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.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/210,926	09/11/2012	8266432	KAMR002US0	7516

58293 7590 08/22/2012

FORTKORT & HOUSTON P.C.
9442 N. CAPITAL OF TEXAS HIGHWAY
ARBORETUM PLAZA ONE, SUITE 500
AUSTIN, TX 78759

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Nader Asghari-Kamrani, Centreville, VA;
Kamran Asghari-Kamrani, Centreville, VA;

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

FORTKORT & HOUSTON P.C.
9442 N. CAPITAL OF TEXAS HIGHWAY
ARBORETUM PLAZA ONE, SUITE 500
AUSTIN, TX 78759

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

Michael P. Fortkort	(Depositor's name)
/Michael P. Fortkort/	(Signature)
August 13, 2012	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/210,926	09/15/2008	Nader Asghari-Kamrani	KAMR002US0	7516

TITLE OF INVENTION:

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	yes	$870	$300	$0	$1170	08/24/2012

EXAMINER	ART UNIT	CLASS-SUBCLASS

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Michael P. Fortkort, Esq.
2 MICHAEL P FORTKORT PC
3 __________

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:

☑ Issue Fee
☑ Publication Fee (No small entity discount permitted)
❑ Advance Order - # of Copies __________

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

❑ A check is enclosed.
☑ Payment by credit card. Form PTO-2038 is attached.
❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number 503776 (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

❑ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.
❑ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature /Michael P. Fortkort/ Date August 13, 2012

Typed or printed name Michael P. Fortkort Registration No. 35,141

This collection of information is required by 37 CFR 1.311. 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, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

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.

Privacy Act Statement

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

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

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

Electronic Patent Application Fee Transmittal

Application Number:	12210926
Filing Date:	15-Sep-2008
Title of Invention:	CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Filer:	Michael P. Fortkort
Attorney Docket Number:	KAMR002US0

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:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl issue fee	2501	1	870	870
Publ. Fee- early, voluntary, or normal	1504	1	300	300

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
	Total in USD ($)			**1170**

Electronic Acknowledgement Receipt

EFS ID:	13481944
Application Number:	12210926
International Application Number:	
Confirmation Number:	7516
Title of Invention:	CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Customer Number:	58293
Filer:	Michael P. Fortkort
Filer Authorized By:	
Attorney Docket Number:	KAMR002US0
Receipt Date:	13-AUG-2012
Filing Date:	15-SEP-2008
Time Stamp:	15:12:22
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$1170
RAM confirmation Number	1764
Deposit Account	503776
Authorized User	FORTKORT,MICHAEL P

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	Issue Fee Payment (PTO-85B)	Fee_transmittal_filed_081312_12210926.pdf	121320 5e504977c82404b64cc23fda3ec6b5a3c2c67c60	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	31899 27baec0b22c4fddc86dc9f425fc3eef91701209a	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	153219	

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.

Certification Under 37 C.F.R. § 1.8

I hereby certify that on May 25, 2012 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: May 25, 2012 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 12/210,926

FILING DATE: September 15, 2008

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

ATTORNEY DOCKET: KAMR002US0

CONFIRMATION NO.: 7516

VIA ELECTRONIC FILING SYSTEM
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

Sir:

INTERVIEW SUMMARY

The Applicants wish to thank Examiner Abdulhakim Nobahar for participating in an interview with their representatives (Mr. Fortkort, Mr. Nader Asghari-Kamrani, Mr. Kamran Asghari-Kamrani and Mr. Hewitt) on April 26, 2012. During the interview, the Applicants' representatives discussed the differences between the prior art and the claims, in particular references by Kaliski and Hill. The Applicants brought an expert in authentication and online transactions, Mr. James Hewitt who explained how the system disclosed by Kaliski operates and highlighted the differences between the claims at issue and the prior art of Kaliski and Hill.

The Applicants noted that the prior art does not teach the use of a dynamic code that is valid for a predetermined time and becomes invalid after being used, which dynamic code is provided by a trusted authenticator and used as the basis for authentication of an individual during an electronic transaction.

CONCLUSION

The Applicant respectfully submits this application is in condition for allowance and requests issuance of a Notice of Allowance.

Although not believed necessary, the Office is hereby authorized to charge any fees required under 37 C.F.R. § 1.16 or § 1.17 or credit any overpayments to the deposit account of MICHAEL P FORTKORT PC, Deposit Account No. 50-3776.

In the event the prosecution of this Application can be efficiently advanced by a phone discussion, it is requested that the undersigned attorney be called at (703) 435-9390.

Respectfully submitted,

By /Michael P. Fortkort/ Date: May 25, 2012
Michael P. Fortkort (Reg. No. 35,141)

MICHAEL P FORTKORT PC
The International Law Center
13164 Lazy Glen Lane
Oak Hill, Virginia 20171

Please direct telephone calls to:
Michael P. Fortkort
703-435-9390
703-435-8857 (facsimile)

Electronic Acknowledgement Receipt

EFS ID:	12864233
Application Number:	12210926
International Application Number:	
Confirmation Number:	7516
Title of Invention:	CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Customer Number:	58293
Filer:	Michael P. Fortkort
Filer Authorized By:	
Attorney Docket Number:	KAMR002US0
Receipt Date:	25-MAY-2012
Filing Date:	15-SEP-2008
Time Stamp:	09:58:24
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	Applicant summary of interview with examiner	Interview_Summary_12210926_042612.pdf	19761 a964b2c2891dd7129f7b00e9afc06f1023eb36aa	no	3

Warnings:

Information:

Total Files Size (in bytes):	19761

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

NOTICE OF ALLOWANCE AND FEE(S) DUE

58293 7590 05/24/2012

FORTKORT & HOUSTON P.C.
9442 N. CAPITAL OF TEXAS HIGHWAY
ARBORETUM PLAZA ONE, SUITE 500
AUSTIN, TX 78759

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	PAPER NUMBER
2432	

DATE MAILED: 05/24/2012

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/210,926	09/15/2008	Nader Asghari-Kamrani	KAMR002US0	7516

TITLE OF INVENTION: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$870	$300	$0	$1170	08/24/2012

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: <u>Mail</u>
Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or <u>Fax</u> (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

58293 7590 05/24/2012
FORTKORT & HOUSTON P.C.
9442 N. CAPITAL OF TEXAS HIGHWAY
ARBORETUM PLAZA ONE, SUITE 500
AUSTIN, TX 78759

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)

(Signature)

(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/210,926	09/15/2008	Nader Asghari-Kamrani	KAMR002US0	7516

TITLE OF INVENTION: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$870	$300	$0	$1170	08/24/2012

EXAMINER	ART UNIT	CLASS-SUBCLASS
NOBAHAR, ABDULHAKIM	2432	713-168000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

□ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

□ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1______________________________

2______________________________

3______________________________

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : □ Individual □ Corporation or other private group entity □ Government

4a. The following fee(s) are submitted:

□ Issue Fee

□ Publication Fee (No small entity discount permitted)

□ Advance Order - # of Copies ______________________

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

□ A check is enclosed.

□ Payment by credit card. Form PTO-2038 is attached.

□ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____________ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

□ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.

□ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature ____ Date ____

Typed or printed name ____ Registration No. _________________________________

This collection of information is required by 37 CFR 1.311. 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, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

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.

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.
12/210,926	09/15/2008	Nader Asghari-Kamrani	KAMR002US0	7516

58293 7590 05/24/2012
FORTKORT & HOUSTON P.C.
9442 N. CAPITAL OF TEXAS HIGHWAY
ARBORETUM PLAZA ONE, SUITE 500
AUSTIN, TX 78759

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	**PAPER NUMBER**
2432	

DATE MAILED: 05/24/2012

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)

(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 0 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 0 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Privacy Act Statement

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

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

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

	Application No.	Applicant(s)	
Notice of Allowability	12/210,926	ASGHARI-KAMRANI ET AL.	
	Examiner	**Art Unit**	
	ABDULHAKIM NOBAHAR	2432	

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

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *amendment filed on 03/01/2012*.

2. □ 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.

3. ☒ The allowed claim(s) is/are *1,4,15-24,36-41,43-48,50-55,58,60,63,64,67-73,75-78,80-82,84-86 and 88-91*.

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

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)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE “MAILING DATE” of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. □ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER’S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. □ CORRECTED DRAWINGS (as “replacement sheets”) must be submitted.

(a) □ including changes required by the Notice of Draftsperson’s Patent Drawing Review (PTO-948) attached

1) □ hereto or 2) □ to Paper No./Mail Date _____.

(b) □ including changes required by the attached Examiner’s Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. □ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner’s comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. □ Notice of References Cited (PTO-892)
2. □ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. □ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. □ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. □ Notice of Informal Patent Application
6. □ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. □ Other _____.

/Abdulhakim Nobahar/
Examiner, Art Unit 2432

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mr. Michael P. Fortkort, Reg. No. 35,141 on 04/30/2012, 05/01/2012 and 05/14/2012.

The application has been amended as follows:

In the claims:

Please replace all prior versions and listings of claims in the application with the following listing of the claims.

1. (Currently Amended) A method for authenticating a user during an electronic transaction between the user and an ~~External-Entity~~ external-entity, the method comprising:

receiving electronically a request for a dynamic ~~SecureCode~~ code for the user by a computer associated with a ~~Central-Entity~~ central-entity during the transaction between the user and the ~~External-Entity~~ external-entity;

generating by the central-entity during the transaction a dynamic ~~SecureCode~~ code for the user in response to the request, wherein the dynamic ~~SecureCode~~ code is valid for a predefined time and becomes invalid after being used;

providing by the computer associated with the central-entity said generated ~~SecureCode~~ dynamic code to the user during the transaction;

receiving electronically by the ~~Central-Entity~~ central-entity a request for authenticating the user from a computer associated with the external-entity based on a user-specific information and the dynamic code as a digital identity included in the request which said dynamic code was received by the user during the transaction and was provided to the external-entity by the user during the transaction~~, which digital identity includes the SecureCode~~; and

authenticating by the ~~Central-Entity~~ central-entity the user and providing a result of the authenticating to the external-entity during the transaction if the digital identity is valid.

2. (Cancelled)

3. (Cancelled)

4. (Currently Amended) A method as recited in claim 1, further comprising:

combining said generated ~~SecureCode~~ dynamic code with [[a]] the user-specific information using a predetermined algorithm to form a combined ~~SecureCode~~ dynamic code and user specific information;

maintaining the combined ~~SecureCode~~ dynamic code and user specific information at the ~~Central-Entity~~ central-entity;

comparing the combined ~~SecureCode~~ dynamic code and user specific information with a received combined ~~SecureCode~~ dynamic code and user specific information to validate the user.

5-11. (Cancelled)

12. (Cancelled)

13. (Cancelled)

14. (Cancelled)

15. (Currently Amended) The method of claim [[14]] 1, wherein the user specific information comprises one or more of the following: an alphanumeric name, an ID, a login name, and an identification phrase.

16. (Original) The method of claim 1, wherein the transaction corresponds to a financial transaction.

17. (Original) The method of claim 1, wherein the transaction corresponds to a non-financial transaction.

18. (Previously Presented) The method of claim 1, wherein the transaction corresponds to access to restricted web-site or restricted computer/server.

19. (Currently Amended) The method of claim 1, wherein said transaction occurs over a communication network, wherein said communication network comprises one or more of the following: [[an]] a public network, the Internet, a wireless network, a mobile network, a satellite network, and a private network.

20. (Currently Amended) The method of claim 1, wherein said transaction occurs over a communication network to which is coupled said user, said ~~Central-Entity~~ central-entity, and said ~~External-Entity~~ external-entity.

21. (Currently Amended) An apparatus for authenticating a user during an electronic transaction with an ~~External-Entity~~ external-entity, the apparatus comprising:

a first ~~Central-Entity~~ central-entity computer adapted to:

generate a dynamic ~~SecureCode~~ code for the user in response to a request during the electronic transaction, wherein the dynamic ~~SecureCode~~ code is valid for a predefined time and becomes invalid after being used; and

provide said ~~SecureCode~~ dynamic code to the user during the electronic transaction;

a second ~~Central-Entity~~ central-entity computer adapted to validate a digital identity in response to an authentication request from the external-entity, which authentication request includes a user-specific information and the dynamic code as the digital identity which dynamic code was received by the user during the electronic transaction and was provided to the external-entity by the user during the electronic transaction~~, which includes said SecureCode~~, and to authenticate the user if the digital identity is valid and to provide a result of the authentication of the user to the external-entity during the electronic transaction.

22. (Currently Amended) The apparatus as recited in claim 21, wherein said user has a pre-existing relationship with the ~~External-Entity~~ external-entity.

23. (Currently Amended) The apparatus as recited in claim 21, wherein said user has no pre-existing relationship with the ~~External-Entity~~ external-entity.

24. (Currently Amended) The apparatus as recited in claim 21, wherein said ~~External-Entity~~ external-entity and said ~~Central-Entity~~ central-entity use a ~~SecureCode~~ dynamic code that is algorithmically combined with said the user-specific information.

25-31. (Cancelled)

32. (Cancelled)

33. (Cancelled)

34. (Cancelled)

35. (Cancelled)

36. (Previously Presented) The apparatus of claim 21, wherein the transaction corresponds to a financial transaction.

37. (Previously Presented) The apparatus of claim 21, wherein the transaction corresponds to a non-financial transaction.

38. (Previously Presented) The apparatus of claim 21, wherein the transaction corresponds to access to restricted web-site or restricted computer/server.

39. (Currently Amended) The apparatus of claim 21, wherein said transaction occurs over a communication network and wherein said communication network comprises one or more of the following[[;]]: a public network, [[an]] the Internet, a wireless network, a mobile network, a satellite network, and a private network.

40. (Currently Amended) The apparatus of claim 21, wherein said transaction occurs over a communication network to which is coupled said user, said ~~Central-Entity~~ central-entity, and said ~~External-Entity~~ external-entity.

41. (Currently Amended) A method as recited in claim 4, wherein said algorithmically combined ~~SecureCode~~ dynamic code and user specific information is used to authenticate a user's identity.

42. (Cancelled)

43. (Currently Amended) A method as recited in claim 4, wherein said ~~Central-Entity~~ central-entity is using said algorithmically combined ~~SecureCode~~ dynamic code and user specific information to authenticate a user's identity.

44. (Currently Amended) A method as recited in claim 1, wherein said ~~External-Entity~~ external-entity and said ~~Central-Entity~~ central-entity are the same entity.

45. (Currently Amended) The method as recited in claim 1, wherein said ~~Central-Entity~~ central-entity invalidates the ~~SecureCode~~ dynamic code after authenticating the user.

46. (Currently Amended) The method as recited in claim 1, wherein the ~~Central-Entity~~ central-entity invalidates the ~~SecureCode~~ dynamic code after a predefined period of time passes from when the ~~SecureCode~~ dynamic code was generated.

47. (Previously Presented) The method as recited in claim 1, wherein said ~~Central-Entity~~ central-entity generates the ~~SecureCode~~ dynamic code with dependence on the user information.

48. (Previously Presented) The method as recited in claim 47, wherein said user information comprises one or more of the following: an alphanumeric name, an ID, a login name, and an identification phrase.

49. (Cancelled)

50. (Currently Amended) A method for authenticating a user during an electronic transaction between the user and an ~~External-Entity~~ external-entity, the method comprising:

receiving electronically a request for a dynamic ~~SecureCode~~ code for the user by a computer associated with a ~~Central-Entity~~ central-entity during the electronic transaction between the user and the ~~External-Entity~~ external-entity;

generating by the central-entity during the electronic transaction a dynamic ~~SecureCode~~ code for the user in response to the request, wherein the dynamic ~~SecureCode~~ code is valid for a predefined time and becomes invalid after being used;

providing by a computer associated with the central-entity said generated ~~SecureCode~~ dynamic code to the user during the transaction;

receiving ~~electronically~~ during the electronic transaction by [[a]] another computer associated with the ~~Central-Entity~~ central-entity a request from the external-entity for authenticating the user based on a user-specific information and the dynamic code as a digital identity included in the request ~~during the transaction~~, which said dynamic code was received by the user during the transaction and was provided by the user to the external-entity during the electronic transaction ~~digital identity includes the SecureCode~~; and

authenticating by the ~~Central-Entity~~ central-entity the user and providing a result of the authentication of the user to the external-entity during the transaction if the digital identity is valid, wherein said ~~SecureCode~~ dynamic code is alphanumeric.

51. (Currently Amended) The method as recited in claim 1, wherein said user communicates with said ~~Central-Entity~~ central-entity over a communication network.

52. (Currently Amended) An apparatus for authenticating a user during an electronic transaction with an ~~External-Entity~~ external-entity, the apparatus comprising:

a first ~~Central-Entity~~ central-entity computer adapted to:

generate a dynamic ~~SecureCode~~ code for the user in response to a request from the user during the electronic transaction, wherein the dynamic ~~SecureCode~~ code is valid for a predefined time and becomes invalid after being used; and provide said ~~SecureCode~~ dynamic code to the user during the electronic transaction;

a second ~~Central-Entity~~ central-entity computer adapted to validate a user-specific information and the dynamic code as a digital identity included in an authentication request from the external-entity, which said dynamic code was received by the user during the electronic transaction and was provided by the user to the external-entity during the electronic transaction ~~includes said SecureCode~~, and to authenticate the user if the digital identity is valid and to provide a result of the authentication of the user to the external-entity during the electronic transaction, wherein said ~~SecureCode~~ dynamic code is alphanumeric.

53. (Currently Amended) The method as recited in claim 1, wherein said user communicates with said ~~External-Entity~~ external-entity over a communication network.

54. (Currently Amended) The apparatus as recited in claim 21, wherein said user communicates with said ~~Central-Entity~~ central-entity over a communication network.

55. (Currently Amended) The apparatus as recited in claim 21, wherein said user communicates with said ~~External-Entity~~ external-entity over a communication network.

56-57. (Cancelled)

58. (Currently Amended) The method as recited in claim 1, wherein said ~~SecureCode~~ dynamic code is generated based on a request submitted by said user over a communication network.

59. (Cancelled)

60. (Previously Presented) The method as recited in claim 58, wherein said request is initiated by said user through a standard interface provided to said user.

61-62. (Cancelled)

63. (Currently Amended) The apparatus according to claim 21, wherein said first ~~Central-Entity~~ central-entity computer and said second ~~Central-Entity~~ central-entity computer are the same.

64. (Currently Amended) The apparatus according to claim 21, wherein said first ~~Central-Entity~~ central-entity computer and said second ~~Central-Entity~~ central-entity computer are different.

65. (Cancelled)

66. (Cancelled)

67. (Currently Amended) A method as recited in claim 1, wherein said digital identity is invalid if the ~~SecureCode~~ dynamic code is invalid.

68. (Currently Amended) A method as recited in claim 1, wherein said digital identity is valid if at least the ~~SecureCode~~ dynamic code is valid.

69. (Currently Amended) A method as recited in claim 1, wherein said ~~External-Entity~~ external-entity authenticates the user upon receiving an affirmation authentication message from the ~~Central-Entity~~ central-entity.

70. (Currently Amended) A method as recited in claim 1, wherein said ~~External-Entity~~ external-entity authenticates the user if said ~~Central-Entity~~ central-entity authenticates the user based on the ~~SecureCode~~ dynamic code.

71. (Currently Amended) The apparatus of claim 21, wherein said digital identity is invalid if the ~~SecureCode~~ dynamic code is invalid.

72. (Currently Amended) The apparatus of claim 21, wherein said digital identity is valid if at least the ~~SecureCode~~ dynamic code is valid.

73. (Currently Amended) The apparatus of claim 21, wherein said ~~External-Entity~~ external-entity authenticates the user upon receiving an affirmation authentication message from the ~~Central-Entity~~ central-entity.

74. (Cancelled)

75. (Currently Amended) The apparatus of claim 21, wherein said ~~Central-Entity~~ central-entity invalidates the ~~SecureCode~~ dynamic code after authenticating the user.

76. (Currently Amended) The apparatus of claim 21, wherein the ~~Central-Entity~~ central-entity invalidates the ~~SecureCode~~ dynamic code after a predefined period of time passes after the ~~SecureCode~~ dynamic code was generated.

77. (Currently Amended) The apparatus of claim 21, wherein said ~~Central-Entity~~ central-entity generates the ~~SecureCode~~ dynamic code based on said user-specific information.

78. (Currently Amended) The apparatus of claim 77, wherein said user-specific information comprises one or more of the following: an alphanumeric name, an ID, a login name, a password, and an identification phrase.

79. (Cancelled)

80. (Currently Amended) The apparatus of claim 21, wherein said ~~External-Entity~~ external-entity authenticates the user if said ~~Central-Entity~~ central-entity authenticates the user based on the ~~SecureCode~~ dynamic code.

81. (Currently Amended) The apparatus of claim 21, wherein said ~~External-Entity~~ external-entity and ~~Central-Entity~~ central-entity are the same entity.

82. (Currently Amended) A method as recited in claim 50, wherein said ~~External-Entity~~ external-entity and ~~Central-Entity~~ central-entity are the same entity.

83. (Cancelled)

84. (Currently Amended) The method of claim [[83]] 50, wherein the user-specific information includes user-identifying information.

85. (Currently Amended) The method of claim [[83]] 50, wherein the user-specific information comprises one or more of the following: an alphanumeric name, an ID, a login name, and an identification phrase.

86. (Currently Amended) The apparatus of claim 52, wherein said ~~External-Entity~~ external-entity and ~~Central-Entity~~ central-entity are the same entity.

87. (Cancelled)

88. (Currently Amended) The apparatus of claim [[87]] 52, wherein the user-specific information includes user-identifying information.

89. (Currently Amended) The method of claim [[87]] 52, wherein the user-specific information comprises one or more of the following: an alphanumeric name, an ID, a login name, and an identification phrase.

90. (Currently Amended) The method of claim [[14]] 1, wherein the user-specific information includes user-identifying information.

91. (Currently Amended) The apparatus of claim [[34]] 21, wherein the user-specific information includes user-identifying information.

Allowable Subject Matter

1. Claims 1, 4, 15-24, 36-41, 43-48, 50-55, 58, 60, 63, 64, 67-73, 75-78, 80-82, 84-86 and 88-91 are allowed.

2. The following is an examiner's statement of reasons for allowance:

The primary reasons for the allowance of the claims 1, 4, 15-24, 36-41, 43-48, 50-55, 58, 60, 63, 64, 67-73, 75-78, 80-82, 84-86 and 88-91 are the inclusion of the following limitations that are not found in the prior arts and they are uniquely distinct features. The closest prior arts are Kaliski, Jr. (US 201/00100724 A1), Jespersen et al. (US 7,171,694 B1) and Chen et al. (US 5,590,197 A). Kaliski discloses a method for accessing encrypted data by a client. The method includes receiving from the client by a server client information derived from a first secret wherein the client information is derived such that the server cannot feasibly determine the first secret. The method also includes providing to the client by the server intermediate data that is derived responsive to the received client information, a server secret, and possibly other information. Jespersen et al. discloses a method for performing a transaction between a legal entity A who has an approval to perform such a transaction, and a legal entity B over a network, the transaction being initiated by the legal entity A, wherein the legal entity A, to verify the approval to the legal entity B, associates the transaction with a verification insignia, and the verification insignia being a unique transitory insignia provided to the legal entity A by a legal entity C who thereby guarantees that the legal entity A has the approval. Chen et al. discloses an invention that enables a party to make electronic payments using a new payment medium referred to herein as the cyber wallet. The cyber wallet may be thought of as an expansion of the credit card concept into a concept involving multiple cards with multiple issuers in a convenient package designed to enable the holder of the cyber wallet to make purchases over the vast global communications network known as the Internet, with full protection of the electronic payment information from not only eavesdroppers, but also from remote merchants, without the need to verify the trustworthiness of the merchant.

However, the above arts, singularly or in combination, fail to anticipate or render the following limitations:

Claims 1, 4, 15-20, 41, 43-48, 51, 53, 58, 60, 67-70 and 90: receiving electronically by the central-entity a request for authenticating the user from a computer associated with the external-entity based on a user-specific information and the dynamic code as a digital identity included in the request which said dynamic code was received by the user during the transaction and was provided to the external-entity by the user during the transaction; and

authenticating by the central-entity the user and providing a result of the authenticating to the external-entity during the transaction if the digital identity is valid.

Claims 21-24, 36-40, 54, 55, 63, 64, 71-73, 75-78, 80, 81 and 91: a second central-entity computer adapted to validate a digital identity in response to an authentication request from the external-entity, which authentication request includes a user-specific information and the dynamic code as the digital identity which dynamic code was received by the user during the electronic transaction and was provided to the external-entity by the user during the electronic transaction, and to authenticate the user if the digital identity is valid and to provide a result of the authentication of the user to the external-entity during the electronic transaction.

