene Gullman's statement that "remembering [PINs] can be burdensome."

In view of the foregoing, the combination of Gullman, which teaches **directly away** from **requesting** a PIN from a user, with Maritzen, which discloses that a PIN is **requested** from a user, is improper and should be withdrawn. Accordingly, the asserted combination fails to teach or suggest "a user interface **configured to *receive* a user input including secret authentication information *known* to the user**," as recited in part by claim 21, and should be withdrawn.

The rejection of claim 40 is improper for similar reasons and should similarly be withdrawn. Claims 22-39 and 41-49 depend from claims 21 and 40, respectively, and are allowable for at least the same reasons. Accordingly, withdrawal of the rejection of claims 21-49 under 35 U.S.C. §103 is respectfully requested.

CONCLUSION

In view of the foregoing amendments and remarks, reconsideration is respectfully requested. This application should now be in condition for allowance; a notice to this effect is respectfully requested. If the Examiner believes, after this amendment, that the application is not in condition for allowance, the Examiner is requested to call the Applicant's attorney at the telephone number listed below.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicant hereby requests any necessary extension of time. If there is a fee occasioned by this response, including an extension fee that is not covered by an accompanying payment, please charge any deficiency to Deposit Account No. 50/2762; Our Ref. W0537-701321.

Dated: July 6, 2017

Respectfully submitted,

Electronic signature: /John N. Anastasi/
John N. Anastasi
Registration No.: 37,765
LANDO & ANASTASI, LLP
Riverfront Office Park
One Main Street, Suite 1100
Cambridge, Massachusetts 02142
(617) 395-7000

Electronic Patent Application Fee Transmittal

Application Number:	14071126
Filing Date:	04-Nov-2013
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Filer:	John N Anastasi/Alexandra Gerard
Attorney Docket Number:	W0537-701321

Filed as Small Entity

Filing Fees for **Utility under 35 USC 111(a)**

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
RCE- 1st Request	2801	1	600	600
	Total in USD ($)			**600**

Electronic Acknowledgement Receipt

EFS ID:	29707232
Application Number:	14071126
International Application Number:	
Confirmation Number:	3814
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Customer Number:	37462
Filer:	John N Anastasi
Filer Authorized By:	
Attorney Docket Number:	W0537-701321
Receipt Date:	06-JUL-2017
Filing Date:	04-NOV-2013
Time Stamp:	19:01:27
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$600
RAM confirmation Number	070717INTEFSW00005685502762
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	Request for Continued Examination (RCE)	Request_for_Continued_Examination_Fillable_PDF.pdf	1350348 ae48f9139bde9d2da9be60b388473be4190bc4c2	no	3
Warnings:					
Information:					
2		Response_to_Final_Office_Action_mailed_4-6-17.pdf	130699 8089b4ea6dddcca11452e7269c446c4060309986	yes	20

Multipart Description/PDF files in .zip description

Document Description	Start	End
Response After Final Action	1	1
Claims	2	7
Applicant Arguments/Remarks Made in an Amendment	8	20

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30226 04d4569424d8b4ceb8f41e23c85758b2f7bad993	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	1511273	

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.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/071,126	Filing Date 11/04/2013	□ 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)		
AMENDMENT	07/06/2017	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 29	Minus	** 29	= 0	x $40 =	0
	Independent (37 CFR 1.16(h))	* 2	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)		
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	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.

LIE
MARGARET BYARS

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.

Search Notes	**Application/Control No.** 14/071,126	**Applicant(s)/Patent Under Reexamination** Weiss, Kenneth P.
	Examiner ISIDORA I IMMANUEL	**Art Unit** 3685

CPC - Searched*

Symbol	Date	Examiner
G06Q	8/22/2016	II

CPC Combination Sets - Searched*

Symbol	Date	Examiner

US Classification - Searched*

Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes

Search Notes	Date	Examiner
See attached notes	8/22/2016	II
See attached notes	3/19/2017	II

Interference Search

US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

	/I.I./ Examiner.Art Unit 3685

Index of Claims	**Application/Control No.** 14/071,126	**Applicant(s)/Patent Under Reexamination** Weiss, Kenneth P.
	Examiner ISIDORA I IMMANUEL	**Art Unit** 3685

✓	**Rejected**	**-**	**Cancelled**	**N**	**Non-Elected**	**A**	**Appeal**
=	**Allowed**	**÷**	**Restricted**	**I**	**Interference**	**O**	**Objected**

CLAIMS

□ Claims renumbered in the same order as presented by applicant □ CPA □ T.D. □ R.1.47

CLAIM		**DATE**							
Final	Original	08/21/2016	03/18/2017	08/07/2017	09/05/2017				
	1	-	-	-	-				
	2	-	-	-	-				
	3	-	-	-	-				
	4	-	-	-	-				
	5	-	-	-	-				
	6	-	-	-	-				
	7	-	-	-	-				
	8	-	-	-	-				
	9	-	-	-	-				
	10	-	-	-	-				
	11	-	-	-	-				
	12	-	-	-	-				
	13	-	-	-	-				
	14	-	-	-	-				
	15	-	-	-	-				
	16	-	-	-	-				
	17	-	-	-	-				
	18	-	-	-	-				
	19	-	-	-	-				
	20	-	-	-	-				
	21	✓	✓	✓	✓				
	22	✓	✓	✓	✓				
	23	✓	✓	✓	✓				
	24	✓	✓	✓	✓				
	25	✓	✓	✓	✓				
	26	✓	✓	✓	✓				
	27	✓	✓	✓	✓				
	28	✓	✓	✓	✓				
	29	✓	✓	✓	✓				
	30	✓	✓	✓	✓				
	31	✓	✓	✓	✓				
	32	✓	✓	✓	✓				
	33	✓	✓	✓	✓				
	34	✓	✓	✓	✓				
	35	✓	✓	✓	✓				
	36	✓	✓	✓	✓				
	37	✓	✓	✓	✓				
	38	✓	✓	✓	✓				
	39	✓	✓	✓	✓				
	40	✓	✓	✓	✓				
	41	✓	✓	✓	✓				
	42	✓	✓	✓	✓				

Index of Claims

Application/Control No. 14/071,126	**Applicant(s)/Patent Under Reexamination** Weiss, Kenneth P.
Examiner ISIDORA I IMMANUEL	**Art Unit** 3685

CLAIM		**DATE**								
Final	Original	08/21/2016	03/18/2017	08/07/2017	09/05/2017					
	43	✓	✓	✓	✓					
	44	✓	✓	✓	✓					
	45	✓	✓	✓	✓					
	46	✓	✓	✓	✓					
	47	✓	✓	✓	✓					
	48	✓	✓	✓	✓					
	49	✓	✓	✓	✓					

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/071,126	11/04/2013	Kenneth P. Weiss	W0537-701321	3814

37462 7590 09/15/2017
LANDO & ANASTASI, LLP
ONE MAIN STREET, SUITE 1100
CAMBRIDGE, MA 02142

EXAMINER	
IMMANUEL, ISIDORA I	

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
09/15/2017	ELECTRONIC

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

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

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@LALaw.com
CKent@LALaw.com

Office Action Summary	**Application No.** 14/071,126	**Applicant(s)** Weiss, Kenneth P.	
	Examiner ISIDORA I IMMANUEL	**Art Unit** 3685	**AIA Status** No

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 07/06/2017 .

□ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____ .

2a)□ This action is **FINAL.** 2b) ☑ This action is non-final.

3)□ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☑ Claim(s) 21-49 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)□ Claim(s) _____ is/are allowed.

7)☑ Claim(s) 21-49 is/are rejected.

8)□ Claim(s) _____ is/are objected to.

9)□ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)□ The specification is objected to by the Examiner.

11)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)□ All b)□ Some** c)□ None of the:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____ .

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

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

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)

2) □ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b)
Paper No(s)/Mail Date _____ .

3) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____ .

4) □ Other: _____ .

DETAILED ACTION

Acknowledgements

1. This office action is in response to the claims filed 07/06/2017.

2. Claims 1-20 are cancelled.

3. Claims 21, 30, 32, 34-37, 40, 41 and 44 are amendment.

4. Claims 21-49 are pending.

5. Claims 21-49 have been examined.

Notice of Pre-AIA or AIA Status

6. The present application is being examined under the pre-AIA first to invent provisions.

Continued Examination Under 37 CFR 1.114

7. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 07/06/2017 has been entered.

Response to Amendment/Arguments

8. Applicant's arguments filed 07/06/2017 have been fully considered but they are not persuasive.

9. 101

10. Applicant's claims recite "receiving… information... receiving…biometric data…authenticating an identity… generating…a non-predictable value and encrypted authentication information and ... communicating the encrypted authentication information …." First, the limitations of the method claims do not require a computer to execute them, a person can carry out the steps, for example a person can verify a user's biometric identity, provide an unpredictable value and an encryption is a mathematical operation that can be performed by a person. Secondly, even with a computer, the computer would be performing conventional functions of a computer such as sending, receiving, comparing and calculating information. Applicant is of the opinion that a biometric authentication cannot be done by "a human mind", but facial or voice recognition are just some examples of biometric authentications performed daily by the "human mind". There is no demonstration of an improvement or enhancement to the particular technological environment.

11. 112

12. Applicant makes the argument "the language used by the Examiner is not an accurate quotation of the limitations of previously-presented claim [], and the rejection is therefore moot." Applicant does not explain what language is not an "accurate

quotation." Applicant does not address a lot of the rejections and concludes the claims to be "clear and accurate as written."

13. "When examining computer-implemented functional claims, examiners should determine whether the specification discloses the computer and the algorithm (e.g., the necessary steps and/or flowcharts) that perform the claimed function in sufficient detail such that one of ordinary skill in the art can reasonably conclude that the inventor invented the claimed subject matter". See MPEP 2161.01. There is no disclosed "system", in the electronic device that is configured to enact the multiple acts claimed by the limitations, the specification also provides no support for a definition of a "secure operation", examples of the claimed secure operation nor does it mention a words "secure operation".

14. Applicant actually makes an argument that "it is unclear what the Examiner is attempting to convey... the claims are clear and accurate as written." To address this argument the rejection has been expanded upon.

15. Claim 21 is directed towards "an electronic device…", dependent claims for example, Claim 34 is directed towards "an electronic device…" but recites "the electronic ID device is configured to not…." The claim recites "the entry of the user input" is not permitted while simultaneously reciting that the biometric input has been received. The only "entry of the user input" made was a secret authentication information, "the entry of the user input" alludes to a past entry. It is therefore unclear as to whether the "entry" is to be viewed as the receiving of the biometric input or a different operation not present in the claim or there is a mistake and Applicant failed to

allude to a future entry of the user input. The claims are unclear and not accurate because as written "the entry of the user input" alludes to a past entry. The Applicant has consistently differentiated between biometric input and user input and the phrase "the entry of the user input" alludes to one specific use. Clarification is needed. The limitation remains unclear, the rejection stands.

16. 103

17. In response to applicant's argument that there is no teaching, suggestion, or motivation to combine the references, the examiner recognizes that obviousness may be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988), *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992), and *KSR International Co. v. Teleflex, Inc.*, 550 U.S. 398, 82 USPQ2d 1385 (2007). In this case, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Gullman to Maritzen. Applicant's proposed invention teaches a user device is configured to allow a user to select any one of a plurality of accounts associated with the user to employ in a financial transaction. In one embodiment, the user device includes a biometric sensor configured to receive a biometric input provided by the user, for authenticating identity or verifying the identity of individuals and other entities seeking access to certain privileges and for selectively granting privileges. Gullman teaches a security apparatus receives a biometric input

from a user, if access to such system is permitted the user is allowed to perform an electronic funds transfer. Maritzen teaches that the invention allows a consumer to utilize a game console to conduct secure transactions and authenticate the identity of the consumer using the game console. Both art utilize PINs, and Gullman does not teach away from the use of PINs as Applicant claims. Gullman says “in an exemplary embodiment of the invention, the biometric security mechanism is an integrated circuit card including a processing unit, memory and a biometric sensor. The memory stores a template of the authorized user's biometric information, along with a verification algorithm. Upon entry of the cardholder's biometric information, the processor executes the verification algorithm. The verification algorithm uses the template data, the biometric input, a fixed code (i.e., PIN, embedded serial number, account number)" and also "for a successful biometric entry or where the user is not informed of a failed biometric entry, the correlation factor is combined with a fixed code (i.e., PIN, embedded serial number, account number)" (column 2, line 48-65, column 4, line 3-11). Applicant also argues that Gullman does not recite “receiving or requesting a PIN from a user….” This argued limitation is not within the entered claims for this particular application. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

18. Applicant repeatedly makes the argument “Examiner has omitted limitations” but there are no limitations not found within the rejections nor does Applicant actually show where or what limitations are missing. Applicant again argues that the combination of

Gullman and Maritzen does not teach “a user interface….” As explained in what Gullman and Maritzen teach and imported from their abstracts and fields of invention, Gullman's user, inputs information gain to access so the user is allowed to perform an electronic funds transfer. Specifically, Gullman says “the biometric security mechanism 14 generates a security token which the user inputs to the access device 12,” (Figure 1; column 4, line 1-20). Gullman explicitly says the user inputs the information to the access device. Maritzen’s secure operation to be executed is for a consumer to utilize a game console to conduct secure transactions. Maritzen also teaches a user interface (¶ 28) saying “A variety of user interfaces may be used. In one embodiment, and input device may be incorporated on the transaction device. Alternately, a supplemental 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 point-of-sale terminals including a personal point-of-sale terminal.”

Examiner’s Comments

19. Regarding claim 21, with respect to claim language “sensor configured to receive...”, “interface configured to receive...”, “interface configured to communicate...”, “processor configured to generate… to encrypt … to communicate...”, claim 22, “transmitter configured to wirelessly transmit ...”, claim 23, “the system…configured to transmit… to receive … to perform...”, claim 24, “system configured to perform...”, claim 25, “interface configured to display options for purchase”, claim 26, “interface configured to accept...for purchase”, claim 27, “system configured to execute...”, “operation is

further configured to manage...", claim 29, "interface configured to initiate...", "system configured to execute...", claim 30, "system configured to execute...", claim 31, "software for authentication…", claim 33, "device to authenticate…", claim 37, "operation that acts to modify…", claim 38, "memory is configured to store...", "processor is configured to generate...", "processor to generate…", and claim 39, "system configured to execute...", recites intended use and therefore does not have patentable weight. See MPEP 2114.

20. Regarding claim 21, the language "programmed such that…", claim 37, "the data such that…" is a result and therefore has not patentable weight (*Minton v. Nat'l Ass'n of Securities Dealers, Inc.,* 336 F.3d 1373, 1381, 67 USPQ2d 1614, 1620 (Fed. Cir. 2003)) that a "'whereby clause in a method claim is not given weight when it simply expresses the intended result of a process step positively recited.'" See MPEP 2111.04.

21. Regarding claim 35, "information… includes a …", are nonfunctional descriptive material and therefore do not have patentable weight. See *In re Gulack*, 217 USPQ 401 (Fed. Cir. 1983), *In re Ngai,* 70 USPQ2d (Fed. Cir. 2004), *In re Lowry*, 32 USPQ2d 1031 (Fed. Cir. 1994); MPEP 2111.05 III.

22. Regarding claim 40, the language "provided to...", and claim 49, "user initiates…" does not disclose a positively recited step and therefore does not patentable weight. See MPEP 2111.04.

23. Regarding claim 43, "entering, via the electronic ID device … if the identity…", similarly, claim 45, "a selected one..." is optional and conditional language and therefore does not have patentable weight. See MPEP 2103(I)(c).

Claim Rejections - 35 USC § 101

24. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

25. Claims 21-49 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Subject Matter Eligibility Standard

26. When considering subject matter eligibility under 35 U.S.C. 101, it must be determined whether the claim is directed to one of the four statutory categories of invention, i.e., process, machine, manufacture, or composition of matter. If the claim does fall within one of the statutory categories, it must then be determined whether the claim is directed to a judicial exception (i.e., law of nature, natural phenomenon, and abstract idea), and if so, it must additionally be determined whether the claim is a patent-eligible application of the exception. If an abstract idea is present in the claim, any element or combination of elements in the claim must be sufficient to ensure that the claim amounts to significantly more than the abstract idea itself. Examples of abstract ideas include fundamental economic practices; certain methods of organizing human activities; an idea itself; and mathematical relationships/formulas. (*Alice Corporation Pty. Ltd. v. CLS Bank International, et al. US Supreme Court, No. 13-298, June 19, 2014*).

Analysis

27. In the instant case, claim 40 is directed to a method and claim 21 is directed to a device.

28. The claim recites “receiving… information... receiving…biometric data…authenticating an identity… generating…a non-predictable value and encrypted authentication information and ... communicating the encrypted authentication information …." Additionally, the claim is directed towards receiving, and processing data and automating mental tasks, in this case an electronic device is used, which is similar to Alice which dealt with receiving, processing, and storing data (*Alice Corp. Pty. Ltd. v. CLS Bank Int’l*, 573 U.S. __, 134 S. Ct. 2347, 2356 (2014)), and Classen which dealt with automating mental tasks. Therefore, based on case law precedent, the claims are claiming subject matter similar to concepts already identified by the courts as dealing with abstract ideas. See Alice Corp. Pty. Ltd., 134 S.Ct. at 2356 (citing Bilski v. Kappos, 561, U.S. 593, 611 (2010)). Claim 21 is directed towards the generic computer used to implement the method of claim 40 and is therefore also directed towards a judicial exception regarding an abstract idea involving the receiving and processing data, based on case law precedent, is claiming subject matter similar to concepts identified by the courts as dealing with abstract ideas.

29. Taking the claim elements separately, the functions performed by the machine at each step of the process are purely conventional. Using a processor, using a device, receiving and processing data. All of these functions are well-understood, routine, conventional activities previously known to the industry. In short, each step does no more than require a generic computer to perform generic computer functions.

30. The claims do not include additional elements that are sufficient to amount to significantly more than the judicial exception because the elements of “authenticating an identity” are drawn to data comparisons in SmartGene and “activating the electronic device…” as explained by Applicant’s specification (PGPub¶ 255) is “the user device **352** is activated for a transaction when the user satisfactorily completes an authentication process with the device”, as the device is already in use, “activating” is drawn to the using of the device for transactions as in automation of tasks in Classen and receiving and processing data in Alice (Alice Corp. Pty. Ltd. v. CLS Bank Int’l, 573 U.S. __, 134 S. Ct. 2347, 2356 (2014)), electronic recordkeeping (Alice Corp. Pty. Ltd. v. CLS Bank Int’l, 573 U.S. __, 134 S. Ct. 2347, 2356 (2014)), automating mental tasks (Bancorp Services LLC v. Sun Life Assurance Co. of Canada (U.S.), 103 USPQ2d 1425 (Fed. Cir. 2012), (Cybersource Corp. v. Retail Decisions, Inc., 654 F.3d 1366, 1372 (Fed. Cir. 2011)) and receiving or transmitting data over a network, e.g., using the Internet to gather data (Ultramercial, Inc. v. Hulu, LLC, 772 F.3d 709, 714-15 (Fed. Cir. 2014), (buySAFE, Inc. v. Google, Inc., 765 F.3d 1350, 1355 (Fed. Cir. 2014), (Cyberfone Systems, LLC v. CNN Interactive Group, Inc., 558 Fed. Appx. 988, 993 (Fed. Cir. 2014)).

31. Viewed as a whole, instructions/method claims simply recite the concept of receiving and processing data as performed by a generic computer. The method claims do not, for example, purport to improve the functioning of the computer itself. Nor do they effect an improvement in any other technology or technical field. Instead, the claims at issue amount to nothing significantly more than an instruction to apply the

abstract idea of receiving and processing data using some unspecified, generic computer. See Alice Corp. Pty. Ltd., 134 S.Ct. at 2360.

32. The use of a device implementing the abstract idea does not render the claim patent eligible because it does not provide meaningful limitations beyond generally linking the use of an abstract idea to a particular technology environment and requires no more than a generic computer to perform generic computer functions.

Conclusion

33. The claim as a whole, does not amount to significantly more than the abstract idea itself. This is because the claim does not affect an improvement to another technology or technical filed; the claim does not amount to an improvement to the functioning of a computer system itself; and the claim does not move beyond a general link of the use of an abstract idea to a particular technological environment.

34. Accordingly, the Examiner concludes that there are no meaningful limitations in the claim that transform the judicial exception into a patent eligible application such that the claim amounts to significantly more than the judicial exception itself.

35. Dependent claims do not resolve the deficiency of independent claims and accordingly stand rejected under 35 USC 101 based on the same rationale.

36. Dependent claims 22-39 and 41-49 are also rejected.

Claim Rejections - 35 USC § 112

37. The following is a quotation of the first paragraph of 35 U.S.C. 112(a):

> (a) IN GENERAL.—The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it

> is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor or joint inventor of carrying out the invention.

The following is a quotation of the first paragraph of pre-AIA 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor of carrying out his invention.

38. Claims 21-49 are rejected under 35 U.S.C. 112(a) or 35 U.S.C. 112 (pre-AIA), first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor or a joint inventor, or for pre-AIA the inventor(s), at the time the application was filed, had possession of the claimed invention.

39. Claim 21 recites "the processor being programmed such that after the electronic ID device receives… the processor is configured to generate…" The language "such that" makes the claim broader in scope than the teachings of the disclosure as it does not limit the claim to the programming described in the disclosure but only requires that it reproduce a result via any and all means. Dependent claims 22-39 are also rejected.

40. Claims 21 and 40 recite "a system configured to execute the secure operation..." claim 23 recites "the system is configured to transmit the encrypted authentication information…." The specification (¶ 275, 276) states "the user device includes a communication link configured to communicate with a secure registry, and a processor coupled to the biometric sensor to receive information concerning the biometric input, the user interface, and the communication link. According to one embodiment, the

processor is configured to generate a non-predictable value and to generate encrypted authentication information from the non-predictable value, the identifying information, and at least one of the information concerning the biometric input and the secret information, and to communicate the encrypted authentication information via the communication link to the secure registry… the communication link wirelessly transmits the encrypted authentication information to a point-of-sale (POS) device, and the POS device is configured to transmit at least a portion of the encrypted authentication information to the secure registry. First the specification does not provide support for a “system” but a “communication link.” The specification also does not have a written description of what constitutes a “secure operation”. The specification also gives an example of a processor being the entity to “to communicate the encrypted authentication information via the communication link to the secure registry.” The language “execute a secure operation” is broad enough in scope to encompass operations not taught by the written disclosure and is overly broad as it is directed towards a genus where the written disclosure does not provide sufficient teachings to support the claiming of a genus and should be rejected under 112 (a) under MPEP § 2163 (II)(A)(3)(a)(ii). “When examining computer-implemented functional claims, examiners should determine whether the specification discloses the computer and the algorithm (e.g., the necessary steps and/or flowcharts) that perform the claimed function in sufficient detail such that one of ordinary skill in the art can reasonably conclude that the inventor invented the claimed subject matter”. See MPEP 2161.01. There is no disclosed “system”, in the electronic device that is configured to enact the multiple acts claimed by the limitations. Dependent claims 22-39 and 41-49 are also rejected.

41. Claims 21 and 40 recite executing a “secure operation”, “an electronic device configured to encrypt information to enable execution of a secure operation…”, “a method of controlling execution of a secure operation….” The recitation of electronic ID device and the system both executing the "secure operation" calls to question the scope of the claims, whether the claim actually encompasses the “secure operation and the claim being directed to a genus of secure operations because there is no limitation on what falls under the banner of “secure operation”. Additionally, disclosure doesn’t provide sufficient teaching to claim a genus. The language “execute a secure operation” is broad enough in scope to encompass operations not taught by the written disclosure and is overly broad as it is directed towards a genus where the written disclosure does not provide sufficient teachings to support the claiming of a genus and should be rejected under 112 (a) under MPEP § 2163 (II)(A)(3)(a)(ii). Dependent claims 22-39 and 41-49 are also rejected.

42. Claim 24 recites “wherein the secure operation includes a secure transaction, and wherein the system configured to perform the secure operation comprises a point-of-sale (POS) device.” The specification (¶ 275, 276) states “the user device includes a communication link configured to communicate with a secure registry, and a processor coupled to the biometric sensor to receive information concerning the biometric input, the user interface, and the communication link. According to one embodiment, the processor is configured to generate a non-predictable value and to generate encrypted

authentication information from the non-predictable value, the identifying information, and at least one of the information concerning the biometric input and the secret information, and to communicate the encrypted authentication information via the communication link to the secure registry… the communication link wirelessly transmits the encrypted authentication information to a point-of-sale (POS) device, and the POS device is configured to transmit at least a portion of the encrypted authentication information to the secure registry. The language "execute a secure operation" is broad enough in scope to encompass operations not taught by the written disclosure and is overly broad as it is directed towards a genus where the written disclosure does not provide sufficient teachings to support the claiming of a genus and should be rejected under 112 (a) under MPEP § 2163 (II)(A)(3)(a)(ii). The specification provides for a communication link that "wirelessly transmits the encrypted authentication information to a point-of-sale (POS) device," the specification does not provides for a system that executes a secure transaction and it includes a POS device.

43. Claim 44 recites "generating a seed from which the encrypted authentication information is generated by employing at least two of the biometric data, the secret authentication information known to the user, and a discrete code unique to the electronic ID device." The specification (page 67) that the "seed is employed in an algorithm that also employs a temporal value…." "When examining computer-implemented functional claims, examiners should determine whether the specification discloses the computer and the algorithm (e.g., the necessary steps and/or flowcharts) that perform the claimed function in sufficient detail such that one of ordinary skill in the

art can reasonably conclude that the inventor invented the claimed subject matter". See MPEP 2161.01. The specification does not disclose an actual algorithm that performs the claimed function.

44. The following is a quotation of 35 U.S.C. 112(b):

> (b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

45. Claims 21-49 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

46. Claim 21 recites "the processor being programmed such that after the electronic ID device receives… the processor is configured to generate…" The claim is unclear because if the limitations of "being programmed" and "configured to" are to be viewed as structural limitations, the claim is implying that if the processor does not receive at least one of the biometric input and the secret authentication information that the structure in the form of the algorithm needed to generate a non-predictable value and encrypt the non-predictable value, information derived, etc., will not exist. Dependent claims 22-39 are also rejected.

47. Claim 21 recites "the processor being programmed such that after the electronic ID device receives at least one of the biometric input and the secret authentication

information, the processor is configured to generate a non-predictable value and to encrypt the non-predictable value, information derived from at least a portion of the biometric input, and information derived from at least a portion of the secret authentication information to generate encrypted authentication information…." Since the device receives at least one of the biometric input and the secret authentication information, it is unclear how the processor would then be able to encrypt both the "information derived from at least a portion of the biometric input, and information derived from at least a portion of the secret authentication information" when it could possibly only have received one of them. Dependent claims 22-39 are also rejected.

48. Claims 21 and 40 recite "information derived from at least a portion of the secret authentication information to generate encrypted authentication information…." The claim is unclear. The processor is set "to encrypt the non-predictable value, information derived from at least a portion of the biometric input, and information derived from at least a portion of the secret authentication information to generate encrypted authentication information…." Yet, as written, the encryption of "at least a portion of the secret authentication information" is the piece of information that yields generated encrypted authentication information…." Dependent claims 22-39 are also rejected.

49. Claims 21 and 40 recite "execute a secure operation". Similarly, claim 24 recites "the secure operation". The term "secure" is a relative term which renders the claim indefinite. The term "secure" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. The term is not

defined within the written disclosure and the word “secure” can be viewed as a relative term, making it unclear as to what does and does not fall under the scope of the claim and is indefinite under 112 (b). Dependent claims 22-39 and 41-49 are also rejected.

50. Claim 21 is directed to an “electronic ID device”, but the claim adopts circular reasoning in the explanation of not what the device comprises but what it does, "after the electronic ID device receives...." Similarly, claim 30 recites “wherein the electronic ID device initiates…”, claim 31 recites “authentication by the electronic ID device…”, claim 34 recites “the electronic device is configured to not permit the entry…”, claim 36, “the electronic ID device successfully authenticates…”, claim 37, “the electronic ID device successfully authenticating…”, and claim 39, “the electronic ID device executes a challenge….” Dependent claims 22-39 are also rejected.

51. Claim 21 is directed towards “an electronic device…”, dependent claims for example, Claim 34 is directed towards “an electronic device…” but recites “the electronic ID device is configured to not….” The claim recites “the entry of the user input” is not permitted while simultaneously reciting that the biometric input has been received. The only “entry of the user input” made was a secret authentication information, “the entry of the user input” alludes to a past entry. It is therefore unclear as to whether the “entry” is to be viewed as the receiving of the biometric input or a different operation not present in the claim or there is a mistake and Applicant failed to allude to a future entry of the user input.

52. Claim 21 recites “an electronic device configured to encrypt information to enable execution of a secure operation… the system configured to execute the secure

operation…", claim 23 recites "the system configured to execute the secure operation, wherein the system is configured to transmit the encrypted authentication information to a secure registry software and to receive authorization to perform the secure operation from the secure registry software." Similarly, claims 24 and 27 recite "the system configured to execute…. " These claim limitations are directed to a system, however, claim 21 is directed towards a device and the system is not part of the device. Therefore the scope is unclear as it cannot be ascertained as to whether the scope only applies to the device of claim 21 or also encompasses elements external to the device. Furthermore, it is unclear how language directed towards an external system places a structural limitation on the device being claimed in claim 21 and raises a question as to whether only the device is being claimed or the device and the system. Dependent claims 22-39 are also rejected.

53. Regarding claim 30, the claim recites "electronic device initiates, responsive to receiving an authentication initiation input from the user, authentication with the system…", however, claim 21, from which claim 30 depends, is directed to an electronic ID device of which the system is not a part of. The claim recites receiving an authentication input from the user and responding by initiating authentication with the system. Therefore, it would be unclear whether infringement of claim 21 occurs based on possession of the device. *In re Katz Interactive Call Processing Patent Litigation*, 639 F.3d 1303 (Fed. Cir. 2011). *IPXL Holdings v. Amazon.com, Inc.*, 430 F.2d 1377, 1384, 77 USPQ2d 1140, 1145 (Fed. Cir. 2005). *Ex parte Lyell*, 17 USPQ2d 1548 (Bd. Pat. App. & Inter. 1990).

54. Claim 38 recites the limitation "the electronic serial number". There is insufficient antecedent basis for this limitation in the claim.

55. Claim 40 recites "subsequent to successful authentication of the identity of the user to the electronic ID device" it is unclear how the electronic device is aware that the authentication was successful without receiving notice of it. Dependent claims 41-49 are rejected.

56. Claim 41 recites "receiving at least a portion of a user's secret authentication information manually within a user interface." The claim is unclear as to whether the Applicant means to say there is a receipt of information that is done by a user and is therefore the user manually entering information, whether the unclear entity is manually given information that was previously in an interface or the information is manually put inside an interface, which would require an expansion of what steps were taken to successfully execute that.

57. The following is a quotation of 35 U.S.C. 112(d):

> (d) REFERENCE IN DEPENDENT FORMS.—Subject to subsection (e), a claim in dependent form shall contain a reference to a claim previously set forth and then specify a further limitation of the subject matter claimed. A claim in dependent form shall be construed to incorporate by reference all the limitations of the claim to which it refers.

The following is a quotation of pre-AIA 35 U.S.C. 112, fourth paragraph:

> Subject to the following paragraph [i.e., the fifth paragraph of pre-AIA 35 U.S.C. 112], a claim in dependent form shall contain a reference to a claim previously set forth and then specify a further limitation of the subject matter claimed. A claim in dependent form shall be construed to incorporate by reference all the limitations of the claim to which it refers.

58. Claim 44 is rejected under 35 U.S.C. 112(d) or pre-AIA 35 U.S.C. 112, 4th paragraph, as being of improper dependent form for failing to further limit the subject

matter of the claim upon which it depends, or for failing to include all the limitations of the claim upon which it depends.

59. Claim 44 recites "generating a seed from which the encrypted authentication information is generated by employing at least two of the biometric data, the secret authentication information known to the user, and a discrete code unique to the electronic ID device." Claim 40 already claims the encrypted authentication information is generated by the electronic ID device encrypting "information derived from at least a portion of the secret authentication information to generate encrypted authentication information." The language of "at least two" creates a possible omission. For example, a possible omission of the secret authentication information from the encrypted authentication information would be removing a limitation from the independent claim. This means claim 44 does not further limit the subject matter of the claim upon which it depends, and fails to include all the limitations of the claim upon which it depends Applicant may cancel the claim(s), amend the claim(s) to place the claim(s) in proper dependent form, rewrite the claim(s) in independent form, or present a sufficient showing that the dependent claim(s) complies with the statutory requirements.

Claim Rejections - 35 USC § 103

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

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

> said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

61. Claims 21-49 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Gullman et al (5,280,527) ("Gullman"), and further in view of Maritzen et al. (2002/0184500) ("Maritzen").

62. Regarding claims 21 and 40, Gullman teaches a biometric sensor configured to receive a biometric input provided by a user(column 4, line 39-49, column 5, line 42-54); a user interface configured to receive a user input including authentication information known to the user and information indicative of a secure operation to be executed (column 4, line 3-8, 39-64); a communication interface configured to communicate with a system configured to execute the secure operation (column3, line 50-55, column 4, line 13-20, 29-36, column 6, line 35-40); a processor coupled to the biometric sensor, the user interface, and the communication interface, the processor being programmed such that after the electronic ID device receives at least one of the biometric input and the authentication information (column 3, line 19-55, column 4, line 3-61, column 6, line 8-20), the processor is configured to generate a non-predictable value and to encrypt the non-predictable value, information derived from at least a portion of the biometric input, and information derived from at least a portion of the authentication information to generate encrypted authentication information (column 3, line 37-46, column 5, line 15-33; claim 1), and to communicate the encrypted authentication information via the communication interface to the system configured to execute the secure operation (Abstract; column 4, line 29-36; column 6, line 35-61; claim 1).

Gullman does not teach secret authentication information known to the user. Maritzen teaches secret authentication information known to the user (¶ 57, 70, 77). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Gullman and Maritzen in order to provide secure authentication of a user to prevent unauthorized access (Maritzen; ¶ 2-4).

63. Regarding claim 22, Maritzen teaches wherein the communication interface comprises a transmitter configured to wirelessly transmit the encrypted authentication information to the system configured to execute the secure operation (¶ 23, 27, 35, 39, 42).

64. Regarding claim 23, Maritzen teaches wherein the system is configured to transmit the encrypted authentication information to a secure registry software and to receive authorization to perform the secure operation from the secure registry software (¶ 28-31).

65. Regarding claim 24, Maritzen teaches wherein the secure operation includes a secure transaction, and wherein the system configured to perform the secure operation comprises a point-of-sale (POS) device (¶ 28, 34, 57, 61).

66. Regarding claim 25, Maritzen teaches wherein the user interface is configured to display options for purchase (¶ 18, 30, 33, 74, 81).

67. Regarding claim 26, Maritzen teaches wherein the user interface is configured to accept user selection of at least one product or service for purchase (¶ 30, 33, 69, 74, 81).

68. Regarding claim 27, Gullman teaches wherein execution of the secure operation permits access to a secure location, and the system configured to execute the secure operation is further configured to manage access to the secure location (column 4, line 29-36, column 6, line 35-45).

69. Regarding claim 28, Maritzen teaches wherein the electronic ID device comprises a discrete code associated with the electronic ID device (¶ 37).

70. Regarding claim 29, Gullman teaches wherein the user interface is configured to initiate authentication with the system configured to execute the secure operation responsive to the user manually entering a secret code (column 3, line 56-68, column 6, line 9-16).

71. Regarding claim 30, Gullman teaches wherein the electronic ID device initiates, responsive to receiving an authentication initiation input from the user, authentication with the system configured to execute the secure operation (column 3, line 56-64, column 6, line 9-16).

72. Regarding claim 31, Gullman teaches wherein at least a portion of the biometric input received by the biometric sensor is communicated to a secure registry software for authentication by the electronic ID device prior to generation of the encrypted authentication information (column 3, line 44-48, column 5, line 57-65).

73. Regarding claim 32, Maritzen teaches wherein the user interface is configured to receive the secret authentication information including the identifying information (¶ 57, 61, 62, 77).

74. Regarding claim 33, Gullman teaches further comprising a memory coupled to the processor, wherein the memory stores information employed by the electronic ID device to authenticate the biometric input received by the biometric sensor (column 3, line 44-48, column 5, line 57-65).

75. Regarding claim 34, Gullman teaches wherein the electronic ID device is configured to not permit the entry of the user input if the biometric input received by the biometric sensor is determined to not belong to an authorized user of the electronic ID device (column 3, line 37-55).

76. Regarding claim 35, Gullman teaches wherein the secret authentication information known to the user includes a Personal Identification Number (PIN), and wherein the processor is configured to generate the non-predictable value and the encrypted authentication information responsive to authentication of both the secret authentication information and the biometric input (column 3, line 37-68, column 4, line 3-36, column 5, line 15-33; claim 1).

77. Regarding claim 36, Gullman teaches wherein data stored in the memory is unavailable to an individual in possession of the electronic ID device until the electronic ID device successfully authenticates at least one of the biometric input and the authentication information (column 3, line 19-55, column 4, line 3-61, column 5, line 64-68, column 6, line 8-20).

78. Regarding claim 37, Maritzen teaches wherein data stored in a memory is subject to encryption that acts to modify the data such that it is unintelligible until the data is subjected to decryption that acts to modify the data such that it is intelligible

responsive to the electronic ID device successfully authenticating at least one of the biometric input and the secret authentication information (¶ 55-57, 70, 77).

79. Regarding claim 38, Gullman teaches wherein the processor is configured to generate a seed using at least two of the electronic serial number, a discrete code associated with the electronic ID device, a Personal Identification Number (PIN), a time value, and information derived from the biometric input to generate the encrypted authentication information, and wherein the seed is employed by the processor to generate the non-predictable value (column 3, line 37-68, column 4, line 3-22). Gullman does not teach wherein the memory is configured to store an electronic code unique to the electronic ID device. Maritzen teaches wherein the memory is configured to store an electronic code unique to the electronic ID device (¶ 37). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Gullman and Maritzen in order to provide secure authentication of a user to prevent unauthorized access (Maritzen; ¶ 2-4).

80. Regarding claim 39, Gullman teaches wherein the electronic ID device executes a challenge-response protocol as part of authentication with the system configured to execute the secure operation (column 3, line 37-68, column 4, line 8-11).

81. Regarding claim 41, Maritzen teaches an act of receiving at least a portion of a user's secret authentication information manually within a user interface (¶ 22, 57).

82. Regarding claim 42, Gullman teaches further comprising an act of displaying, on a user interface, indicators for a plurality of user accounts stored in a memory of the electronic ID device (column 5, line 57-65).

83. Regarding claim 43, Maritzen teaches further comprising an act of entering, by the electronic ID device, de-active state without generating the encrypted authentication information if the identity of the user is not successfully authenticated to the electronic ID device (¶ 57).

84. Regarding claim 44, Gullman teaches further comprising an act of generating a seed from which the encrypted authentication information is generated by employing at least two of the biometric data, the secret authentication information known to the user, and a discrete code unique to the electronic ID device (column 3, line 37-68, column 4, line 3-22).

85. Regarding claim 45, Gullman teaches further comprising an act of generating encrypted authentication information in a manner that allows identification of the user and a selected one of a plurality of user accounts by secure registry software (column 4, line 23-36, column 5, line 57-65).

86. Regarding claim 46, Maritzen teaches further comprising displaying options for selection of the system configured to execute the secure operation on a user interface (¶ 33, 69, 74).

87. Regarding claim 47, Gullman teaches further comprising selecting with the user interface at least one product, service, or secure operation (Abstract; column 3, line 50-55, column 4, line 59-62; claim 2, 3).

88. Regarding claim 48, Maritzen teaches further comprising maintaining an audit trail of purchases made (¶ 32, 42, 82).

89. Regarding claim 49, Gullman teaches wherein the user initiates an authentication request on the electronic ID device triggering communication of the encrypted authentication information from the electronic ID device to the system configured to execute the secure operation (column 3, line 56-68, column 4, line 50-64).