Claims 50, 82, 84 and 85: receiving during the electronic transaction by another computer associated with the central-entity a request from the external-entity for authenticating the user based on a user-specific information and the dynamic code as a digital identity included in the request, which said dynamic code was received by the user during the transaction and was provided by the user to the external-entity during the electronic transaction.

Claims 52, 86, 88 and 89: a second central-entity computer adapted to validate a user-specific information and the dynamic code as a digital identity included in an authentication request from the external-entity, which said dynamic code was received by the user during the electronic transaction and was provided by the user to the external-entity during the electronic transaction, and to authenticate the user if the digital identity is valid and to provide a result of the authentication of the user to the external-entity during the electronic transaction.

Conclusion

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 571-272-3808. The examiner can normally be reached on M-T 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432

/Abdulhakim Nobahar/
Examiner, Art Unit 2432

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	5	ASGHARI-KAMRANI near2 (NADER KAMRAN)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/05/03 11:48
L3	1	"09/796675"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/05/03 11:54
L4	17481	(713/182-186).ccls. (726/2,5,8,18,27,28).ccls. (705/64,67,72,76,78).ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/05/03 11:58
L7	10816	4 and (online Internet electronic$4 web website digital cyber network) near2 (bank$3 shop$4 commerc$3 purchas$3 buy$3 trad$3 business retail$3 sell$3 transact$3 communicat$3 financ$4 vend$3 procur$5 exchang$3)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/05/03 12:02
L8	8958	7 and (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper trader entity member party pay$2 spender partner counterpart) same (online Internet electronic$4 web website digital cyber network) near2 (bank$3 shop$4 commerc$3 purchas$3 buy$3 trad$3 business retail$3 sell$3 transact$3 communicat$3 financ$4 vend$3 procur$5 exchang$3)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/05/03 12:03
L9	2308	8 and (authenticat$3 verification verifying validation validity) near2 (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper trader entity member party pay$2 spender partner counterpart) same (online Internet electronic$4 web website digital cyber network) near2 (bank$3 shop$4 commerc$3 purchas$3 buy$3 trad$3 business retail$3 sell$3 transact$3 communicat$3 financ$4 vend$3 procur$5 exchang$3)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/05/03 12:03
L10	1980	9 and (server trust$3 third authority bank issu$3 institution organization authenticator center$3 central$5 centre	US-PGPUB; USPAT; FPRS;	OR	ON	2012/05/03 12:07

		centralization or broker$4 authoritative or authorized official$3) with (authenticat$3 verification verifying validation validity) near2 (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper trader entity member party pay$2 spender partner counterpart)	EPO; JPO;
			DERWENT;
			IBM_TDB			

L11	1224	10 and (server trust$3 third authority bank issu$3 institution organization authenticator center$3 central$5 centre centralization or broker$4 authoritative or authorized official$3) with (authenticat$3 verification verifying validation validity) near2 (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper trader entity member party pay$2 spender partner counterpart) same (online Internet electronic$4 web website digital cyber network) near2 (bank$3 shop$4 commerc$3 purchas$3 buy$3 trad$3 business retail$3 sell$3 transact$3 communicat$3 financ$4 vend$3 procur$5 exchang$3)	US-PGPUB;
			USPAT;
			FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2012/05/03 12:08

L12	1066	11 and (server trust$3 third authority bank issu$3 institution organization authenticator center$3 central$5 centre centralization broker$4 authoritative authorized official$3) same (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper member pay$2 spender partner counterpart) same (online Internet electronic$4 web digital cyber) same (website site entity shop commercial company business retailer store seller vendor trader dealer provider supplier merchant trade mercantile producer party merchandiser)	US-PGPUB;
			USPAT;
			FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2012/05/03 12:32

L13	1065	12 and (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper party pay$2 spender partner counterpart) near3 (data information key password passcode passname passphrase phrase paraphrase code securecode seed PIN pincode secret ID SID SSID identification identity identif$4 credential)	US-PGPUB;
			USPAT;
			FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2012/05/03 12:38

L15	1063	13 and (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper party pay$2 spender partner counterpart) with (data information key password passcode passname passphrase phrase paraphrase code securecode seed PIN pincode secret ID SID SSID identification identity identif$4 credential) with (server trust$3 third authority bank issu$3 institution	US-PGPUB;
			USPAT;
			FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2012/05/03 12:45

		organization authenticator cent$5 central$5 centralization broker$4 authoritative authorized official$3)				
L16	1036	15 and (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper party pay$2 spender partner counterpart) with (data information key password passcode passname passphrase phrase paraphrase code securecode seed PIN pincode secret ID SID SSID identification identity identif$4 credential) with (server trust$3 third authority bank issu$3 institution organization authenticator cent$5 central$5 centralization broker$4 authoritative authorized official$3) with (authentic$5 verification verifying valid$5)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/05/03 12:46
L17	392	16 and (dynamic$4 variable vary$3 changeable changing unpredictable non predictable one-time onetime once) near3 (data information key password passcode passname passphrase phrase paraphrase code securecode seed PIN pincode secret ID SID SSID identification identity identif$4 credential) same (server trust$3 third authority bank issu$3 institution organization authenticator cent$5 central$5 centralization broker$4 authoritative authorized official$3) with (authentic$5 verification verifying valid$5)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/05/03 12:48
L18	573	16 and (time tempora$4 duration during lapse elapse interval interim expir$5 period$6 span length extent transi$5 temp ephemeral short life liv$3 time-depend$4 time-based timebased time-wise timewise provision$4) near3 (data information key password passcode passname passphrase phrase paraphrase code securecode seed PIN pincode secret ID SID SSID identification identity identif$4 credential) same (server trust$3 third authority bank issu$3 institution organization authenticator cent$5 central$5 centralization broker$4 authoritative authorized official$3) with (authentic$5 verification verifying valid$5)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/05/03 12:49
L19	677	17 18	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/05/03 12:49
L20	59	19 and @PD>"20110725"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/05/03 12:53

L21	2	"5,590,197".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/05/03 13:04
L22	945226	(online Internet electronic$4 web website digital cyber network) near2 (bank$3 shop$4 commerc$3 purchas$3 buy$3 trad$3 business retail$3 sell$3 transact$3 communicat$3 financ$4 vend$3 procur$5 exchang$3)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/05/03 13:38
L23	94248	22 and (authenticat$3 verification verifying validation validity) near2 (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper trader entity member party pay$2 spender partner counterpart)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/05/03 13:39
L24	46930	23 and (server trust$3 third authority bank issu$3 institution organization authenticator center$3 central$5 centre centralization or broker$4 authoritative or authorized official$3) with (authenticat$3 verification verifying validation validity) near2 (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper trader entity member party pay$2 spender partner counterpart)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/05/03 13:41
L25	5200	24 and @PD>"20110725"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/05/03 13:42
L26	4427	25 and (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper trader entity member party pay$2 spender partner counterpart) same (online Internet electronic$4 web website digital cyber network) near2 (bank$3 shop$4 commerc$3 purchas$3 buy$3 trad$3 business retail$3 sell$3 transact$3 communicat$3 financ$4 vend$3 procur$5 exchang$3)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/05/03 13:43
L27	1271	26 and (authenticat$3 verification verifying validation validity) near2 (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper trader entity member party pay$2 spender partner counterpart) same (online Internet electronic$4 web website digital cyber network) near2 (bank$3 shop$4 commerc$3 purchas$3 buy$3 trad$3 business retail$3 sell$3 transact$3 communicat$3 financ$4 vend$3 procur$5 exchang$3)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/05/03 13:43
L28	1271	27 and (server trust$3 third authority	US-PGPUB;	OR	ON	2012/05/03

		bank issu$3 institution organization authenticator center$3 central$5 centre centralization or broker$4 authoritative or authorized official$3) with (authenticat$3 verification verifying validation validity) near2 (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper trader entity member party pay$2 spender partner counterpart)	USPAT;
			FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
						13:44

L29	874	28 and (server trust$3 third authority bank issu$3 institution organization authenticator center$3 central$5 centre centralization or broker$4 authoritative or authorized official$3) with (authenticat$3 verification verifying validation validity) near2 (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper trader entity member party pay$2 spender partner counterpart) same (online Internet electronic$4 web website digital cyber network) near2 (bank$3 shop$4 commerc$3 purchas$3 buy$3 trad$3 business retail$3 sell$3 transact$3 communicat$3 financ$4 vend$3 procur$5 exchang$3)	US-PGPUB;
			USPAT;
			FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2012/05/03 13:45

L30	649	29 and (server trust$3 third authority bank issu$3 institution organization authenticator center$3 central$5 centre centralization broker$4 authoritative authorized official$3) same (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper member pay$2 spender partner counterpart) same (online Internet electronic$4 web digital cyber) same (website site entity shop commercial company business retailer store seller vendor trader dealer provider supplier merchant trade mercantile producer party merchandiser)	US-PGPUB;
			USPAT;
			FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2012/05/03 13:46

L31	640	30 and (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper party pay$2 spender partner counterpart) near3 (data information key password passcode passname passphrase phrase paraphrase code securecode seed PIN pincode secret ID SID SSID identification identity identif$4 credential)	US-PGPUB;
			USPAT;
			FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2012/05/03 13:46

L32	634	31 and (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper party pay$2 spender partner counterpart) with (data information key password passcode passname passphrase phrase paraphrase code securecode seed PIN pincode secret ID SID SSID identification identity identif$4	US-PGPUB;
			USPAT;
			FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2012/05/03 13:47

		credential) with (server trust$3 third authority bank issu$3 institution organization authenticator cent$5 central$5 centralization broker$4 authoritative authorized official$3)				
L33	579	32 and (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper party pay$2 spender partner counterpart) with (data information key password passcode passname passphrase phrase paraphrase code securecode seed PIN pincode secret ID SID SSID identification identity identif$4 credential) with (server trust$3 third authority bank issu$3 institution organization authenticator cent$5 central$5 centralization broker$4 authoritative authorized official$3) with (authentic$5 verification verifying valid$5)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/05/03 13:47
L34	181	33 and (dynamic$4 variable vary$3 changeable changing unpredictable non predictable one-time onetime once) near3 (data information key password passcode passname passphrase phrase paraphrase code securecode seed PIN pincode secret ID SID SSID identification identity identif$4 credential) same (server trust$3 third authority bank issu$3 institution organization authenticator cent$5 central$5 centralization broker$4 authoritative authorized official$3) with (authentic$5 verification verifying valid$5)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/05/03 13:47
L35	274	33 and (time tempora$4 duration during lapse elapse interval interim expir$5 period$6 span length extent transi$5 temp ephemeral short life liv$3 time-depend$4 time-based timebased time-wise timewise provision$4) near3 (data information key password passcode passname passphrase phrase paraphrase code securecode seed PIN pincode secret ID SID SSID identification identity identif$4 credential) same (server trust$3 third authority bank issu$3 institution organization authenticator cent$5 central$5 centralization broker$4 authoritative authorized official$3) with (authentic$5 verification verifying valid$5)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/05/03 13:48
L36	321	34 35	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/05/03 13:48
L37	65	36 and (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper party pay$2 spender partner	US-PGPUB; USPAT; FPRS; EPO; JPO;	OR	ON	2012/05/03 13:51

		counterpart) with (dynamic$4 variable vary$3 changeable changing unpredictable non predictable one-time onetime once) near3 (data information key password passcode passname passphrase phrase paraphrase code securecode seed PIN pincode secret ID SID SSID identification identity identif$4 credential) with (server trust$3 third authority bank issu$3 institution organization authenticator cent$5 central$5 centralization broker$4 authoritative authorized official$3) with (authentic$5 verification verifying valid$5)	DERWENT; IBM_TDB			

L38	121	36 and (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper party pay$2 spender partner counterpart) with (time tempora$4 duration during lapse elapse interval interim expir$5 period$6 span length extent transi$5 temp ephemeral short life liv$3 time-depend$4 time-based timebased time-wise timewise provision$4) near3 (data information key password passcode passname passphrase phrase paraphrase code securecode seed PIN pincode secret ID SID SSID identification identity identif$4 credential) with (server trust$3 third authority bank issu$3 institution organization authenticator cent$5 central$5 centralization broker$4 authoritative authorized official$3) with (authentic$5 verification verifying valid$5)	US-PGPUB;
			USPAT;
			FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2012/05/03 13:51

L39	163	37 38	US-PGPUB;
			USPAT;
			FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2012/05/03 13:52

L40	52	39 and (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper party pay$2 spender partner counterpart) with (dynamic$4 variable vary$3 changeable changing unpredictable non predictable one-time onetime once) with (server trust$3 third authority bank issu$3 institution organization authenticator cent$5 central$5 centralization broker$4 authoritative authorized official$3) with (authentic$5 verification verifying valid$5) same (website site entity shop commercial company business retailer store seller vendor trader dealer provider supplier merchant trade mercantile producer party merchandiser)	US-PGPUB;
			USPAT;
			FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2012/05/03 13:55

L41	110	39 and (user client person individual subscriber member consumer customer	US-PGPUB;
			USPAT;
				OR	ON	2012/05/03 13:55

		request$2 buyer purchaser shopper party pay$2 spender partner counterpart) with (time tempora$4 duration during lapse elapse interval interim expir$5 period$6 span length extent transi$5 temp ephemeral short life liv$3 time-depend$4 time-based timebased time-wise timewise provision$4) with (server trust$3 third authority bank issu$3 institution organization authenticator cent$5 central$5 centralization broker$4 authoritative authorized official$3) with (authentic$5 verification verifying valid$5) same (website site entity shop commercial company business retailer store seller vendor trader dealer provider supplier merchant trade mercantile producer party merchandiser)	FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB			

L42	123	40 41	US-PGPUB;
			USPAT;
			FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2012/05/03
						13:56

5/3/2012 2:06:19 PM
H:\ EAST\ Workspaces\ 11333400_12210926.wsp

Issue Classification	**Application/Control No.** 12210926	**Applicant(s)/Patent Under Reexamination** ASGHARI-KAMRANI ET AL.
	Examiner ABDULHAKIM NOBAHAR	**Art Unit** 2432

ORIGINAL	
CLASS	**SUBCLASS**
713	168

CROSS REFERENCE(S)

CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**				
713	184				
705	67	74	78		

INTERNATIONAL CLASSIFICATION									
CLAIMED					**NON-CLAIMED**				
H	0	4	L	29 / 06 (2006.0)					
G	0	6	Q	20 / 00 (2012.01.01)					

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

Final	**Original**	**Final**	**Original**	**Final**	**Original**	**Final**	**Original**	**Final**	**Original**	**Final**	**Original**	**Final**	**Original**	**Final**	**Original**
1	1	5	17		33		49		65	46	81				
	2	6	18		34	48	50		66	49	82				
	3	7	19		35	16	51	20	67		83				
2	4	8	20	29	36	52	52	21	68	50	84				
	5	25	21	30	37	17	53	22	69	51	85				
	6	26	22	31	38	34	54	23	70	53	86				
	7	27	23	32	39	35	55	38	71		87				
	8	28	24	33	40		56	39	72	54	88				
	9		25	9	41		57	40	73	55	89				
	10		26		42	18	58		74	24	90				
	11		27	10	43		59	41	75	47	91				
	12		28	11	44	19	60	42	76						
	13		29	12	45		61	43	77						
	14		30	13	46		62	44	78						
3	15		31	14	47	36	63		79						
4	16		32	15	48	37	64	45	80						

/ABDULHAKIM NOBAHAR/ Examiner.Art Unit 2432 (Assistant Examiner)	05/04/2012 (Date)	**Total Claims Allowed:** 55	
/GILBERTO BARRON JR/ Supervisory Patent Examiner.Art Unit 2432 (Primary Examiner)	05/14/2012 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 1

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12210926	ASGHARI-KAMRANI ET AL.
	Examiner	**Art Unit**
	ABDULHAKIM NOBAHAR	2432

✓	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	07/06/2009	11/20/2009	04/28/2010	09/12/2010	01/11/2011	08/11/2011	01/02/2012	05/04/2012	
1	1	✓	✓	✓	✓	✓	✓	✓	=	
	2	✓	✓	✓	✓	✓	✓	✓	-	
	3	✓	✓	✓	✓	✓	✓	✓	-	
2	4	✓	✓	✓	✓	✓	✓	✓	=	
	5	✓	-	-	-	-	-	-	-	
	6	✓	-	-	-	-	-	-	-	
	7	✓	-	-	-	-	-	-	-	
	8	✓	-	-	-	-	-	-	-	
	9	✓	-	-	-	-	-	-	-	
	10	✓	-	-	-	-	-	-	-	
	11	✓	-	-	-	-	-	-	-	
	12	✓	✓	✓	✓	✓	✓	✓	-	
	13	✓	✓	✓	✓	✓	✓	✓	-	
	14	✓	✓	✓	✓	✓	✓	✓	-	
3	15	✓	✓	✓	✓	✓	✓	✓	=	
4	16	✓	✓	✓	✓	✓	✓	✓	=	
5	17	✓	✓	✓	✓	✓	✓	✓	=	
6	18	✓	✓	✓	✓	✓	✓	✓	=	
7	19	✓	✓	✓	✓	✓	✓	✓	=	
8	20	✓	✓	✓	✓	✓	✓	✓	=	
25	21	✓	✓	✓	✓	✓	✓	✓	=	
26	22	✓	✓	✓	✓	✓	✓	✓	=	
27	23	✓	✓	✓	✓	✓	✓	✓	=	
28	24	✓	✓	✓	✓	✓	✓	✓	=	
	25	✓	-	-	-	-	-	-	-	
	26	✓	-	-	-	-	-	-	-	
	27	✓	-	-	-	-	-	-	-	
	28	✓	-	-	-	-	-	-	-	
	29	✓	-	-	-	-	-	-	-	
	30	✓	-	-	-	-	-	-	-	
	31	✓	-	-	-	-	-	-	-	
	32	✓	✓	✓	✓	✓	✓	✓	-	
	33	✓	✓	✓	✓	✓	✓	✓	-	
	34	✓	✓	✓	✓	✓	✓	✓	-	
	35	✓	✓	✓	✓	✓	✓	✓	-	
29	36	✓	✓	✓	✓	✓	✓	✓	=	

Index of Claims	**Application/Control No.** 12210926	**Applicant(s)/Patent Under Reexamination** ASGHARI-KAMRANI ET AL.
	Examiner ABDULHAKIM NOBAHAR	**Art Unit** 2432

✓	**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	07/06/2009	11/20/2009	04/28/2010	09/12/2010	01/11/2011	08/11/2011	01/02/2012	05/04/2012	
30	37	✓	✓	✓	✓	✓	✓	✓	=	
31	38	✓	✓	✓	✓	✓	✓	✓	=	
32	39	✓	✓	✓	✓	✓	✓	✓	=	
33	40	✓	✓	✓	✓	✓	✓	✓	=	
9	41	✓	✓	✓	✓	✓	✓	✓	=	
	42	✓	-	✓	-	-	-	-	-	
10	43	✓	✓	✓	✓	✓	✓	✓	=	
11	44	✓	✓	✓	✓	✓	✓	✓	=	
12	45	✓	✓	✓	✓	✓	✓	✓	=	
13	46	✓	✓	✓	✓	✓	✓	✓	=	
14	47	✓	✓	✓	✓	✓	✓	✓	=	
15	48	✓	✓	✓	✓	✓	✓	✓	=	
	49	✓	-	-	-	-	-	-	-	
48	50	✓	✓	✓	✓	✓	✓	✓	=	
16	51	✓	✓	✓	✓	✓	✓	✓	=	
52	52	✓	✓	✓	✓	✓	✓	✓	=	
17	53	✓	✓	✓	✓	✓	✓	✓	=	
34	54	✓	✓	✓	✓	✓	✓	✓	=	
35	55	✓	✓	✓	✓	✓	✓	✓	=	
	56	✓	-	-	-	-	-	-	-	
	57	✓	-	-	-	-	-	-	-	
18	58	✓	✓	✓	✓	✓	✓	✓	=	
	59	✓	-	-	-	-	-	-	-	
19	60	✓	✓	✓	✓	✓	✓	✓	=	
	61	✓	-	-	-	-	-	-	-	
	62	✓	-	-	-	-	-	-	-	
36	63				✓	✓	✓	✓	=	
37	64				✓	✓	✓	✓	=	
	65				✓	✓	✓	✓	-	
	66				✓	✓	✓	✓	-	
20	67				✓	✓	✓	✓	=	
21	68				✓	✓	✓	✓	=	
22	69				✓	✓	✓	✓	=	
23	70				✓	✓	✓	✓	=	
38	71				✓	✓	✓	✓	=	
39	72				✓	✓	✓	✓	=	

Index of Claims	**Application/Control No.** 12210926	**Applicant(s)/Patent Under Reexamination** ASGHARI-KAMRANI ET AL.
	Examiner ABDULHAKIM NOBAHAR	**Art Unit** 2432

✓	**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	07/06/2009	11/20/2009	04/28/2010	09/12/2010	01/11/2011	08/11/2011	01/02/2012	05/04/2012	
40	73				✓	✓	✓	✓	=	
	74				✓	✓	✓	✓	-	
41	75				✓	✓	✓	✓	=	
42	76				✓	✓	✓	✓	=	
43	77				✓	✓	✓	✓	=	
44	78				✓	✓	✓	✓	=	
	79				✓	✓	✓	✓	-	
45	80				✓	✓	✓	✓	=	
46	81							✓	=	
49	82							✓	=	
	83							✓	-	
50	84							✓	=	
51	85							✓	=	
53	86							✓	=	
	87							✓	-	
54	88							✓	=	
55	89							✓	=	
24	90							✓	=	
47	91							✓	=	

EAST Search History

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L45	8042	(713/182-186).ccls. (726/2,5,8,18,27,28).ccls. (705/64,67,72,76,78).ccls.	US-PGPUB	OR	ON	2012/05/03 14:07
L46	1139	45 and ((user client person individual subscriber member consumer customer request$2 buyer purchaser shopper trader entity member party pay$2 spender partner counterpart) near6 (data information key password passcode passname passphrase phrase paraphrase code securecode seed PIN pincode secret ID SID SSID identification identity identif$4 credential) near3 (dynamic$4 variable vary$3 changeable changing unpredictable non predictable onetime once time tempora$4 duration during lapse elapse interval interim expir$5 period$6 span length extent transi$5 temp ephemeral short life liv$3 time-depend$4 time-based timebased time-wise timewise provision$4)).CLM.	US-PGPUB	OR	ON	2012/05/03 14:15
L47	41	46 and ((server trust$3 third authority bank issu$3 institution organization authenticator cent$5 central$5 centralization broker$4 authoritative authorized official$3) with (website site entity shop commercial company business retailer store seller vendor trader dealer provider supplier merchant trade mercantile producer party merchandiser) same (online Internet electronic$4 web website digital cyber network) near3 (bank$3 shop$4 commerc$3 purchas$3 buy$3 trad$3 business retail$3 sell$3 transact$3 communicat$3 financ$4 vend$3 procur$5 exchang$3)same (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper trader entity member party pay$2 spender partner counterpart) near5 (authenticat$3 verif$4 verification valid$5)).CLM.	US-PGPUB	OR	ON	2012/05/03 14:23
L48	30	47 and ((deny$4 den$4 reject$4 approv$4 disapprov$4 accept$4 allow$4 disallow$3 grant$3 permit$4 permission authoriz$5 refus$3 forbid$4 inhibit$3 prohibit$3 fail$3) same (server trust$3 third authority bank issu$3 institution organization authenticator cent$5 central$5 centralization broker$4 authoritative authorized official$3) same (website site entity shop commercial company business retailer store seller vendor trader dealer provider supplier merchant trade mercantile producer party merchandiser)).CLM.	US-PGPUB	OR	ON	2012/05/03 14:28
L50	23	48 and ((deny$4 den$4 reject$4 approv$4 disapprov$4 accept$4 allow$4 disallow$3	US-PGPUB	OR	ON	2012/05/03 14:31

		grant$3 permit$4 permission authoriz$5 refus$3 forbid$4 inhibit$3 prohibit$3 fail$3) same (server trust$3 third authority bank issu$3 institution organization authenticator cent$5 central$5 centralization broker$4 authoritative authorized official$3) with (website site entity shop commercial company business retailer store seller vendor trader dealer provider supplier merchant trade mercantile producer party merchandiser) same (online Internet electronic$4 web website digital cyber network) near3 (bank$3 shop$4 commerc$3 purchas$3 buy$3 trad$3 business retail$3 sell$3 transact$3 communicat$3 financ$4 vend$3 procur$5 exchang$3)same (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper trader entity member party pay$2 spender partner counterpart) near5 (authenticat$3 verif$4 verification valid$5)).CLM.				

5/3/2012 2:36:28 PM
H:\ EAST\ Workspaces\ 11333400_12210926.wsp

Search Notes	**Application/Control No.** 12210926	**Applicant(s)/Patent Under Reexamination** ASGHARI-KAMRANI ET AL.
	Examiner ABDULHAKIM NOBAHAR	**Art Unit** 2432

SEARCHED

Class	Subclass	Date	Examiner
726	2,5,8,18,27,28	7/26/2011	AN
713	182-186	7/26/2011	AN
705	64,67,72,76,78	7/26/2011	AN
	Search updated (See attached report)	12/16/2011 12/29/2011 5/3/2012	AN

SEARCH NOTES

Search Notes	Date	Examiner
East Inventors names search (see attached report)	7/6/2009 9/23/2009	AN
EAST text search only (see attached report)	12/16/2011 12/29/2011	AN
PALM inventors names search	9/23/2009	AN
Search updated (See attached report)	12/16/2011 12/29/2011 5/3/2012	AN

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner
726	2,5,8,18,27,28	5/3/2012	AN
713	155,168,170	5/3/2012	AN
705	35,39,44,50,64,67	5/3/2012	AN
	See attached report		

/ABDULHAKIM NOBAHAR/ Examiner.Art Unit 2432	

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.
12/210,926	09/15/2008	Nader Asghari-Kamrani	KAMR002US0	7516

58293 7590 05/03/2012
FORTKORT & HOUSTON P.C.
9442 N. CAPITAL OF TEXAS HIGHWAY
ARBORETUM PLAZA ONE, SUITE 500
AUSTIN, TX 78759

EXAMINER	
NOBAHAR, ABDULHAKIM	

ART UNIT	PAPER NUMBER
2432	

NOTIFICATION DATE	DELIVERY MODE
05/03/2012	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):

58293@foholaw.com
rbernfeld@foholaw.com

Applicant-Initiated Interview Summary	**Application No.** 12/210,926	**Applicant(s)** ASGHARI-KAMRANI ET AL.	
	Examiner ABDULHAKIM NOBAHAR	**Art Unit** 2432	

All participants (applicant, applicant's representative, PTO personnel):

(1) *ABDULHAKIM NOBAHAR*.

(2) *Mr. Michael Fortkort, Reg. No. 35,141*.

(3) *Mr. Nader Kamrani & Mr. Kamran Kamrani* .

(4) *Mr. James Hewitt*.

Date of Interview: *26 April 2012*.

Type: □ Telephonic □ Video Conference
☒ Personal [copy given to: □ applicant □ applicant's representative]

Exhibit shown or demonstration conducted: □ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed □101 □112 □102 ☒103 □Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *1,21,43,50 and 52*.

Identification of prior art discussed: *US 2010/0100724 & US 6236981*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Claims limitations versus the prior arts Kaliski and Hill teachings were discussed. It was found that Kaliski-Hill does not teach sending user information plus a temporary single-use code to a trusted server by a web server operated by an entity such as a merchant, requesting from the trusted server to authenticate the user based on the user information and the the temporary single-use code. Examiner will further conduct a search to see if there is a prior art disclosing this limitation.

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.

□ Attachment

/Abdulhakim Nobahar/
Examiner, Art Unit 2432

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
– Application Number (Series Code and Serial Number)
– Name of applicant
– Name of examiner
– Date of interview
– Type of interview (telephonic, video-conference, or personal)
– Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
– An indication whether or not an exhibit was shown or a demonstration conducted
– An identification of the specific prior art discussed
– An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
– The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:
1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
(The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

Doc Code: M865 or FAI.REQ.INTV

PTOL-413A (08-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Applicant Initiated Interview Request Form

Application No.: 12/210,926　First Named Applicant: ASGHARi-KAMRANI, Nader et al.
Examiner: Mr. Abdulhakim Nobahar　Art Unit: 2432　Status of Application: Pending

Tentative Participants:
(1) Michael P. Fortkort　**(2)** Nader Kamrani

(3) Kamran Kamrani　**(4)** James Hewitt

Proposed Date of Interview: April 26, 2012　**Proposed Time:** 11:00 a.m. **(AM/PM)**

Type of Interview Requested:
(1) [ ] Telephonic　(2) [✓] Personal　(3) [ ] Video Conference

Exhibit To Be Shown or Demonstrated: [ ] YES　[✓] NO
If yes, provide brief description:

Issues To Be Discussed

Issues (Rej., Obj., etc)	Claims/ Fig. #s	Prior Art	Discussed	Agreed	Not Agreed
(1) Rej	All	Kaliski/Hill	[✓]	[ ]	[ ]
(2)			[ ]	[ ]	[ ]
(3)			[ ]	[ ]	[ ]
(4)			[ ]	[ ]	[ ]

[ ] Continuation Sheet Attached　[ ] Proposed Amendment or Arguments Attached

Brief Description of Arguments to be Presented: Combination of Kaliski and Hill fails to state a prima facie case of obviousness. For example, digital tokens are not used for authentication and authentication not based on code generated during transaction.

An interview was conducted on the above-identified application on April 26, 2012

<u>NOTE</u>: This form should be completed and filed by applicant in advance of the interview (see MPEP § 713.01). If this form is signed by a registered practitioner not of record, the Office will accept this as an indication that he or she is authorized to conduct an interview on behalf of the principal (37 CFR 1.32(a)(3)) pursuant to 37 CFR 1.34. This is not a power of attorney to any above named practitioner. See the Instruction Sheet for this form, which is incorporated by reference. By signing this form, applicant or practitioner is certifying that he or she has read the Instruction Sheet. After the interview is conducted, applicant is advised to file a statement of the substance of this interview (37 CFR 1.133(b)) as soon as possible. This application will not be delayed from issue because of applicant's failure to submit a written record of this interview.

/Michael P. Fortkort/
Applicant/Applicant's Representative Signature

Examiner/SPE Signature

Michael P. Fortkort
Typed/Printed Name of Applicant or Representative

35,141
Registration Number, if applicable

This collection of information is required by 37 CFR 1.133. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 24 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.

Electronic Acknowledgement Receipt

EFS ID:	12553103
Application Number:	12210926
International Application Number:	
Confirmation Number:	7516
Title of Invention:	Centralized Identification and Authentication System and Method
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Customer Number:	58293
Filer:	Michael P. Fortkort
Filer Authorized By:	
Attorney Docket Number:	KAMR002US0
Receipt Date:	16-APR-2012
Filing Date:	15-SEP-2008
Time Stamp:	17:50:33
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	First Action Interview - Schedule Interview request	interview_request_for_042612_filed_041612_12210926.pdf	175832 214daa60a2effe8b3d2a4ec7b13aa8d19523009b	no	1

Warnings:

Information:

Total Files Size (in bytes):	175832

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.

Certification Under 37 C.F.R. § 1.8

I hereby certify that on March 1, 2012 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: March 1, 2012 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 12/210,926

FILING DATE: September 15, 2008

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

ATTORNEY DOCKET: KAMR002US0

CONFIRMATION NO.: 7516

VIA ELECTRONIC FILING SYSTEM
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

RESPONSE TO NON-FINAL OFFICE ACTION

Sir:

In response to the non-final Office Action mailed January 6, 2012, the Applicants hereby respectfully submit the following amendments and remarks:

Amendments to the Claims begin on page 2.

Remarks begin on page 15.

In the Claims:

Please amend the claims as follows:

1. (Currently Amended) A method for authenticating a user during an electronic transaction between the user and an External-Entity, the method comprising:

receiving electronically a request for a dynamic SecureCode for the user by a Central-Entity during the transaction between the user and the External-Entity;

generating during the transaction a dynamic SecureCode for the user in response to the request, wherein the dynamic SecureCode is valid for a predefined time and becomes invalid after being used;

providing said generated SecureCode to the user during the transaction;

receiving electronically ~~by a Central-Entity~~ by the Central-Entity a request for authenticating the user based on a digital identity during the transaction, which digital identity includes the SecureCode; and

authenticating by the Central-Entity the user during the transaction if the digital identity is valid.

Please cancel claims 2-3 without disclaimer of or prejudice to the subject matter contained therein.

2. (Cancelled) A method as recited in claim 1, wherein said user has a pre-existing relationship with the External-Entity.

3. (Cancelled) A method as recited in claim 1, wherein said user has no pre-existing relationship with the External-Entity.

4. (Currently Amended) A method as recited in claim 1, further comprising:

combining said generated SecureCode with a user-specific information using a predetermined algorithm to form a combined Secure-Code and user specific information;

maintaining the combined Secure-Code and user specific information at the Central-Entity;

~~using the predetermined algorithm to combine received user specific information received by the Central-Entity with a received SecureCode received by the Central-Entity to form a combined received SecureCode and received user specific information~~;

comparing the combined Secure-Code and user specific information with a received combined Secure-Code and user specific information ~~the combined received SecureCode and received user specific information~~ to validate the user.

5-11. (Cancelled)

12. (Previously Presented) A method as recited in claim 1, wherein said External-Entity receives the user's digital identity.

13. (Previously Presented) A method as recited in claim 1, wherein said External-Entity submits a digital identity to the Central-Entity.

14. (Previously Presented) The method of claim 1, wherein said digital identity includes a user-specific information.

15. (Previously Presented) The method of claim 14, wherein the user specific information comprises one or more of the following: an alphanumeric name, an ID, a login name, and an identification phrase.

16. (Original) The method of claim 1, wherein the transaction corresponds to a financial transaction.

17. (Original) The method of claim 1, wherein the transaction corresponds to a non-financial transaction.

18. (Previously Presented) The method of claim 1, wherein the transaction corresponds to access to restricted web-site or restricted computer/server.

19. (Previously Presented) The method of claim 1, wherein said transaction occurs over a communication network, wherein said communication network comprises one or more of the following: an Internet, a wireless network, a mobile network, a satellite network, and a private network.

20. (Previously Presented) The method of claim 1, wherein said transaction occurs over a communication network to which is coupled said user, said Central-Entity, and said External-

Entity.

21. (Previously Presented) An apparatus for authenticating a user during an electronic transaction with an External-Entity, the apparatus comprising:

a first Central-Entity computer adapted to:

generate a dynamic SecureCode for the user in response to a request during the transaction, wherein the dynamic SecureCode is valid for a predefined time and becomes invalid after being used; and

provide said SecureCode to the user;

a second Central-Entity computer adapted to validate a digital identity, which includes said SecureCode, and authenticate the user if the digital identity is valid.

22. (Previously Presented) The apparatus as recited in claim 21, wherein said user has a pre-existing relationship with the External-Entity.

23. (Previously Presented) The apparatus as recited in claim 21, wherein said user has no pre-existing relationship with the External-Entity.

24. (Previously Presented) The apparatus as recited in claim 21, wherein said External-Entity and said Central-Entity use a SecureCode that is algorithmically combined with said user-specific information.

25-31. (Cancelled)

32. (Previously Presented) The apparatus as recited in claim 21, wherein the user submits a digital identity to the External-Entity.

33. (Previously Presented) The apparatus as recited in claim 21, wherein the External-Entity submits a digital identity to the Central-Entity.

34. (Previously Presented) The apparatus of claim 21, wherein the digital identity includes a user-specific information.

35. (Previously Presented) The apparatus of claim 34, wherein the user specific information comprises one or more of the following; an alphanumeric name, an ID, a login name, and an identification phrase.

36. (Previously Presented) The apparatus of claim 21, wherein the transaction corresponds to a financial transaction.

37. (Previously Presented) The apparatus of claim 21, wherein the transaction corresponds to a non-financial transaction.

38. (Previously Presented) The apparatus of claim 21, wherein the transaction corresponds to access to restricted web-site or restricted computer/server.

39. (Previously Presented) The apparatus of claim 21, wherein said transaction occurs over a communication network and wherein said communication network comprises one or more of the following; an Internet, a wireless network, a mobile network, a satellite network, and a private network.

40. (Previously Presented) The apparatus of claim 21, wherein said transaction occurs over a communication network to which is coupled said user, said Central-Entity, and said External-Entity.

41. (Currently Amended) A method as recited in claim 4, wherein said ~~External-Entity is using said~~ algorithmically combined SecureCode and user specific information is used to authenticate a user's identity.

42. (Cancelled)

43. (Previously Presented) A method as recited in claim 4, wherein said Central-Entity is using said algorithmically combined SecureCode to authenticate a user's identity.

44. (Original) A method as recited in claim 1, wherein said External-Entity and said Central-Entity are the same entity.

45. (Previously Presented) The method as recited in claim 1, wherein said Central-Entity invalidates the SecureCode after authenticating the user.

46. (Previously Presented) The method as recited in claim 1, wherein the Central-Entity invalidates the SecureCode after a predefined period of time passes from when the SecureCode was generated.

47. (Previously Presented) The method as recited in claim 1, wherein said Central-Entity generates the SecureCode with dependence on the user information.

48. (Previously Presented) The method as recited in claim 47, wherein said user information comprises one or more of the following: an alphanumeric name, an ID, a login name, and an identification phrase.

49. (Cancelled)

50. (Previously Presented) A method for authenticating a user during an electronic transaction between the user and an External-Entity, the method comprising:

receiving electronically a request for a dynamic SecureCode for the user by a Central-Entity during the transaction between the user and the External-Entity;

generating during the transaction a dynamic SecureCode for the user in response to the request, wherein the dynamic SecureCode is valid for a predefined time and becomes invalid after being used;

providing said generated SecureCode to the user during the transaction;

receiving electronically by a Central-Entity a request for authenticating the user based on a digital identity during the transaction, which digital identity includes the SecureCode; and

authenticating by the Central-Entity the user during the transaction if the digital identity is valid, wherein said SecureCode is alphanumeric.

51. (Original) The method as recited in claim 1, wherein said user communicates with said Central-Entity over a communication network.

52. (Previously Presented) An apparatus for authenticating a user during an electronic transaction with an External-Entity, the apparatus comprising:

a first Central-Entity computer adapted to:

generate a dynamic SecureCode for the user in response to a request during the transaction, wherein the dynamic SecureCode is valid for a predefined time and becomes invalid after being used; and

provide said SecureCode to the user;

a second Central-Entity computer adapted to validate a digital identity, which includes said SecureCode, and authenticate the user if the digital identity is valid, wherein said SecureCode is alphanumeric.

53. (Original) The method as recited in claim 1, wherein said user communicates with said External-Entity over a communication network.

54. (Previously Presented) The apparatus as recited in claim 21, wherein said user communicates with said Central-Entity over a communication network.

55. (Previously Presented) The apparatus as recited in claim 21, wherein said user communicates with said External-Entity over a communication network.

56-57. (Cancelled)

58. (Previously Presented) The method as recited in claim 1, wherein said SecureCode is generated based on a request submitted by said user over a communication network.

59. (Cancelled)

60. (Previously Presented) The method as recited in claim 58, wherein said request is initiated by said user through a standard interface provided to said user.

61-62. (Cancelled)

63. (Previously Presented) The apparatus according to claim 21, wherein said first Central-Entity computer and said second Central-Entity computer are the same.

64. (Previously Presented) The apparatus according to claim 21, wherein said first Central-Entity computer and said second Central-Entity computer are different.

65. (Previously Presented) A method as recited in claim 1, wherein said digital identity

comprises the SecureCode and a user-specific information.

66. (Previously Presented) A method as recited in claim 1, wherein said digital identity comprises the SecureCode.

67. (Previously Presented) A method as recited in claim 1, wherein said digital identity is invalid if the SecureCode is invalid.

68. (Previously Presented) A method as recited in claim 1, wherein said digital identity is valid if at least the SecureCode is valid.

69. (Previously Presented) A method as recited in claim 1, wherein said External-Entity authenticates the user upon receiving an affirmation authentication message from the Central-Entity.

70. (Previously Presented) A method as recited in claim 1, wherein said External-Entity authenticates the user if said Central-Entity authenticates the user based on the SecureCode.

71. (Previously Presented) The apparatus of claim 21, wherein said digital identity is invalid if the SecureCode is invalid.

72. (Previously Presented) The apparatus of claim 21, wherein said digital identity is valid if at least the SecureCode is valid.

73. (Previously Presented) The apparatus of claim 21, wherein said External-Entity authenticates the user upon receiving an affirmation authentication message from the Central-Entity.

74. (Previously Presented) The apparatus of claim 21, wherein said digital identity comprises the SecureCode.

75. (Previously Presented) The apparatus of claim 21, wherein said Central-Entity invalidates the SecureCode after authenticating the user.

76. (Previously Presented) The apparatus of claim 21, wherein the Central-Entity invalidates the SecureCode after a predefined period of time passes after the SecureCode was generated.

77. (Previously Presented) The apparatus of claim 21, wherein said Central-Entity generates the SecureCode based on said user information.

78. (Previously Presented) The apparatus of claim 77, wherein said user information comprises one or more of the following: an alphanumeric name, an ID, a login name, a password, and an identification phrase.

79. (Previously Presented) The method of claim 65, wherein the user specific information

comprises one or more of the following: an alphanumeric name, an ID, a login name, and an identification phrase.

80. (Previously Presented) The apparatus of claim 21, wherein said External-Entity authenticates the user if said Central-Entity authenticates the user based on the SecureCode.

81. (Previously Presented) The apparatus of claim 21, wherein said External-Entity and Central-Entity are the same entity.

82. (Previously Presented) A method as recited in claim 50, wherein said External-Entity and Central-Entity are the same entity.

83. (Previously Presented) The method of claim 50, wherein said digital identity includes a user-specific information.

84. (Previously Presented) The method of claim 83, wherein the user-specific information includes user-identifying information.

85. (Previously Presented) The method of claim 83, wherein the user-specific information comprises one or more of the following: an alphanumeric name, an ID, a login name, and an identification phrase.

86. (Previously Presented) The apparatus of claim 52, wherein said External-Entity and

Central-Entity are the same entity.

87. (Previously Presented) The apparatus of claim 52, wherein said digital identity includes an user-specific information.

88. (Previously Presented) The apparatus of claim 87, wherein the user-specific information includes user-identifying information.

89. (Previously Presented) The method of claim 87, wherein the user-specific information comprises one or more of the following: an alphanumeric name, an ID, a login name, and an identification phrase.

90. (Previously Presented) The method of claim 14, wherein the user-specific information includes user-identifying information.

91. (Previously Presented) The apparatus of claim 34, wherein the user-specific information includes user-identifying information.

REMARKS

Claims 1-4, 12-24, 32-41, 43-48, 50-55, 58, 60 and 63-91were previously pending. Claims 5-11, 25-31, 42, 49, 56-57, 59 and 61-62 have been previously cancelled without disclaimer of or prejudice to the subject matter contained therein. Claims 2-3 have been cancelled without disclaimer of or prejudice to the subject matter contained therein. Claims 1, 4 and 41 have been amended as indicated below. Claims 1, 4, 12-24, 32-41, 43-48, 50-55, 58, 60 and 63-91 remain pending.

OBJECTION TO THE SPECIFICATION

The Examiner objected to the specification for failing to provide proper antecedent basis for the claimed subject matter citing 37 C.F.R. § 1.74(d) and MPEP § 608.01(o). Specifically, the Examiner contends claims 2 and 3 lack support for whether the user has a pre-existing relationship with the External Entity or not. While the Applicants respectfully disagree with the Examiner's contentions, to expedite issuance of a notice of allowance, claims 2-3 have been cancelled without disclaimer of or prejudice to the subject matter contained therein.

With regard to claim 4, the Examiner contends this claim remains unclear. The Applicants have amended claim 4 to be consistent with the specification, at page 14, first full paragraph.

With regard to claim 41, the Examiner contends this claim is not supported in the specification. The Applicants have amended claim 41 to be consistent with the specification at page 14, first full paragraph.

In light of the foregoing amendments, the Applicants respectfully request reconsideration and withdrawal of the objection to the specification and claims 2-4, and 41.

CLAIM OBJECTIONS

The Examiner objected to claim 1 based on a certain informality, which has been corrected. In light of the correction, the Applicants respectfully request reconsideration and withdrawal of the objection to claim1.

CLAIMS REMAIN PATENTABLE OVER *KALISKI, JR.* AND *HILL* EITHER TAKEN ALONE OR IN COMBINATION

The Office Action rejected claims 1-4, 12-20, 22-24, 32-41, 43-48, 50-55, 58, 60, 63 and 65-91 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent Publication No. 2010/0100724 A1 by Kaliski, Jr.[hereinafter "*Kaliski, Jr.*"] in view of U.S. Patent No. 6,236,981 by Hill [hereinafter "Hill"]. Generally, the Office Action contends that *Kaliski, Jr.* discloses all of the elements of the claims, except for certain missing features that it contends can be found in *Hill*, and further contends that it would have been obvious to one of ordinary skill in the art to modify the system of *Kaliski, Jr.* using these certain missing features from *Hill* for various specified reasons. For example with regard to claim 1, the Office Action asserts that *Kaliski, Jr.* discloses all of the elements of the claim at issue, except for "that the dynamic SecureCode becomes invalid after being used." The Applicants respectfully disagree with the Office Action's characterization of these references vis-à-vis the claims at issue and respectfully request reconsideration and withdrawal of the rejection in light of the following remarks.

Factual Inquiries Set Forth in Graham v. John Deere Show Non-Obviousness

1. Determining Scope of Prior Art

Kaliski, Jr. teaches a technique for developing a hardened password that is then used to derive a decryption key or as the decryption key, which decryption key is then used to successfully decrypt user information thereby verifying the authenticity of the user. Thus, the hardened password is not used to authenticate the user, but rather successful decryption is the basis for authenticating the user. *Aff. N. Kamrani filed 030112, ¶¶13-15; Aff. K. Kamrani filed 030112, ¶¶14-16; Aff. Hewitt filed 030112, ¶¶17-19;* and *Aff. Hosseinzadeh filed 030112, ¶¶13-15.*

Hill teaches the use of digital tokens as a payment mechanism. The digital tokens are not used to authenticate the user. The issuer merely authenticates the digital tokens as valid payment but not as authentication of the user. *Aff. N. Kamrani filed 030112, ¶¶16-19; Aff. K. Kamrani filed 030112, ¶¶17-20; Aff. Hewitt filed 030112, ¶¶21-23;* and *Aff. Hosseinzadeh filed 030112, ¶¶16-19.*

2. Ascertaining the Differences Between the Prior Art and Claims at Issue

The Claims at issue include the limitations that the dynamic SecureCode is generated during the transaction between the user and the External-Entity and that the so generated dynamic SecureCode is then used by a Central Entity to authenticate the user to an External Entity. *Kaliski, Jr.* does not authenticate a user based on any code generated during the transaction between the user and the merchant because successful decryption forms the basis of authentication in *Kaliski, Jr. Aff. N. Kamrani filed 030112, ¶¶13-15; Aff. K. Kamrani filed 030112, ¶¶14-16; Aff. Hewitt filed 030112, ¶¶17-19;* and *Aff. Hosseinzadeh filed 030112, ¶¶13-15.*

Hill also does not authenticate a user based on a code generated during the transaction. In fact, *Hill* fails to teach any authentication of the user but merely authentication of payment tokens, which are not used for authentication of the user. *Aff. N. Kamrani filed 030112, ¶¶16-*

19; Aff. K. Kamrani filed 030112, ¶¶17-20; Aff. Hewitt filed 030112, ¶¶21-23; and *Aff. Hosseinzadeh filed 030112, ¶¶16-19. Hill* is merely cited for the claim element that the SecureCode becomes invalid after use.