Conclusion

90. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ISIDORA I IMMANUEL whose telephone number is (469)295-9094. The examiner can normally be reached on Monday-Friday 9:00 am to 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, CALVIN L HEWITT can be reached on 571-272-6709. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/I. I./
Examiner, Art Unit 3685

/JAMES D NIGH/
Primary Examiner, Art Unit 3685

Notice of References Cited	Application/Control No. 14/071,126	Applicant(s)/Patent Under Reexamination Weiss, Kenneth P.	
	Examiner ISIDORA I IMMANUEL	Art Unit 3685	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	5,280,527 A	01-1994	Gullman; Lawrence S.	G06K19/0718	713/184
*	B	2002/0184500 A1	12-2002	Maritzen, Michael	G06Q20/18	713/170
	C					
	D					
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Electronic Acknowledgement Receipt

EFS ID:	30729230
Application Number:	14071126
International Application Number:	
Confirmation Number:	3814
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Customer Number:	37462
Filer:	John N Anastasi
Filer Authorized By:	
Attorney Docket Number:	W0537-701321
Receipt Date:	23-OCT-2017
Filing Date:	04-NOV-2013
Time Stamp:	15:58:53
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	Transmittal Letter	Information_Disclosure_Statement.pdf	27803 4e34ea810d8c9a5ba3f602b37b6a4b865480ba4a	no	2

Warnings:

Information:					
2	Information Disclosure Statement (IDS) Form (SB08)	Information_Disclosure_Statement_Fillable_PDF.pdf	1035483 ee869a94455e57cdfa0aebbbc84b7dfe93866252	no	5
Warnings:					
Information:					
3	Foreign Reference	WO0106699A2.pdf	1563724 6acb7595652db408436f13d4b49afdccbd5759d8	no	36
Warnings:					
Information:					
4	Foreign Reference	WO0124123A1.pdf	5596868 186f605363494049e13a2ef3491c483828f71b73	no	118
Warnings:					
Information:					
5	Non Patent Literature	Jin_et_al_Biohashing_2004.pdf	868209 fc470313ab11bd5228326b651a0e3e4422b1a69c	no	11
Warnings:					
Information:					
6	Non Patent Literature	EX1015_Schneier_Applied_Cryptography_.pdf	8429727 95870a126b0681dba933a733fa6c5c20237cc3ce	no	1027
Warnings:					
Information:					
7	Non Patent Literature	ANSI_X9.pdf	11234403 0afc964b590f71e41c807c91b554b124c5e149b1	no	168
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
8	Non Patent Literature	W0537-701320_Notice_of_Petition_for_IPR.pdf	718373 253de8f4b14b01e5ec453c5b1b219a15f01e6395	no	73
Warnings:					

Information:					
9	Non Patent Literature	Dr_Cole_CV.pdf	318284 668eb2c7cc4aab5693180dda1b3296a3488c0c19	no	6
Warnings:					
Information:					
10	Non Patent Literature	Cole_Declaration.pdf	429812 5f05e9089bdbef8ac8d0353d52acecac27e76fbd	no	47
Warnings:					
Information:					
11	Non Patent Literature	813_Patent_File_History.pdf	10684685 6327473ff99d11370e3c716b11dc610a60d13e79	no	860
Warnings:					
Information:					
Total Files Size (in bytes):	40907371				

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.

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted via the Office electronic filing system in accordance with 37 CFR § 1.6(a)(4).

Dated: October 23, 2017
Electronic Signature for John N. Anastasi: /John N. Anastasi/

Docket No.: W0537-701321
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Kenneth P. Weiss

Application No.: 14/071,126 Confirmation No.: 3814

Filed: November 4, 2013 Art Unit: 3685

For: UNIVERSAL SECURE REGISTRY Examiner: I. I. Immanuel

INFORMATION DISCLOSURE STATEMENT (IDS)

MS Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Pursuant to 37 C.F.R. §§ 1.56, 1.97, and 1.98, the attention of the United States Patent and Trademark Office is hereby directed to the references listed on the attached PTO/SB/08. It is respectfully requested that the information be expressly considered during the prosecution of the above-identified application, and that the references be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

This Information Disclosure Statement is filed more than three months after the filing date of this application, OR more than three months after the date of entry of the national stage in the international application, AND after the mailing date of a first Office Action on the merits, but before the mailing date of any of a Final Action under 37 C.F.R. § 1.113, a Notice of Allowance under 37 C.F.R. § 1.311 or an action that otherwise closes prosecution in this application (37 C.F.R. § 1.97(c)).

Pursuant to 37 C.F.R. § 1.97(e)(2), no item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application and, to my knowledge after making reasonable inquiry, no item of information contained in this Information Disclosure Statement was known to any individual designated in 37 C.F.R. § 1.56(c) more than three months prior to the filing of this Information Disclosure Statement.

In accordance with 37 C.F.R. § 1.98(a)(2)(ii), copies of U.S. patents and U.S. patent application publications are not submitted. Submitted herewith are copies of foreign patents and non-patent literature in accordance with 37 C.F.R. § 1.98(a)(2).

Applicant would like to bring to the Examiner's attention the attached Petition for Inter Partes Review of U.S. Patent 8,577,813 dated October 16, 2017, CV of Dr. Eric Cole (Exhibit to the Petition), Declaration of Dr. Eric Cole (Exhibit to the Petition), and File History of US Patent 8,577,813 (Exhibit to the Petition).

In accordance with 37 C.F.R. § 1.97(g), the filing of this Information Disclosure Statement shall not be construed as a representation that a search has been made. In accordance with 37 C.F.R. § 1.97(h), the filing of this Information Disclosure Statement shall not be construed to be an admission that the information cited in this Information Disclosure Statement is, or is considered to be, material to the patentability as defined in 37 C.F.R. § 1.56(b).

It is submitted that the Information Disclosure Statement is in compliance with 37 C.F.R. § 1.98, and the Examiner is respectfully requested to consider the listed references.

Applicant believes no fee is due with this submission. However, if a fee is due, please charge our Deposit Account No. 50/2762, under Order No. W0537-701321 from which the undersigned is authorized to draw.

Dated: October 23, 2017

Respectfully submitted,

Electronic signature: /John N. Anastasi/
John N. Anastasi
Registration No.: 37,765
John T. Spangenberger
LANDO & ANASTASI, LLP
Riverfront Office Park
One Main Street, Suite 1100
Cambridge, Massachusetts 02142
(617) 395-7000

L&A | LANDO &
ANASTASI

Date November 28, 2017 **Number of pages** (including cover): 3

To: Examiner Immanuel (P# 469-295-9094)

Email: Isidora.Immanuel@USPTO.gov

From: John Spangenberger (P#: 617-395-7030)
John Anastasi (P#: 617-395-7001)

Application No.: 14/071,126

Our Docket No.: W0537-701321

ORIGINAL DOCUMENTS WILL NOT BE MAILED.

Message: Below is a proposed Agenda for the Telephone Interview for Wednesday, November 29th, 2017 at 1:00 p.m. EST:

Applicant's representatives would like to discuss the rejections made in the most recent Office Action under 35 U.S.C. §§ 101, 103, and 112. In particular, Applicant's representatives would like to discuss the following:

- Rejections under 35 U.S.C. § 101
  - Applicant's representative is unaware of any precedent which has held encryption-related claims patent-ineligible. To the contrary, Applicant's representative referred in its response to the most recent Office Action two decisions[1, 2] which held encryption-related claims to be patent-eligible. Applicant's representative would like to review the claims and discuss further why the claims as previously presented are patent-eligible in view of the remarks made in the cited decisions, which emphasized that encryption-related claims are patent-eligible.
  - Applicant's representative would like to discuss why the claims are directed to an abstract idea in view of DDR Holdings, LLC v. Hotels.com, L.P., which found the claims at issue to be patent-eligible in part because "the claimed solution is necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer networks." 773 F.3d at 1257. Similarly, the claims are directed to a problem which arises specifically in the realm of computer networks and are therefore patent-eligible.
  - Applicant's representative would like to discuss that even if the claims are considered to be directed to an abstract idea, the arrangement of elements recited in the claims renders the claims patent-eligible. As discussed in BASCOM Global Internet v. AT&T Mobility LLC[3], even though the high-level concept of content filtering was known, the elements were arranged to address problems specific to an Internet context. Similarly, the present application details how the arrangement of elements provides a system which is resistant to malicious actors who attempt to fraudulently access remotely-transmitted data.
- Rejections under 35 U.S.C. § 103
  - The Applicant's representative would like to discuss the Examiner's assertions that Gullman teaches the claimed element of "a user interface configured to receive a user input including authentication information known to the user and information indicative of a secure operation to be executed (column 4, line 3-8, 39-64 [of Gullman])." (Office Action, Page 23.)

    - Applicant's representative would like to discuss the cited portions of Gullman, which refer to a biometric security apparatus 14 which includes a biometric sensor, an on/off switch, and a display, none of which are "configured to receive.... authentication information **known to the user**" or "information **indicative of a secure operation to be executed**."

- Rejections under 35 U.S.C. § 112
  - Applicant's representative would appreciate clarification of the rejection made in section 48 on page 18 of the Office Action.

Tentative Participants:
John Anastasi (Reg. No.: 37,765)
John Spangenberger (Reg. No.: 76,607)
Examiner Immanuel

REFERENCES

[1]On pages 12-13 of the most recent response, Applicant's representative cited Paone v. Broadcom Corp., which held that "it would require an overly broad view of the Supreme Court's § 101 jurisprudence to find that a patent directed at a method of encryption does not claim eligible subject matter *per se*, as long as it is specific enough… [I]n TQP, Judge Bryson ***rejected the notion that the claimed encryption method was a 'mental process' ineligible under [Gottschalk]***, because 'the invention involves a several-step manipulation of data that, except perhaps in its most simplistic form, ***could not conceivably be performed in the human mind or with pencil and paper***." 2015 U.S. Dist. LEXIS 109725 (2015), citing TQP Dev., LLC v. Intuit Inc., 2014 U.S. Dist. LEXIS 20077 (2014).

[2]On page 13 of the most recent response, Applicant's representative cited TQP Dev., LLC v. Intuit Inc., which held that "that "[t]ypically, transforming data from one form to another does not qualify as the kind of transformation that the Supreme Court in Bilski regarded as an important indicator of patent eligibility… ***In the case of an invention in the field of encryption, however, the entire object of the invention is to transform data from one form into another*** that will be recognizable by the intended recipient but secure against decryption by unintended recipients. In that setting***, it does not make sense to say that the transformation of data from one form to another cannot qualify as a patent-eligible invention, because that is what the field of cryptology is all about***." 2014 U.S. Dist. LEXIS 20077 (2014).

[3]"...the claims [do not] preempt all ways of filtering content on the Internet; rather, they recite **a specific, discrete implementation of the abstract idea of filtering content**. Filtering content on the Internet was already a known concept, and the patent describes how its particular arrangement of elements is **a technical improvement over prior art ways of filtering such content**. As explained earlier, prior art filters were either **susceptible to hacking** and dependent on local hardware and software, or confined to an inflexible one-size-fits-all scheme.... [T]he claims may [therefore] be read to '**improve[] an existing technological process**.' [...] [A]lthough the invention in the '606 patent is engineered in the content of filtering content, the invention is **not claiming the idea of filtering content simply applied to the Internet**. The '606 patent is instead claiming **a technology-based solution** (not an abstract-idea-based solution implemented with generic technical components in a conventional way) to filter content on the Internet that **overcomes existing problems with other Internet filtering systems**.... [T]he claimed invention represents a 'software-based invention[] that improve[s] the performance of the computer system itself." BASCOM Global Internet v. AT&T Mobility LLC, 827 F.3d at 1350-51 (Fed. Cir. 2016).

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/071,126	11/04/2013	Kenneth P. Weiss	W0537-701321	3814

37462 7590 12/05/2017
LANDO & ANASTASI, LLP
ONE MAIN STREET, SUITE 1100
CAMBRIDGE, MA 02142

EXAMINER	
IMMANUEL, ISIDORA I	

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
12/05/2017	ELECTRONIC

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

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

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@LALaw.com
CKent@LALaw.com

Applicant-Initiated Interview Summary	**Application No.** 14/071,126	**Applicant(s)** Weiss, Kenneth P.		
	Examiner ISIDORA I IMMANUEL	**Art Unit** 3685	**AIA (First Inventor to File) Status** No	**Page** **1 of** 2

All participants (applicant, applicants representative, PTO personnel):

1. ISIDORA I IMMANUEL(Examiner); Telephonic
2. JOHN SPANGENBERGER(Attorney); Telephonic
3. JOHN ANASTASI(Attorney); Telephonic

Date of Interview: 29 November 2017

Claims Discussed: Discussed claim 40, 101 rejection, overall claimed idea and claim language.

Brief Description of the main topic(s) of discussion: Discussed 101 and the use of encryptions in 101 rejections . Discussed case law and Applicant's argument for encryption overcoming the 101 rejection. No agreements reached.

Issues Discussed:

Item(s) under 35 U.S.C. 101:
Discussed case law and encrypting

Attachment(s): Agenda,

/I.I.I./ Examiner, Art Unit 3685	/JAMES D NIGH/ Primary Examiner, Art Unit 3685

Applicant is reminded that a complete written statement as to the substance of the interview must be made of record in the application file. It is the applicants responsibility to provide the written statement, unless the interview was initiated by the Examiner and the Examiner has indicated that a written summary will be provided. See MPEP 713.04
Please further see:
MPEP 713.04
Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews, paragraph (b)
37 CFR § 1.2 Business to be transacted in writing

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted via the Office electronic filing system in accordance with 37 CFR § 1.6(a)(4).

Dated: December 15, 2017
Electronic Signature for John N. Anastasi: /John N. Anastasi/

Docket No.: W0537-701321
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Kenneth P. Weiss

Application No.: 14/071,126

Confirmation No.: 3814

Filed: November 4, 2013

Art Unit: 3685

For: UNIVERSAL SECURE REGISTRY

Examiner: I. I. Immanuel

AMENDMENT IN RESPONSE TO NON-FINAL OFFICE ACTION UNDER 37 C.F.R. § 1.111

MS Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

INTRODUCTORY COMMENTS

In response to the Office Action dated September 15, 2017, please amend the above-identified U.S. patent application as follows:

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks/Arguments begin on page 8 of this paper.

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1-20 (Cancelled)

21. (Currently Amended) An electronic ID device for performing a financial transaction between an authenticated user and a second party ~~configured to encrypt information to enable execution of a secure operation~~, comprising:

a biometric sensor configured to receive a user biometric comprising at least one of a user fingerprint and facial scan information ~~input provided by a user~~;

a user interface configured to receive a user input including secret authentication information known to the user and a selection ~~information indicative~~ of the financial transaction ~~a secure operation~~ to be executed;

a communication interface configured to communicate with [[a]] an external system ~~configured to execute the secure operation~~;

a processor coupled to the biometric sensor, the user interface, and the communication interface, and ~~the processor~~ being programmed to generate, ~~such that after the electronic ID device~~ responsive to receiving ~~receives~~ at least one of the user biometric [[input]] and the secret authentication information, ~~the processor is configured to generate~~ a non-predictable value and to encrypt the non-predictable ~~value,~~ value and at least one of information derived from at least a portion of the user biometric ~~input,~~ and information derived from at least a portion of the secret authentication information, to generate encrypted authentication information, and to communicate the encrypted authentication information via the communication interface to the external system ~~configured to execute the secure operation~~.

22. (Currently Amended) The electronic ID device of claim 21, wherein the communication interface comprises a transmitter configured to wirelessly transmit the encrypted authentication information to the external system configured to execute the financial transaction ~~secure operation~~.

23. (Canceled)

24. (Currently Amended) The electronic ID device of claim 21, ~~further comprising the system configured to execute the secure operation,~~ wherein the communication interface is configured to communicate with ~~secure operation includes a secure transaction, and wherein the system configured to perform the secure operation comprises~~ a point-of-sale (POS) device, and wherein the processor is configured to communicate the encrypted authentication information via the communication interface to the POS device.

25. (Previously Presented) The electronic ID device of claim 24, wherein the user interface is configured to display options for purchase.

26. (Previously Presented) The electronic ID device of claim 24, wherein the user interface is configured to accept user selection of at least one product or service for purchase.

27. (Canceled)

28. (Previously Presented) The electronic ID device of claim 21, wherein the electronic ID device comprises a discrete code associated with the electronic ID device.

29. (Currently Amended) The electronic ID device of claim 21, wherein the user interface is configured to initiate authentication with the external system ~~configured to execute the secure operation~~ responsive to receiving, from a user, a manually-entered ~~the user manually entering a~~ secret code.

30. (Currently Amended) The electronic ID device of claim 21, wherein the electronic ID device is configured to initiate, ~~initiates,~~ responsive to receiving an authentication initiation input from the user, authentication with the external system ~~configured to execute the secure operation~~.

31. (Currently Amended) The electronic ID device of claim 21, wherein the electronic ID device is further configured to communicate at least a portion of the user biometric [[input]] received by the biometric sensor ~~is communicated~~ to a secure registry software ~~for authentication by the electronic ID device~~ prior to generation of the encrypted authentication information.

32. (Previously Presented) The electronic ID device of claim 21, wherein the user interface is configured to receive the secret authentication information including identifying information.

33. (Currently Amended) The electronic ID device of claim 21, further comprising a memory coupled to the processor, wherein the memory stores information employed by the electronic ID device to authenticate the user biometric [[input]] received by the biometric sensor.

34. (Currently Amended) The electronic ID device of claim 33, wherein the electronic ID device is configured to not permit [[the]] entry of the user input if the user biometric [[input]] received by the biometric sensor is determined to not belong to an authorized user of the electronic ID device.

35. (Currently Amended) The electronic ID device of claim 32, wherein the secret authentication information known to the user includes a Personal Identification Number (PIN), and wherein the processor is configured to generate the non-predictable value and the encrypted authentication information responsive to authentication of both the secret authentication information and the user biometric [[input]].

36. (Currently Amended) The electronic ID device of claim 32, wherein the electronic ID device is configured to prevent access by an individual in possession of the electronic ID device to data stored in a memory ~~is unavailable to an individual in possession of the electronic ID device~~ until the electronic ID device successfully authenticates at least one of the user biometric [[input]] and the secret authentication information.

37. (Currently Amended) The electronic ID device of claim 32 [[34]], wherein the electronic ID device is configured to decrypt encrypted data stored in a memory ~~is subject to encryption that acts to modify the data such that it is unintelligible until the data is subjected to decryption that acts to modify the data such that it is intelligible~~ responsive to ~~the electronic ID device~~ successfully authenticating at least one of the user biometric [[input]] and the secret authentication information.

38. (Canceled)

39. (Currently Amended) The electronic ID device of claim 21, wherein the electronic ID device is configured to execute ~~executes~~ a challenge-response protocol as part of authentication with the external system ~~configured to execute the secure operation~~.

40. (Currently Amended) A method of performing a financial transaction between an authenticated user and a second party ~~controlling execution of a secure operation~~, the method comprising acts of:

receiving, from a user by an electronic ID device, an indication of a selection of a user account for ~~information indicative of~~ the financial transaction ~~secure operation~~ to be executed;

receiving, by the electronic ID device from the user, a user biometric including at least one of a user fingerprint and facial scan information, [[data]] and secret authentication information known to the user;

authenticating an identity of the user to the electronic ID device based on at least one of the user biometric [[data]] received by the electronic ID device from the user and the secret authentication information known to the user and received by ~~provided to~~ the electronic ID device; and

subsequent to successful authentication of the identity of the user to the electronic ID device:

generating, with the electronic ID device, a non-predictable value;

encrypting, by the electronic ID device, the non-predictable value, information derived from at least a portion of the user biometric [[input]], and information derived from at least a portion of the secret authentication information to generate encrypted authentication information; and

communicating the encrypted authentication information from the electronic ID device to [[a]] an external system ~~configured to execute the secure operation~~.

41. (Currently Amended) The method of claim 40, further comprising an act of receiving at least a portion of a user's secret authentication information via ~~manually within~~ a user interface.

42. (Previously Presented) The method of claim 40, further comprising an act of displaying, on a user interface, indicators for a plurality of user accounts stored in a memory of the electronic ID device.

43. (Currently Amended) The method of claim 40, further comprising: ~~an act of~~

determining, by the electronic ID device, that the identity of the user is not successfully authenticated to the electronic ID device; and

entering, by the electronic ID device, a de-active state without generating the encrypted authentication information [[if]] responsive to determining that the identity of the user is not successfully authenticated to the electronic ID device.

44. (Canceled)

45. (Currently Amended) The method of claim 40, further comprising an act of generating the encrypted authentication information in a manner that allows identification of the user and a selected one of a plurality of user accounts by secure registry software.

46. (Currently Amended) The method of claim 40, further comprising displaying options for selection of the external system ~~configured to execute the secure operation~~ on a user interface.

47. (Currently Amended) The method of claim 46, further comprising selecting with the user interface at least one product, service, or financial transaction ~~secure operation~~.

48. (Previously Presented) The method of claim 46, further comprising maintaining an audit trail of purchases made.

49. (Currently Amended) The method of claim 40, further comprising initiating ~~wherein the user initiates~~ an authentication request on the electronic ID device, and triggering communication of the encrypted authentication information from the electronic ID device to the external system ~~configured to execute the secure operation~~.

50. (New) The electronic ID device of claim 28, wherein the processor is further configured to communicate, via the communications interface, the discrete code to the external system.

51. (New) The electronic ID device of claim 21, wherein the processor is further programmed to communicate, via the communications interface, information indicative of the selection of the financial transaction to be executed to the external system.

52. (New) The method of claim 40, further comprising communicating the indication of the selection of the user account from the electronic ID device to the external system.

53. (New) The method of claim 40, further comprising communicating a discrete device code associated with the electronic ID device to the external system.

REMARKS

In response to the Office Action mailed September 15, 2017, Applicant respectfully requests reconsideration in view of the amendments and the following remarks. Claims 21-49 were previously pending in this application. By this amendment, Applicant is canceling claims 23, 27, 38, and 44 without prejudice or disclaimer. Claims 21, 22, 24, 29-31, 33-37, 39-41, 43, 45-47, and 49 have been amended. Claims 50-53 have been added. As a result claims 21, 22, 24-26, 28-37, 39-43, and 45-53 are pending for examination with claims 21 and 40 being independent claims. No new matter has been added.

Examiner Interview Summary

Applicant's below-signed attorneys would like to thank Examiner Immanuel for the courtesies extended during the telephonic interview conducted on November 29th, 2017. During the interview, participants discussed the alleged rejection of the claims under 35 U.S.C. § 101. No agreement as to the allowability of the claims was reached.

Response to Examiner's Comments

The Examiner asserts that claims 21-27, 29-31, 33, and 37-39 include claim language which "recites intended use and therefore do[] not have patentable weight. See MPEP 2114." (Office Action, p. 8). The Examiner has not provided any arguments or explanations supporting these statements. As such, Applicant assumes for the sake of argument that the Examiner is asserting that all limitations including the language "configured to" recite intended use.

As a threshold matter, Applicant notes that no section of the MPEP, including § 2114, states that language associated with the phrase "configured to" recites intended use. Indeed, MPEP § 2114 does not so much as mention the language "configured to." Furthermore, the Examiner has not provided any evidence or arguments in support of the position that the aforementioned claim limitations lack patentable weight.

Nonetheless, it is well established that a claim term is to be accorded "the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention." *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005). *Phillips* also indicated that evidence for the meaning of a term may be derived from "the words of the claims themselves, the remainder of the specification, the prosecution history, and extrinsic evidence concerning relevant scientific principles, the meaning of technical terms, and the state of the art." *Id.* at 1314.

Applicant respectfully submits that the present specification supports an interpretation where the phrase "configured to" denotes an actual state of configuration that fundamentally ties the limitations following the phrase "configured to" to physical characteristics of the limitations preceding the phrase "configured to." Because the language following the limitation "configured to" further limits the claimed invention, it does not recite intended use. Accordingly, the Examiner's comments should be withdrawn.

The Examiner asserts that "[r]egarding claim 21, the language 'programmed such that...', claim 37, 'the data such that...' is a result and therefore has not patentable weight (*Minton v. Nat'l Ass'n of Securities Dealers, Inc.*, 336 F.3d 1373, 1381, 67 USPQ2d 1614, 1620 (Fed. Cir. 2003)) that a 'whereby clause in a method claim is not given weight when it simply expresses the intended result of a process step positively recited.'' See MPEP 2111.04." (Office Action, p. 8).

It is unclear how the legal authority cited by the Examiner is relevant to the cited claim language. Claim 21 does not include "a whereby clause." Claim 37 is not directed to "a method claim," and is instead directed to an "electronic ID device." Because the authority cited by the Examiner is not relevant to the identified claims, Applicant submits that the claims as previously presented are in compliance with MPEP § 2111.04. Furthermore, claims 21and 37 have been amended and no longer include the language identified by the Examiner.

The Examiner asserts that "[r]egarding claim 35, 'information... includes a ...', are nonfunctional descriptive material and therefore do not have patentable weight. See *In re Gulack*, 217 USPQ 401 (Fed. Cir. 1983), *In re Ngai*, 70 USPQ2d (Fed. Cir. 2004), *In re Lowry*, 32 USPQ2d 1031 (Fed. Cir. 1994); MPEP 2111.05 III." (Office Action, p. 8). The Examiner has not provided any arguments or explanations in support of the assertion that the claim limitations "are nonfunctional descriptive material," and Applicant is unable to discern any provision of MPEP § 2111.05 which would support the Examiner's assertions.

Nonetheless, an explanation will be given as to why claim 35 complies with each and every provision of MPEP § 2111.05. MPEP §§ 2111.05(I) and (II) relate to claims including printed matter. MPEP § 2111.05(III) relates to claims directed to a computer-readable medium.

MPEP § 2111.05 is not relevant to claim 35 at least because (1) claim 35 does not relate to printed matter; and (2) claim 35 is not directed to a computer-readable medium. Accordingly, MPEP § 2111.05 is not relevant to claim 35, and it is submitted that all limitations of claim 35 should be given patentable weight under MPEP § 2111.05.

The Examiner asserts that "[r]egarding claim 40, the language 'provided to...', and claim 49, 'user initiates...' does not disclose a positively recited step and therefore does not patentable weight. See MPEP 2111.04." (Office Action, p.8).

MPEP § 2111.04 is directed to "'Adapted to,' 'Adapted for,' 'Wherein,' and 'Whereby' Clauses," and makes no mention of "positively recited step[s]." The language cited by the Examiner does not include an adapted to, adapted for, wherein, or whereby clause.

Accordingly, Applicant submits that claims 40 and 49 are in compliance with MPEP § 2111.04 at least because MPEP § 2111.04 does not appear to be relevant to claims 40 and 49, and because the Examiner has not provided any arguments to explain an alleged connection. Moreover, claims 40 and 49 have been amended and the cited language no longer appears in the claims as amended.

The Examiner asserts that "[r]egarding claim 43, 'entering, via the electronic ID device ... if the identity...', similarly, claim 45, 'a selected one...' is optional and conditional language and therefore does not have patentable weight. See MPEP 2103(I)(c)." (Office Action, p. 8).

Without acceding to the correctness of the rejection, claim 43 has been amended to recite, "entering, by the electronic ID device, a de-active state... **responsive to** determining that...." As amended, claim 43 is in compliance with MPEP § 2103(I)(C).

With respect to claim 45, Applicant respectfully requests clarification of the Examiner's remarks, as it is unclear how the claim language "a selected one" is not in full compliance with MPEP § 2103(I)(C).

Applicant respectfully notes that claim 45 does not include any optional language. MPEP § 2103(I)(C) does not mention the patentable weight of "conditional language" and Applicant therefore respectfully requests clarification as to how MPEP § 2103(I)(C) is relevant to "conditional language." In light of the foregoing, claim 45 is believed to be in full compliance with MPEP § 2103(I)(C).

Rejections Under 35 U.S.C. § 101

I. Summary of Examiner's Argument

Claims 21-49 were rejected under 35 U.S.C. § 101 on the grounds that the claimed invention is allegedly directed to non-statutory subject matter. More specifically, the Examiner asserted that,

> "the claim is directed towards receiving, and processing data and automating mental tasks, in this case an electronic device is used, which is similar to Alice which dealt with receiving, processing and storing data..., and Classen which dealt with automating mental tasks.... Claim 21 is directed towards the generic computer used to implement the method of claim 40 and is therefore also directed towards a judicial exception regarding an abstract idea involving the receiving and processing data, based on case law precedent, is claiming subject matter similar to concepts identified by the courts as dealing with abstract ideas.... The claims do not include additional elements that are sufficient to amount to significantly more than the judicial exception because the elements of 'authenticating an identity' are drawn to data comparisons in SmartGene.... The claim as a whole, does not amount to significantly more than the abstract idea itself. This is because the claim does not affect [*sic*] an improvement to another technology or technical field; the claim does not amount to an improvement to the functioning of a computer system itself; and the claim does not move beyond a general link of the use of an abstract idea to a particular technological environment."

(Office Action, Pages 10-12. Emphasis added).

II. Overview of Applicant's Response

Applicant respectfully disagrees on two grounds. First, the Examiner characterizes the claims too broadly in asserting that the claims are directed to no more than "receiving, and processing data and automating mental tasks." Second, contrary the Examiner's assertion that the claims "[do not effect] an improvement in any other technology or technical field," the claims clearly provide significant improvements to the field of secure transactions as described in extensive detail in the specification.

III. Brief Description of Disclosure

A brief description of the disclosure will be provided to emphasize the particular problem in the art addressed by the present claims. Electronic payment transactions using credit cards and other payment cards have become commonplace. There are major risks in such transactions, however, because bad actors can steal and then misuse a person's information. For example, when a person pays a merchant by credit card, the account data for that card is exposed to the risk of misuse by the merchant or by someone who intercepts the data as it is sent over a network to the merchant and/or the credit card company.

The present disclosure addresses the need for technology that allows consumers to make mobile payment-card transactions conveniently and with a high degree of security. The disclosure provides an innovative and highly secure identification, authentication and transaction authorization system, generally referred to as a Universal Secure Registry ("USR"). Using inventive aspects of the USR technology, the user device does not store or send any sensitive information, such as personal account information or payment card details that, if compromised, could be used for fraudulent purposes. Instead, each time a transaction occurs, the improved user device locally generates and sends one-time use data that, even if compromised, would provide no benefit to a malicious interceptor.

The user device can also require the user to authenticate him/herself via entry of biometric information (e.g., a fingerprint) and/or secret information (e.g., a PIN) before the user device will carry out a payment request. If this improved user device is lost or stolen or the one-time cryptographic value is intercepted, neither the user device nor the value can be used to make a fraudulent purchase request. Also, the described system avoids the problem of storing any sensitive information at the merchant that can be misused in fraudulent payment requests.

IV. Detailed Response

A. The Examiner Characterizes the Claims At Too High a Level

Turning to the first point, the Examiner has characterized the claims at an impermissibly high level by suggesting that the claims are directed to no more than "receiving, and processing data and automating mental tasks." As discussed in greater detail below, courts have repeatedly admonished against characterizing claims too broadly, noting that ***any claim*** may be considered abstract if viewed from a high enough level. While the claims may ***include*** acts of receipt and processing, it is inaccurate to assert that the claims are ***directed to*** no more than that; conversely, the claims address previously-unsolved problems unique to securing transactions over a digital network, which is not a fundamental economic practice executed pursuant to conventional activities.

A claim does not embody an unpatentable abstract idea unless that abstractness "exhibit[s] itself so manifestly as to override the broad statutory categories of eligible subject matter." *Research Corp. Techs., Inc. v. Microsoft Corp., 627* F.3d 859, 868 (Fed. Cir. 2010). The Examiner's characterization of the claims does not account for several express claim limitations, running afoul of a host of precedent. For example, in *Enfish, LLC v. Microsoft Corp.*, the court noted that "[d]escribing the claims at such a high level of abstraction and untethered from the language of the claims all but ensures that the exceptions to § 101 swallow the rule." 822 F.3d 1327, 1337 (Fed. Cir. 2016).

The Examiner's assertion that the claims are directed to no more than "receiving, and processing data and automating mental tasks" clearly "run[s] afoul of the Federal Circuit's guidance in *Enfish* that courts should not 'oversimplif[y]' key inventive concepts or 'downplay' an invention's benefits in conducting a step-1analysis." *MAZ Encryption Techs. LLC v. Blackberry Corp.*, 2016 WL 5661981 at *6 (D. Del. Sept. 29, 2016). "Whether at step one or step two of the *Alice* test…, a court must look to the claims as an ordered combination, ***without ignoring the requirements of the individual steps***." *McRO, Inc. v. Bandai Namco Games Am. Inc.*, 837 F.3d 1299, 1313 (Fed. Cir. 2016) (emphasis added).

The Examiner's assertion is improper at least because it fails to account for various claim requirements. Claim 21 recites a communications interface, a processor, a user interface, and a biometric sensor all working together in a specific way to provide a secure transaction resistant to fraudulent "eavesdroppers." For example, the processor enables a transaction that is structured to allow authentication without potentially compromising user information if the information is intercepted.

Far from being directed to the mere idea of receiving and processing data, claim 21 is directed to a ***specific, concrete, technological*** solution that improves network security for mobile electronic transactions. The "level of abstraction" "in describing the claims must be consonant with the level of abstraction expressed in the claims themselves." *Idexx Labs., Inc. v. Charles River Labs., Inc.*, 2016 WL 3647971 (D. Del. Jul. 1, 2016), at *4. Only by applying the highest possible level of abstraction could one conclude that claim 1 claims nothing more than the abstract idea of "receiving, and processing data," as Examiner contends.

Viewed through the lens of the Examiner's analysis, every claim is abstract. "If one looks at almost any patent from far enough away, it could arguably claim an abstract idea." *Messaging Gateway Solutions LLC v. Amdocs, Inc.*, 2015 WL 1744343 (D. Del. April 5, 2015) at *5 (Noting that Alexander Graham Bell's "invention was not the concept of oral communication itself; it was a technological innovation that allowed a type of oral communication between people who could otherwise not communicate in that way.").

Viewed in light of the specification, claim 21 is ***not*** directed to "receiving, and processing data" as was the claimed invention held to be patent-ineligible in *Alice*. *See Alice*, 134 S. Ct. at 2355–56. The invention in *Alice* covered concepts that had been "long prevalent in our system of commerce," *Alice*, 134 S. Ct. at 2356. Indeed, the invention in *Alice* included little more than applying the known concept of risk hedging to the Internet, **without any specific improvements or tailoring to the Internet environment**.

Claim 21 fundamentally differs from the claims at issue in *Alice* because the claims provide a solution to problems ***specific to remote transactions over a network***, a problem unknown to the world prior to the rise of distributed networks. More specifically, this problem includes the potential for malicious users to intercept digitally-transmitted information communicated over a network.

The Examiner has not identified a "long prevalent" practice that carried out the specific secure authentication transaction in the same way as claim 21, and Applicant submits that the area addressed by the claims – secure transactions using mobile electronic devices – is in fact a very nascent field.

In summary, Applicant submits that the claims have not been considered as a whole to determine if their focus is directed to an impermissible abstract idea, and that when viewed as a whole, the claims are not directed to an abstract idea. *See MAZ Encryption*, 2016 WL 5661981 at *2 (At *Alice* step 1, "the claims are considered ***in their entirety*** to ascertain whether their ***character as a whole*** is directed to excluded subject matter") (emphasis added). Accordingly, the claims are not directed to an abstract idea under step 1 of the *Alice*. Withdrawal of the rejection of claims 21-49 under 35 U.S.C. § 101 is therefore respectfully requested.

B. The Claims Provide Improvements to a Technical Field

The Examiner asserts that the claims "do[] not affect an improvement in any other technology or technical field," which is unsupported by any specific arguments. To the contrary, and as described in extensive depth in the specification, the claims include limitations which provide significant advantages in the field of secure transactions. Even assuming for the sake of argument that the claims are directed to an abstract idea, the claims include limitations which transform the claim into a patent-eligible application.

Under *Alice*'s second step, the Court "considers the elements of each claim both individually and 'as an ordered combination' to determine whether the additional elements 'transform the nature of the claim' into a patent-eligible application." *Alice,* 134 S. Ct. at 2355 (quoting *Mayo*, 132 S. Ct. at 1297-8). It is improper to analyze the claim as individual limitations. *Diamond v. Diehr*, 450 U.S. 175, 188-89 (1981); *King Pharms., Inc. v. Eon Labs, Inc.*, 616 F.3d 1267, 1277 (Fed. Cir. 2010) ("The Supreme Court has stated that a § 101 patentability analysis is directed to the claim as a whole, not individual limitations."). "[I]t is irrelevant that any individual step or limitation of such processes by itself would be unpatentable under § 101." *In re Bilski*, 545 F.3d 943, 958 (Fed. Cir. 2008); *Bascom Glob. Internet Servs., Inc. v. AT&T Mobility, LLC*, 827 F.3d 1341, 1350 (Fed. Cir. 2016) ("The inventive concept inquiry requires more than recognizing that each claim element, by itself, was known in the art.")

The claims provide specific improvements in mobile electronic transaction authentication that allow transactions to be executed in a more secure manner. The claims are, therefore, unlike the claims found unpatentable in *Alice* and *Versata Dev. Group v. SAP America, Inc.,* 793 F.3d 1306 (Fed. Cir. 2015), which **simply added conventional computer components to well-known business practices**. *See Alice,* 134 S. Ct. at 2358–60; *Versata.,* 793 F.3d at 1333–34 (computer performed "purely conventional" steps directed to the "abstract idea of determining a price using organization and product group hierarchies").

The claims fundamentally differ from those in *Alice* because *Alice* simply took known hedging techniques and applied them to the Internet ***without fundamentally altering those***

techniques. In contrast, the claims in the present application are ***specifically tailored*** to addressing problems ***unique to remote networks***.

Similar claims were found to be directed to patent-eligible subject matter in *Bascom Global Internet v. AT&T Mobility LLC* (hereinafter *Bascom*), which included content filters specifically arranged to address problems particular to the Internet. 827 F.3d 1341 (Fed. Cir. 2016). The court reasoned that,

> "...the claims [do not] preempt all ways of filtering content on the Internet; rather, they recite **a specific, discrete implementation of the abstract idea of filtering content**. Filtering content on the Internet was already a known concept, and the patent describes how its particular arrangement of elements is **a technical improvement over prior art ways of filtering such content**. As explained earlier, prior art filters were either **susceptible to hacking** and dependent on local hardware and software, or confined to an inflexible one-size-fits-all scheme.... [T]he claims may [therefore] be read to '**improve[] an existing technological process**.' [...] [A]lthough the invention in the '606 patent is engineered in the content of filtering content, the invention is **not claiming the idea of filtering content simply applied to the Internet**. The '606 patent is instead claiming **a technology-based solution** (not an abstract-idea-based solution implemented with generic technical components in a conventional way) to filter content on the Internet that **overcomes existing problems with other Internet filtering systems**.... [T]he claimed invention represents a 'software-based invention[] that improve[s] the performance of the computer system itself."

Id. at 1350-1351. (Emphasis added.)

In summary, *Bascom* found the claims at issue to be patent eligible because they were not simply directed to applying known filters to the Internet. Rather, they addressed a known problem with prior art filters applied to the Internet by providing a particularly-advantageous arrangement of the filters.

Similarly, the claims in the present application are not simply directed to applying the known concept of performing a transaction over the Internet. Rather, they are directed to a solution which overcomes several known problems associated with performing transactions over the Internet. Advantages are accomplished at least in part because of the arrangement of elements (including, for example, the user device and the USR), similar to the novel arrangement of filters in *Bascom*.

Accordingly, the claims are patent-eligible when viewed through the analysis provided by *Bascom* even if the claims are considered to be directed to an abstract idea. In light of the foregoing arguments, withdrawal of the rejection of claims 21-49 under 35 U.S.C. § 101 is respectfully requested.

V. Conclusion

In summary, the claims are directed to patentable subject matter pursuant to the two-step *Alice* analysis. Contrary to the Examiner's contention that the claims are directed to "receiving, and processing data and automating mental tasks," Applicant submits that the claims are directed more specifically to addressing problems associated with executing secure transactions over a network, which is not an abstract idea.

Furthermore, even if the claims did recite an abstract idea, the claims are nonetheless directed to patentable subject matter because additional elements of the claim transform the nature of the claim into a patent-eligible application by tailoring the claims specifically to the realm of computer-based transactions, and by improving the field of secure transactions over digital networks. Accordingly, the claims are believed to be in allowable condition and withdrawal of the rejection of claims 21-49 under 35 U.S.C. § 101 is respectfully requested.

Rejections Under 35 U.S.C. § 112

Claims 21-49 were rejected under 35 U.S.C. § 112(a) or 35 U.S.C. § 112 (pre-AIA), first paragraph, as allegedly failing to comply with the written description requirement. The Examiner's specific rejections are addressed in turn below.

The Examiner asserts that "[c]laim 21 recites 'the processor being programmed such that after the electronic ID device receives... the processor is configured to generate...' The language 'such that' makes the claim broader in scope than the teachings of the disclosure as it does not limit the claim to the programming described in the disclosure but only requires that it reproduce a result via any and all means." (Office Action, p. 13).

Without acceding to the correctness of the rejection, claim 21 has been amended. As amended, claim 21 does not recite the language identified by the Examiner, and the rejection thereof is therefore moot. Withdrawal of the rejection of claims 21-39 under 35 U.S.C. § 112(a) or 35 U.S.C. § 112 (pre-AIA), first paragraph, is respectfully requested.

The Examiner asserts that "[c]laims 21 and 40 recite 'a system configured to execute the secure operation...' claim 23 recites 'the system is configured to transmit the encrypted authentication information...' [...] First the specification does not provide support for a 'system' but a 'communication link.' The specification also does not have a written description of what constitutes a 'secure operation'. The specification also gives an example of a processor being the entity to 'to communicate the encrypted authentication information via the communication link to the secure registry.'" (Office Action, p. 14). Applicant has interpreted the Examiner's rejection as three separate arguments, each of which is addressed in turn below.