Nonce Is Not Recited SecureCode

The Examiner equates the nonce of *Kaliski, Jr.* to the SecureCode of the present application ("wherein the nonce corresponds to the recited dynamic SecureCode." Office Action, p. 4). But the Applicants respectfully submit that the nonce is not equivalent to the recited dynamic SecureCode. *Aff. N. Kamrani filed 030112, ¶¶5-8; Aff. K. Kamrani filed 030112, ¶¶6-9; Aff. Hewitt filed 030112, ¶¶9-12;* and *Aff. Hosseinzadeh filed 030112, ¶¶5-8.* A nonce is merely a session identifier that is associated with each user's session in a client server arrangement. *Id.*

Authentication Not Based on SecureCode

Next, the Office Action contends that *Kaliski, Jr.* teaches the claim element "authenticating ... the user during the transaction if the digital identity is valid." For this claim element, the Examiner refers to paragraph [0112] of *Kaliski, Jr.* However, in *Kaliski, Jr.* authentication is not based on the digital identity that includes the nonce, but rather authentication is based on successful decryption of an electronic signature. *Aff. N. Kamrani filed 030112, ¶¶13-15; Aff. K. Kamrani filed 030112, ¶¶14-16; Aff. Hewitt filed 030112, ¶¶17-19;* and *Aff. Hosseinzadeh filed 030112, ¶¶13-15.*

In *Kaliski, Jr.* authentication is not based on the nonce, rather the nonce is merely an identifier used to indicate "whether or not the authentication attempt associated with the nonce was successful." *Kaliski, Jr., ¶ [0112]. Aff. N. Kamrani filed 030112, ¶¶5-8; Aff. K. Kamrani* *filed 030112, ¶¶6-9; Aff. Hewitt filed 030112, ¶¶9-12;* and *Aff. Hosseinzadeh filed 030112, ¶¶5-8.*

Authentication Server Equated with the Central Entity by the Office Action Does Not Authenticate the User as Recited in the Claims

The Office Action equates the recited Central Entity with the Authentication Server 730 of FIG. 7 from *Kaliski, Jr. Office Action, p. 4.* Claim 1 specifically states "authenticating by the Central Entity the user during the transaction..." However, the Authentication Server 730 of *Kaliski, Jr.* does not authenticate the user, but rather the web server 710 authenticates the user based on successful decryption of the user's digital signature. *Aff. N. Kamrani filed 030112, ¶¶10-12; Aff. K. Kamrani filed 030112, ¶¶11-13; Aff. Hewitt filed 030112, ¶¶14-16;* and *Aff. Hosseinzadeh filed 030112, ¶¶10-12.*

Authentication Server Equated with the Central Entity by the Office Action Does Not Receive Authentication Request as Recited in the Claims

Claim 1 also recites "receiving electronically by the Central Entity a request for authenticating the user based on a digital identity during the transaction, which digital identity includes the SecureCode." However, the Authentication Server 730 of *Kaliski, Jr.* does not receive a request for authenticating the user because the web server 710 authenticates the user based on successful decryption of the user's digital signature. *Aff. N. Kamrani filed 030112, ¶9; Aff. K. Kamrani filed 030112, ¶10; Aff. Hewitt filed 030112, ¶13;* and *Aff. Hosseinzadeh filed 030112, ¶9.* Thus, neither reference includes the recited claim elements of: (1) authenticating the user based on a SecureCode; (2) receiving an authentication request message by a Central Entity, which message includes a SecureCode generated by the Central Entity; (3) authenticating the user by the Central Entity that generated the SecureCode. Without these features, the suggested combination fails to state a *prima facie* case of obviousness. Reconsideration and withdrawal of the rejection of these claims is therefore respectfully requested.

CLAIMS REMAIN PATENTABLE OVER *KALISKI, JR.* AND *HILL* TAKEN ALONE OR IN COMBINATION WITH CERTAIN OFFICIAL NOTICE

The Office Action rejected claims 23, 66, 68, 70 and 71 under 35 U.S.C. § 103(a) as being unpatentable over the combination of *Kaliski, Jr.* and *Hill* and further in view of certain Official Notice. The Office Action contends that the above mentioned combination of *Kaliski, Jr.* and *Hill* discloses all of the elements of the claim at issue, except for "wherein the request for the dynamic code is received by a computer associated with a first trusted authenticator and the authentication request is received by a computer associated with a second trusted authenticator that is different than the first trusted authenticator," for which the Office Action provides certain Official Notice. The Office Action takes Official Notice for this teaching absent from *Kaliski, Jr.* and *Hill.* Specifically, the Office Action states:

> Official Notice is taken that it is old and well-known practice in the art that in some system or arrangement more than one computer is used to provide services to their clients (i.e., different computers for different purposes and services). Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made [sic] to modify the system of Kaliski-Hill to deploy one computer for providing a dynamic code to a client and another computer for authenticating the dynamic code (i.e., verifying the identity of the user) whenever the user request [sic] a service because this arrangement would make the system of Kaliski-Hill capable of handling cases such as when the entity and the user have their own different trusted authenticators.

Office Action, p. 9.

The Applicants respectfully submit that the Official Notice does not encompass the claimed subject matter. The cited claim element states that there are different trusted authenticators for the request for a dynamic code and the authentication request based on the dynamic code. The Official Notice taken does not state that it is old and well-known in the art to use different trusted authenticators, but merely that different computers are used for different purposes. There is a missing feature in the Official Notice – that different trusted authenticators are used for these specific different purposes. Therefore, the Applicants respectfully submit that splitting up the functions of receiving a request for a dynamic code and receiving an authentication request between different trusted authenticators is not a well-known practice, and if the Examiner is assuming so, then the Applicants respectfully request that the Examiner provide support for this contention from the prior art.

According to the M.P.E.P. § 2144.03(C), "If Applicant Challenges a Factual Assertion as Not Properly Officially Noticed or Not Properly Based Upon Common Knowledge, the Examiner Must Support the Finding With Adequate Evidence." In this instance, the Applicants have shown that the recited Official Notice is different than the claim element at issue. Therefore, the Applicants respectfully submit they have adequately traversed the finding of Official Notice.

> To adequately traverse [a finding of Official Notice], an applicant must specifically point out the supposed errors in the examiner's action, which would include stating why the noticed fact is not considered to be common knowledge or well-known in the art. *See 37 CFR 1.111(b). See also Chevenard,* 139 F.2d at 713, 60 USPQ at 241 ("[I]n the absence of any demand by appellant for the examiner to produce authority for his statement, we will not consider this contention.").

M.P.E.P § 2144.03(C).

The Applicants contend that merely knowing that "more than one computer [can be] used to provide services to their clients (i.e., different computers for different purposes and services)" does not lead one to the conclusion that one should use different trusted authenticators for the different recited purposes.

> If applicant adequately traverses the examiner's assertion of official notice, the examiner must provide documentary evidence in the next Office action if the rejection is to be maintained. *See 37 CFR 1.104(c)(2). See also Zurko*, 258 F.3d at 1386, 59 USPQ2d at 1697 ("[T]he Board [or examiner] must point to some concrete evidence in the record in support of these findings" to satisfy the substantial evidence test). If the examiner is relying on personal knowledge to support the finding of what is known in the art, the examiner must provide an affidavit or declaration setting forth specific factual statements and explanation to support the finding. *See 37 CFR 1.104(d)(2).*

M.P.E.P § 2144.03(C).

The Applicants therefore specifically request that the Examiner provide documentary evidence in the next Office action that different trusted authenticators are used for receiving a request for a dynamic code and receiving an authentication request based on the dynamic code, if this rejection is to be maintained.

Moreover, these claims remain patentable for at least the reasons set forth above with respect to the combination of *Kaliski, Jr.* and *Hill.* The Applicants therefore respectfully request reconsideration and withdrawal of the rejection of claims 23, 66, 68, 70 and 71.

CONCLUSION

The Applicant respectfully submits this application is in condition for allowance and requests issuance of a Notice of Allowance.

Although not believed necessary, the Office is hereby authorized to charge any fees required under 37 C.F.R. § 1.16 or § 1.17 or credit any overpayments to the deposit account of MICHAEL P FORTKORT PC, Deposit Account No. 50-3776.

In the event the prosecution of this Application can be efficiently advanced by a phone discussion, it is requested that the undersigned attorney be called at (703) 435-9390.

Respectfully submitted,

By /Michael P. Fortkort/ Date: March 1, 2012
Michael P. Fortkort (Reg. No. 35,141)

MICHAEL P FORTKORT PC
The International Law Center
13164 Lazy Glen Lane
Oak Hill, Virginia 20171

Please direct telephone calls to:
Michael P. Fortkort
703-435-9390
703-435-8857 (facsimile)

Certification Under 37 C.F.R. § 1.8

I hereby certify that on March 1, 2012 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: March 1, 2012 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 12/210,926

FILING DATE: September 15, 2008

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

ATTORNEY DOCKET: KAMR002US0

CONFIRMATION NO.: 7516

VIA ELECTRONIC FILING SYSTEM
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

AFFIDAVIT UNDER RULE 132

Applicants hereby submit this affidavit in support of their response to the Office Action mailed January 6, 2012 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 12/210,926, and pursuant to the provisions of 37 C.F.R. § 1.132. The witness hereby avers and testifies as follows:

U.S. Patent Application No. 12/210,926
Attorney Docket No. KAMR002US0

1. I am Nader Asghari-Kamrani, one of the inventors listed in U.S. patent Application, which is the subject of the present proceeding ("*Kamrani*").

2. I received a degree in computer science from Technical University of Vienna, in Vienna, Austria in 1993. I have been working in the field of authentication over communication networks since 2000. I am one of skill in the art of authentication and electrical transactions, including PKI and digital signature, online credit card payment as well as banking transactions.

3. I am familiar with the specification and pending claims of the present Application.

4. I have reviewed U.S. Patent Publication No. 2010/0100724 A1 by Kaliski, Jr. ("*Kaliski, Jr.*").

Nonce Not Equivalent to SecureCode

5. One of skill in the authentication art would understand that an **identifier** is non secret information such as a name or label that identifies an entity. And in the world of authentication an identifier is only used for identification of an entity and not for authentication of the entity.

6. One of skill in the authentication art would understand that in *Kaliski, Jr.*, a nonce is a **session identifier**. "The authentication server 730 returns the blinded result R to the client 715, along with **a nonce or other session identifier** 772." *Kaliski, Jr.*, ¶ [0111] (emphasis supplied).

A *cryptographic nonce* is an arbitrary number used to establish the uniqueness or discreteness of an operation. That is, an operation such as a data request is accompanied by a nonce in order to demonstrate that the request is not a repeat or re-play of a previous request.

A *session* is a series of information exchanges between two communicating parties, usually involving an initiation protocol and more than one message in each direction.

In *Kaliski, Jr.* a nonce is used for identification of a user's session. In the client/server world, a session refers to all the requests that a single client makes to a server. A session is specific to each user and for each user a new session is created to track all the requests from that user. Every user has a separate session and separate session identifier is associated with that session.

7. One of skill in the authentication art would understand that the nonce in *Kaliski, Jr.* is not equivalent to the SecureCode of the present application. A nonce is a session identifier associated with a user's session, but a nonce is not used for authentication of a user, as is the SecureCode recited in the claims of *Kamrani.*

8. One of skill in the authentication art would understand that the statement "the nonce corresponds to the recited dynamic SecureCode" is inaccurate. In *Kaliski, Jr.* the web server receives the nonce and hardened password from the client and authenticates the user based on successful decryption of a digital signature associated with the hardened password. *Kaliski, Jr.*, ¶¶ *[0109] and [0112].* The nonce is used by the web server to identify the user and the hardened password used in the authentication process of authenticating the user. In *Kamrani*, a dynamic code authenticates a user whereas in *Kaliski, Jr.* a nonce is a session identifier. Therefore the argument that "the nonce corresponds to the recited dynamic code" is invalid.

No Authentication Request Message

9. One of skill in the authentication art would understand that in the system of *Kaliski, Jr.* there is nothing equivalent to a Central Entity receiving an authentication request message, as recited in the claims at issue. The Office Action equates the claimed authentication request message to message 776 of *Kaliski, Jr.* But, message 776 that the authentication server in FIG 7 of *Kaliski, Jr.* receives is NOT an authentication request message. Rather, message 776 indicates simply whether or not the authentication of the

client by the web server was successful. *See Kaliski, Jr.* ¶¶ *[0109] through [0112]*. This message 776 is a one way acknowledgement and expects no return, whereas the authentication request message as recited in the claims at issue is a different type of message than the cited acknowledgement as the claimed authentication request should generate a response because it is a REQUEST as opposed to an acknowledgement. Thus, the message in *Kaliski, Jr.* cited by the Office Action at issue is not equivalent to the claimed authentication request message in *Kamrani*. Thus, one of skill in the authentication art would understand that the argument in the Office Action equating the claimed authentication request message to the acknowledgement message 776 in *Kaliski, Jr.* is not valid.

No Central Entity Authenticating User

10. One of skill in the authentication art would understand that there is nothing in *Kaliski, Jr.* equivalent to a Central Entity authenticating the user as recited in the claims at issue. The Office Action equates the Central Entity to the authentication server 730 in *Kaliski, Jr.* But, the authentication server 730 in FIG 7 never authenticates the client. Rather, the web server 710 authenticates the client based on successful decryption of the client's digital signature associated with the hardened password. *See Kaliski, Jr.* ¶¶ [0109] through [0112]. Moreover, the web server 710 of *Kaliski, Jr.* does not generate anything equivalent to the claimed SecureCode, as recited in the claims at issue. Thus, neither the web server 710 nor the authentication server 730 of *Kaliski, Jr.* performs the functions of the Central Entity recited in the claims.

11. One of skill in the authentication art would understand that in *Kaliski, Jr.* a user's client application generates a hardened password (based on the blinded result R received from the authentication server) and submits the generated hardened password to the web server and not to the authentication server cited by the Office Action. In *Kaliski, Jr.* the

client receives the blinded result R along with a nonce from the authentication server and generates the hardened password at the client side for authentication to the web server. *Kaliski, Jr.*, ¶ [0111].

12. One of skill in the authentication art would understand that the argument in the Office Action equating the claimed "authenticating by the Central-Entity the user during the transaction, if the digital identity is valid" with the authentication protocol in *Kaliski, Jr.* is not valid. The authentication server 730 does not authenticate the client; it is the web server that authenticates the client. And, the web server 710 of *Kaliski, Jr.* also cannot be the claimed Central Entity because the web server does not generate anything equivalent to the claimed SecureCode. Thus, there is no Central Entity authenticating the user in *Kaliski, Jr.*

Authentication Process Different

13. The web server of *Kaliski, Jr.*stores the user's personal information as encryption secrets (See *Kaliski, Jr.*, ¶ *[0103]*) and the encrypted secrets are stored such that they can be decrypted with a decryption key/hardened password. In *Kaliski, Jr.* a blind function evaluation protocol is used by the client to drive a decryption key/hardened password from a blinded result R received from the authentication server (See *Kaliski, Jr.*, ¶ *[0111]*), to decrypt the encrypted secrets. The web server authenticates the client if the hardened password received from the client successfully decrypt user's information.

14. It is clear that in *Kaliski, Jr.*, authentication is based on a cryptographic protocol. The use of this cryptographic approach allows authenticity of a client to be checked by creating a digital signature of a user's personal information using the encryption key, which can be verified using hardened password as the decryption key received from the client during the transaction.

15. One of skill in the authentication art would understand that in the blind function evaluation protocol used in *Kaliski, Jr.* (*See, Kaliski, Jr.* ¶ *[0038]*), the client has some secret

information and the authentication server has some secret information, and together the client and the authentication server provide their respective secrets as an input to a jointly calculated function, with only the client obtaining the output of the jointly calculated function (the output is the decryption key or hardened password). This means that only the client obtains the hardened password (decryption key) as the output of the blind function evaluation protocol. See *Kaliski, Jr.* Figure 7. The authentication server of *Kaliski, Jr.* which the Office Action equated to the Central Entity of the claims cannot generate the hardened password (decryption key) since the authentication server does not have access to the client's secret information. See *Kaliski, Jr.* ¶ [0040], which states:

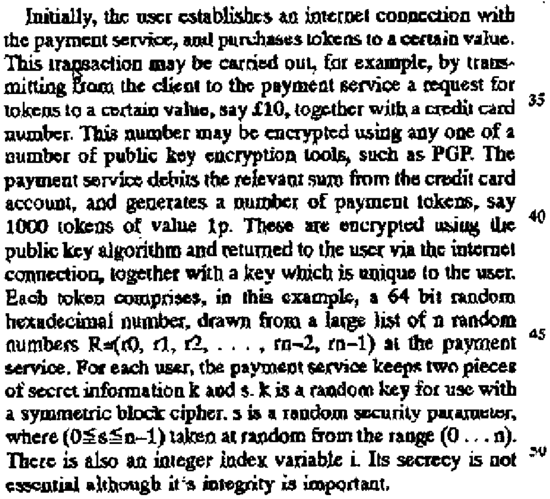
> The use of a blind function evaluation protocol, or other embodiments in which the decryption key is derived from the client information, provides additional security benefits resulting from the fact that the first server 30 does not have the decryption key in an unblinded form. Even if the first server 30 is compromised, and a server secret obtained, it will still be necessary for an attacker to do more work to transform the server secret into the decryption key. Just as one example, in one such embodiment, the first server 30 and client 15 engage in a blind function evaluation protocol that results in the first server 30 providing to the client 15 a blinded key as the intermediate data 22. The client 15 has information used to unblind the decryption key 24, which is then used to decrypt the encrypted secrets 5. Compromise of the first server 30 would still not directly reveal the decryption key 25 to an attacker.

Thus, the entire basis for authentication in *Kaliski, Jr.* is different than the claimed SecureCode authentication process of *Kamrani*, and one of ordinary skill in the art would understand this difference.

Hill et al.

16. One of skill in the authentication and payment art would understand that the user of *Hill et al.* purchases a set of payment tokens from the payment service provider before the user being involved in any transaction with the merchant. *Hill et al., col. 5, lines 31-51*

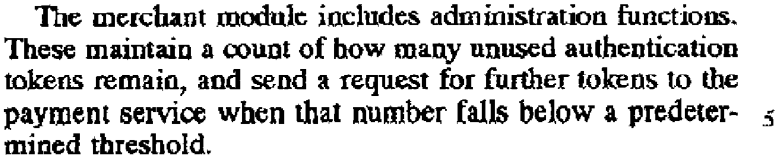
and col. 8, lines 1-9. The tokens are not valid for a predefined period of time because the user buys them. The tokens are like real money and will be used for online purchases.



Initially, the user establishes an internet connection with the payment service, and purchases tokens to a certain value. This transaction may be carried out, for example, by transmitting from the client to the payment service a request for tokens to a certain value, say £10, together with a credit card number. This number may be encrypted using any one of a number of public key encryption tools, such as PGP. The payment service debits the relevant sum from the credit card account, and generates a number of payment tokens, say 1000 tokens of value 1p. These are encrypted using the public key algorithm and returned to the user via the internet connection, together with a key which is unique to the user. Each token comprises, in this example, a 64 bit random hexadecimal number, drawn from a large list of n random numbers R=(r0, r1, r2, . . . , rn−2, rn−1) at the payment service. For each user, the payment service keeps two pieces of secret information k and s. k is a random key for use with a symmetric block cipher. s is a random security parameter, where (0≦s≦n−1) taken at random from the range (0 . . . n). There is also an integer index variable i. Its secrecy is not essential although it's integrity is important.

17. One of skill in the authentication art would understand that the payment server of *Hill et al.* encrypt the generated set of tokens with user's public key and send it to the user before the user starting any transactions with a merchant. *Hill et al., col. 5, lines 40-42.* The Carnet program installed on user's computer stores the tokens. *Hill Col. 5, lines 25-30 and lines 52-65; Col 6, lines 3-20.*

18. One of skill in the authentication art would understand that the merchant stores a set of authentication tokens before starting any transaction with the user. *Hill et al., col. 6, lines 46-47 and col. 13, lines 1-5.*



The merchant module includes administration functions. These maintain a count of how many unused authentication tokens remain, and send a request for further tokens to the payment service when that number falls below a predetermined threshold.

19. One of skill in the authentication art would understand that the authentication tokens of the merchant are similar to the payment tokens of the user. The tokens are issued to the merchant at the time of registration and before the merchant or the user being involved in any transaction. *Hill et al.*, col 6, lines 25-32. The merchant and the user do not receive any tokens at the time of the transaction and the tokens stored at the user or merchant's computer are not valid for a predefined period of time. Hill's tokens do not serve an identification function, but rather act is a fungible financial instrument. That is, a given quantity or value of tokens is equivalent to their stated value in dollars.

I affirm that all statements made herein of my own knowledge are true, and that all statements made herein on information and belief are believed to be true. I understand that willful false statements and the like are punishable by fine or imprisonment, or both (18 U.S.C. 1001), and may jeopardize the validity of the present patent application or any patent issuing thereon.

FURTHER AFFIANT SAYETH NOT.

It witness whereof,

Nader Asghari-Kamrani

02/27/2012
Date

U.S. Patent Application No. 12/210,926
Attorney Docket No. KAMR002US0

Certification Under 37 C.F.R. § 1.8

I hereby certify that on March 1, 2012 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: March 1, 2012 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 12/210,926

FILING DATE: September 15, 2008

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

ATTORNEY DOCKET: KAMR002US0

CONFIRMATION NO.: 7516

VIA ELECTRONIC FILING SYSTEM
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

AFFIDAVIT UNDER RULE 132

Applicants hereby submit this affidavit in support of their response to the Office Action mailed January 6, 2012 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 12/210,926, and pursuant to the provisions of 37 C.F.R. § 1.132. The witness hereby avers and testifies as follows:

1. I am Kamran Asghari-Kamrani, one of the inventors listed in U.S. patent Application, which is the subject of the present proceeding.

2. Bachelor of Computer Science – Specialization: Data Management and Database Design, Technical University of The Hague, The Hague, Netherlands.

3. Director, CGI Federal. Senior level business and IT professional with over 18 years of experience in architecting and leading complex enterprise-wide solutions for Fortune 1000 companies and the federal government; an Expert in authorization and authentication, fraud and identity theft prevention; Devoted much of my time to studying, and devising solutions for these multifaceted problems; Knowledgeable in the computer Architecture Software and Information Security area.

4. I am familiar with the specification and pending claims of the present Application.

5. I have reviewed U.S. Patent Publication No. 2010/0100724 A1 by Kaliski, Jr. ("*Kaliski, Jr.*").

Nonce Not Equivalent to SecureCode

6. One of skill in the authentication art would understand that an **identifier** is non secret information such as a name or label that identifies an entity. And in the world of authentication an identifier is only used for identification of an entity and not for authentication of the entity.

7. One of skill in the authentication art would understand that in *Kaliski, Jr.*, a nonce is a **session identifier**. "The authentication server 730 returns the blinded result R to the client 715, along with **a nonce or other session identifier** 772." *Kaliski, Jr.*, ¶ [0111] (emphasis supplied).

A *cryptographic nonce* is an arbitrary number used to establish the uniqueness or discreteness of an operation. That is, an operation such as a data request is accompanied by a nonce in order to demonstrate that the request is not a repeat or re-play of a previous request.

A *session* is a series of information exchanges between two communicating parties, usually involving an initiation protocol and more than one message in each direction.

In *Kaliski, Jr.* a nonce is used for identification of a user's session. In the client/server world, a session refers to all the requests that a single client makes to a server. A session is specific to each user and for each user a new session is created to track all the requests from that user. Every user has a separate session and separate session identifier is associated with that session.

8. One of skill in the authentication art would understand that the nonce in *Kaliski, Jr.* is not equivalent to the SecureCode of the present application. A nonce is a session identifier associated with a user's session, but a nonce is not used for authentication of a user, as is the SecureCode recited in the claims of *Kamrani.*

9. One of skill in the authentication art would understand that the statement "the nonce corresponds to the recited dynamic SecureCode" is inaccurate. In *Kaliski, Jr.* the web server receives the nonce and hardened password from the client and authenticates the user based on successful decryption of a digital signature associated with the hardened password. *Kaliski, Jr.*, ¶¶ *[0109] and [0112].* The nonce is used by the web server to identify the user and the hardened password used in the authentication process of authenticating the user. In *Kamrani*, a dynamic code authenticates a user whereas in *Kaliski, Jr.* a nonce is a session identifier. Therefore the argument that "the nonce corresponds to the recited dynamic code" is invalid.

No Authentication Request Message

10. One of skill in the authentication art would understand that in the system of *Kaliski, Jr.* there is nothing equivalent to a Central Entity receiving an authentication request message, as recited in the claims at issue. The Office Action equates the claimed authentication request message to message 776 of *Kaliski, Jr.* But, message 776 that the authentication server in FIG 7 of *Kaliski, Jr.* receives is NOT an authentication request message. Rather, message 776 indicates simply whether or not the authentication of the client by the web server was successful. *See Kaliski, Jr. ¶¶ [0109] through [0112]*. This message 776 is a one way acknowledgement and expects no return, whereas the authentication request message as recited in the claims at issue is a different type of message than the cited acknowledgement as the claimed authentication request should generate a response because it is a REQUEST as opposed to an acknowledgement. Thus, the message in *Kaliski, Jr.* cited by the Office Action at issue is not equivalent to the claimed authentication request message in *Kamrani*. Thus, one of skill in the authentication art would understand that the argument in the Office Action equating the claimed authentication request message to the acknowledgement message 776 in *Kaliski, Jr.* is not valid.

No Central Entity Authenticating User

11. One of skill in the authentication art would understand that there is nothing in *Kaliski, Jr.* equivalent to a Central Entity authenticating the user as recited in the claims at issue. The Office Action equates the Central Entity to the authentication server 730 in *Kaliski, Jr.* But, the authentication server 730 in FIG 7 never authenticates the client. Rather, the web server 710 authenticates the client based on successful decryption of the client's digital signature associated with the hardened password. *See Kaliski, Jr.* ¶¶ [0109] through [0112]. Moreover, the web

server 710 of *Kaliski, Jr.* does not generate anything equivalent to the claimed SecureCode, as recited in the claims at issue. Thus, neither the web server 710 nor the authentication server 730 of *Kaliski, Jr.* performs the functions of the Central Entity recited in the claims.