With reference to the Examiner's argument that "the specification does not provide support for a 'system' but a 'communication link'," Applicant respectfully requests clarification of the Examiner's argument, as Applicant is unable to understand the grounds for rejection. To the extent that Applicant has interpreted the Examiner's comments as an assertion that the "system" and the "communication link" are the same entity, Applicant notes that they are not. Furthermore, claim 21 ha been amended and no longer recites portions of the language identified by the Examiner.

With reference to the Examiner's argument that "[t]he specification also does not have a written description of what constitutes a 'secure operation'," the identified claim language no longer appears in the claims, as amended, and the rejection is therefore moot.

With reference to the Examiner's argument that "[t]he specification also gives an example of a processor being the entity to 'to communicate the encrypted authentication information via the communication link to the secure registry'," claim 23 has been canceled and the rejection thereof is therefore moot.

In light of the foregoing remarks, withdrawal of the rejection of claims 21-49 under 35 U.S.C. § 112(a) or 35 U.S.C. § 112 (pre-AIA), first paragraph, is respectfully requested.

The Examiner asserts that "[c]laims 21 and 40 recite executing a 'secure operation', 'an electronic device configured to encrypt information to enable execution of a secure operation...', 'a method of controlling execution of a secure operation....'" (Office Action, p. 15). Claims 21 and 40 have been amended, and the identified claim language no longer appears in the claims. The rejection is therefore moot. Withdrawal of the rejection of claims 21-49 under 35 U.S.C. § 112(a) or 35 U.S.C. § 112 (pre-AIA), first paragraph, is therefore respectfully requested.

The Examiner asserts that "[c]laim 24 recites 'wherein the secure operation includes a secure transaction, and wherein the system configured to perform the secure operation comprises a point-of-sale (POS) device'.... [T]he specification does not provides for a system that executes a secure transaction and it includes a POS device." (Office Actions, pp. 15-16). Claim 24 has been amended, and the identified claim language no longer appears in the claims. Accordingly, the rejection of claim 24 is moot. Withdrawal of the rejection of claim 24 under 35 U.S.C. § 112(a) or 35 U.S.C. § 112 (pre-AIA), first paragraph, is respectfully requested.

The Examiner asserts that "[c]laim 44 recites [limitations....] The specification does not disclose an actual algorithm that performs the claimed function." (Office Action, Page 17). Claim 44 has been canceled, and the rejection thereof is therefore moot. Accordingly, withdrawal of the rejection of claim 44 under 35 U.S.C. § 112(a) or 35 U.S.C. § 112 (pre-AIA), first paragraph, is respectfully requested.

Claims 21-49 were rejected under 35 U.S.C. § 112(b) or 35 U.S.C. § 112 (pre-AIA), second paragraph, as allegedly being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

The Examiner asserts that "[c]laim 21 recites 'the processor being programmed such that after the electronic ID devices receives... the processor is configured to generate...' The claim is unclear because... if the processor does not receive at least one of the biometric input and the secret authentication information that the structure in the form of the algorithm... will not exist." (Office Action, p. 17). The identified claim language no longer appears in the claims, as amended, and the rejection is therefore moot. Withdrawal of the rejection of claims 21-39 under 35 U.S.C. § 112(b) or 35 U.S.C. § 112 (pre-AIA), second paragraph, is therefore respectfully requested.

The Examiner asserts that "[c]laim 21 recites 'the processor[...] is configured to[...] encrypt the non-predictable value, information derived from at least a portion of the biometric input, and information derived from at least a portion of the secret authentication information to generate encrypted authentication information....' [... I]t is unclear how the processor would then be able to encrypt both the 'information derived from at least a portion of the biometric input, and information derived from at least a portion of the secret authentication information' when it could possibly only have received one of them." (Office Action, pp. 17-18).

Claim 21 has been amended to recite, "a processor... being programmed... to encrypt the non-predictable value **and at least one of** information derived from at least a portion of the user biometric and information derived from at least a portion of the secret authentication information." (Emphasis added.) As amended, claim 21 is clear and accurate as written. Withdrawal of the rejection of claims 21-39 under 35 U.S.C. § 112(b) or 35 U.S.C. § 112 (pre-AIA), second paragraph, is therefore respectfully requested.

The Examiner asserts that "[c]laims 21 and 40 recite 'information derived from at least a portion of the secret authentication information to generate encrypted authentication information...' The claim is unclear. The processor is set 'to encrypt the non-predictable value, information derived from at least a portion of the biometric input, and information derived from at least a portion of the secret authentication information to generate encrypted authentication information....' Yet, as written, the encryption of 'at least a portion of the secret authentication information is the piece of information that yields generated encrypted authentication information....'" (Office Action, p. 18).

Applicant respectfully disagrees that the claim as previously presented is unclear, but has amended the claims to include a comma after "secret authentication information" to advance prosecution. Withdrawal of the rejection of claims 21-40 under 35 U.S.C. § 112(b) or 35 U.S.C. § 112 (pre-AIA), second paragraph, is therefore respectfully requested.

The Examiner asserts that "[c]laims 21 and 40 recite 'execute a secure operation'. Similarly, claim 24 recites 'the secure operation'. The term 'secure' is a relative term which renders the claim indefinite." (Office Action, p. 18). Claims 21, 24, and 40 have been amended. The identified claim language no longer appears in the claims, as amended, and the rejection is therefore moot. Withdrawal of the rejection of claims 21-49 under 35 U.S.C. § 112(b) or 35 U.S.C. § 112 (pre-AIA), second paragraph, is therefore respectfully requested.

The Examiner asserts that "[c]laim 21 is directed to an 'electronic ID device', but the claim adopts circular reasoning in the explanation of not what the device comprises but what it does." (Office Action, p. 19). The Examiner also rejects claims 30, 31, 36, 37, and 39 on the same grounds. *Id.* Claims 21, 30, 31, 36, 37, and 39 have been amended. The identified claim language no longer appears in the claims, as amended, and the rejection of claims 21, 30, 31, 36, 37, and 39 is therefore moot.

The Examiner also rejects 34 on the same grounds, and asserts that "claim 34 recites 'the electronic device is configured to not permit the entry...'." *Id.* Applicant respectfully disagrees. The claim does not claim "what the device comprises but what it does." Conversely, claim 34 recites that the electronic ID device "**is configured to**...," which is a structural limitation. Accordingly, claims 22-39 are believed to be in condition for allowance and withdrawal of the rejection of claims 21-39 under 35 U.S.C. § 112(b) or 35 U.S.C. § 112 (pre-AIA), second paragraph, is therefore respectfully requested.

The Examiner asserts that "[c]laim 21 is directed towards 'an electronic device...', dependent claims for example, Claim 34 is directed towards 'an electronic device...' but recites 'the electronic ID device is configured to not...' The claim recites 'the entry of the user input' is not permitted while simultaneously reciting that the biometric input has been received. The only 'entry of the user input' made was a secret authentication information, 'the entry of the user input' alludes to a past entry. It is therefore unclear as to whether the 'entry' is to be viewed as the receiving of the biometric input or a different operation not present in the claim or there is a mistake and Applicant failed to allude to a future entry of the user input." (Office Action, p. 19).

Applicant respectfully disagrees. The Examiner's argument appears to be premised on there being confusion regarding what "the entry of the user input" refers to. However, claim 21, from which claim 34 depends, recites, "a user interface configured to receive **a user input** including...."

Applicant respectfully disagrees that a person of ordinary skill in the art would be confused as to what "the entry of the user input" refers to, in view of the fact that claim 21 explicitly recites "a user input" as a different limitation than "the biometric input" of previously-presented claim 21. Furthermore, claims 21 and 34 have been amended and portions of the cited language no longer appear in the claims.

Accordingly, Applicant submits that claims 21 and 34 are clear and accurate as written. Withdrawal of the rejection of claims 21 and 34 under 35 U.S.C. § 112(b) or 35 U.S.C. § 112 (pre-AIA), second paragraph, is therefore respectfully requested.

The Examiner asserts that "[c]laim 21 recites 'an electronic device configured to encrypt information to enable execution of a secure operation... the system configured to execute the secure operation...', claim 23 recites 'the system configured to execute the secure operation, wherein the system is configured to transmit the encrypted authentication information to a secure registry software and to receive authorization to perform the secure operation from the secure registry software.' Similarly, claims 24 and 27 recite 'the system configured to execute....' These claim limitations are directed to a system, however, claim 21 is directed towards a device and the system is not part of the device. Therefore the scope is unclear as it cannot be ascertained as to whether the scope only applies to the device of claim 21 or also encompasses elements external to the device. Furthermore, it is unclear how language directed towards an external system places a structural limitation on the device being claimed." (Office Action, pp. 19-20).

Claims 21, 23, and 24 have been amended. The identified claim language no longer appears in the claims, as amended, and the rejection is therefore moot. Withdrawal of the rejection of claims 21-39 under 35 U.S.C. § 112(b) or 35 U.S.C. § 112 (pre-AIA), second paragraph, is therefore respectfully requested.

The Examiner asserts that "[r]egarding claim 30, the claim recites 'electronic device initiates, responsive to receiving an authentication initation input from the user, authentication with the system...", however, claim 21, from which claim 30 depends, is directed to an electronic ID device of which the system if not a part of.... Therefore, it would be unclear whether infringement of claim 21 occurs based on possession of the device. *In re Katz Interactive Call Processing Patent Litigation*, 639 F.3d 1303 (Fed. Cir. 2011). *IPXL Holdings v. Amazon.com, Inc.*, 430 F.2d [*sic*] 1377, 1384, 77 USPQ2d 1140, 1145 (Fed. Cir. 2005). *Ex parte Lyell*, 17 USPQ2d 1548 (Bd. Pat. App. & Inter. 1990)." (Office Action, p. 20).

Applicant respectfully disagrees. The authority cited by the Examiner refers to claims which attempted to claim external use of claimed subject matter. For example, claim 25 of *IPXL Holdings* recited, "[t]he system of claim 2 [including an input means] wherein... **the user uses the input means** to either change the predicted transaction information or accept the displayed transaction type." 430 F.3d at 1384 (emphasis added).

The court held that claim 25 was invalid under § 112, noting that it would be unclear whether infringement of claim 25 occurs when one creates a system that allows the user to change information, or whether infringement occurs when the user actually uses the input means. *Id.*

In contrast, claim 30 as amended recites, "the electronic ID device is configured to initiate, responsive to receiving an authentication initiation input from the user, authentication with the external system." The claim recites "receiving an authentication initiation input from the user," which is a limitation on the device, not the user. Furthermore, the claim recites "the electronic ID device is configured to initiate... authentication with the external system," which is a limitation on the device, not the external system.

Accordingly, Applicant submits that claim 30 is in condition for allowance, and withdrawal of the rejection of claim 30 under 35 U.S.C. § 112(b) or 35 U.S.C. § 112 (pre-AIA), second paragraph, is therefore respectfully requested.

The Examiner notes that "[c]laim 38 recites the limitation 'the electronic serial number'. There is insufficient antecedent basis for this limitation in the claim." (Office Action, p. 21). Claim 38 has been amended to recite "an electronic serial number." Accordingly, withdrawal of the rejection of claim 38 under 35 U.S.C. § 112(b) or 35 U.S.C. § 112 (pre-AIA), second paragraph, is respectfully requested.

The Examiner asserts that "[c]laim 40 recites 'subsequent to successful authentication of the identity of the user to the electronic ID device' it is unclear how the electronic device is aware that the authentication was successful without receiving notice of it." (Office Action, p. 21).

Applicant respectfully disagrees. It is unclear why the Examiner believes that the electronic ID device should notify itself that it has successfully authenticated the identity of the user. Applicant submits that the claim is clear and accurate as written in view of the specification, and withdrawal of the rejection of claim 40-49 under 35 U.S.C. § 112(b) or 35 U.S.C. § 112 (pre-AIA), second paragraph, is therefore respectfully requested.

The Examiner asserts that "[c]laim 41 recites 'receiving at least a portion of a user's secret authentication information manually within a user interface.' The claim us unclear as to whether... the information is manually put inside an interface." (Office Action, p. 21).

Although Applicant respectfully disagrees that a person of ordinary skill in the art would interpret the foregoing limitations as manually putting an input inside of a user interface, claim 41 has been amended. The identified claim language no longer appears in the claims, as amended, and the rejection is therefore moot. Withdrawal of the rejection of claim 41 under 35

U.S.C. § 112(b) or 35 U.S.C. § 112 (pre-AIA), second paragraph, is therefore respectfully requested.

Claim 44 is rejected under 35 U.S.C. § 112(d) or pre-AIA 35 U.S.C. § 112, 4th paragraph, as being of improper dependent form for failing to further limit the subject matter of the claim upon which it depends, or for failing to include all the limitations of the claim upon which it depends. Claim 44 has been canceled, and the rejection thereof is therefore moot. Accordingly, withdrawal of the rejection of claim 44 under 35 U.S.C. § 112 is respectfully requested.

Rejections Under 35 U.S.C. § 103

Claims 21-49 stand rejected under pre-AIA 35 U.S.C. § 103(a) as allegedly being unpatentable over U.S. Patent No. 5,280,527 to Gullman et al. ("Gullman"), and further in view of U.S. Publication No. 2002/0184500 to Maritzen et al. ("Maritzen"). Applicant respectfully traverses the rejection.

Claim 21 recites, in part, "[a]n electronic ID device... comprising... a user interface configured to receive a user input including secret authentication information known to the user and a selection of the financial transaction to be executed."

Gullman is directed to "[a] security apparatus [which] receives a biometric input from a user... to generate a token. The token is displayed to the user, who then enters the token at an access device.... The access device forwards the token to the host." (Abstract). For example, the "access device 12" may be "an automated teller machine." (Column 3, Lines 27-31). The "biometric security apparatus 14" is a separate entity which may include "a power source 15, on/off switch 16, biometric sensor 18, display 20, processor 22..., biometric input section 33..., code generator 26 and display drivers 30." (Column 4, Lines 40-47).

Maritzen is directed to "providing a secure transaction and authentication system through a gaming console." (Abstract).

The Examiner asserts that "Gullman teaches... a user interface configured to receive a user input including authentication information known to the user.... (column 4, line 3-8, 39-64)." (Office Action, Page 23). Applicant respectfully disagrees.

The sections of Gullman identified by the Examiner focus on operation of the security apparatus 14. Accordingly, Applicant has interpreted the Examiner's arguments as an assertion that the security apparatus 14 teaches or suggests the "electronic ID device" of claim 21.

As illustrated by FIG. 3 of Gullman, the security apparatus 14 includes an on/off switch 16, a biometric sensor 18, and a display 20, none of which is "configured to receive a user input including authentication information **known to the user**." For example, although the biometric sensor 18 of Gullman receives a biometric input, a biometric input is not "information known to the user."

Applicant made similar arguments in the most recent Office Action response, to which the Examiner replied, "Gullman's user, inputs information gain to access so the user is allowed to perform an electronic funds transfer. Specifically, Gullman says 'the biometric security mechanism 14 generates a security token which the user inputs to the access device 12,' (Figure 1; column 4, line 1-20). **Gullman explicitly says the user inputs the information to the access device**." (Office Action, Page 7) (emphasis added).

Applicant respectfully notes that the security apparatus 14 and the access device 12 are **separate entities**. Although Gullman discloses that the user inputs information (specifically, a token) into the access device 12, the user does not input information known to the user into the security apparatus 14. Conversely, the user provides a biometric (e.g., a fingerprint, which is not "information known to a user") to the security apparatus 14, which generates and displays a token that the user inputs into the access device 12. Accordingly, Applicant disagrees with the Examiner because the Examiner is referring to features of the access device 12, not the security apparatus 14.

Alternatively, if the Examiner's position is that the access device 12 teaches or suggests the "electronic ID device" of claim 21, Applicant respectfully asserts that Gullman fails to teach or suggest "[a]n electronic ID device... comprising[] a biometric sensor," as recited by claim 21.

Accordingly, Gullman fails to teach or suggest "[a]n electronic ID device... comprising[] a biometric sensor... [and] a user interface configured to receive a user input including... authentication information known to the user."

In addition to the foregoing deficiencies, claim 21 has been amended to recite, "[a]n electronic ID device... comprising[] a biometric sensor... [and] a user interface configured to receive... **a selection of the financial transaction to be executed**." Gullman and Maritzen, whether taken alone or in combination, fail to teach or suggest the foregoing limitations. Accordingly, claim 21 is in allowable condition in view of Gullman and Maritzen.

The Examiner admits that "Gullman does not teach secret authentication information known to the user," and relies on Maritzen to cure the deficiencies of Gullman. (Office Action, Page 24). As a threshold matter, Applicant respectfully requests clarification as to what the Examiner asserts Gullman does and does not teach. Despite the Examiner's admission that "**Gullman fails to teach** secret **authentication information known to the user**," the Examiner also asserts that "**Gullman teaches**... a user interface configured to receive a user input including **authentication information known to the user**." (Office Action, Page 23). Applicant respectfully requests that the Examiner point out with specificity which limitations of the claims are believed to be taught by Gullman, and which are not.

Furthermore, Applicant maintains that there is no teaching, suggestion, or motivation to modify Gullman according to Maritzen. The Examiner relies on Maritzen to teach or suggest, "a user interface configured to receive... secret authentication information known to the user." The Examiner asserts that "it would have been obvious... to combine Gullman and Maritzen in order to provide secure authentication of a user." (Office Action, Page 24). Applicant respectfully disagrees.

As Applicant has noted in previous responses, Gullman is specifically directed to providing secure access (e.g., via ATMs) without requiring users to remember and input PINs, which can be burdensome. (See Column 1, Lines 28-55 of Gullman). Accordingly, Applicant respectfully disagreed that one would find it obvious to modify Gullman to include a user interface configured to receive a PIN, on the grounds that the entire point of Gullman is to alieve users of the need to remember PINs.

Applicant did acknowledge that Gullman discloses the use of PINs; however, there is no indication that those PINs are received from a user. A user does not enter the PINs into the security apparatus 14, because the security apparatus 14 does not have a user interface through which to enter a PIN.

In response, the Examiner asserted that "**Gullman does not teach away from the use of PINs as Applicant claims**. Gullman says 'in an exemplary embodiment... the processor executes [a] verification algorithm. The verification algorithm uses the template data, the biometric input, a fixed code (i.e., PIN, embedded serial number, account number)'." (Office Action, Page 6) (emphasis added).

However, Applicant never argued that Gullman teaches away from the use of PINs. To the contrary, **Applicant expressly acknowledged that Gullman teaches the use of PINs**. ("However, although Gullman recites the **use** of PINs...." [Response to Office Action, Page 18, submitted July 6th, 2017] [emphasis in original].)

Although Gullman teaches the **use** of PINs, however, Gullman does not disclose that the PINs are **received from a user**. The security apparatus 14 of Gullman is not capable of receiving PINs from user, such that the user does not need to remember PINs. The sections of Gullman identified by the Examiner **merely disclose the use of a PIN in a verification algorithm**, but do not disclose that the PIN has been received from a user.

Although the Examiner is correct in noting that "'receiving or requesting a PIN from a user...' [...] is not within the entered claims," Applicant does not argue that the claims recite "receiving or requesting a PIN from a user." (Office Action, Page 6). Applicant is highlighting the fact that Gullman teaches directly away from the receipt or request of PINs from a user, and that it would therefore be improper to modify Gullman according to Maritzen to include a user interface for receiving PINs from users. The proposed modification is counter to the teachings of Gullman. Accordingly, one of ordinary skill in the art would not be motivated to modify Gullman according to Maritzen to teach or suggest "a user interface configured to **receive a user input** including secret authentication information," as recited by claim 21.

In light of the foregoing remarks, Gullman and Maritzen fail to teach or suggest each and every limitation of claim 21. Furthermore, it would be improper to modify Gullman according to Maritzen, at least because Gullman expressly teaches away from receiving PINs from users. Claim 40 recites similar limitations, and is allowable for similar reasons. Claims 22-39 and 41-49 depend from claims 21 and 40, respectively, and are allowable for similar reasons. Accordingly, withdrawal of the rejection of claims 21-49 under 35 U.S.C. § 103(a) is respectfully requested.