12. One of skill in the authentication art would understand that in *Kaliski, Jr.* a user's client application generates a hardened password (based on the blinded result R received from the authentication server) and submits the generated hardened password to the web server and not to the authentication server cited by the Office Action. In *Kaliski, Jr.* the client receives the blinded result R along with a nonce from the authentication server and generates the hardened password at the client side for authentication to the web server. *Kaliski, Jr.*, ¶ [0111].

13. One of skill in the authentication art would understand that the argument in the Office Action equating the claimed "authenticating by the Central-Entity the user during the transaction, if the digital identity is valid" with the authentication protocol in *Kaliski, Jr.* is not valid. The authentication server 730 does not authenticate the client; it is the web server that authenticates the client. And, the web server 710 of *Kaliski, Jr.* also cannot be the claimed Central Entity because the web server does not generate anything equivalent to the claimed SecureCode. Thus, there is no Central Entity authenticating the user in *Kaliski, Jr.*

Authentication Process Different

14. The web server of *Kaliski, Jr.* stores the user's personal information as encryption secrets (See *Kaliski, Jr., ¶ [0103]*) and the encrypted secrets are stored such that they can be decrypted with a decryption key/hardened password. In *Kaliski, Jr.* a blind function evaluation protocol is used by the client to drive a decryption key/hardened password from a blinded result R received from the authentication server (See *Kaliski, Jr., ¶ [0111]*), to decrypt the encrypted

secrets. The web server authenticates the client if the hardened password received from the client successfully decrypt user's information.

15. It is clear that in *Kaliski, Jr.*, authentication is based on a cryptographic protocol. The use of this cryptographic approach allows authenticity of a client to be checked by creating a digital signature of a user's personal information using the encryption key, which can be verified using hardened password as the decryption key received from the client during the transaction.

16. One of skill in the authentication art would understand that in the blind function evaluation protocol used in *Kaliski, Jr.* (*See, Kaliski, Jr.* ¶ *[0038]*), the client has some secret information and the authentication server has some secret information, and together the client and the authentication server provide their respective secrets as an input to a jointly calculated function, with only the client obtaining the output of the jointly calculated function (the output is the decryption key or hardened password). This means that only the client obtains the hardened password (decryption key) as the output of the blind function evaluation protocol. See *Kaliski, Jr.* Figure 7. The authentication server of *Kaliski, Jr.* which the Office Action equated to the Central Entity of the claims cannot generate the hardened password (decryption key) since the authentication server does not have access to the client's secret information. See *Kaliski, Jr.* ¶ [0040], which states:

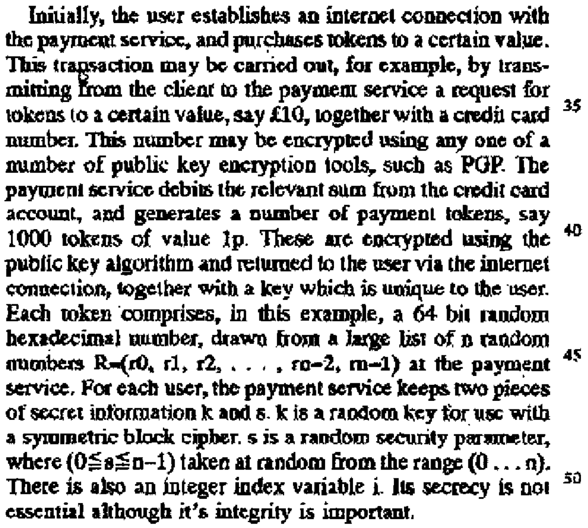
> The use of a blind function evaluation protocol, or other embodiments in which the decryption key is derived from the client information, provides additional security benefits resulting from the fact that the first server 30 does not have the decryption key in an unblinded form. Even if the first server 30 is compromised, and a server secret obtained, it will still be necessary for an attacker to do more work to transform the server secret into the decryption key. Just as one example, in one such embodiment, the first server 30 and client 15 engage in a blind function evaluation protocol that results in the first server 30 providing to the client 15 a blinded key as the intermediate data 22. The client

> 15 has information used to unblind the decryption key 24, which is then used to decrypt the encrypted secrets 5. Compromise of the first server 30 would still not directly reveal the decryption key 25 to an attacker.

Thus, the entire basis for authentication in *Kaliski, Jr.* is different than the claimed SecureCode authentication process of *Kamrani*, and one of ordinary skill in the art would understand this difference.

Hill et al.

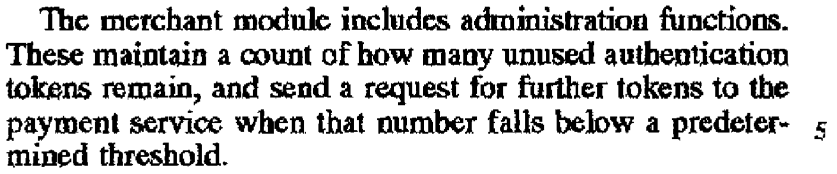
17. One of skill in the authentication and payment art would understand that the user of *Hill et al.* purchases a set of payment tokens from the payment service provider before the user being involved in any transaction with the merchant. *Hill et al., col. 5, lines 31-51 and col. 8, lines 1-9.* The tokens are not valid for a predefined period of time because the user buys them. The tokens are like real money and will be used for online purchases.



Initially, the user establishes an internet connection with the payment service, and purchases tokens to a certain value. This transaction may be carried out, for example, by transmitting from the client to the payment service a request for tokens to a certain value, say £10, together with a credit card number. This number may be encrypted using any one of a number of public key encryption tools, such as PGP. The payment service debits the relevant sum from the credit card account, and generates a number of payment tokens, say 1000 tokens of value 1p. These are encrypted using the public key algorithm and returned to the user via the internet connection, together with a key which is unique to the user. Each token comprises, in this example, a 64 bit random hexadecimal number, drawn from a large list of n random numbers $R=(r0, r1, r2, \ldots, rn-2, rn-1)$ at the payment service. For each user, the payment service keeps two pieces of secret information k and s. k is a random key for use with a symmetric block cipher. s is a random security parameter, where $(0 \leqq s \leqq n-1)$ taken at random from the range $(0 \ldots n)$. There is also an integer index variable i. Its secrecy is not essential although it's integrity is important.

18. One of skill in the authentication art would understand that the payment server of *Hill et al.* encrypt the generated set of tokens with user's public key and send it to the user before the user starting any transactions with a merchant. *Hill et al., col. 5, lines 40-42.* The Carnet program installed on user's computer stores the tokens. *Hill Col. 5, lines 25-30 and lines 52-65; Col 6, lines 3-20.*

19. One of skill in the authentication art would understand that the merchant stores a set of authentication tokens before starting any transaction with the user. *Hill et al., col. 6, lines 46-47 and col. 13, lines 1-5.*



The merchant module includes administration functions. These maintain a count of how many unused authentication tokens remain, and send a request for further tokens to the payment service when that number falls below a predetermined threshold.

20. One of skill in the authentication art would understand that the authentication tokens of the merchant are similar to the payment tokens of the user. The tokens are issued to the merchant at the time of registration and before the merchant or the user being involved in any transaction. *Hill et al.*, col 6, lines 25-32. The merchant and the user do not receive any tokens at the time of the transaction and the tokens stored at the user or merchant's computer are not valid for a predefined period of time. Hill's tokens do not serve an identification function, but rather act is a fungible financial instrument. That is, a given quantity or value of tokens is equivalent to their stated value in dollars.

I affirm that all statements made herein of my own knowledge are true, and that all statements made herein on information and belief are believed to be true. I understand that willful false statements and the like are punishable by fine or imprisonment, or both (18 U.S.C.

1001), and may jeopardize the validity of the present patent application or any patent issuing thereon.

FURTHER AFFIANT SAYETH NOT.

It witness whereof,

Kamran Asghari-Kamrani

02/27/2012
Date

Certification Under 37 C.F.R. § 1.8

I hereby certify that on March 1, 2012 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: March 1, 2012 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 12/210,926

FILING DATE: September 15, 2008

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

ATTORNEY DOCKET: KAMR002US0

CONFIRMATION NO.: 7516

VIA ELECTRONIC FILING SYSTEM
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

AFFIDAVIT UNDER RULE 132

Applicants hereby submit this affidavit in support of their response to the Office Action mailed January 6, 2012 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 12/210,926, and pursuant to the provisions of 37 C.F.R. § 1.132. The witness hereby avers and testifies as follows:

1. I am Abolfazl Hosseinzadeh, with address of PO Box 3043, Bellevue, WA 98009.

2. I am an electrical engineer with more than 20 years of proven technical leadership and multi-disciplined experience in the area of systems engineering and development, program management, information security and e-commerce.

3. I am familiar with the specification and pending claims of the present Application.

4. I have reviewed U.S. Patent Publication No. 2010/0100724 A1 by Kaliski, Jr. ("*Kaliski, Jr.*").

Nonce Not Equivalent to SecureCode

5. One of skill in the authentication art would understand that an **identifier** is non secret information such as a name or label that identifies an entity. And in the world of authentication an identifier is only used for identification of an entity and not for authentication of the entity.

6. One of skill in the authentication art would understand that in *Kaliski, Jr.*, a nonce is a **session identifier**. "The authentication server 730 returns the blinded result R to the client 715, along with **a nonce or other session identifier** 772." *Kaliski, Jr.*, ¶ [0111] (emphasis supplied).

A *cryptographic nonce* is an arbitrary number used to establish the uniqueness or discreteness of an operation. That is, an operation such as a data request is accompanied by a nonce in order to demonstrate that the request is not a repeat or re-play of a previous request.

A *session* is a series of information exchanges between two communicating parties, usually involving an initiation protocol and more than one message in each direction.

In *Kaliski, Jr.* a nonce is used for identification of a user's session. In the client/server world, a session refers to all the requests that a single client makes to a server. A session is specific to each user and for each user a new session is created to track all the requests from that user. Every user has a separate session and separate session identifier is associated with that session.

7. One of skill in the authentication art would understand that the nonce in *Kaliski, Jr.* is not equivalent to the SecureCode of the present application. A nonce is a session identifier associated with a user's session, but a nonce is not used for authentication of a user, as is the SecureCode recited in the claims of *Kamrani.*

8. One of skill in the authentication art would understand that the statement "the nonce corresponds to the recited dynamic SecureCode" is inaccurate. In *Kaliski, Jr.* the web server receives the nonce and hardened password from the client and authenticates the user based on successful decryption of a digital signature associated with the hardened password. *Kaliski, Jr.*, ¶¶ *[0109] and [0112].* The nonce is used by the web server to identify the user and the hardened password used in the authentication process of authenticating the user. In *Kamrani*, a dynamic code authenticates a user whereas in *Kaliski, Jr.* a nonce is a session identifier. Therefore the argument that "the nonce corresponds to the recited dynamic code" is invalid.

No Authentication Request Message

9. One of skill in the authentication art would understand that in the system of *Kaliski, Jr.* there is nothing equivalent to a Central Entity receiving an authentication request message, as recited in the claims at issue. The Office Action equates the claimed authentication request message to message 776 of *Kaliski, Jr.* But, message 776 that the authentication server in FIG 7 of *Kaliski, Jr.* receives is NOT an authentication request message. Rather, message 776 indicates simply whether or not the authentication of the client by the web server was successful. *See Kaliski, Jr.* ¶¶ *[0109] through [0112].* This message 776 is a one way acknowledgement and expects no return, whereas the

authentication request message as recited in the claims at issue is a different type of message than the cited acknowledgement as the claimed authentication request should generate a response because it is a REQUEST as opposed to an acknowledgement. Thus, the message in *Kaliski, Jr.* cited by the Office Action at issue is not equivalent to the claimed authentication request message in *Kamrani.* Thus, one of skill in the authentication art would understand that the argument in the Office Action equating the claimed authentication request message to the acknowledgement message 776 in *Kaliski, Jr.* is not valid.

No Central Entity Authenticating User

10. One of skill in the authentication art would understand that there is nothing in *Kaliski, Jr.* equivalent to a Central Entity authenticating the user as recited in the claims at issue. The Office Action equates the Central Entity to the authentication server 730 in *Kaliski, Jr.* But, the authentication server 730 in FIG 7 never authenticates the client. Rather, the web server 710 authenticates the client based on successful decryption of the client's digital signature associated with the hardened password. *See Kaliski, Jr.* ¶¶ [0109] through [0112]. Moreover, the web server 710 of *Kaliski, Jr.* does not generate anything equivalent to the claimed SecureCode, as recited in the claims at issue. Thus, neither the web server 710 nor the authentication server 730 of *Kaliski, Jr.* performs the functions of the Central Entity recited in the claims.

11. One of skill in the authentication art would understand that in *Kaliski, Jr.* a user's client application generates a hardened password (based on the blinded result R received from the authentication server) and submits the generated hardened password to the web server and not to the authentication server cited by the Office Action. In *Kaliski, Jr.* the client receives the blinded result R along with a nonce from the authentication server and

generates the hardened password at the client side for authentication to the web server. *Kaliski, Jr.*, ¶ [0111].

12. One of skill in the authentication art would understand that the argument in the Office Action equating the claimed "authenticating by the Central-Entity the user during the transaction, if the digital identity is valid" with the authentication protocol in *Kaliski, Jr.* is not valid. The authentication server 730 does not authenticate the client; it is the web server that authenticates the client. And, the web server 710 of *Kaliski, Jr.* also cannot be the claimed Central Entity because the web server does not generate anything equivalent to the claimed SecureCode. Thus, there is no Central Entity authenticating the user in *Kaliski, Jr.*

Authentication Process Different

13. The web server of *Kaliski, Jr.* stores the user's personal information as encryption secrets (See *Kaliski, Jr.*, ¶ *[0103]*) and the encrypted secrets are stored such that they can be decrypted with a decryption key/hardened password. In *Kaliski, Jr.* a blind function evaluation protocol is used by the client to drive a decryption key/hardened password from a blinded result R received from the authentication server (See *Kaliski, Jr.*, ¶ *[0111]*), to decrypt the encrypted secrets. The web server authenticates the client if the hardened password received from the client successfully decrypt user's information.

14. It is clear that in *Kaliski, Jr.*, authentication is based on a cryptographic protocol. The use of this cryptographic approach allows authenticity of a client to be checked by creating a digital signature of a user's personal information using the encryption key, which can be verified using hardened password as the decryption key received from the client during the transaction.

15. One of skill in the authentication art would understand that in the blind function evaluation protocol used in *Kaliski, Jr.* (*See, Kaliski, Jr.* ¶ *[0038]*), the client has some secret information and the authentication server has some secret information, and together the client

and the authentication server provide their respective secrets as an input to a jointly calculated function, with only the client obtaining the output of the jointly calculated function (the output is the decryption key or hardened password). This means that only the client obtains the hardened password (decryption key) as the output of the blind function evaluation protocol. See *Kaliski, Jr.* Figure 7. The authentication server of *Kaliski, Jr.* which the Office Action equated to the Central Entity of the claims cannot generate the hardened password (decryption key) since the authentication server does not have access to the client's secret information. See *Kaliski, Jr.* ¶ [0040], which states:

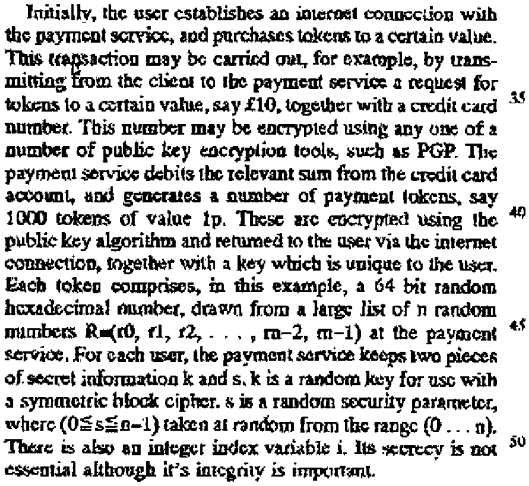
> The use of a blind function evaluation protocol, or other embodiments in which the decryption key is derived from the client information, provides additional security benefits resulting from the fact that the first server 30 does not have the decryption key in an unblinded form. Even if the first server 30 is compromised, and a server secret obtained, it will still be necessary for an attacker to do more work to transform the server secret into the decryption key. Just as one example, in one such embodiment, the first server 30 and client 15 engage in a blind function evaluation protocol that results in the first server 30 providing to the client 15 a blinded key as the intermediate data 22. The client 15 has information used to unblind the decryption key 24, which is then used to decrypt the encrypted secrets 5. Compromise of the first server 30 would still not directly reveal the decryption key 25 to an attacker.

Thus, the entire basis for authentication in *Kaliski, Jr.* is different than the claimed SecureCode authentication process of *Kamrani*, and one of ordinary skill in the art would understand this difference.

Hill et al.

16. One of skill in the authentication and payment art would understand that the user of *Hill et al.* purchases a set of payment tokens from the payment service provider before the user being involved in any transaction with the merchant. *Hill et al., col. 5, lines 31-51*

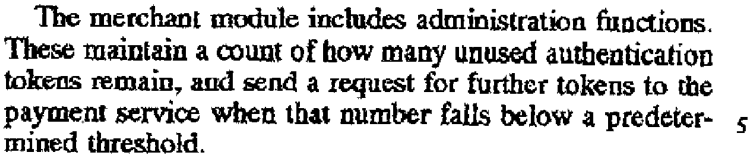
and col. 8, lines 1-9. The tokens are not valid for a predefined period of time because the user buys them. The tokens are like real money and will be used for online purchases.



Initially, the user establishes an internet connection with the payment service, and purchases tokens to a certain value. This transaction may be carried out, for example, by transmitting from the client to the payment service a request for tokens to a certain value, say £10, together with a credit card number. This number may be encrypted using any one of a number of public key encryption tools, such as PGP. The payment service debits the relevant sum from the credit card account, and generates a number of payment tokens, say 1000 tokens of value 1p. These are encrypted using the public key algorithm and returned to the user via the internet connection, together with a key which is unique to the user. Each token comprises, in this example, a 64 bit random hexadecimal number, drawn from a large list of n random numbers $R=(r0, r1, r2, \ldots, rn-2, rn-1)$ at the payment service. For each user, the payment service keeps two pieces of secret information k and s. k is a random key for use with a symmetric block cipher. s is a random security parameter, where $(0 \leqq s \leqq n-1)$ taken at random from the range $(0 \ldots n)$. There is also an integer index variable i. Its secrecy is not essential although it's integrity is important.

17. One of skill in the authentication art would understand that the payment server of *Hill et al.* encrypt the generated set of tokens with user's public key and send it to the user before the user starting any transactions with a merchant. *Hill et al., col. 5, lines 40-42.* The Carnet program installed on user's computer stores the tokens. *Hill Col. 5, lines 25-30 and lines 52-65; Col 6, lines 3-20.*

18. One of skill in the authentication art would understand that the merchant stores a set of authentication tokens before starting any transaction with the user. *Hill et al., col. 6, lines 46-47 and col. 13, lines 1-5.*



The merchant module includes administration functions. These maintain a count of how many unused authentication tokens remain, and send a request for further tokens to the payment service when that number falls below a predetermined threshold.

19. One of skill in the authentication art would understand that the authentication tokens of the merchant are similar to the payment tokens of the user. The tokens are issued to the merchant at the time of registration and before the merchant or the user being involved in any transaction. *Hill et al.*, col 6, lines 25-32. The merchant and the user do not receive any tokens at the time of the transaction and the tokens stored at the user or merchant's computer are not valid for a predefined period of time. Hill's tokens do not serve an identification function, but rather act is a fungible financial instrument. That is, a given quantity or value of tokens is equivalent to their stated value in dollars.

I affirm that all statements made herein of my own knowledge are true, and that all statements made herein on information and belief are believed to be true. I understand that willful false statements and the like are punishable by fine or imprisonment, or both (18 U.S.C. 1001), and may jeopardize the validity of the present patent application or any patent issuing thereon.

FURTHER AFFIANT SAYETH NOT.

It witness whereof,

Abolfazl Hosseinzadeh

2-28-12
Date

Certification Under 37 C.F.R. § 1.8

I hereby certify that on March 1, 2012 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: March 1, 2012 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 12/210,926

FILING DATE: September 15, 2008

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

ATTORNEY DOCKET: KAMR002US0

CONFIRMATION NO.: 7516

VIA ELECTRONIC FILING SYSTEM
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

AFFIDAVIT UNDER RULE 132

Applicants hereby submit this affidavit in support of their response to the Office Action mailed January 6, 2012 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 12/210,926, and pursuant to the provisions of 37 C.F.R. § 1.132. The witness hereby avers and testifies as follows:

1. I am James Hewitt, residing at 12587 Fair Lakes Circle, #202, Fairfax, Virginia 22033.

2. I received a Bachelors of Arts in Philosophy from Vassar College in 1983.

3. I have been a Certified Information System Security Professional since 2001. My certification number is #21060 per ISC2.org.

4. From 1998-2002, I was Director of Professional Services at CertCo, Inc. in Cambridge, Massachusetts. During this time, I produced cryptographic systems used by Tier 1 banks for authentication of users, machines and financial transactions.

5. From 2002-2003, I was Secure Messaging Project Manager for the Commonwealth of Massachusetts Information Technology Division. During this period, I implemented a system for securing healthcare-related transactions statewide.

6. Since 2004 I have been Director of Security Governance for CGI Federal in Fairfax, Virginia. In this position, I design, implement and manage the security of large-scale applications for government and commercial clients.

7. I am familiar with the specification and pending claims of the present Application.

8. I have reviewed U.S. Patent Publication No. 2010/0100724 A1 by Kaliski, Jr. ("*Kaliski, Jr.*").

Nonce Not Equivalent to SecureCode

9. One of skill in the authentication art would understand that an **identifier** is non secret information such as a name or label that identifies an entity. And in the world of authentication an identifier is only used for identification of an entity and not for authentication of the entity.

10. One of skill in the authentication art would understand that in *Kaliski, Jr.*, a nonce is a **session identifier**. "The authentication server 730 returns the blinded result R to

the client 715, along with **a nonce or other session identifier** 772." *Kaliski, Jr.*, ¶ [0111] (emphasis supplied).

A *cryptographic nonce* is an arbitrary number used to establish the uniqueness or discreteness of an operation. That is, an operation such as a data request is accompanied by a nonce in order to demonstrate that the request is not a repeat or re-play of a previous request.

A *session* is a series of information exchanges between two communicating parties, usually involving an initiation protocol and more than one message in each direction.

In *Kaliski, Jr.* a nonce is used for identification of a user's session. In the client/server world, a session refers to all the requests that a single client makes to a server. A session is specific to each user and for each user a new session is created to track all the requests from that user. Every user has a separate session and separate session identifier is associated with that session.

11. One of skill in the authentication art would understand that the nonce in *Kaliski, Jr.* is not equivalent to the SecureCode of the present application. A nonce is a session identifier associated with a user's session, but a nonce is not used for authentication of a user, as is the SecureCode recited in the claims of *Kamrani.*

12. One of skill in the authentication art would understand that the statement "the nonce corresponds to the recited dynamic SecureCode" is inaccurate. In *Kaliski, Jr.* the web server receives the nonce and hardened password from the client and authenticates the user based on successful decryption of a digital signature associated with the hardened password. *Kaliski, Jr.,* ¶¶ *[0109] and [0112].* The nonce is used by the web server to identify the user and the hardened password used in the authentication process of authenticating the user. In *Kamrani*, a dynamic code authenticates a user whereas in *Kaliski, Jr.* a nonce is a session identifier. Therefore the argument that "the nonce corresponds to the recited dynamic code" is invalid.

No Authentication Request Message

13. One of skill in the authentication art would understand that in the system of *Kaliski, Jr.* there is nothing equivalent to a Central Entity receiving an authentication request message, as recited in the claims at issue. The Office Action equates the claimed authentication request message to message 776 of *Kaliski, Jr.* But, message 776 that the authentication server in FIG 7 of *Kaliski, Jr.* receives is NOT an authentication request message. Rather, message 776 indicates simply whether or not the authentication of the client by the web server was successful. *See Kaliski, Jr.* ¶¶ *[0109] through [0112]*. This message 776 is a one way acknowledgement and expects no return, whereas the authentication request message as recited in the claims at issue is a different type of message than the cited acknowledgement as the claimed authentication request should generate a response because it is a REQUEST as opposed to an acknowledgement. Thus, the message in *Kaliski, Jr.* cited by the Office Action at issue is not equivalent to the claimed authentication request message in *Kamrani.* Thus, one of skill in the authentication art would understand that the argument in the Office Action equating the claimed authentication request message to the acknowledgement message 776 in *Kaliski, Jr.* is not valid.

No Central Entity Authenticating User

14. One of skill in the authentication art would understand that there is nothing in *Kaliski, Jr.* equivalent to a Central Entity authenticating the user as recited in the claims at issue. The Office Action equates the Central Entity to the authentication server 730 in *Kaliski, Jr.* But, the authentication server 730 in FIG 7 never authenticates the client. Rather, the web server 710 authenticates the client based on successful decryption of the client's digital signature associated with the hardened password. *See Kaliski, Jr.* ¶¶ [0109] through [0112]. Moreover, the web server 710 of *Kaliski, Jr.* does not generate anything

equivalent to the claimed SecureCode, as recited in the claims at issue. Thus, neither the web server 710 nor the authentication server 730 of *Kaliski, Jr.* performs the functions of the Central Entity recited in the claims.

15. One of skill in the authentication art would understand that in *Kaliski, Jr.* a user's client application generates a hardened password (based on the blinded result R received from the authentication server) and submits the generated hardened password to the web server and not to the authentication server cited by the Office Action. In *Kaliski, Jr.* the client receives the blinded result R along with a nonce from the authentication server and generates the hardened password at the client side for authentication to the web server. *Kaliski, Jr.*, ¶ [0111].

16. One of skill in the authentication art would understand that the argument in the Office Action equating the claimed "authenticating by the Central-Entity the user during the transaction, if the digital identity is valid" with the authentication protocol in *Kaliski, Jr.* is not valid. The authentication server 730 does not authenticate the client; it is the web server that authenticates the client. And, the web server 710 of *Kaliski, Jr.* also cannot be the claimed Central Entity because the web server does not generate anything equivalent to the claimed SecureCode. Thus, there is no Central Entity authenticating the user in *Kaliski, Jr.*

Authentication Process Different

17. The web server of *Kaliski, Jr.*stores the user's personal information as encryption secrets (See *Kaliski, Jr.*, ¶ *[0103]*) and the encrypted secrets are stored such that they can be decrypted with a decryption key/hardened password. In *Kaliski, Jr.* a blind function evaluation protocol is used by the client to drive a decryption key/hardened password from a blinded result R received from the authentication server (See *Kaliski, Jr.*, ¶ *[0111]*), to decrypt the encrypted secrets. The web server authenticates the client if the hardened password received from the client successfully decrypt user's information.

18. It is clear that in *Kaliski, Jr.*, authentication is based on a cryptographic protocol. The use of this cryptographic approach allows authenticity of a client to be checked by creating a digital signature of a user's personal information using the encryption key, which can be verified using hardened password as the decryption key received from the client during the transaction.

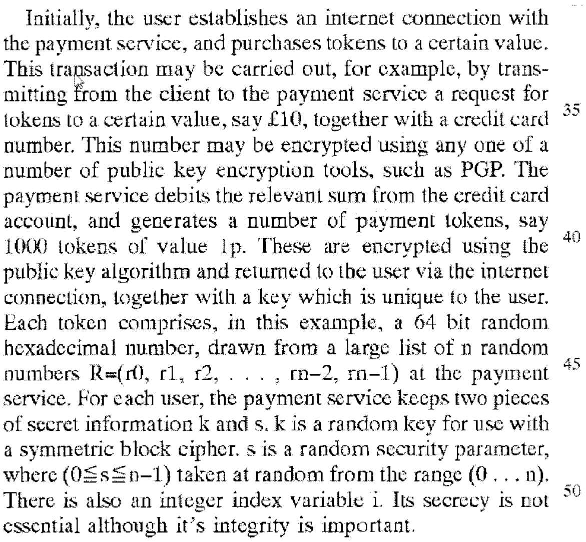
19. One of skill in the authentication art would understand that in the blind function evaluation protocol used in *Kaliski, Jr.* (*See, Kaliski, Jr.* ¶ *[0038]),* the client has some secret information and the authentication server has some secret information, and together the client and the authentication server provide their respective secrets as an input to a jointly calculated function, with only the client obtaining the output of the jointly calculated function (the output is the decryption key or hardened password). This means that only the client obtains the hardened password (decryption key) as the output of the blind function evaluation protocol. See *Kaliski, Jr.* Figure 7. The authentication server of *Kaliski, Jr.* which the Office Action equated to the Central Entity of the claims cannot generate the hardened password (decryption key) since the authentication server does not have access to the client's secret information. See *Kaliski, Jr.* ¶ [0040], which states:

> The use of a blind function evaluation protocol, or other embodiments in which the decryption key is derived from the client information, provides additional security benefits resulting from the fact that the first server 30 does not have the decryption key in an unblinded form. Even if the first server 30 is compromised, and a server secret obtained, it will still be necessary for an attacker to do more work to transform the server secret into the decryption key. Just as one example, in one such embodiment, the first server 30 and client 15 engage in a blind function evaluation protocol that results in the first server 30 providing to the client 15 a blinded key as the intermediate data 22. The client 15 has information used to unblind the decryption key 24, which is then used to decrypt the encrypted secrets 5. Compromise of the first server 30 would still not directly reveal the decryption key 25 to an attacker.

Thus, the entire basis for authentication in *Kaliski, Jr.* is different than the claimed SecureCode authentication process of *Kamrani*, and one of ordinary skill in the art would understand this difference.

Hill et al.

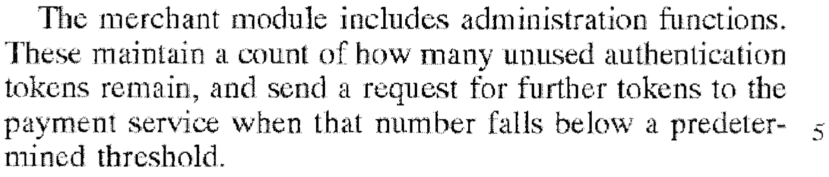
20. One of skill in the authentication and payment art would understand that the user of *Hill et al.* purchases a set of payment tokens from the payment service provider before the user being involved in any transaction with the merchant. *Hill et al., col. 5, lines 31-51 and col. 8, lines 1-9.* The tokens are not valid for a predefined period of time because the user buys them. The tokens are like real money and will be used for online purchases.



Initially, the user establishes an internet connection with the payment service, and purchases tokens to a certain value. This transaction may be carried out, for example, by transmitting from the client to the payment service a request for tokens to a certain value, say £10, together with a credit card number. This number may be encrypted using any one of a number of public key encryption tools, such as PGP. The payment service debits the relevant sum from the credit card account, and generates a number of payment tokens, say 1000 tokens of value 1p. These are encrypted using the public key algorithm and returned to the user via the internet connection, together with a key which is unique to the user. Each token comprises, in this example, a 64 bit random hexadecimal number, drawn from a large list of n random numbers R=(r0, r1, r2, . . . , rn−2, rn−1) at the payment service. For each user, the payment service keeps two pieces of secret information k and s. k is a random key for use with a symmetric block cipher. s is a random security parameter, where (0≦s≦n−1) taken at random from the range (0 . . . n). There is also an integer index variable i. Its secrecy is not essential although it's integrity is important.

21. One of skill in the authentication art would understand that the payment server of *Hill et al.* encrypt the generated set of tokens with user's public key and send it to the user before the user starting any transactions with a merchant. *Hill et al., col. 5, lines 40-42.* The Carnet program installed on user's computer stores the tokens. *Hill Col. 5, lines 25-30 and lines 52-65; Col 6, lines 3-20.*

22. One of skill in the authentication art would understand that the merchant stores a set of authentication tokens before starting any transaction with the user. *Hill et al., col. 6, lines 46-47 and col. 13, lines 1-5.*



> The merchant module includes administration functions. These maintain a count of how many unused authentication tokens remain, and send a request for further tokens to the payment service when that number falls below a predetermined threshold.

23. One of skill in the authentication art would understand that the authentication tokens of the merchant are similar to the payment tokens of the user. The tokens are issued to the merchant at the time of registration and before the merchant or the user being involved in any transaction. *Hill et al., c*ol 6, lines 25-32. The merchant and the user do not receive any tokens at the time of the transaction and the tokens stored at the user or merchant's computer are not valid for a predefined period of time. Hill's tokens do not serve an identification function, but rather act is a fungible financial instrument. That is, a given quantity or value of tokens is equivalent to their stated value in dollars.

I affirm that all statements made herein of my own knowledge are true, and that all statements made herein on information and belief are believed to be true. I understand that willful false statements and the like are punishable by fine or imprisonment, or both (18 U.S.C. 1001), and may jeopardize the validity of the present patent application or any patent issuing thereon.

FURTHER AFFIANT SAYETH NOT.

It witness whereof,

James Hewitt
James Hewitt

Feb 28 2012
Date

Electronic Acknowledgement Receipt

EFS ID:	12198792
Application Number:	12210926
International Application Number:	
Confirmation Number:	7516
Title of Invention:	Centralized Identification and Authentication System and Method
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Customer Number:	58293
Filer:	Michael P. Fortkort
Filer Authorized By:	
Attorney Docket Number:	KAMR002US0
Receipt Date:	01-MAR-2012
Filing Date:	15-SEP-2008
Time Stamp:	10:42:09
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	Amendment/Req. Reconsideration-After Non-Final Reject	12210926_Response_to_Office_Action_Mailed_010612_filed_030112.pdf	90911 b17ff4486800294585be29dac6ccc6ebac40cb86	no	23

Warnings:

Information:

2	Rule 130, 131 or 132 Affidavits	12210926_132_Affidavit_NKamrani_filed_030112.pdf	348903 a1915f1572d19e1efa06da4df563c24a8186de56	no	8
Warnings:					
Information:					
3	Rule 130, 131 or 132 Affidavits	12210926_132_Affidavit_KKamrani_filed_030112.pdf	371323 301ad2114c4e3bdcb61ca818d3a074c9c3a2faed	no	9
Warnings:					
Information:					
4	Rule 130, 131 or 132 Affidavits	12210926_132_Affidavit_Hossienzadeh_filed_030112.pdf	326232 27eda6ad41d680cc1c387875ec6ce4e4fd734204	no	8
Warnings:					
Information:					
5	Rule 130, 131 or 132 Affidavits	12210926_132_Affidavit_Hewitt_filed_030112.pdf	2674493 ad755258a103c25b5c1ebc9f6c8d2e0acd3235db	no	8
Warnings:					
Information:					
		Total Files Size (in bytes):	3811862		

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 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.
12/210,926	09/15/2008	Nader Asghari-Kamrani	KAMR002US0	7516

58293 7590 01/06/2012
FORTKORT & HOUSTON P.C.
9442 N. CAPITAL OF TEXAS HIGHWAY
ARBORETUM PLAZA ONE, SUITE 500
AUSTIN, TX 78759

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	PAPER NUMBER
2432	
NOTIFICATION DATE	DELIVERY MODE
01/06/2012	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):

58293@foholaw.com
rbernfeld@foholaw.com

Office Action Summary	**Application No.** 12/210,926	**Applicant(s)** ASGHARI-KAMRANI ET AL.	
	Examiner ABDULHAKIM NOBAHAR	**Art Unit** 2432	

-- 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* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, 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 *17 November 2011*.

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) *1-4,12-24,32-41,43-48,50-55,58,60 and 63-91* 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) *1-4, 12-24, 32-41, 43-48, 50-55, 58, 60 and 63-91* is/are rejected.

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

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

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).

12)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

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

a)□ All b)□ Some * c)□ None of:

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) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This office action is in response to applicants' Pre-Appeal Brief Conference request on 11/17/2011.

2. Claims 1-4, 12-24, 32-41, 43-48, 50-55, 58, 60 and 63-91 are pending.

Response to Arguments

Applicant's arguments, see the Remarks (e.g., pages 17-19) and Affidavits, filed on 11/17/2011, with respect to the rejection(s) of claim(s) 1-4, 12-24, 32-41, 43-48, 50-55, 58, 60 and 63-80 under *35 USC § 103* have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon updating the search new prior arts were discovered requiring new grounds rejection as follows.

Specification

The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required:

Claim 2 recites "user has a pre-existing relationship with the External-Entity" which is not described in the specification.

Claim 3 recites "user has no pre-existing relationship with the External-Entity" which is not described in the specification.

Claim 4 recites "using the predetermined algorithm to combine received user specific information received by the Central-Entity with a received SecureCode received by the Central-Entity to form a combined received SecureCode and received user specific information;

comparing the combined Secure-Code and user specific information with the combined received SecureCode and received user specific information to validate the user" which are not described in the specification. The specification only describes that the Central-Entity combines the SecureCode with user's information such as UserName once before sending the SecureCode to the user but does not describe to do the same for a second time after receiving the SecureCode from an External-Entity. The user receives an algorithmically combined SecureCode and UserName from the Central-Entity (according to the specification page 11) and gives it to the External-Entity to transfer it to the Central-Entity for authentication. There is no need for the Central-Entity to perform again the algorithmic operation to combine the SecureCode with the UserName because they are already combined. Therefore, in view of the specification the limitation "using the predetermined algorithm…" makes the claim 4 unclear.

Claim 411 recites "said External-Entity is using said algorithmically combined SecureCode to authenticate a user's identity" which is not described in the specification. The specification describes that the Central-Entity authenticates the user.

Claim Objections

Claim 1 is objected to because of the following informalities: Claim 1 in line 9 recites "by a Central-Entity" where it is not clear whether it is referring to the same Central-Entity recited in line 3. Appropriate correction is required.

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 1-4, 12-20, 22-24, 32-41, 43-48, 50-55, 58, 60, 63 and 65-91 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kaliski, Jr. (US 2010/0100724 A1), hereinafter Kaliski in view of Hill (US 6,236,981 B1).

Regarding claims 1, 50, 52 and 74, Kaliski discloses:

A method for authenticating a user during an electronic transaction between the user and an External-Entity (see, e.g., [0006], were the server corresponds to the recited External-Entity), the method comprising:

receiving electronically a request for a dynamic SecureCode for the user by a Central-Entity during the transaction between the user and the External-Entity (see, e.g., [0110] and Fig. 7, where the authentication server 730 corresponds to the recited Central-Entity and providing client information 772 to the authentication server 730 corresponds to the recited request for a dynamic SecureCode);

generating during the transaction a dynamic SecureCode for the user in response to the request, wherein the dynamic SecureCode is valid for a predefined time (see, e.g., [0036]: “derive…”, [0044]: “time-based code”, [0057]: “The authentication 65 thus can take place in various ways, including without limitation by transmission… time-based code”, [0096], [0110] and Fig. 7, where the nonce corresponds to the recited dynamic SecureCode);

providing said generated SecureCode to the user during the transaction (see, e.g., [0111] and Fig. 7),

receiving electronically by a Central-Entity a request for authenticating the user based on a digital identity during the transaction, which digital identity includes the SecureCode (see, e.g., Fig. 7, step 776 and [0112], where the message includes the nonce; and

authenticating by the Central-Entity the user during the transaction if the digital identity is valid (see, e.g., [0112]).

Kaliski, however, does not expressly disclose that the dynamic SecureCode becomes invalid after being used.

Hill discloses a digital payment transaction system (see, e.g., abstract and col. 1, line 3) in which a payment server issues a digital payment token to a user for making a payment to a merchant and the token is authenticated by the payment server when received from the merchant (see, e.g., col. 2, lines 5-23, Fig. 1 and Fig. 6). Hill also discloses that the token functions like a one-time password (corresponding to the recited becomes invalid after being used) (see, e.g., col. 6, lines 25-30).

It would have been obvious to a person of ordinary skill in the art at the time of the invention was made to modify the system of Kaliski to generate a one-time password as taught in Hill in addition of being a time-based code because it would make the system of Kaliski a high level of cryptographic security, while completely removing the processing overhead from the vendor (see Hill, col. 2, lines 35-40).

Claims 21 and 64 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kaliski-Hill as applied to claim 21 above and further in view of the examiner Official Notice.

Regarding claims 21 and 64, these claims are rejected as applied to the like elements of claims 1, 50, 52 and 74 above and further the following:

Kaliski-Hill does not expressly disclose that the computer that generates a SecureCode is different from the computer that authenticates the SecureCode.

Official Notice is taken that it is old and well-known practice in the art that in some system (i.e., organizations and institutions) more than one computer are used to provide services to their clients (i.e., different computer for different purpose and service). Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to modify the system of Kaliski-Hill to deploy one computer for providing a client a SecureCode and another computer for authenticating the SecureCode (i.e., the user) whenever the user request a service. For example, if the External-Entity has its own Central-Entity different from the Central-Entity of the user, then the computer of the External-Entity's Central-Entity will be used for authenticating the SecureCode which is different from the computer of the user’s Central-Entity that has generated the SecureCode.

Regarding claims 2 and 22, Kaliski discloses:

A method as recited in claim 1, wherein said user has a pre-existing relationship with the External-Entity (see, e.g., [0003], where the user stores a secret at the server before doing any transaction, [0101] and [0105], where the server 610 keeps the encrypted user's secrete for future transaction which means the user has a pre-existing relationship with the server 610 when executing the next transaction).

Regarding claims 3 and 23, Kaliski discloses:

A method as recited in claim 1, wherein said user has no pre-existing relationship with the External-Entity (see, e.g., [0109], where the user does not have any pre-existing relationship with the web server 710 when starting his first transaction with the web server 710).

Regarding claims 4, 24 and 43, Kaliski discloses:

combining said generated SecureCode with a user-specific information using a predetermined algorithm to form a combined Secure-Code and user specific information (see, e.g., [0111], where the blinded result R and nonce or other session identifier corresponds to the recited combined Secure-Code and user specific information);

maintaining the combined Secure-Code and user specific information at the Central-Entity (see, e.g., [0112], where the authentication server 730 performs an authentication which means the authentication server stores the same information that has transmitted to the client previously);

using the predetermined algorithm to combine received user specific information received by the Central-Entity with a received SecureCode received by the Central-Entity to form a combined received SecureCode and received user specific information (see, e.g., [0111]-[0112] and Fig. 7, where in the process of authentication a combined information of R and nonce are used);

comparing the combined Secure-Code and user specific information with the combined received SecureCode and received user specific information to validate the user (see, e.g., [0112], where the authentication performed by the server 730 means comparing).

Regarding claims 12 and 32, Kaliski discloses:

A method as recited in claim 1, wherein the External-Entity receives the user's digital identity (see, Fig. 7, step 774).

Regarding claims 13 and 33, Kaliski discloses:

A method as recited in claim 1, wherein said External-Entity submits a digital identity to the Central-Entity (see, e.g., Fig. 7, step 776).

Regarding claims 14, 34, 65, 66, 83 and 87, Kaliski discloses that the web server sends a message which includes the received nonce from the client, to the authentication server (see Fig. 7, step 776 and [0112]) but does not expressly disclose:

wherein said digital identity includes a user-specific information.

Hill, however, discloses:

wherein said digital identity includes a user-specific information (see, e.g., col. 6, lines 16-25, where the modified token includes the user's PIN which is specific to the user).

It would have been obvious to a person of ordinary skill in the art at the time of the invention was made to modify the system of Kaliski to include user's specific information in the digital identity as taught in Hill in order to authorize payment to merchant by the payment server (see Hill, col. 6, lines 16-20).

Regarding claims 15, 35, 48, 78, 79, 84, 85 and 88-91, Hill discloses:
The method of claim 14, wherein the user-specific information comprises one or more of the following: an alphanumeric name, an ID, a login name, and an identification phrase, (see, e.g., col. 6, lines 16-25, where the modified token includes the user's PIN which is equivalent to an ID).

Regarding claims 16 and 36, Kaliski-Hill discloses:
The method of claim 1, wherein the transaction corresponds to a financial transaction (see, e.g., Kaliski: [0101] and Hill: col. 2, line 3, where the digital payment transaction system indicates a financial transaction).

Regarding claims 17 and 37, Kaliski discloses:
The method of claim 1, wherein the transaction corresponds to a non-financial transaction (see, e.g., [0006], where accessing data is a non-financial transaction).

Regarding claims 18 and 38, Kaliski-Hill discloses:

The method of claim 1, wherein the transaction corresponds to access to restricted web-site or restricted computer/server (see, e.g., Kaliski: [0030] and Hill: col. 6, line 5-9).

Regarding claims 19 and 39, Kaliski discloses:

The method of claim 1, wherein said transaction occurs over a communication network, wherein said communication network comprises one or more of the following: an Internet, a wireless network, a mobile network, a satellite, and a private network (see, e.g., Fig. 6 and [0032]).

Regarding claims 20, 40, 51, 53-55 and 58, Kaliski discloses:

The method of claim 1, wherein said transaction occurs over a communication network to which is coupled said user, said Central-Entity, and said External-Entity (see, e.g., Figs. 6 and 7).

Regarding claim 41, Kaliski discloses:

A method as recited in claim 4, wherein said External-Entity is using said algorithmically combined SecureCode to authenticate a user's identity (see, e.g., [0111]-[0112] and Fig. 7, where in the process of authentication a combined information of R and nonce are used).

Regarding claims 44, 81, 82 and 86, Kaliski discloses:

The method of claim 1, wherein said External-Entity and said Central-Entity are the same entity (see, e.g., [0101]-[0103], where the user only interacts with the web server 610).

Regarding claims 45 and 75, Hill discloses:

The method as recited in claim 1, wherein said Central-Entity invalidates the SecureCode after authenticate the user (see, e.g., col. 6, lines 25-30: one-time password).

Regarding claims 46 and 76, Kaliski discloses:

The method as recited in claim 1, wherein the Central-Entity invalidates the SecureCode after a predefined period of time passes from when the SecureCode was generated (see, e.g., [0044]: “time-based code”).

Regarding claims 47 and 77, Kaliski discloses:

The method as recited in claim 1, wherein said Central-Entity generates the SecureCode with dependence on the user information (see, e.g., [0033], [0035] and [0110], where the client transfers its information to the authentication server to receive a blinded result R and a nonce or a session identifier).

Regarding claim 60, Kaliski discloses:

The method as recited in claim 58, wherein said request is initiated by a user through a standard interface provided to said user (see, e.g., [0033]).

Regarding claim 63, Kaliski discloses:

The apparatus according to claim 21, wherein said first Central-Entity computer and said second Central-Entity computer are the same (see, e.g., Fig. 7, authentication server 730).

Regarding claim 64, Kaliski-Hill does not expressly disclose:

The apparatus according to claim 21, wherein said first Central-Entity computer and said second Central-Entity computer are different.

Official Notice is taken that it is old and well-known practice in the art that some organizations such as banks my use more than one computer to provide services to their clients. Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to modify the system of Kaliski-Hill to deploy more than one computer to provide to a client a SecureCode by one computer and authenticate it whenever the user request a service by another computer.

Regarding claims 67 and 71, Kaliski discloses:

A method as recited in claim 1, wherein said digital identity is invalid if the SecureCode is invalid (see, e.g., Fig. 7 and [0111]-[0112], where if the provided nonce to the authentication server is not valid the user will not be authenticated).

Regarding claims 68, and 72, Kaliski discloses:

A method as recited in claim 1, wherein said digital identity is invalid if the SecureCode is invalid (see, e.g., Fig. 7 and [0111]-[0112], where if the provided nonce to the authentication server is valid the user will be authenticated).

Regarding claims 69, 70, 73 and 80, Kaliski discloses:

A method as recited in claim 1, wherein said External-Entity authenticates the user upon receiving an affirmation authentication message from the Central-Entity (see, e.g., Fig. 7 and [0111]-[0112]).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See attached PTO-892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ABDULHAKIM NOBAHAR whose telephone number is (571)272-3808. The examiner can normally be reached on M-F 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. 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.

/Abdulhakim Nobahar/
Examiner, Art Unit 2432

Notice of References Cited

Application/Control No. 12/210,926	Applicant(s)/Patent Under Reexamination ASGHARI-KAMRANI ET AL.	
Examiner ABDULHAKIM NOBAHAR	Art Unit 2432	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,236,981 B1	05-2001	Hill, Jake	705/67
*	B	US-2010/0100724 A1	04-2010	Kaliski, JR., Burton S.	713/155
*	C	US-2004/0030752 A1	02-2004	Selgas et al.	709/206
*	D	US-2002/0133412 A1	09-2002	OLIVER et al.	705/26
*	E	US-2002/0040346 A1	04-2002	Kwan, Khai Hee	705/51
*	F	US-6,067,621 A	05-2000	Yu et al.	713/172
*	G	US-7,150,038 B1	12-2006	Samar, Vipin	726/8
*	H	US-2002/0184143 A1	12-2002	Khater, Ali Mohamed	705/39
*	I	US-2002/0046189 A1	04-2002	Morita et al.	705/67
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	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.