CONCLUSION

In view of the foregoing amendments and remarks, reconsideration is respectfully requested. This application should now be in condition for allowance; a notice to this effect is respectfully requested. If the Examiner believes, after this amendment, that the application is not in condition for allowance, the Examiner is requested to call the Applicant's attorney at the telephone number listed below.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicant hereby requests any necessary extension of time. If there is a fee occasioned by this response, including an extension fee that is not covered by an accompanying payment, please charge any deficiency to Deposit Account No. 50/2762; Our Ref. W0537-701321.

Dated: December 15, 2017

Respectfully submitted,

Electronic signature: /John N. Anastasi/
John N. Anastasi
Registration No.: 37,765
LANDO & ANASTASI, LLP
Riverfront Office Park
One Main Street, Suite 1100
Cambridge, Massachusetts 02142
(617) 395-7000

Electronic Acknowledgement Receipt

EFS ID:	31237961
Application Number:	14071126
International Application Number:	
Confirmation Number:	3814
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Customer Number:	37462
Filer:	John N Anastasi
Filer Authorized By:	
Attorney Docket Number:	W0537-701321
Receipt Date:	15-DEC-2017
Filing Date:	04-NOV-2013
Time Stamp:	16:01:42
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		Response_to_NFOA_mailed_9_15_17.pdf	181990 2702d05244966c313e3bc2f286114fb4232794e8	yes	28

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	7
	Applicant Arguments/Remarks Made in an Amendment	8	28

Warnings:

Information:

Total Files Size (in bytes):	181990

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 14/071,126	Filing Date 11/04/2013	□ 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)		
AMENDMENT	**12/15/2017**	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 29	Minus	** 29	= 0	x $40 =	0
	Independent (37 CFR 1.16(h))	* 2	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)		
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	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.

SLIE
KIMBERLY WHITE

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	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/071,126	11/04/2013	Kenneth P. Weiss	W0537-701321

CONFIRMATION NO. 3814

IMPROPER CFR REQUEST

37462
LANDO & ANASTASI, LLP
ONE MAIN STREET, SUITE 1100
CAMBRIDGE, MA 02142

OC000000096159946

Date Mailed: 12/22/2017

RESPONSE TO REQUEST FOR CORRECTED FILING RECEIPT

Power of Attorney, Claims, Fees, System Limitations, and Miscellaneous

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

- Any request to correct or update the name of the applicant must include an application data sheet (ADS) in compliance with 37 CFR 1.76 specifying the correct or updated name of the applicant in the applicant information section. Any request to change the applicant after an original applicant has been specified under 37 CFR 1.46(b) must include a new ADS in compliance with 37 CFR 1.76 specifying the applicant in the applicant information section and comply with 37 CFR 3.71 and 3.73. See 37 CFR 1.46(c).

Questions about the contents of this notice and the
requirements it sets forth should be directed to the Office
of Data Management, Application Assistance Unit, at
(571) 272-4000 or **(571) 272-4200** or **1-888-786-0101**.

/rmohamed/

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
14/071,126	11/04/2013	Kenneth P. Weiss	W0537-701321

CONFIRMATION NO. 3814

IMPROPER CFR REQUEST

37462
LANDO & ANASTASI, LLP
ONE MAIN STREET, SUITE 1100
CAMBRIDGE, MA 02142

OC000000097224510

Date Mailed: 02/07/2018

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:

- The priority or continuity claim has not been entered because it was not filed during the required time period. Applicant may wish to consider filing a petition to accept an unintentionally delayed claim for priority. See 37 CFR 1.55 or 1.78.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/byemane/

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted via the Office electronic filing system in accordance with 37 C.F.R. § 1.6(a)(4).

Dated: March 8, 2018
Electronic Signature for John T. Spangenberger: /John T. Spangenberger/

Docket No.: W0537-701321
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Kenneth P. Weiss

Application No.: 14/071,126	Confirmation No.: 3814
Filed: November 4, 2013	Art Unit: 3685
For: UNIVERSAL SECURE REGISTRY	Examiner: I. I. Immanuel

Commissioner for Patents

PETITION UNDER 37 C.F.R. § 1.78(b) TO ACCEPT UNINTENTIONALLY DELAYED PRIORITY CLAIM

Applicant hereby petitions for acceptance of an unintentionally delayed priority claim.

Applicant respectfully requests entry of a late priority claim that was not recognized in an application data sheet as required under 37 C.F.R. 1.78(a)(3).

This application claims the benefit under 35 U.S.C. § 120 as a continuation of U.S. patent application No. 13/237,184 filed September 20, 2011, which is a continuation of U.S. patent application No. 12/393,586 filed February 26, 2009, which is a continuation-in-part of each of U.S. patent application serial no. 11/760,732 filed June 8, 2007, now U.S. Patent No. 7,809,651; U.S. patent application serial no. 11/760,729 filed June 8, 2007, now U.S. Patent No. 7,805,372; and U.S. patent application serial no. 11/677,490 filed February 21, 2007, now U.S. Patent No. 8,001,055. U.S. patent application No. 13/237,184 also claims the benefit under 35 U.S.C. § 120 as a continuation-in-part of U.S. patent application no. 13/168,556 filed on June 24, 2011, which claims the benefit under 35 U.S.C. § 120 as a continuation of U.S. application no. 11/677,490. Each of U.S. application nos. 11/760,732, 11/760,729 and 11/677,490 claim priority under 35 U.S.C. § 119 (e) to U.S. Provisional Application Nos. 60/812,279 filed on June 9, 2006, and 60/859,235 filed on November 15, 2006. Each of U.S. application Nos. 11/760,732 and 11/760,729 claim the benefit under 35 U.S.C. § 120 as continuations of U.S. application no.

11/677,490. U.S. application no. 11/677,490 also claims priority under 35 U.S.C. § 119(e) to U.S. Provisional Application No. 60/775,046 filed on February 21, 2006. Application serial no. 12/393,586 filed February 26, 2009 claims priority under 35 U.S.C. § 119(e) to U.S. Provisional Application Serial No. 61/031,529, titled "UNIVERSAL SECURE REGISTRY," filed on February 26, 2008. Each of the above-identified applications is hereby incorporated herein by reference in its entirety.

In compliance with the requirements set forth in 37 C.F.R. § 1.78(a)(3), a Supplemental Application Data Sheet reflecting this claim to priority and a Request for Corrected Filing Receipt reflecting the above correction are filed herewith.

The entire period of delay between the date the priority claim was due and the date of submission of the present petition was unintentional.

A payment of the surcharge set forth in § 1.17(m) is submitted herewith. Please charge any additional fees, or make any credits to Deposit Account No. 50-2762, referencing attorney Docket No. W0537-701321.

Dated: March 8, 2018

Respectfully submitted,

Electronic signature: /John T. Spangenberger/
John T. Spangenberger
Registration No.: 76,607
John N. Anastasi
Registration No.: 37,765
LANDO & ANASTASI, LLP
Riverfront Office Park
One Main Street, Suite 1100
Cambridge, Massachusetts 02142
(617) 395-7000

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted via the Office electronic filing system in accordance with 37 C.F.R. § 1.6(a)(4).

Dated: March 8, 2018
Electronic Signature for John T. Spangenberger: /John T. Spangenberger/

Docket No.: W0537-701321
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Kenneth P. Weiss

Application No.: 14/071,126

Confirmation No.: 3814

Filed: November 4, 2013

Art Unit: 3685

For: UNIVERSAL SECURE REGISTRY

Examiner: I. I. Immanuel

REQUEST FOR CORRECTED FILING RECEIPT

Office of Initial Patent Examination's Filing Receipt Corrections
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicant hereby requests that a corrected Filing Receipt be issued in the above-identified patent application. Corrections are shown by underlining for added matter and ~~strikethrough~~ for deleted matter. Please correct the Applicants' information as follows:

Domestic Priority data as claimed by applicant:

This appliction is a CON of 13/237,184 9/20/2011
which is a CIP of 13/168,556 6/24/2011
which is a CON of 11/677,490 2/21/2007
which claims benefit of 60/859,235 11/15/2006
and claims benefit of 60/812,279 6/9/2006
and claims benefit of 60/775,046 2/21/2006
and said 13/237,184 is a CON of 12/393,586 2/26/2009
which claims benefit of 61/031,529 2/26/2008
and is a CIP of 11/760,732 6/8/2007
which is a CON of 11/677,490 2/21/2007
and claims benefit of 60/812,279 6/9/2006
and claims benefit of 60/859,235 11/15/2006
and said 12/393,586 is a CIP of 11/760,729 6/8/2007
which is a CON of 11/677,490 2/21/2007
and claims benefit of 60/821,279 6/9/2006
and claims benefit of 60/859,235 11/15/2006

and said 12/393,586 is a CIP of 11/677,490 2/21/2007

Thus, the corrected filing receipt should read as follows:

Domestic Priority data as claimed by applicant:

This appliction is a CON of 13/237,184 9/20/2011
which is a CIP of 13/168,556 6/24/2011
which is a CON of 11/677,490 2/21/2007
which claims benefit of 60/859,235 11/15/2006
and claims benefit of 60/812,279 6/9/2006
and claims benefit of 60/775,046 2/21/2006
and said 13/237,184 is a CON of 12/393,586 2/26/2009
which claims benefit of 61/031,529 2/26/2008
and is a CIP of 11/760,732 6/8/2007
which is a CON of 11/677,490 2/21/2007
and claims benefit of 60/812,279 6/9/2006
and claims benefit of 60/859,235 11/15/2006
and said 12/393,586 is a CIP of 11/760,729 6/8/2007
which is a CON of 11/677,490 2/21/2007
and claims benefit of 60/821,279 6/9/2006
and claims benefit of 60/859,235 11/15/2006
and said 12/393,586 is a CIP of 11/677,490 2/21/2007

A copy of the Filing Receipt with the corrections indicated is attached. As shown above, the Domestic Priority Data is being corrected to match the Domestic Benefit Information provided in the supplemental Application Data Sheet (ADS) submitted herewith.

It is respectfully requested that the corrected Filing Receipt be issued reflecting the above-noted corrections.

A payment of the Petition for the delayed submission of a priority or benefit claim surcharge set forth in § 1.17(m) is submitted herewith. Please charge any deficiencies or overpayments to Deposit Account No. 50-2762; Our Ref. No. W0537-701321. Should any questions arise, the undersigned may be contacted at the telephone number listed below.

Dated: March 8, 2018

Respectfully submitted,

Electronic signature: /John T. Spangenberger/
John T. Spangenberger
Registration No.: 76,607
John N. Anastasi
Registration No.: 37,765
LANDO & ANASTASI, LLP
Riverfront Office Park
One Main Street, Suite 1100
Cambridge, Massachusetts 02142
(617) 395-7000

MARKED UP COPY

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
14/071,126	11/04/2013		0.00	W0537-701321	20	3

CONFIRMATION NO. 3814

37462
LANDO & ANASTASI, LLP
ONE MAIN STREET, SUITE 1100
CAMBRIDGE, MA 02142

FILING RECEIPT

OC000000065050284

Date Mailed: 11/22/2013

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)

Kenneth P. Weiss, Newton, MA;

Applicant(s)

Kenneth P. Weiss, Newton, MA;

Assignment For Published Patent Application

UNIVERSAL SECURE REGISTRY, LLC, Newton, MA

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CON of 13/237,184 09/20/2011 PAT 8577813
which is a CIP of 13/168,556 06/24/2011 PAT 8271397
which is a CON of 11/677,490 02/21/2007 PAT 8001055
which claims benefit of 60/859,235 11/15/2006
and claims benefit of 60/812,279 06/09/2006
and claims benefit of 60/775,046 02/21/2006
and said 13/237,184 09/20/2011
is a CON of 12/393,586 02/26/2009 PAT 8234220
which claims benefit of 61/031,529 02/26/2008
and is a CIP of 11/760,732 06/08/2007 PAT 7809651
which is a CON of 11/677,490 02/21/2007 PAT 8001055 and claims benefit of 60/812,279 6/9/2006
and said 12/393,586 02/26/2009 and claims benefit of 60/859,235 11/15/2006
is a CIP of 11/760,729 06/08/2007 PAT 7805372
which is a CON of 11/677,490 02/21/2007 PAT 8001055 and claims benefit of 60/812,279 6/9/2006
and said 12/393,586 02/26/2009 and claims benefit of 60/859,235 11/15/2006
is a CIP of 11/677,490 02/21/2007 PAT 8001055

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: 11/18/2013
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/071,126**
Projected Publication Date: To Be Determined - pending completion of Missing Parts
Non-Publication Request: No
Early Publication Request: No
Title

UNIVERSAL SECURE REGISTRY

Preliminary Class

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.

Corrected Application Data Sheet

Inventor Information

Inventor Number::	1
Given Name::	Kenneth
Middle Name::	P.
Family Name::	Weiss
City of Residence::	Newton
State or Province of Residence::	MA
Country of Residence::	US
Street of mailing address::	59 Sargent Street
City of mailing address::	Newton
State or Province of mailing address::	MA
Country of mailing address::	US
Postal or Zip Code of mailing address::	02458

Correspondence Information

Correspondence Customer Number::	37462

Application Information

Application Number::	14/071,126
Filing Date::	11/04/13
Application Type::	Regular
Subject Matter::	Utility

CD-ROM or CD-R?::	None
Sequence submission?::	None
Computer Readable Form (CRF)?::	No
Title::	UNIVERSAL SECURE REGISTRY
Attorney Docket Number::	W0537-701321
Request for Early Publication?::	No
Request for Non-Publication?::	No
Suggested Drawing Figure::	31
Total Drawing Sheets::	29
Small Entity?::	Yes
Petition included?::	No
Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2::	No
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::	No

Representative Information

Representative Customer Number::	37462

Domestic Priority Information

Application::	Continuity Type::	Parent Application::	Parent Filing Date::	Prior Appl Status::
This Application	Continuation of	13/237184	09/20/11	Patented
13/237184	Continuation in part of	13/168556	06/24/11	Patented
13/168556	Continuation of	11/677490	02/21/07	Patented
11/677490	Claims benefit of provisional	60/859235	11/15/06	Expired
11/677490	Claims benefit of provisional	60/812279	06/09/06	Expired
11/677490	Claims benefit of provisional	60/775046	02/21/06	Expired
13/237184	Continuation of	12/393586	02/26/09	Patented
12/393586	Claims benefit of provisional	61/031529	02/26/08	Expired
12/393586	Continuation in part of	11/760732	06/08/07	Patented
11/760732	Continuation of	11/677490	02/21/07	Patented
11/760732	Claims benefit of provisional	60/859235	11/15/06	Expired
11/760732	Claims benefit of provisional	60/812279	06/09/06	Expired
12/393586	Continuation in part of	11/760729	06/08/07	Patented
11/760729	Continuation of	11/677490	02/21/07	Patented
11/760729	Claims benefit of provisional	60/859235	11/15/06	Expired
11/760729	Claims benefit of provisional	60/812279	06/09/06	Expired

12/393586	Continuation in part of	11/677490	02/21/07	Patented

Foreign Priority Information

Applicant Information

Applicant Number::	1
Applicant Type::	Assignee
Organization Name::	UNIVERSAL SECURE REGISTRY, LLC
Street of mailing address::	59 Sargent Street
City of mailing address::	Newton
State or Province of mailing address::	MA
Country of mailing address::	US
Postal or Zip Code of mailing address::	02458

Assignee Information Including Non-Applicant Assignee Information

Signature:

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). **However, if this Application Data Sheet is submitted with the INITIAL filing of the application and either box A or B is not checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).**

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	/John T. Spangenberger/	Date (YYYY-MM-DD)	2018-03-08
Name	John T. Spangenberger	Registration Number	76,607

Electronic Patent Application Fee Transmittal

Application Number:	14071126
Filing Date:	04-Nov-2013
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Filer:	John T. Spangenberger/Erin McKissick
Attorney Docket Number:	W0537-701321

Filed as Small Entity

Filing Fees for **Utility under 35 USC 111(a)**

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
PET. DELAY SUB OR RESTORE PRIORITY-CLAIM	2454	1	1000	1000
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**1000**

Electronic Acknowledgement Receipt

EFS ID:	31997304
Application Number:	14071126
International Application Number:	
Confirmation Number:	3814
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Customer Number:	37462
Filer:	John T. Spangenberger
Filer Authorized By:	
Attorney Docket Number:	W0537-701321
Receipt Date:	08-MAR-2018
Filing Date:	04-NOV-2013
Time Stamp:	16:14:33
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$1000
RAM confirmation Number	030918INTEFSW00003201502762
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	Petition for review by the Office of Petitions	Petition_under_178b_to_accept_priority_claim.pdf	28116 54925eaa533e2a01ac95096b4667178ea8882f7d	no	2
Warnings:					
Information:					
2	Request for Corrected Filing Receipt	Request_for_Corrected_Filing_Receipt.pdf	29349 691d5367df0b9c1e00d9c75d8557fb92f0099762	no	3
Warnings:					
Information:					
3	Request for Corrected Filing Receipt	Marked_Up_Copy_of_Filing_Receipt.PDF	429078 ec0bd16aa63894f209ca11678ac2defc167c5e97	no	4
Warnings:					
Information:					
4	Application Data Sheet	Supplemental_Application_Data_Sheet.pdf	35240 75b25ac85b21d3ae9707bb59908f86b212a3b781	no	5
Warnings:					
Information:					
This is not an USPTO supplied ADS fillable form					
5	Fee Worksheet (SB06)	fee-info.pdf	30612 4b67a1b356d8b9fa92c418972cae0ff6c70fdc96	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	552395		

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.

Office of Petitions: Routing Sheet

4700

Application No. 14071126

This application is being forwarded to your office for further processing. A decision has been rendered on a petition filed in this application, as indicated below. For details of this decision, please see the document PET.OP.DEC filed on the same date as this document.

□ **GRANTED**

☒ **DISMISSED**

□ **DENIED**

Office of Petitions: Decision Count Sheet

Mailing Month 5

Application No. 14071126

14071126

For US serial numbers: enter number only, no slashes or commas. Ex: 10123456
For PCT: enter "51+single digit of year of filing+last 5 numbers", Ex. for PCT/US05/12345, enter 51512345

Deciding Official: ALESIA M. BROWN

Count (1) - Palm Credit 14071126

Decision: DISMISSED

FINANCE WORK NEEDED
□ Select Check Box for YES

DISMISSED

Decision Type: 535 - 37 CFR 1.78(a)(3) & (a)(6) UNINTENTIONAL DELAY

535

Notes:

Count (2)

Decision: n/a

FINANCE WORK NEEDED
☑ Select Check Box for YES

Decision Type: NONE

Notes:

Count (3)

Decision: n/a

FINANCE WORK NEEDED
□ Select Check Box for YES

Decision Type: NONE

Notes:

Initials of Approving Official (if required)

If more than 3 decisions, attach 2nd count sheet & mark this box □

Printed on: 5/26/2018

Office of Petitions Internal Document - Ver. 5.0

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/071,126	11/04/2013	Kenneth P. Weiss	W0537-701321	3814

37462 7590 05/31/2018
LANDO & ANASTASI, LLP
ONE MAIN STREET, SUITE 1100
CAMBRIDGE, MA 02142

EXAMINER	
IMMANUEL, ISIDORA I	

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
05/31/2018	ELECTRONIC

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

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

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@LALaw.com
CKent@LALaw.com

UNITED STATES PATENT AND TRADEMARK OFFICE

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

In re Application of :
Weiss, et al. :
Application No. 14/071,126 : DECISION ON PETITIONS
Filed: November 4, 2013 :
Atty. Dkt. No.: W0537-701321 :

This is a decision on the petition under 37 CFR §§ 1.78(c) and 1.78(e), filed March 8, 2018, to accept an unintentionally delayed claim under 35 U.S.C. §§ 119(e) and 120 for the benefit of priority to the prior-filed provisional and nonprovisional applications set forth in the concurrently filed Application Data Sheet (ADS).

A petition for acceptance of a claim for late priority under 37 CFR §§ 1.78(c) and 1.78(e) is only applicable after the expiration of the period specified in 37 CFR §§ 1.78(a)(4) and 1.78(d)(3). In addition, the petition under 37 CFR §§ 1.78(c) and 1.78(e) must be accompanied by:

(1) the reference required by 35 U.S.C. §§ 120 and 119(e) and 37 CFR §§ 1.78(d)(2) and 1.78(a)(3) of the prior-filed application, which must be filed in an Application Data Sheet, unless previously submitted;
(2) the petition fee set forth in § 1.17(m); and
(3) a statement that the entire delay between the date the claim was due under 37 CFR §§ 1.78(d)(3) and 1.78(a)(4) and the date the claim was filed was unintentional. The Director may require additional where there is a question whether the delay was unintentional.

The petition does not comply with item (1). Preliminary review of applicants' claim for priority reveals that the claim for priority as set forth on the updated ADS cannot be entered because it is not fully supported by the prior application to which priority is claimed. A proper benefit claim to a chain of prior applications must include proper references to each prior application in order to establish copendency throughout the entire chain of prior applications. Appropriate references must have been made in each intermediate application in the chain of prior applications. In other words, a benefit claim to a chain of prior applications will only be effective if each prior application actually includes a proper benefit chain.

The continuity data of record for App. No. 13/237,184 does not reflect that 11/760,732 is a continuation of 11/677,490.

The continuity data of record for App. No. 13/237,184 does not reflect that 11/760,729 is a continuation of 11/677,490.

Review of the priority data of record for the earlier filed applications is suggested.

Any request for reconsideration must include an updated Application Data Sheet in compliance with 37 CFR 1.76(c)(2).

Request for reconsideration of this decision does not require additional petition fee.

Further correspondence with respect to this matter should be delivered through one of the following mediums:

By mail: Mail Stop PETITIONS
Commissioner for Patents
Post Office Box 1450
Alexandria, VA 22313-1450

By hand: Customer Service Window
Mail Stop Petitions
Randolph Building
401 Dulany Street
Alexandria, VA 22314

By fax: (571) 273-8300
ATTN: Office of Petitions

By internet: EFS-Web[1]

Any questions concerning this matter may be directed to the undersigned at (571) 272-3205.

/ALESIA M. BROWN/

Alesia M. Brown
Attorney Advisor
Office of Petitions

[1] www.uspto.gov/ebc/efs_help.html (for help using EFS-Web call the Patent Electronic Business Center at (866) 217-9197)

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/071,126	11/04/2013	Kenneth P. Weiss	W0537-701321	3814

37462 7590 06/14/2018

LANDO & ANASTASI, LLP
ONE MAIN STREET, SUITE 1100
CAMBRIDGE, MASSACHUSETTS 02142
UNITED STATES OF AMERICA

EXAMINER	
IMMANUEL, ISIDORA I	

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
06/14/2018	ELECTRONIC

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

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

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

CKent@LALaw.com
docketing@LALaw.com

Office Action Summary	Application No. 14/071,126	Applicant(s) Weiss, Kenneth P.	
	Examiner ISIDORA I IMMANUEL	**Art Unit** 3685	**AIA Status** No

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 12/15/2017.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☑ This action is **FINAL.** 2b) ☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 21-22,24-26,28-37,39-43 and 45-53 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 21-22,24-26,28-37,39-43 and 45-53 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

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

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)

2) ☑ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b)
Paper No(s)/Mail Date 10/13/2017, 10/23/2017, 12/14/2017.

3) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

DETAILED ACTION

Acknowledgements

1. This office action is in response to the claims filed 12/15/2017.

2. Claims 1-20, 23, 27, 38 and 44 are cancelled.

3. Claims 21, 22, 29-31, 33-37, 39-41, 43, 45-47 and 49 are amendment.

4. Claims 50-53 are new.

5. Claims 21, 22, 24-26, 28-37, 39-43 and 45-53 are pending.

6. Claims 21, 22, 24-26, 28-37, 39-43 and 45-53 have been examined.

Notice of Pre-AIA or AIA Status

7. The present application is being examined under the pre-AIA first to invent provisions.

Response to Amendment/Arguments

8. Applicant's arguments filed 12/15/2017 have been fully considered but they are not persuasive.

9. 101

10. The 101 rejection is based on *Alice Corporation Pty. Ltd. v. CLS Bank International, et al*, 573 U.S.___ , 134 S.Ct. 2347 (2014), a case decided by the Supreme court of the United States, therefore making *Alice* the prevailing and governing decision in subject matter eligibility.

11. Applicant's claims recite "receiving… an indication... receiving… a user biometric …authenticating an identity… generating…a non-predictable value and encrypted authentication information and ... communicating the encrypted authentication information …." First, the limitations of the method claims do not require a computer to execute them, a person can carry out the steps, for example a person can verify a user's biometric identity, provide an unpredictable value and an encryption is a mathematical operation that can be performed by a person. Secondly, even with a computer, the computer would be performing conventional functions of a computer such as sending, receiving, comparing and encrypting information. Applicant argues the claims "are directed to a solution which overcomes several known problems associated with performing transactions over the internet". The possible internet usage recited in Applicant's limitations are directed to the transmission and receipt of data, all other limitations are performed within one device, with no limitations reciting its network usage. Applicant has not shown what technological improvement their claims make to transmitting data over the internet. There is no demonstration of an improvement or enhancement to the particular technological environment.

12. 112

13. Claim 21 recites "to encrypt the non-predictable value and at least one of information derived from at least a portion of the user biometric and information derived from at least a portion of the secret authentication information, to generate encrypted authentication information..." and claim 40 recites " encrypting, by the electronic ID device, the non-predictable value, information derived from at least a portion of the user biometric, and information derived from at least a portion of the secret authentication

information to generate encrypted authentication information" According to the specification (¶ 275, 276), "the processor is configured to generate a non-predictable value and to generate encrypted authentication information from the non-predictable value, the identifying information, and at least one of the information concerning the biometric input and the secret information, and to communicate the encrypted authentication information via the communication link to the secure registry…." The specification requires the use of essential additional information, "identifying information", that is missing, but needed, to generate the "encrypted authentication information". "When examining computer-implemented functional claims, examiners should determine whether the specification discloses the computer and the algorithm (e.g., the necessary steps and/or flowcharts) that perform the claimed function in sufficient detail such that one of ordinary skill in the art can reasonably conclude that the inventor invented the claimed subject matter". See MPEP 2161.01. The recited claims leave out essential elements of the limitations and therefore the claims are broader than the teachings of the disclosure (MPEP 2163.05 I A).

14. 103

15. In response to applicant's argument that there is no teaching, suggestion, or motivation to combine the references, the examiner recognizes that obviousness may be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988), *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992), and *KSR*

International Co. v. Teleflex, Inc., 550 U.S. 398, 82 USPQ2d 1385 (2007). In this case, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Gullman to Maritzen. Applicant's proposed invention teaches a user device is configured to allow a user to select any one of a plurality of accounts associated with the user to employ in a financial transaction. In one embodiment, the user device includes a biometric sensor configured to receive a biometric input provided by the user, for authenticating identity or verifying the identity of individuals and other entities seeking access to certain privileges and for selectively granting privileges. Gullman teaches a security apparatus receives a biometric input from a user, if access to such system is permitted the user is allowed to perform an electronic funds transfer. Maritzen teaches that the invention allows a consumer to utilize a game console to conduct secure transactions and authenticate the identity of the consumer using the game console. Both art utilize PINs, and Gullman does not teach away from the use of PINs as Applicant claims. Gullman says "in an exemplary embodiment of the invention, the biometric security mechanism is an integrated circuit card including a processing unit, memory and a biometric sensor. The memory stores a template of the authorized user's biometric information, along with a verification algorithm. Upon entry of the cardholder's biometric information, the processor executes the verification algorithm. The verification algorithm uses the template data, the biometric input, a fixed code (i.e., PIN, embedded serial number, account number)" and also "for a successful biometric entry or where the user is not informed of a failed biometric entry, the correlation factor is combined with a fixed code (i.e., PIN, embedded serial number, account number)" (column 2, line 48-65, column 4, line 3-11).

Applicant also argues that Gullman does not recite "receiving or requesting a PIN from a user…." This argued limitation is not within the entered claims for this particular application. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

16. Gullman says "the biometric security mechanism 14 generates a security token which the user inputs to the access device 12," (Figure 1; column 4, line 1-20). Gullman explicitly says the user inputs the information to the access device. The Pin used in Gullman is an example of authentication information known to a user. Maritzen's secure operation to be executed is for a consumer to utilize a game console to conduct secure transactions. Maritzen also teaches a user interface (¶ 28) saying "A variety of user interfaces may be used. In one embodiment, and input device may be incorporated on the transaction device. Alternately, a supplemental 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 point-of-sale terminals including a personal point-of-sale terminal."

17. First, Applicant's disclosure does not teach a selection of the financial transaction to be executed, (See 112(a) rejection). Maritzen teaches a selection of the financial transaction to be executed (¶ 24, 60, 90). According to Maritzen, " In one embodiment, the personal transaction **170** is configured to control the individual accounts by way of entering a unique biometric identifier associated with that particular account. Further, the user may select different information by entering unique biometric identifiers through the personal transaction device **170**. In Block **1020**, a secure link is

automatically established between the merchant bank and the selected consumer account designated by the consumer through the profile information without additional interaction by the consumer or the merchant."

Claim Rejections - 35 USC § 101

18. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers anynew and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

19. Claims 21, 22, 24-26, 28-37, 39-43 and 45-53 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Subject Matter Eligibility Standard

20. When considering subject matter eligibility under 35 U.S.C. 101, it must be determined whether the claim is directed to one of the four statutory categories of invention, i.e., process, machine, manufacture, or composition of matter. If the claim does fall within one of the statutory categories, it must then be determined whether the claim is directed to a judicial exception (i.e., law of nature, natural phenomenon, and abstract idea), and if so, it must additionally be determined whether the claim is a patent-eligible application of the exception. If an abstract idea is present in the claim, any element or combination of elements in the claim must be sufficient to ensure that the claim amounts to significantly more than the abstract idea itself. Examples of abstract ideas include fundamental economic practices; certain methods of organizing human activities; an idea itself; and mathematical relationships/formulas. (*Alice Corporation Pty. Ltd. v. CLS Bank International, et al. US Supreme Court, No. 13-298, June 19, 2014*).

Analysis

21. In the instant case, claim 40 is directed to a method and claim 21 is directed to a product.

22. The claim recites "receiving... an indication... receiving... a user biometric ...authenticating an identity... generating...a non-predictable value and encrypted authentication information and ... communicating the encrypted authentication information ...." Additionally, the claim is directed towards a fundamental economic practice, in this case receiving information to authenticate a customer, creating a pin for the customer, encrypting the customer authentication information and sending the information. This case is which is similar to Alice which dealt with intermediate settlement (*Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 573 U.S. __, 134 S. Ct. 2347, 2356 (2014)). The encryption of data (without exposing information) is also the abstract idea, of an algorithm, and an idea of itself. The second part of Alice is to identify the technology in the claim, and if present, determine whether the technology is merely automating or implementing the abstract idea. In this case, "The computer system may be a general purpose computer system" mentioned are implementing the abstract idea, see ¶ 68, 69, PGPub.

23. Therefore, based on case law precedent, the claims are claiming subject matter similar to concepts already identified by the courts as dealing with abstract ideas. See Alice Corp. Pty. Ltd., 134 S.Ct. at 2356 (citing Bilski v. Kappos, 561, U.S. 593, 611 (2010)). Claim 21 is directed towards the generic computer used to implement the method of claim 40 and is therefore also directed towards a judicial exception regarding an abstract idea involving the receiving and processing data, based on case law

precedent, is claiming subject matter similar to concepts identified by the courts as dealing with abstract ideas.

24. Taking the claim elements separately, the functions performed by the machine at each step of the process are purely conventional. Using a processor, using a device for receiving, sending, authenticating, encrypting and processing data. All of these functions are well-understood, routine, conventional activities previously known to the industry. In short, each step does no more than require a generic computer to perform generic computer functions.

25. The claims do not include additional elements that are sufficient to amount to significantly more than the judicial exception because the elements of "authenticating an identity" are drawn to data comparisons in SmartGene and "activating the electronic device..." as explained by Applicant's specification (PGPub¶ 255) is "the user device **352** is activated for a transaction when the user satisfactorily completes an authentication process with the device", as the device is already in use, "activating" is drawn to the using of the device for transactions as in automation of tasks in Classen and receiving and processing data in Alice (Alice Corp. Pty. Ltd. v. CLS Bank Int'l, 573 U.S. __, 134 S. Ct. 2347, 2356 (2014)), electronic recordkeeping (Alice Corp. Pty. Ltd. v. CLS Bank Int'l, 573 U.S. __, 134 S. Ct. 2347, 2356 (2014)), automating mental tasks (Bancorp Services LLC v. Sun Life Assurance Co. of Canada (U.S.), 103 USPQ2d 1425 (Fed. Cir. 2012), (Cybersource Corp. v. Retail Decisions, Inc., 654 F.3d 1366, 1372 (Fed. Cir. 2011)) and receiving or transmitting data over a network, e.g., using the Internet to gather data (Ultramercial, Inc. v. Hulu, LLC, 772 F.3d 709, 714-15 (Fed. Cir. 2014), (buySAFE, Inc. v. Google, Inc., 765 F.3d 1350, 1355 (Fed. Cir. 2014),

(Cyberfone Systems, LLC v. CNN Interactive Group, Inc., 558 Fed. Appx. 988, 993 (Fed. Cir. 2014)).

26. Viewed as a whole, instructions/method claims simply recite the concept of receiving and processing data as performed by a generic computer. The method claims do not, for example, purport to improve the functioning of the computer itself. Nor do they effect an improvement in any other technology or technical field. Instead, the claims at issue amount to nothing significantly more than an instruction to apply the abstract idea of receiving and processing data using some unspecified, generic computer. See Alice Corp. Pty. Ltd., 134 S.Ct. at 2360.

27. The use of a device implementing the abstract idea does not render the claim patent eligible because it does not provide meaningful limitations beyond generally linking the use of an abstract idea to a particular technology environment and requires no more than a generic computer to perform generic computer functions.

Conclusion

28. The claim as a whole, does not amount to significantly more than the abstract idea itself. This is because the claim does not affect an improvement to another technology or technical filed; the claim does not amount to an improvement to the functioning of a computer system itself; and the claim does not move beyond a general link of the use of an abstract idea to a particular technological environment.

29. Accordingly, the Examiner concludes that there are no meaningful limitations in the claim that transform the judicial exception into a patent eligible application such that the claim amounts to significantly more than the judicial exception itself.

30. Dependent claims do not resolve the deficiency of independent claims and accordingly stand rejected under 35 USC 101 based on the same rationale.

31. Dependent claims 22, 24-26, 28-37, 39, 41-43 and 45-53 are also rejected.

Claim Rejections - 35 USC § 112

32. The following is a quotation of the first paragraph of 35 U.S.C. 112(a):

> (a) IN GENERAL.—The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor or joint inventor of carrying out the invention.

The following is a quotation of the first paragraph of pre-AIA 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor of carrying out his invention.

33. Claims 21, 22, 24-26, 28-37, 39-43 and 45-53 are rejected under 35 U.S.C. 112(a) or 35 U.S.C. 112 (pre-AIA), first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor or a joint inventor, or for pre-AIA the inventor(s), at the time the application was filed, had possession of the claimed invention.

34. Claim 21 recites "to encrypt the non-predictable value and at least one of information derived from at least a portion of the user biometric and information derived from at least a portion of the secret authentication information, to generate encrypted authentication information..." and claim 40 recites " encrypting, by the electronic ID device, the non-predictable value, information derived from at least a portion of the user

biometric, and information derived from at least a portion of the secret authentication information to generate encrypted authentication information" According to the specification (¶ 275, 276), "the processor is configured to generate a non-predictable value and to generate encrypted authentication information from the non-predictable value, the identifying information, and at least one of the information concerning the biometric input and the secret information, and to communicate the encrypted authentication information via the communication link to the secure registry…." The specification requires the use of essential additional information, "identifying information", that is missing, but needed, to generate the "encrypted authentication information". "When examining computer-implemented functional claims, examiners should determine whether the specification discloses the computer and the algorithm (e.g., the necessary steps and/or flowcharts) that perform the claimed function in sufficient detail such that one of ordinary skill in the art can reasonably conclude that the inventor invented the claimed subject matter". See MPEP 2161.01. The recited claims leave out essential elements of the limitations and therefore the claims are broader than the teachings of the disclosure (MPEP 2163.05 I A). Dependent claims 22, 24-26, 28-37, 39, 41-43 and 45-53 are also rejected.

35. Claim 21 recites "a selection of the financial transaction to be executed" and Claim 46 recites "displaying options for selection of the external system…" According to the specification (¶ 148, 270, 284), "According to this embodiment, the user selects from the plurality of secure systems **1804** a secure system that the user would like to access. With the access device **1802**, the user communicates authentication information directly to the selected secure system **1804**, e.g., without gaining access to the

system….Accordingly, the POS device **354** may be employed to select from a plurality of users to conduct a transaction. For example, where an image of each of the users in the vicinity is displayed at the POS device **354**, the individual operating the POS device **354** may select the user (and associated accounts) by selecting the photo of the user who is employing the user device **352** for the current transaction." The specification presents multiple options for "a user interface" to choose options of the external system. The specification does not provide support for a selection of a financial transaction, there are selections of accounts but not financial transactions. The claim limitation is broad as to what options for selection of the external system, the arbitrary user interface displays information. Therefore, the claim is broader than the teachings of the disclosure (MPEP 2163.05 I A). Dependent claims 22, 24-26, 28-37, 39, 50 and 51 are also rejected.

36. Claim 29 recites "the user interface is configured to initiate authentication with the external system, responsive to receiving, from a user, a manually-entered secret code…" According to the specification (¶ 105, 106, 110, 116, 131, 133), "the user initiates a purchase (**800**), enters a secret code in the electronic ID device (**802**) and presents the resultant code to the merchant … the user enters a secret code into the electronic ID card and presents the resulting code to the merchant along with the check …the user initiates an anonymous purchase by entering a secret code into the electronic ID device and transmitting the result to the on-line merchant…the user enters a secret code in the electronic ID device and provides the electronic ID code to the party." The specification teaches a user initiating a purchase by entering information into the electronic ID device and presenting the electronic ID device to the merchant or third

party. The specification does not provide support for a user interface that initiates communication and an authentication with a third party based on a user's manual input. There is additionally no algorithm provided that accounts for an interface initiating authentication with an external system.

37. Claim 37 recites "the electronic ID device is configured to decrypt encrypted data stored in a memory, responsive to successfully authenticating…." According to the specification (¶ 178-183, 186), "the public key of a first user, for example, stored in memory **24**of the second wireless device can be used to decrypt the DES key, and the DES key can be used to decrypt at least a portion of the biometric data of the first user to use in the authentication of the identity of the first user." In the specification, information stored in the memory is decrypted and used in "authentication of the identity of the first user." This is a stark contrast from the claim limitations that recite decrypting the encrypted stored information responsive to successful authentication. Unlike the supported material in the specification, where the decrypted information is used in authenticating the user, the claim language first performs an authentication before the decryption. The claim limitation is not supported by the disclosure.

38. Claim 40 recites "receiving… an indication of a selection…", similarly, claim 51 recites "communicate…information indicative…" and claim 52 recites "communicating the indication of selection…." According to the specification (¶ 18, 163, 165, 211, 225), "the secure system receives an indication from the USR concerning whether the entity is authorized to access the system. In one embodiment, the indication is transmitted from the USR to the secure system via the Internet. At stage **2016**, the secure system grants or denies the entity access to the secure system based on the indication

received from the USR. The processor **138** may also be configured to provide signals to operate the indicating light **148**. The indicating light **148** may provide an indication of the operational status of the converter device **102**, for example, the indicating light… the converter device **102** may receive an indication that the user has sufficient funds to cover the amount of the check that is presented at a point of sale. Alternatively, or in addition, the information may include indicia related to the authorized holder of the user device **104**, such as a picture ID." The specification provides numerous examples of what could be possible indicia or indications used. The claim limitations cover the breadth of possibilities that are not necessarily limited to those posed in the specification, and therefore the claim is broader than the teachings of the disclosure (MPEP 2163.05 I A). Dependent claims 41-43, 45-49, 52 and 53 are also rejected.

39. Claim 53 recites "communicating a discrete code associated with the electronic ID device to the external system." According to the specification (¶ 262), "In one embodiment, the discrete code is unique to the user device **352**. In accordance with one embodiment, the discrete code is inaccessible to an individual in possession of the device. Further, the discrete code may be maintained by the user device **352** such that any indication that the security of the device is compromised results in the discrete code being set to a default value (for example, zero) which effectively prevents valid authentication information from being generated by the user device **352**." First, the specification does not provide support for communicating the discrete code to the external system. Secondly, the specification presents the "user device" as the structure that maintains the discrete code. Finally, the specification explains that "the discrete code is inaccessible to an individual in possession of the device". The disclosure does

not provide support for the communication of a discrete code to the external system, or an open ended possibility of actors that enact the claimed step which makes the claim broader than the teachings of the disclosure (MPEP 2163.05 I A).