Search Notes	Application/Control No. 12210926	Applicant(s)/Patent Under Reexamination ASGHARI-KAMRANI ET AL.
	Examiner ABDULHAKIM NOBAHAR	**Art Unit** 2432

SEARCHED

Class	Subclass	Date	Examiner
726	2,5,8,18,27,28	7/26/2011	AN
713	182-186	7/26/2011	AN
705	64,67,72,76,78	7/26/2011	AN
	Search updated (See attached report)	12/16/2011 12/29/2011	AN

SEARCH NOTES

Search Notes	Date	Examiner
East Inventors names search (see attached report)	7/6/2009 9/23/2009	AN
EAST text search only (see attached report)		AN
PALM inventors names search	9/23/2009	AN
Search updated (See attached report)	12/16/2011 12/29/2011	AN

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner
726	2,5,8,18,27,28	12/16/2011	AN
713	155,168,170	12/16/2011	AN
705	35,39,44,50,64,67	12/16/2011	AN
	See attached report		

/ABDULHAKIM NOBAHAR/
Examiner.Art Unit 2432

EAST Search History

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L19	7795	(713/182-186).ccls. (726/2,5,8,18,27,28).ccls. (705/64,67,72,76,78).ccls.	US-PGPUB	OR	ON	2011/12/16 10:02
L22	8	19 and ((dynamic$4 tempora $4 time transi$5 temp) near3 (key password passcode passname passphrase phrase paraphrase code seed PIN pincode secret ID SID SSID identification identity identif$4 credential) same (key password passcode passname passphrase phrase paraphrase code seed PIN pincode secret ID SID SSID identification identity identif$4 credential) near5 (valid$4 invalid$4 authentic$4 expir$5 verifi$4 unverif$4 confirmed unconfirmed trust$4 untrust$4 correct incorrect) same (authentic$5 verification verif $4 valid$5) near4 (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper trader entity member party pay$2 spender partner counterpart) same (online Internet electronic$4 web website digital cyber network) near4 (bank$3 shop$4 commerc$3 purchas$3 buy$3 trad$3 business retail$3 sell$3 transact$3 communicat$3 financ$4 vend$3 procur$5 exchang$3)).CLM.	US-PGPUB	OR	ON	2011/12/16 10:15

12/16/2011 10:19:50 AM
H:\EAST\Workspaces\11333400_12210926.wsp

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	5	ASGHARI-KAMRANI near2 (NADER KAMRAN)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/16 08:18
L2	16552	(713/182-186).ccls. (726/2,5,8,18,27,28).ccls. (705/64,67,72,76,78).ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/16 08:28
L3	3762	2 and (dynamic$4 tempora$4 time transi$5 temp) near3 (key password passcode passname passphrase phrase paraphrase code seed PIN pincode secret ID SID SSID identification identity identif$4 credential) same (authentic$5 verification verif$4 valid$5)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/16 08:36
L4	197	3 and @PD> "20110725"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/16 08:37
L5	77	2 and FOB same (authentic$5 verification verifying validation validity) near2 (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper trader entity member party pay$2 spender partner counterpart)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/16 08:38
L6	6	5 and @PD> "20110725"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/16 08:38

L9	117	4 and (dynamic$4 tempora$4 time transi$5 temp) near3 (key password passcode passname passphrase phrase paraphrase code seed PIN pincode secret ID SID SSID identification identity identif$4 credential) same (authentic$5 verification verif$4 valid$5) near4 (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper trader entity member party pay$2 spender partner counterpart)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/16 08:40
L10	531380	(dynamic$4 tempora$4 time transi$5 temp) near3 (key password passcode passname passphrase phrase paraphrase code seed PIN pincode secret ID SID SSID identification identity identif$4 credential)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/16 09:25
L11	46249	10 and (dynamic$4 tempora$4 time transi$5 temp) near3 (key password passcode passname passphrase phrase paraphrase code seed PIN pincode secret ID SID SSID identification identity identif$4 credential) same (authentic$5 verification verif$4 valid$5)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/16 09:26
L12	2272	11 and @PD>"20110725"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/16 09:26
L13	860	12 and (dynamic$4 tempora$4 time transi$5 temp) near3 (key password passcode passname passphrase phrase paraphrase code seed PIN pincode secret ID SID SSID identification identity identif$4 credential) same (authentic$5 verification verif$4 valid$5) near4 (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper trader entity member party pay$2 spender partner counterpart)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/16 09:28

L14	144	13 and (dynamic$4 tempora$4 time transi$5 temp) adj2 (key password code seed PIN pincode secret) with (authenticat$3 verification verif $4 valid$5) same (authenticat $3 verification verifying validation validity) near2 (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper trader entity member party pay$2 spender partner counterpart)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/16 09:46
L15	111	14 and (online Internet electronic$4 web website digital cyber network) near4 (bank$3 shop$4 commerc$3 purchas$3 buy$3 trad$3 business retail$3 sell$3 transact $3 communicat$3 financ$4 vend$3 procur$5 exchang$3)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/16 09:47
L17	431	FOB same (authentic$5 verification verifying validation validity) near2 (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper trader entity member party pay$2 spender partner counterpart)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/16 09:59
L18	29	17 and @PD> "20110725"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/16 10:00

12/16/2011 10:19:37 AM
H:\ EAST\ Workspaces\ 11333400_12210926.wsp

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S75	5	ASGHARI-KAMRANI near2 (NADER KAMRAN)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/16 08:18
S76	16552	(713/182-186).ccls. (726/2,5,8,18,27,28).ccls. (705/64,67,72,76,78).ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/16 08:28
S77	3762	S76 and (dynamic$4 tempora$4 time transi$5 temp) near3 (key password passcode passname passphrase phrase paraphrase code seed PIN pincode secret ID SID SSID identification identity identif$4 credential) same (authentic$5 verification verif$4 valid$5)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/16 08:36
S78	197	S77 and @PD>"20110725"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/16 08:37
S79	77	S76 and FOB same (authentic $5 verification verifying validation validity) near2 (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper trader entity member party pay$2 spender partner counterpart)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/16 08:38
S80	6	S79 and @PD>"20110725"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/16 08:38

S83	117	S78 and (dynamic$4 tempora$4 time transi$5 temp) near3 (key password passcode passname passphrase phrase paraphrase code seed PIN pincode secret ID SID SSID identification identity identif$4 credential) same (authentic$5 verification verif$4 valid$5) near4 (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper trader entity member party pay$2 spender partner counterpart)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/16 08:40
S84	531380	(dynamic$4 tempora$4 time transi$5 temp) near3 (key password passcode passname passphrase phrase paraphrase code seed PIN pincode secret ID SID SSID identification identity identif$4 credential)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/16 09:25
S85	46249	S84 and (dynamic$4 tempora$4 time transi$5 temp) near3 (key password passcode passname passphrase phrase paraphrase code seed PIN pincode secret ID SID SSID identification identity identif$4 credential) same (authentic$5 verification verif$4 valid$5)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/16 09:26
S86	2272	S85 and @PD>"20110725"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/16 09:26
S87	860	S86 and (dynamic$4 tempora$4 time transi$5 temp) near3 (key password passcode passname passphrase phrase paraphrase code seed PIN pincode secret ID SID SSID identification identity identif$4 credential) same (authentic$5 verification verif$4 valid$5) near4 (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper trader entity member party pay$2 spender partner counterpart)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/16 09:28

S88	144	S87 and (dynamic$4 tempora$4 time transi$5 temp) adj2 (key password code seed PIN pincode secret) with (authenticat$3 verification verif$4 valid$5) same (authenticat$3 verification verifying validation validity) near2 (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper trader entity member party pay$2 spender partner counterpart)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/16 09:46
S89	111	S88 and (online Internet electronic$4 web website digital cyber network) near4 (bank$3 shop$4 commerc$3 purchas$3 buy$3 trad$3 business retail$3 sell$3 transact$3 communicat$3 financ$4 vend$3 procur$5 exchang$3)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/16 09:47
S91	431	FOB same (authentic$5 verification verifying validation validity) near2 (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper trader entity member party pay$2 spender partner counterpart)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/16 09:59
S92	29	S91 and @PD>"20110725"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/16 10:00
S93	2	"20020069174".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/16 12:41
S98	2	"20030110381".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/29 12:34
S99	2	"6993666".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/29 12:35
S100	2	"5805803".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/29 12:44

S101	340	microsoft adj passport	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/29 12:45
S102	11	S101 and request$3 near3 passport	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/29 14:19
S103	13	S101 and request$3 near5 passport	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/29 14:19
S104	0	S101 and (single adj use)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/29 14:22
S105	2	S101 and (OTP (time adj passport))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/29 14:23
S106	10	S101 and (OTP (time adj password))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/29 14:23
S107	10	S105 S106	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/29 14:23
S108	9296	OTP (one adj time adj password)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/29 20:44
S109	0	(single adj use) adj2 (password passport token)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/29 20:49
S110	0	single adj use adj2 password	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/29 20:50
S111	1537	use adj2 password	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/29 20:50

S112	1402	single adj2 password	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/29 20:50
S113	3312	one adj time adj password	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/29 20:51
S114	11007	one adj3 password	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/29 20:51
S115	18643	S108 S111 S112 S113 S114	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/29 20:52
S116	4050	S115 and (online Internet electronic$4 web digital cyber) near3 (shop$4 commerc$3 purchas$3 buy$3 trad$3 business retail$3 sell$3 transact $3 bank$3)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/29 21:18
S117	3405	S116 and (authentic$5 verification verifying valid$5) with (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper trader entity party pay$2 spender partner counterpart)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/29 21:19
S118	2788	S117 and (authentic$5 verification verifying valid$5) with (password passport token)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/29 21:20
S119	2728	S118 and (authentic$5 verification verifying valid$5) with (password passport token) same (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper trader entity party pay$2 spender partner counterpart)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/29 21:20
S120	1193	S119 and (dynamic$4 tempora $4 time transi$5 temp) adj2 (password passport token)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/29 21:21

S121	989	S119 and (short life liv$3 variable time-depend$4 time-based timebased time-wise timewise changeable changing unpredictable non predictable onetime once) near5 (password passport token)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/29 21:27
S122	1585	S120 S121	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/29 21:27
S123	1429	S122 and (authentic$5 verification verifying valid$5) with (third server authority cent$5 bank financ$5 institution trust$3 issuing organization authenticator centralization or broker$4 authoritative or authorized official)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/29 21:35
S124	1421	S123 and (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper trader entity party pay$2 spender partner counterpart) with (third server authority cent$5 bank financ$5 institution trust$3 issuing organization authenticator centralization or broker$4 authoritative or authorized official)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/29 21:35
S125	1203	S124 and (user client person individual subscriber member consumer customer request$2 buyer purchaser entity party pay$2 spender partner counterpart recipient receiver) with (third server authority cent$5 bank financ$5 institution trust$3 issuing organization authenticator centralization or broker$4 authoritative or authorized official) with (shop$4 commercial trad$3 business retail$3 sell$3 provid$3 suppl$4 merchant produc$4 merchandis$4)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/29 21:50

S126	737	S125 and (user client person individual subscriber member consumer customer request$2 buyer purchaser entity party pay $2 spender partner counterpart recipient receiver) with (third server authority cent$5 bank financ$5 institution trust$3 issuing organization authenticator centralization or broker$4 authoritative or authorized official) with (authentic$5 verification verifying valid$5) with (shop$4 commercial trad$3 business retail$3 sell$3 provid$3 suppl$4 merchant produc$4 merchandis $4)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/29 21:51
S127	394	S126 and (user client person individual subscriber member consumer customer request$2 buyer purchaser entity party pay $2 spender partner counterpart recipient receiver) with (third server authority cent$5 bank financ$5 institution trust$3 issuing organization authenticator centralization or broker$4 authoritative or authorized official) with (authentic$5 verification verifying valid$5) with (shop$4 commercial trad$3 business retail$3 sell$3 provid$3 suppl$4 merchant produc$4 merchandis $4) same (password passport token)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/29 21:53
S128	145	S127 and (user client person individual subscriber member consumer customer request$2 buyer purchaser entity party pay $2 spender partner counterpart recipient receiver) with (third server authority cent$5 bank financ$5 institution trust$3 issuing organization authenticator centralization or broker$4 authoritative or authorized official) with (authentic$5 verification verifying valid$5) with (shop$4 commercial trad$3 business retail$3 sell$3 provid$3 suppl$4 merchant produc$4 merchandis $4) same (dynamic$4 tempora $4 time transi$5 temp short life liv$3 variable time-depend$4 time-based timebased time-wise timewise changeable	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/29 21:55

		changing unpredictable non predictable onetime once) near5 (password passport token)				
S129	37	("5999525" "20100100724" "20040030752" "20020184143" "20020133412" "20020046189" "20020040346" "20020029275" "20010054148" "7975056" "7742996" "7716484" "7324972" "6731625" "6601192" "6236981" "6571290" "6067621").pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/29 22:26
S130	18	S129 and (user client person individual subscriber member consumer customer request$2 buyer purchaser entity party pay $2 spender partner counterpart recipient receiver) with (third server authority cent$5 bank financ$5 institution trust$3 issuing organization authenticator centralization or broker$4 authoritative or authorized official) with (authentic$5 verification verifying valid$5) with (shop$4 commercial trad$3 business retail$3 sell$3 provid$3 suppl$4 merchant produc$4 merchandis $4) same (dynamic$4 tempora $4 time transi$5 temp short life liv$3 variable time-depend$4 time-based timebased time-wise timewise changeable changing unpredictable non predictable onetime once) near5 (password passport token)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/29 22:27
S131	18	S130 and (OTP (time adj password) (use adj2 password) (single adj2 password) (one adj3 password))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/29 23:06
S132	14	S131 and (dynamic$4 tempora $4 time transi$5 temp short life liv$3 variable time-depend$4 time-based timebased time-wise timewise changeable changing unpredictable non predictable onetime once) adj2 (password passport token)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/29 23:08

S133	17	("5999525" "20100100724" "20040030752" "20020184143" "20020133412" "20020046189" "20020040346" "20020029275" "20010054148" "7975056" "7742996" "7716484" "7324972" "6731625" "6601192" "6236981" "6571290" "6067621").pn. and (tempora$4 duration during lapse elapse interval interim expir$5 period$6 interval span length extent transi$5 temp ephemeral short life liv$3 time-depend$4 time-based timebased time-wise timewise provision$4) near5 (password passport token passphrase passcode pincode code phrase paraphrase)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/30 14:06
S134	17	S133 and (dynamic$4 variable vary$3 changeable changing unpredictable non predictable one-time onetime once) near5 (password passport token passphrase passcode pincode code phrase paraphrase)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/30 14:10
S135	20	("5999525" "20100100724" "20040030752" "20020184143" "20020133412" "20020046189" "20020040346" "20020029275" "20010054148" "7975056" "7742996" "7716484" "7324972" "6731625" "6601192" "6236981" "6571290" "6067621").pn. and (dynamic$4 variable vary$3 changeable changing unpredictable non predictable one-time onetime once) near5 (password passport token passphrase passcode pincode code phrase paraphrase)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/30 15:00
S136	20	S134 S135	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/30 15:00

S137	17	S135 and (tempora$4 duration during lapse elapse interval interim expir$5 period$6 interval span length extent transi$5 temp ephemeral short life liv$3 time-depend$4 time-based timebased time-wise timewise provision$4) near5 (password passport token passphrase passcode pincode code phrase paraphrase)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/30 15:01
S138	17	S134 S137	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/30 15:02

1/2/2012 11:41:38 PM
H:\ EAST\ Workspaces\ 11333400_12210926.wsp

Index of Claims	Application/Control No. 12210926	Applicant(s)/Patent Under Reexamination ASGHARI-KAMRANI ET AL.
	Examiner ABDULHAKIM NOBAHAR	Art Unit 2432

✓	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	07/06/2009	11/20/2009	04/28/2010	09/12/2010	01/11/2011	08/11/2011	01/02/2012		
	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.** 12210926	**Applicant(s)/Patent Under Reexamination** ASGHARI-KAMRANI ET AL.
	Examiner ABDULHAKIM NOBAHAR	**Art Unit** 2432

✓	**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	07/06/2009	11/20/2009	04/28/2010	09/12/2010	01/11/2011	08/11/2011	01/02/2012		
	37	✓	✓	✓	✓	✓	✓	✓		
	38	✓	✓	✓	✓	✓	✓	✓		
	39	✓	✓	✓	✓	✓	✓	✓		
	40	✓	✓	✓	✓	✓	✓	✓		
	41	✓	✓	✓	✓	✓	✓	✓		
	42	✓	-	✓	-	-	-	-		
	43	✓	✓	✓	✓	✓	✓	✓		
	44	✓	✓	✓	✓	✓	✓	✓		
	45	✓	✓	✓	✓	✓	✓	✓		
	46	✓	✓	✓	✓	✓	✓	✓		
	47	✓	✓	✓	✓	✓	✓	✓		
	48	✓	✓	✓	✓	✓	✓	✓		
	49	✓	-	-	-	-	-	-		
	50	✓	✓	✓	✓	✓	✓	✓		
	51	✓	✓	✓	✓	✓	✓	✓		
	52	✓	✓	✓	✓	✓	✓	✓		
	53	✓	✓	✓	✓	✓	✓	✓		
	54	✓	✓	✓	✓	✓	✓	✓		
	55	✓	✓	✓	✓	✓	✓	✓		
	56	✓	-	-	-	-	-	-		
	57	✓	-	-	-	-	-	-		
	58	✓	✓	✓	✓	✓	✓	✓		
	59	✓	-	-	-	-	-	-		
	60	✓	✓	✓	✓	✓	✓	✓		
	61	✓	-	-	-	-	-	-		
	62	✓	-	-	-	-	-	-		
	63				✓	✓	✓	✓		
	64				✓	✓	✓	✓		
	65				✓	✓	✓	✓		
	66				✓	✓	✓	✓		
	67				✓	✓	✓	✓		
	68				✓	✓	✓	✓		
	69				✓	✓	✓	✓		
	70				✓	✓	✓	✓		
	71				✓	✓	✓	✓		
	72				✓	✓	✓	✓		

Index of Claims	**Application/Control No.** 12210926	**Applicant(s)/Patent Under Reexamination** ASGHARI-KAMRANI ET AL.
	Examiner ABDULHAKIM NOBAHAR	**Art Unit** 2432

✓	**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	07/06/2009	11/20/2009	04/28/2010	09/12/2010	01/11/2011	08/11/2011	01/02/2012		
	73				✓	✓	✓	✓		
	74				✓	✓	✓	✓		
	75				✓	✓	✓	✓		
	76				✓	✓	✓	✓		
	77				✓	✓	✓	✓		
	78				✓	✓	✓	✓		
	79				✓	✓	✓	✓		
	80				✓	✓	✓	✓		
	81							✓		
	82							✓		
	83							✓		
	84							✓		
	85							✓		
	86							✓		
	87							✓		
	88							✓		
	89							✓		
	90							✓		
	91							✓		

Application Number	**Application/Control No.** 12/210,926	**Applicant(s)/Patent under Reexamination** ASGHARI-KAMRANI ET AL.

Document Code - DISQ	**Internal Document – DO NOT MAIL**

TERMINAL DISCLAIMER	☒ APPROVED	☐ DISAPPROVED
Date Filed : 12/12/11	**This patent is subject to a Terminal Disclaimer**	

Approved/Disapproved by:
Janice Ford

U.S. Patent and Trademark Office

TERMINAL DISCLAIMER TO OBVIATE A PROVISIONAL DOUBLE PATENTING REJECTION OVER A PENDING "REFERENCE" APPLICATION	Docket Number (Optional) KAMR002US0

In re Application of: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

Application No.: 12/210,926

Filed: SEPTEMBER 15, 2008

For: Centralized Identification and Authentication System and Method

The owner*, N. Asghari-Kamrani & K. Asghari-Kamrani, of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of any patent granted on pending **reference** Application Number 11/333,400, filed JANUARY 18, 2006, as the term of any patent granted on said **reference** application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending **reference** application. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and any patent granted on the **reference** application are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term of any patent granted on said **reference** application, "as the term of any patent granted on said **reference** application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending **reference** application," in the event that: any such patent: granted on the pending **reference** application: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321, has all claims canceled by a reexamination certificate, is reissued, or is in any manner terminated prior to the expiration of its full statutory term as shortened by any terminal disclaimer filed prior to its grant.

Check either box 1 or 2 below, if appropriate.

1. □ For submissions on behalf of a business/organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the business/organization.

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 willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2. ☑ The undersigned is an attorney or agent of record. Reg. No. 35,141

/Michael P. Fortkort/
Signature

December 12, 2011
Date

MICHAEL P. FORTKORT
Typed or printed name

703-435-9390
Telephone Number

☑ Terminal disclaimer fee under 37 CFR 1.20(d) is included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner). Form PTO/SB/96 may be used for making this statement. See MPEP § 324.

This collection of information is required by 37 CFR 1.321. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 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.

Privacy Act Statement

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

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

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

Electronic Patent Application Fee Transmittal

Application Number:	12210926
Filing Date:	15-Sep-2008
Title of Invention:	Centralized Identification and Authentication System and Method
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Filer:	Michael P. Fortkort
Attorney Docket Number:	KAMR002US0

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:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Statutory or terminal disclaimer	2814	1	80	80
		Total in USD ($)		**80**

Electronic Acknowledgement Receipt

EFS ID:	11590004
Application Number:	12210926
International Application Number:	
Confirmation Number:	7516
Title of Invention:	Centralized Identification and Authentication System and Method
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Customer Number:	58293
Filer:	Michael P. Fortkort
Filer Authorized By:	
Attorney Docket Number:	KAMR002US0
Receipt Date:	12-DEC-2011
Filing Date:	15-SEP-2008
Time Stamp:	10:01:36
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$80
RAM confirmation Number	8390
Deposit Account	503776
Authorized User	FORTKORT,MICHAEL P
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	Terminal Disclaimer Filed	Terminal_Disclaimer_12210926_filed_121211.pdf	342521 afa0acf7be31ec33df3e93ac1854685aca400693	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	29912 d202301a27eb49da86f0d9fa289e283eb5f2de6b	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	372433	

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.

Certification Under 37 C.F.R. § 1.8

I hereby certify that on November 17, 2011 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: November 17, 2011 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 12/210,926

FILING DATE: September 15, 2008

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

ATTORNEY DOCKET: KAMR002US0

CONFIRMATION NO.: 7516

VIA ELECTRONIC FILING SYSTEM
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

RESPONSE TO NON-FINAL OFFICE ACTION

Sir:

In response to the non-final Office Action mailed August 17, 2011, the Applicants hereby respectfully submit the following amendments and remarks:

Amendments to the Claims begin on page 2.

Remarks begin on page 16.

In the Claims:

Please amend the claims as follows:

1. (Currently Amended) A method for authenticating a user during an electronic transaction between the user and an External-Entity, the method comprising:

receiving electronically a request for a dynamic SecureCode for the user by a Central-Entity during the transaction between the user and the External-Entity;

generating during the transaction a dynamic SecureCode for the user in response to the request, wherein the dynamic SecureCode is valid for a predefined time and becomes invalid after being used;

providing said generated SecureCode to the user during the transaction;

receiving electronically by a Central-Entity a request for authenticating the user based on a digital identity during the transaction, which digital identity includes the SecureCode; and

authenticating by the Central-Entity the user during the transaction if the digital identity is valid.

2. (Original) A method as recited in claim 1, wherein said user has a pre-existing relationship with the External-Entity.

3. (Original) A method as recited in claim 1, wherein said user has no pre-existing relationship with the External-Entity.

4. (Previously Presented) A method as recited in claim 1, further comprising:

combining said generated SecureCode with a user-specific information using a predetermined algorithm to form a combined Secure-Code and user specific information;

maintaining the combined Secure-Code and user specific information at the Central-Entity;

using the predetermined algorithm to combine received user specific information received by the Central-Entity with a received SecureCode received by the Central-Entity to form a combined received SecureCode and received user specific information;

comparing the combined Secure-Code and user specific information with the combined received SecureCode and received user specific information to validate the user.

5-11. (Cancelled)

12. (Previously Presented) A method as recited in claim 1, wherein said External-Entity receives the user's digital identity.

13. (Previously Presented) A method as recited in claim 1, wherein said External-Entity submits a digital identity to the Central-Entity.

14. (Previously Presented) The method of claim 1, wherein said digital identity includes a user-specific information.

15. (Currently Amended) The method of claim 14, wherein the user specific information comprises one or more of the following: an alphanumeric name, an ID, a login name, and an

identification phrase~~, wherein said identification phrase comprises one or more of the following: an account number, a telephone number, an IP address, a hardware key, a software key, a session ID, a token and a serial number~~.

16. (Original) The method of claim 1, wherein the transaction corresponds to a financial transaction.

17. (Original) The method of claim 1, wherein the transaction corresponds to a non-financial transaction.

18. (Previously Presented) The method of claim 1, wherein the transaction corresponds to access to restricted web-site or restricted computer/server.