40. The following is a quotation of 35 U.S.C. 112(b):

> (b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

41. Claims 21, 22, 24-26, 28-37, 39-43 and 45-53 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

42. Claim 21 is directed to an “electronic ID device for performing a financial transaction… comprising”, However, the body of the following claims, for example claim 30 recites “wherein the electronic ID device initiates…”, claim 31, “wherein the electronic ID device is further configured to communicate…”, claim 36, “wherein the electronic ID device is further configured to prevent…”, claim 37, “wherein the electronic ID device is further configured to decrypt…”, and claim 39, “wherein the electronic ID device is further configured to execute…”, therefore, the scope of the claim is unclear as an electronic ID device cannot comprise itself, that is circular reasoning. Similarly, See *In re Zletz*, 13 USPQ2d 1320 (Fed. Cir. 1989)(“An essential purpose of patent examination is to fashion claims that are precise, clear, correct, and unambiguous. Only in this way can uncertainties of claim scope be removed…”).

43. Claim 21 is directed towards “an electronic device…”, dependent claims for example, Claim 34 is directed towards “an electronic device…” but recites “the electronic ID device is configured to not permit entry of the user input….” The claim recites “the entry of the user input” is not permitted while simultaneously reciting that the user biometric has been received. The only “entry of the user input” made was a secret authentication information. The claim is unclear as to where within the scope of claim 21, the biometric is received, authenticated and the electronic ID device is alerted to the conclusion of the authentication and then gives a command to not allow a user input. The claim language is indefinite as to whether the “entry” is to be viewed as occurring after receiving of the biometric or a different operation not present in the claim or there is a mistake and Applicant failed to allude to a future entry of the user input that is somehow dependent on unspecified operations not within the scope of claim 21.

44. Claim 21 is directed to “an electronic ID device for performing a financial transaction between an authenticated user and a second party….” Claim 22 recites “the external system configured to execute the financial transaction. The scope of the claims is indefinite. The claim is unclear as to whether the electronic ID device or the external system performs or executes the financial transaction, or whether the words perform and execute are being used in different ways than their regular meaning and whether Applicant intended the scope of claim 21 to be an embodiment where the electronic ID device facilitates the financial transaction and claim 22 is another embodiment where the external system facilitates the financial transaction. The scope of the claims are unclear.

45. Claim 21 is directed to "an electronic ID device for performing a financial transaction between an authenticated user and a second party…." and claim 22 recites "the external system configured to execute the financial transaction." Both claims are directed to a product. However, the scope of claim 22 is unclear, as the cited language is not directed to the product but how the external system, not a part of the product, performs. *In re Katz Interactive Call Processing Patent Litigation*, 639 F.3d 1303 (Fed. Cir. 2011). *IPXL Holdings v. Amazon.com, Inc.*, 430 F.2d 1377, 1384, 77 USPQ2d 1140, 1145 (Fed. Cir. 2005). *Ex parte Lyell*, 17 USPQ2d 1548 (Bd. Pat. App. & Inter. 1990).

46. Claim 40 recites "authenticating an identity of the user **to** the electronic ID device… and received by the electronic ID device… subsequent to successful authentication of the identity of the user to the electronic ID device…." The claim is unclear and indefinite as to whether applicant is claiming the authentication of user identity and the receipt of the authentication by the electronic ID device. Also, if the device receives the authentication, it is unclear what entity performs the authentication, as the authentication is claimed "to" and "received by" the electronic ID device. Additionally, it is unclear how the electronic device is aware that the authentication was successful without receiving notice of it. Dependent claims 41-43, 45-49, 52 and 53 are also rejected.

47. Claim 40 recites "authenticating an identity of the user **to** the electronic ID device… and received by the electronic ID device… subsequent to successful authentication of the identity of the user to the electronic ID device…." Claim 43 recites "determining, by the electronic ID device, that the identity of the user is not successfully

authenticated ....” The scope of claim 40, from which claim 43 depends, involves the successful authentication of the identity of the user. Claim 43 is therefore unclear and indefinite as to where within the scope of claim 40 a determination is made that the authentication was not successful.

Claim Rejections - 35 USC § 103

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

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

49. Claims 21, 22, 24-26, 28-37, 39-43 and 45-53 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Gullman et al (5,280,527) (“Gullman”), and further in view of Maritzen et al. (2002/0184500) (“Maritzen”).

50. Regarding claims 21 and 40, Gullman teaches a biometric sensor configured to receive a user biometric comprising at least one of a user fingerprint and facial scan information (Abstract; Figure 2; column 4, line 39-49, column 5, line 42-54); a user interface configured to receive a user input including secret authentication information known to the user (column 3, line 37-46, column 4, line 3-8, 39-64); a communication interface configured to communicate with an external system column3, line 50-55, column 4, line 13-20, 29-36, column 6, line 35-40); a processor coupled to the biometric sensor, the user interface, and the communication interface, and being programmed to generate, responsive to receiving at least one of the user biometric and the secret authentication information, a non-predictable value (column 3, line 19-55, column 4, line

3-61, column 6, line 8-20) and to encrypt the non-predictable value and at least one of information derived from at least a portion of the user biometric and information derived from at least a portion of the secret authentication information, to generate encrypted authentication information (column 3, line 37-46, column 5, line 15-33; claim 1), and to communicate the encrypted authentication information via the communication interface to the external system (Abstract; column 4, line 29-36; column 6, line 35-61; claim 1).

Gullman does not teach and a selection of the financial transaction to be executed. Maritzen teaches and a selection of the financial transaction to be executed (¶ 24, 60, 90). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Gullman and Maritzen in order to provide secure authentication of a user to prevent unauthorized access (Maritzen; ¶ 2-4).

51. Regarding claim 22, Maritzen teaches wherein the communication interface comprises a transmitter configured to wirelessly transmit the encrypted authentication information to the external system configured to execute the financial transaction (¶ 23, 27, 35, 39, 42).

52. Regarding claim 24, Gullman teaches wherein the processor is configured to communicate the encrypted authentication information via the communication interface (Abstract; column 4, line 29-36, column 6, line 35-61; claim 1). Maritzen teaches wherein the communication interface is configured to communicate with a point-of-sale (POS) device, and to the POS device (¶ 23, 27, 35, 39, 42). Gullman does not teach and a selection of the financial transaction to be executed. Maritzen teaches and a selection of the financial transaction to be executed (¶ 24, 60, 90). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to

combine Gullman and Maritzen in order to provide secure authentication of a user to prevent unauthorized access (Maritzen; ¶ 2-4).

53. Regarding claim 25, Maritzen teaches wherein the user interface is configured to display options for purchase (¶ 18, 30, 33, 74, 81).

54. Regarding claim 26, Maritzen teaches wherein the user interface is configured to accept user selection of at least one product or service for purchase (¶ 30, 33, 69, 74, 81).

55. Regarding claim 28, Maritzen teaches wherein the electronic ID device comprises a discrete code associated with the electronic ID device (¶ 37).

56. Regarding claim 29, Gullman teaches wherein the user interface is configured to initiate authentication with the external system responsive to receiving, from a user, a manually-entered secret code (column 3, line 56-68, column 6, line 9-16).

57. Regarding claim 30, Gullman teaches wherein the electronic ID device is configured to initiate, responsive to receiving an authentication initiation input from the user, authentication with the external system (column 3, line 56-64, column 6, line 9-16).

58. Regarding claim 31, Gullman teaches wherein the electronic ID device is further configured to communicate at least a portion of the user biometric received by the biometric sensor to a secure registry software prior to generation of the encrypted authentication information (column 3, line 44-48, column 5, line 57-65).

59. Regarding claim 32, Maritzen teaches wherein the user interface is configured to receive the secret authentication information including the identifying information (¶ 57, 61, 62, 77).

60. Regarding claim 33, Gullman teaches further comprising a memory coupled to the processor, wherein the memory stores information employed by the electronic ID device to authenticate the user biometric received by the biometric sensor (column 3, line 44-48, column 5, line 57-65).

61. Regarding claim 34, Gullman teaches wherein the electronic ID device is configured to not permit entry of the user input if the user biometric received by the biometric sensor is determined to not belong to an authorized user of the electronic ID device (column 3, line 37-55).

62. Regarding claim 35, Gullman teaches wherein the secret authentication information known to the user includes a Personal Identification Number (PIN), and wherein the processor is configured to generate the non-predictable value and the encrypted authentication information responsive to authentication of both the secret authentication information and the user biometric (column 3, line 37-68, column 4, line 3-36, column 5, line 15-33; claim 1).

63. Regarding claim 36, Gullman teaches until the electronic ID device successfully authenticates at least one of the user biometric and the secret authentication information(column 3, line 19-55, column 4, line 3-61, column 5, line 64-68, column 6, line 8-20). Maritzen teaches wherein the electronic ID device is configured to prevent access by an individual in possession of the electronic ID device to data stored in a memory (¶ 74, 81). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Gullman and Maritzen in order to provide secure authentication of a user to prevent unauthorized access (Maritzen; ¶ 2-4).

64. Regarding claim 37, Gullman teaches wherein the electronic ID device is configured to decrypt encrypted data stored in a memory (column 5, line 15-33, column 6, line 35-45). Maritzen teaches responsive to successfully authenticating at least one of the user biometric and the secret authentication information (¶ 55-57, 70, 77). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Gullman and Maritzen in order to provide secure authentication of a user to prevent unauthorized access (Maritzen; ¶ 2-4).

65. Regarding claim 39, Gullman teaches wherein the electronic ID device is configured to execute a challenge-response protocol as part of authentication with the external system (column 3, line 37-68, column 4, line 8-11).

66. Regarding claim 41, Maritzen teaches an act of receiving at least a portion of a user's secret authentication information a user interface (¶ 22, 57).

67. Regarding claim 42, Gullman teaches further comprising an act of displaying, on a user interface, indicators for a plurality of user accounts stored in a memory of the electronic ID device (column 5, line 57-65).

68. Regarding claim 43, Maritzen teaches further comprising determining, by the electronic ID device, that the identity of the user is not successfully authenticated to the electronic ID device (¶ 57, 59) entering, by the electronic ID device, de-active state without generating the encrypted authentication information responsive to determining that the identity of the user is not successfully authenticated to the electronic ID device (¶ 57).

69. Regarding claim 45, Gullman teaches further comprising an act of generating the encrypted authentication information in a manner that allows identification of the user

and a selected one of a plurality of user accounts by secure registry software (column 4, line 23-36, column 5, line 57-65).

70. Regarding claim 46, Maritzen teaches further comprising displaying options for selection of the external system on a user interface (¶ 33, 69, 74).

71. Regarding claim 47, Gullman teaches further comprising selecting with the user interface at least one product, service, or financial transaction (Abstract; column 3, line 50-55, column 4, line 59-62; claim 2, 3).

72. Regarding claim 48, Maritzen teaches further comprising maintaining an audit trail of purchases made (¶ 32, 42, 82).

73. Regarding claim 49, Gullman teaches initiating an authentication request on the electronic ID device and triggering communication of the encrypted authentication information from the electronic ID device to the external system (column 3, line 56-68, column 4, line 50-64).

74. Regarding claims 50 and 53, Gullman teaches wherein the processor is further configured to communicate, via the communications interface, the discrete code to the external system (column 3, line 37-68, column 4, line 3-22).

75. Regarding claim 51, Maritzen teaches wherein the processor is further programmed to communicate, via the communications interface, information indicative of the selection of the financial transaction to be executed to the external system (¶ 24, 60, 90).

76. Regarding claim 52, Maritzen teaches communicating the indication of the selection of the user account from the electronic ID device to the external system (¶ 24, 60, 90).

Conclusion

77. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ISIDORA I IMMANUEL whose telephone number is (469)295-9094. The examiner can normally be reached on Monday-Friday 9:00 am to 5:00pm.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, NEHA PATEL can be reached on 571-270-1492. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/I.I.I./
Examiner, Art Unit 3685

/NEHA PATEL/
Supervisory Patent Examiner, Art Unit 3685

Notice of References Cited	Application/Control No. 14/071,126	Applicant(s)/Patent Under Reexamination Weiss, Kenneth P.
	Examiner ISIDORA I IMMANUEL	Art Unit 3685 — Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	5,280,527 A	01-1994	Gullman; Lawrence S.	G06K19/0718	713/184
*	B	2002/0184500 A1	12-2002	Maritzen, Michael	G06Q20/18	713/170
	C					
	D					
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Index of Claims	**Application/Control No.** 14/071,126	**Applicant(s)/Patent Under Reexamination** Weiss, Kenneth P.
	Examiner ISIDORA I IMMANUEL	**Art Unit** 3685

✓	**Rejected**	-	**Cancelled**	N	**Non-Elected**	A	**Appeal**
=	**Allowed**	÷	**Restricted**	I	**Interference**	O	**Objected**

CLAIMS

□ Claims renumbered in the same order as presented by applicant □ CPA □ T.D. □ R.1.47

CLAIM		**DATE**								
Final	Original	08/21/2016	03/18/2017	08/07/2017	09/05/2017	04/05/2018				
	1	-	-	-	-	-				
	2	-	-	-	-	-				
	3	-	-	-	-	-				
	4	-	-	-	-	-				
	5	-	-	-	-	-				
	6	-	-	-	-	-				
	7	-	-	-	-	-				
	8	-	-	-	-	-				
	9	-	-	-	-	-				
	10	-	-	-	-	-				
	11	-	-	-	-	-				
	12	-	-	-	-	-				
	13	-	-	-	-	-				
	14	-	-	-	-	-				
	15	-	-	-	-	-				
	16	-	-	-	-	-				
	17	-	-	-	-	-				
	18	-	-	-	-	-				
	19	-	-	-	-	-				
	20	-	-	-	-	-				
	21	✓	✓	✓	✓	✓				
	22	✓	✓	✓	✓	✓				
	23	✓	✓	✓	✓	-				
	24	✓	✓	✓	✓	✓				
	25	✓	✓	✓	✓	✓				
	26	✓	✓	✓	✓	✓				
	27	✓	✓	✓	✓	-				
	28	✓	✓	✓	✓	✓				
	29	✓	✓	✓	✓	✓				
	30	✓	✓	✓	✓	✓				
	31	✓	✓	✓	✓	✓				
	32	✓	✓	✓	✓	✓				
	33	✓	✓	✓	✓	✓				
	34	✓	✓	✓	✓	✓				
	35	✓	✓	✓	✓	✓				
	36	✓	✓	✓	✓	✓				
	37	✓	✓	✓	✓	✓				
	38	✓	✓	✓	✓	-				
	39	✓	✓	✓	✓	✓				
	40	✓	✓	✓	✓	✓				
	41	✓	✓	✓	✓	✓				
	42	✓	✓	✓	✓	✓				

Index of Claims	**Application/Control No.** 14/071,126	**Applicant(s)/Patent Under Reexamination** Weiss, Kenneth P.
	Examiner ISIDORA I IMMANUEL	**Art Unit** 3685

CLAIM		**DATE**								
Final	Original	08/21/2016	03/18/2017	08/07/2017	09/05/2017	04/05/2018				
	43	✓	✓	✓	✓	✓				
	44	✓	✓	✓	✓	-				
	45	✓	✓	✓	✓	✓				
	46	✓	✓	✓	✓	✓				
	47	✓	✓	✓	✓	✓				
	48	✓	✓	✓	✓	✓				
	49	✓	✓	✓	✓	✓				
	50					✓				
	51					✓				
	52					✓				
	53					✓				

Search Notes	**Application/Control No.** 14/071,126	**Applicant(s)/Patent Under Reexamination** Weiss, Kenneth P.
	Examiner ISIDORA I IMMANUEL	**Art Unit** 3685

CPC - Searched*		
Symbol	**Date**	**Examiner**
G06Q	8/22/2016	II

CPC Combination Sets - Searched*		
Symbol	**Date**	**Examiner**

US Classification - Searched*			
Class	**Subclass**	**Date**	**Examiner**

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	**Date**	**Examiner**
See attached notes	8/22/2016	II
See attached notes	3/19/2017	II
IPR2018-0067- Reviewed petition for inter partes review of US patent NO. 8,577,813, doctument # 2	04/15/2018	II

Interference Search			
US Class/CPC Symbol	**US Subclass/CPC Group**	**Date**	**Examiner**

	/I.I./ Examiner.Art Unit 3685

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**		
	Application Number	14071126
	Filing Date	2013-11-04
	First Named Inventor	Kenneth P. Weiss
	Art Unit	3685
	Examiner Name	I. I. Immanuel
	Attorney Docket Number	W0537-701321

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code1	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code1	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/I.I.I./	1	20030226017	A1	2003-12-04	Palekar et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number3	Country Code2 i	Kind Code4	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T5
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	14071126
	Filing Date	2013-11-04
	First Named Inventor	Kenneth P. Weiss
	Art Unit	3685
	Examiner Name	I. I. Immanuel
	Attorney Docket Number	W0537-701321

	1		

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/ISIDORA I IMMANUEL/	Date Considered	06/06/2018

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	14071126
	Filing Date	2013-11-04
	First Named Inventor	Kenneth P. Weiss
	Art Unit	3685
	Examiner Name	I. I. Immanuel
	Attorney Docket Number	W0537-701321

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☒ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/John N. Anastasi/	Date (YYYY-MM-DD)	2017-12-14
Name/Print	John N. Anastasi	Registration Number	37,765

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1 hour 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.**

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 record s.

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.

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. OMB 0651-0031
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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	14071126
	Filing Date	2013-11-04
	First Named Inventor	Kenneth P. Weiss
	Art Unit	3685
	Examiner Name	I. I. Immanuel
	Attorney Docket Number	W0537-701321

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code1	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/I.I.I./	1	6163771		2000-12-19	Walker et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code1	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/I.I.I./	1	20030028481	A1	2003-02-06	Flitcroft et al.	
/I.I.I./	2	20070245152	A1	2007-10-18	Pizano et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number3	Country Code2 i	Kind Code4	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T5
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number		14071126
	Filing Date		2013-11-04
	First Named Inventor	Kenneth P. Weiss	
	Art Unit		3685
	Examiner Name	I. I. Immanuel	
	Attorney Docket Number		W0537-701321

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1		

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/ISIDORA I IMMANUEL/	Date Considered	06/06/2018

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14071126
	Filing Date	2013-11-04
	First Named Inventor	Kenneth P. Weiss
	Art Unit	3685
	Examiner Name	I. I. Immanuel
	Attorney Docket Number	W0537-701321

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☒ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/John N. Anastasi/	Date (YYYY-MM-DD)	2017-10-13
Name/Print	John N. Anastasi	Registration Number	37,765

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1 hour 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.**

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 record s.

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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	14071126
	Filing Date	2013-11-04
	First Named Inventor	Kenneth P. Weiss
	Art Unit	3685
	Examiner Name	I. I. Immanuel
	Attorney Docket Number	W0537-701321

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code1	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/I.I.I./	1	6016476		2000-01-18	Maes et al.	
/I.I.I./	2	7865448		2011-01-04	Pizarro	
/I.I.I./	3	5615277		1997-03-25	Hoffman	
/I.I.I./	4	8751801		2014-06-10	Harris et al.	
/I.I.I./	5	6950939		2005-09-27	Tobin	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code1	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/I.I.I./	1	20040107170	A1	2004-06-03	Labrou et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	14071126
	Filing Date	2013-11-04
	First Named Inventor	Kenneth P. Weiss
	Art Unit	3685
	Examiner Name	I. I. Immanuel
	Attorney Docket Number	W0537-701321

/I.I.I./	2	20030219121	A1	2003-11-27	van Someren	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number3	Country Code2 i	Kind Code4	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T5
/I.I.I./	1	200106699	WO	A2	2001-01-25	Rsa Security Inc		
/I.I.I./	2	2001024123	WO	A1	2001-04-05	Chameleon Network Inc		

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
/I.I.I./	1	Jin et al., Biohashing: two factor authentication featuring fingerprint data and tokenized random number, Pattern Recognition 37 (11), pp. 2245-2255 (2004)	
/I.I.I./	2	Bruce Schneier, Applied Cryptography, 2d Ed (1996)	
/I.I.I./	3	American Bankers Association, Financial Institution Key Management (Wholesale), ANSI X9.17 (1995)	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/ISIDORA I IMMANUEL/	Date Considered	06/06/2018

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	14071126
	Filing Date	2013-11-04
	First Named Inventor	Kenneth P. Weiss
	Art Unit	3685
	Examiner Name	I. I. Immanuel
	Attorney Docket Number	W0537-701321

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number		14071126
	Filing Date		2013-11-04
	First Named Inventor	Kenneth P. Weiss	
	Art Unit		3685
	Examiner Name	I. I. Immanuel	
	Attorney Docket Number		W0537-701321

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☒ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/John N. Anastasi/	Date (YYYY-MM-DD)	2017-10-23
Name/Print	John N. Anastasi	Registration Number	37,765

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1 hour 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.**

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 record s.

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.