19. (Previously Presented) The method of claim 1, wherein said transaction occurs over a communication network, wherein said communication network comprises one or more of the following: an Internet, a wireless network, a mobile network, a satellite network, and a private network.

20. (Previously Presented) The method of claim 1, wherein said transaction occurs over a communication network to which is coupled said user, said Central-Entity, and said External-Entity.

21. (Currently Amended) An apparatus for authenticating a user during an electronic

transaction with an External-Entity, the apparatus comprising:

a first Central-Entity computer adapted to:

generate a dynamic SecureCode for the user in response to a request during the transaction, wherein the dynamic SecureCode is valid for a predefined time and becomes invalid after being used; and

provide said SecureCode to the user;

a second Central-Entity computer adapted to validate a digital identity, which includes said SecureCode, and authenticate the user if the digital identity is valid.

22. (Previously Presented) The apparatus as recited in claim 21, wherein said user has a pre-existing relationship with the External-Entity.

23. (Previously Presented) The apparatus as recited in claim 21, wherein said user has no pre-existing relationship with the External-Entity.

24. (Previously Presented) The apparatus as recited in claim 21, wherein said External-Entity and said Central-Entity use a SecureCode that is algorithmically combined with said user-specific information.

25-31. (Cancelled)

32. (Previously Presented) The apparatus as recited in claim 21, wherein the user submits a digital identity to the External-Entity.

33. (Previously Presented) The apparatus as recited in claim 21, wherein the External-Entity submits a digital identity to the Central-Entity.

34. (Previously Presented) The apparatus of claim 21, wherein the digital identity includes a user-specific information.

35. (Currently Amended) The apparatus of claim 34, wherein the user specific information comprises one or more of the following; an alphanumeric name, an ID, a login name, and an identification phrase~~, wherein said identification phrase comprises one or more of the following: an account number, a telephone number, an IP address, a hardware key, a software key, a session ID, or token, and a serial number~~.

36. (Previously Presented) The apparatus of claim 21, wherein the transaction corresponds to a financial transaction.

37. (Previously Presented) The apparatus of claim 21, wherein the transaction corresponds to a non-financial transaction.

38. (Previously Presented) The apparatus of claim 21, wherein the transaction corresponds to access to restricted web-site or restricted computer/server.

39. (Previously Presented) The apparatus of claim 21, wherein said transaction occurs

over a communication network and wherein said communication network comprises one or more of the following; an Internet, a wireless network, a mobile network, a satellite network, and a private network.

40. (Previously Presented) The apparatus of claim 21, wherein said transaction occurs over a communication network to which is coupled said user, said Central-Entity, and said External-Entity.

41. (Previously Presented) A method as recited in claim 4, wherein said External-Entity is using said algorithmically combined SecureCode to authenticate a user's identity.

42. (Cancelled)

43. (Previously Presented) A method as recited in claim 4, wherein said Central-Entity is using said algorithmically combined SecureCode to authenticate a user's identity.

44. (Original) A method as recited in claim 1, wherein said External-Entity and said Central-Entity are the same entity.

45. (Currently Amended) The method as recited in claim 1, wherein said Central-Entity invalidates the SecureCode after authenticating the user ~~becomes invalid after being used for authentication~~.

46. (Currently Amended) The method as recited in claim 1, wherein the Central-Entity invalidates the SecureCode ~~becomes invalid when~~ after a predefined period of time passes from when the SecureCode was generated.

47. (Currently Amended) The method as recited in claim 1, wherein said Central-Entity generates the SecureCode with dependence on the user information ~~one or more alphanumeric values~~.

48. (Currently Amended) The method as recited in claim 47, wherein said ~~one or more alphanumeric values~~ user information comprises one or more of the following: an alphanumeric name, ~~an unique key,~~ an ID, a login name, ~~a password,~~ and an identification phrase~~, wherein said identification phrase comprises an account number, a telephone number, an IP address, a Hardware key, a software key a session ID, a token, a seed, and a serial number~~.

49. (Cancelled)

50. (Currently Amended) A method for authenticating a user during an electronic transaction between the user and an External-Entity, the method comprising:

receiving electronically a request for a dynamic SecureCode for the user by a Central-Entity during the transaction between the user and the External-Entity;

generating during the transaction a dynamic SecureCode for the user in response to the request, wherein the dynamic SecureCode is valid for a predefined time and becomes invalid after being used;

providing said generated SecureCode to the user during the transaction;

receiving electronically by a Central-Entity a request for authenticating the user based on a digital identity during the transaction, which digital identity includes the SecureCode; and

authenticating by the Central-Entity the user during the transaction if the digital identity is valid, wherein said SecureCode is alphanumeric.

51. (Original) The method as recited in claim 1, wherein said user communicates with said Central-Entity over a communication network.

52. (Currently Amended) An apparatus for authenticating a user during an electronic transaction with an External-Entity, the apparatus comprising:

a first Central-Entity computer adapted to:

generate a dynamic SecureCode for the user in response to a request during the transaction, wherein the dynamic SecureCode is valid for a predefined time and becomes invalid after being used; and

provide said SecureCode to the user;

a second Central-Entity computer adapted to validate a digital identity, which includes said SecureCode, and authenticate the user if the digital identity is valid, wherein said SecureCode is alphanumeric.

53. (Original) The method as recited in claim 1, wherein said user communicates with said External-Entity over a communication network.

54. (Previously Presented) The apparatus as recited in claim 21, wherein said user communicates with said Central-Entity over a communication network.

55. (Previously Presented) The apparatus as recited in claim 21, wherein said user communicates with said External-Entity over a communication network.

56-57. (Cancelled)

58. (Previously Presented) The method as recited in claim 1, wherein said SecureCode is generated based on a request submitted by said user over a communication network.

59. (Cancelled)

60. (Previously Presented) The method as recited in claim 58, wherein said request is initiated by said user through a standard interface provided to said user.

61-62. (Cancelled)

63. (Previously Presented) The apparatus according to claim 21, wherein said first Central-Entity computer and said second Central-Entity computer are the same.

64. (Previously Presented) The apparatus according to claim 21, wherein said first Central-Entity computer and said second Central-Entity computer are different.

65. (Previously Presented) A method as recited in claim 1, wherein said digital identity comprises the SecureCode and a user-specific information.

66. (Previously Presented) A method as recited in claim 1, wherein said digital identity comprises the SecureCode.

67. (Previously Presented) A method as recited in claim 1, wherein said digital identity is invalid if the SecureCode is invalid.

68. (Previously Presented) A method as recited in claim 1, wherein said digital identity is valid if at least the SecureCode is valid.

69. (Previously Presented) A method as recited in claim 1, wherein said External-Entity authenticates the user upon receiving an affirmation authentication message from the Central-Entity.

70. (Previously Presented) A method as recited in claim 1, wherein said External-Entity authenticates the user if said Central-Entity authenticates the user based on the SecureCode.

71. (Previously Presented) The apparatus of claim 21, wherein said digital identity is invalid if the SecureCode is invalid.

72. (Previously Presented) The apparatus of claim 21, wherein said digital identity is valid if at least the SecureCode is valid.

73. (Previously Presented) The apparatus of claim 21, wherein said External-Entity authenticates the user upon receiving an affirmation authentication message from the Central-Entity.

74. (Previously Presented) The apparatus of claim 21, wherein said digital identity comprises the SecureCode.

75. (Currently Amended) The apparatus of claim 21, wherein said Central-Entity invalidates the SecureCode ~~becomes invalid after being used for authentication~~ after authenticating the user.

76. (Currently Amended) The apparatus of claim 21, wherein the Central-Entity invalidates the SecureCode ~~becomes invalid when~~ after a predefined period of time passes after the SecureCode was generated.

77. (Previously Presented) The apparatus of claim 21, wherein said Central-Entity generates the SecureCode based on said user information ~~one or more alphanumeric values~~.

78. (Currently Amended) The apparatus of claim 77, wherein said ~~one or more~~

~~alphanumeric values~~ user information comprises one or more of the following: an alphanumeric name, ~~an unique key,~~ an ID, a login name, a password, and an identification phrase~~, wherein said identification phrase comprises an account number, a telephone number, an IP address, a Hardware key, a software key, a session id or token, a seed and a serial number~~.

79. (Currently Amended) The method of claim 65, wherein the user specific information comprises one or more of the following: an alphanumeric name, an ID, a login name, and an identification phrase~~, wherein said identification phrase comprises one or more of the following: an account number, a telephone number, an IP address, a hardware key, a software key, a session id or token and a serial number~~.

80. (Previously Presented) The apparatus of claim 21, wherein said External-Entity authenticates the user if said Central-Entity authenticates the user based on the SecureCode.

81. (New) The apparatus of claim 21, wherein said External-Entity and Central-Entity are the same entity.

82. (New) A method as recited in claim 50, wherein said External-Entity and Central-Entity are the same entity.

83. (New) The method of claim 50, wherein said digital identity includes a user-specific information.

84. (New) The method of claim 83, wherein the user-specific information includes user-identifying information.

85. (New) The method of claim 83, wherein the user-specific information comprises one or more of the following: an alphanumeric name, an ID, a login name, and an identification phrase.

86. (New) The apparatus of claim 52, wherein said External-Entity and Central-Entity are the same entity.

87. (New) The apparatus of claim 52, wherein said digital identity includes an user-specific information.

88. (New) The apparatus of claim 87, wherein the user-specific information includes user-identifying information.

89. (New) The method of claim 87, wherein the user-specific information comprises one or more of the following: an alphanumeric name, an ID, a login name, and an identification phrase.

90. (New) The method of claim 14, wherein the user-specific information includes user-identifying information.

91. (New) The apparatus of claim 34, wherein the user-specific information includes user-identifying information.

REMARKS

Claims 1-4, 12-24, 32-41, 43-48, 50-55, 58, 60 and 63-80 were previously pending. Claims 5-11, 25-31, 42, 49, 56-57, 59 and 61-62 have been previously cancelled without disclaimer of or prejudice to the subject matter contained therein. Claims 1, 15, 21, 35, 45, 46, 47, 48, 50, 52, and 75-79 have been amended to more particularly recite the claimed invention. Claims 81-91 have been added to further claim the present invention. Claims 1-4, 12-24, 32-41, 43-48, 50-55, 58, 60 and 63-91 remain pending.

CLAIMS REMAIN PATENTABLE OVER *FRANKLIN ET AL.* AND *FOX ET AL.* TAKEN ALONE OR IN COMBINATION

The Office Action rejected claims 1-4, 12-24, 32-41, 43, 45-48, 50-55, 58, 60 and 63-80 under 35 U.S.C. § 103(a) as being unpatentable over by U.S. Patent No. 5,883,810 A to *Franklin et al.* [hereinafter "*Franklin et al.*"] in view of U.S. Patent Publication No. 2002/0069174 A1 by Fox et al. [hereinafter "*Fox et al.*"]. Generally, the Office Action contends that *Franklin et al.* discloses all of the elements of the claims, except for certain missing features that it contends can be found in *Fox et al.*, and further contends that it would have been obvious to one of ordinary skill in the art to modify the system of *Franklin et al.* using these certain missing features from *Fox et al.* for various specified reasons. For example with regard to claim 1, the Office Action asserts that Franklin discloses all of the elements of the claim at issue, except for "receiving electronically by a Central-Entity a request for authenticating the user based on a digital identity during the transaction, which digital identity includes the SecureCode" and "authenticating by the Central-Entity the user during the transaction if the digital identity is valid." The Applicants respectfully disagree with the Office Action's characterization of these references vis-à-vis the claims at issue and respectfully request reconsideration and withdrawal of the rejection in light of the following remarks.

Factual Inquiries Set Forth in Graham v. John Deere Show Non-Obviousness

1. Determining Scope of Prior Art

Franklin et al. teaches the use of a temporary transaction number to replace one's actual credit card number to avoid exposing the actual credit card number to fraud. However, *Franklin* fails to teach any authentication method, since *Franklin et al.* relates merely to authorization of payment, which is not the same as authentication of the user. *See Aff. Hosseinzadeh filed 11/17/2011,¶7; Aff. Hewitt filed 11/17/2011, ¶11; Aff. N.Kamrani filed 11/17/2011, ¶6; Aff. K.Kamrani filed 11/17/2011, ¶6.*

Fox et al. teaches using a digital signature as the basis for authentication because only a valid digitally signed certificate is used for authenticating the user. *See Aff. Hosseinzadeh filed 11/17/2011,¶9; Aff. Hewitt filed 11/17/2011, ¶13; Aff. N.Kamrani filed 11/17/2011, ¶8; Aff. K.Kamrani filed 11/17/2011, ¶8.*

2. Ascertaining the Differences Between the Prior Art and Claims at Issue

The Claims at issue include the limitations that the dynamic SecureCode is generated during the transaction between the user and the External-Entity and that the so generated dynamic code is then used to authenticate the user. *Franklin et al.* does not authenticate a user based on any code generated during the transaction between the user and the merchant because there is no authentication being performed in *Franklin et al. See Aff. Hosseinzadeh filed 1/18/2011, ¶9-14; Aff. Laing filed 1/11/2011,¶9-14; Aff. Hewitt filed 1/18/2011,¶9-14; Aff. N.Kamrani filed 1/18/2011, ¶10-16; Aff. K.Kamrani filed 1/18/2011, ¶9-14.*

Fox et al. does not authenticate a user based on a code generated during the transaction, but requires use of a digital key obtained offline to digitally sign a certificate, which is then used for authentication of the user. *See Aff. Hosseinzadeh filed 11/17/2011,¶10; Aff. Hewitt filed 11/17/2011, ¶14; Aff. N.Kamrani filed 11/17/2011, ¶9; Aff. K.Kamrani filed 11/17/2011, ¶9.* Thus, neither reference generates a dynamic SecureCode during the transaction that is then used to authenticate the user for the transaction. Without these features, the suggested combination fails to state a *prima facie* case of obviousness.

Response to Office Action Remarks

The Office Action's argument includes several flaws in its logic. To show the presence of some claim elements in the prior art of *Franklin et al.*, the Office Action equates the recited dynamic SecureCode to the temporary transaction number of *Franklin et al.* But then in a slight of hand, the Office Action equates the GRC of *Fox et al.* to the recited dynamic SecureCode for later claim steps. So, for certain claim steps, the Office Action uses the temporary transaction number of *Franklin et al.* as the recited dynamic SecureCode and for other claim steps the Office Action uses the GRC as the recited dynamic SecureCode. A proper argument should use the same element in one reference for the same element throughout the claim. In short, the Office Action has not presented any prior art showing the use of a dynamic SecureCode in the manner recited and the differences between the prior art and the claims remain significant.

Each of the temporary transaction number and the GRC include features that preclude their use in the claimed method.

The second factual inquiry under the *Graham v. John Deere Co.* test requires ascertaining the differences between the prior art and the claims at issue. The first difference is that the same dynamic SecureCode requested during authentication of the individual is then generated and sent to the user. The same dynamic SecureCode is then received as part of an authentication request and the user is authenticated based on the same dynamic SecureCode.

The temporary transaction number of *Franklin et al.* cannot be used to authenticate the individual because it is the same as a credit card number – which is never used to authenticate people. *See Aff. Hosseinzadeh filed 1/18/2011, ¶9-14; Aff. Laing filed 1/11/2011,¶9-14; Aff. Hewitt filed 1/18/2011,¶9-14; Aff. N.Kamrani filed 1/18/2011, ¶10-16; Aff. K.Kamrani filed 1/18/2011, ¶9-14.*

The GRC of *Fox et al.* is issued at the time of registration and such is not generated during the transaction. Col. 9, lines 62-65, GUMP Method Registration Protocol. *See Aff. Hosseinzadeh filed 11/17/2011,¶9-20; Aff. Hewitt filed 11/17/2011, ¶13-24; Aff. N.Kamrani filed 11/17/2011, ¶9-19; Aff. K.Kamrani filed 11/17/2011, ¶9-19.* Moreover, the authentication process used in *Fox et al.* requires use of a public/private key combination that must be obtained out-of-band. *See Aff. Hosseinzadeh filed 11/17/2011,¶9-20; Aff. Hewitt filed 11/17/2011, ¶13-24; Aff. N.Kamrani filed 11/17/2011, ¶9-19; Aff. K.Kamrani filed 11/17/2011, ¶9-19.* Consequently, the GRC of *Fox et al.* cannot replace the temporary transaction number of *Franklin et al.* to arrive at the claimed invention because the GRC cannot be generated during the transaction, and requires elements that must be obtained offline or at least outside the transaction between the user and the External-Entity, which is required in the claims at issue. The only reason that the digitally signed GRC of *Fox et al.* can be used for authentication purposes is because it employs a public/private key that is used to sign the GRC; as a result the GRC by itself is not used to authenticate the individual but rather the digitally signed GRC is used for authentication so that only a GRC that is properly signed is considered authentic. *See Aff. Hosseinzadeh filed 11/17/2011,¶9-20; Aff. Hewitt filed 11/17/2011, ¶13-24; Aff. N.Kamrani filed*

11/17/2011, ¶9-19; Aff. K.Kamrani filed 11/17/2011, ¶9-19. Without the digital signature, the GRC is not used for authentication and *Fox et al.* requires that the authentication is only valid if the signature is valid. *Id.*

Furthermore, the temporary transaction number of *Fox et al.* is used to protect the actual credit card number from being exposed on the Internet during an online transaction. Combining *Fox et* al. with *Franklin et al.* would eliminate the need for the temporary transaction number. Because in *Fox et al.* the temporary transaction numbers or actual credit card numbers have no value without the user's digital signature. See *Fox et al.*, column 8, line 29-32 which states "If a digital signature and signature check were required on every credit card transaction, then the card number alone would have no value."

Moreover, one of ordinary skill in the art upon reading *Fox et al.* and *Franklin et al.* would not consider authenticating the individual using the temporary transaction number because *Fox et al.* teaches using a digital signature as the basis for authentication, which digital signature has a tremendous investment associated with it from obtaining the keys to perform the digital signature. *Id.*

The Office Action equates the claimed "dynamic SecureCode" of the present invention with the GRC of *Fox et al.*, which describes the GRC as follows:

> The Internet analog of an SOF is a Certified Public Signature Key (CPSK). The GUMP Registration Meta-Protocol (GRMP) is a framework for designing and implementing a financial institution's certification policies to produce a client's CPSK, packaged as a GUMP Relationship Certificate (GRC). The GRC, of course, is public information that can be sent with transaction packets, stored in online directories, and cached on distributed machines without concern that it might be accessed by unauthorized parties.

¶ [0071]

However, the GRC of *Fox et al.* is not used to authenticate the user. Rather the digital signature is used to authenticate the user. *See Aff. Hosseinzadeh filed 11/17/2011,¶9-20; Aff. Hewitt filed 11/17/2011, ¶13-24; Aff. N.Kamrani filed 11/17/2011, ¶9-19; Aff. K.Kamrani filed 11/17/2011, ¶9-19.*

The Office Action states "Fox discloses that a financial institution issues upon a request a certificate which includes a one-time secret (OTS) to the buyer, to conduct the electronic transaction with the seller where the GRC corresponds to the recited dynamic code because it is issued to the client for one electronic transaction and includes the OTS." Yet one of skill in the art of user authentication and electronic transactions would understand that this statement is inaccurate. *See Aff. Hosseinzadeh filed 11/17/2011,¶21-22; Aff. Hewitt filed 11/17/2011, ¶27-28; Aff. N.Kamrani filed 11/17/2011, ¶21-22; Aff. K.Kamrani filed 11/17/2011, ¶21-22.* The OTS in the GRC is only used to tie the client's public key to the GRC, and the OTS is an unsecret from the time the user receives digitally signed GRC certificate from the institution. *Id. Fox et al.* discloses that the institution digitally signs and sends back a GRC binding the client's public signature key to the OTS. *Id.* From this point on, the OTS becomes an unsecret (Column 3, line 1-7). *Id. Fox et al.* suggests that the OTS be derived from the user's financial account numbers, which are static. *Id.* GRC does not correspond to recited dynamic code because GRC is public information and OTS is not a secret number from the time the user receives GRC from a financial institutions. *Id.*

The statement from the Office Action"the GRC corresponds to the recited dynamic code" is inaccurate. *Id.* In *Fox et al.* a financial institution verifies the identity of the user by verifying user's digital signature using user's public key. *Id.* If a user does not digitally sign the GRC or any other document, the financial institution would not be able to verify the user and the document (GRC). *Id.* Therefore the statement "GRC correspond to dynamic code" is an invalid statement. *Id.* The claimed invention does not require a digital signature and public key protocol to verify a user. *Id.* In the present invention, a dynamic code authenticates a user whereas in *Fox et al.* a GRC does not authenticate a user. *Id.* In *Fox et al.*, it is the user's digital signature and public key that verifies the user who controls the private key. *Id.*

Furthermore, *Fox et al.* teaches away from using the GRC by itself for authentication. *See Aff. Hosseinzadeh filed 11/17/2011,¶9-20; Aff. Hewitt filed 11/17/2011, ¶13-24; Aff. N.Kamrani filed 11/17/2011, ¶9-19; Aff. K.Kamrani filed 11/17/2011, ¶9-19.* Upon reading *Fox et al.*, one of skill in the art would be taught to rely on the digital signature for authentication, but using the GRC by itself without a digital signature would be directly opposed to the teaching of *Fox et al.* Therefore, *Fox et al.* teaches away from using the GRC as the basis for authentication. As such, one of ordinary skill in the art would not modify *Franklin et al.* in the manner suggested by the Office Action because he would rely upon the teaching from *Fox et al.* of using a digital signature as the basis for authentication. But, the digital signature capability cannot be generated during the transaction as claimed, hence the claimed invention would not have been obvious to one of ordinary skill in the art based on *Fox et al.* and *Franklin et al.*

Thus, for at least these reasons the Applicants respectfully submit that the claims at issue are neither anticipated by nor rendered obvious by *Franklin et al.* and *Fox et al.*, either taken alone or in combination. Reconsideration and withdrawal of the rejection of these claims is respectfully requested.

CLAIMS REMAIN PATENTABLE OVER *FRANKLIN ET AL.* AND *FOX ET AL.* TAKEN ALONE OR IN COMBINATION WITH CERTAIN OFFICIAL NOTICE

The Office Action rejected claim 44 under 35 U.S.C. § 103(a) as being unpatentable over the combination of *Franklin et al.* and *Fox et al.* and further in view of certain Official Notice. The Office Action contends that the above mentioned combination of *Franklin et al.* and *Fox et al.* discloses all of the elements of the claim at issue, except for "wherein the External-Entity and the Central-Entity are the same," for which the Office Action provides certain Official Notice. The Office Action takes Official Notice for this teaching missing from *Franklin et al.* and *Fox et al.* Even assuming *arguendo* that the Office Action's application of Official Notice in combination with *Franklin et al.* and *Fox et al.* is proper, because this claim ultimately depends from independent claim 1, which has been shown to be patentable over the combination of *Franklin et al.* and *Fox et al.*, claim 44 remains patentable over the combination of *Franklin et al., Fox et al.* and the certain Official Notice for at least the same reasons discussed above. The Applicants therefore respectfully request reconsideration and withdrawal of the rejection of claim 44.

CONCLUSION

The Applicant respectfully submits this application is in condition for allowance and requests issuance of a Notice of Allowance.

Although not believed necessary, the Office is hereby authorized to charge any fees required under 37 C.F.R. § 1.16 or § 1.17 or credit any overpayments to the deposit account of MICHAEL P FORTKORT PC, Deposit Account No. 50-3776.

In the event the prosecution of this Application can be efficiently advanced by a phone discussion, it is requested that the undersigned attorney be called at (703) 435-9390.

Respectfully submitted,

By /Michael P. Fortkort/ Date: November 17, 2011
Michael P. Fortkort (Reg. No. 35,141)

MICHAEL P FORTKORT PC
The International Law Center
13164 Lazy Glen Lane
Oak Hill, Virginia 20171

Please direct telephone calls to:
Michael P. Fortkort
703-435-9390
703-435-8857 (facsimile)

Certification Under 37 C.F.R. § 1.8

I hereby certify that on November 17, 2011 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: November 17, 2011 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 12/210,926

FILING DATE: September 15, 2008

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

ATTORNEY DOCKET: KAMR002US0

CONFIRMATION NO.: 7516

VIA ELECTRONIC FILING SYSTEM
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

AFFIDAVIT UNDER RULE 132

Applicants hereby submit this affidavit in support of their response to the Office Action mailed August 17, 2011 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 12/210,926 and pursuant to the provisions of 37 C.F.R. § 1.132. The witness hereby avers and testifies as follows:

1. I am Kamran Asghari-Kamrani, one of the inventors listed in U.S. patent Application No. 12/210,926, which is the subject of the present proceeding.

2. Bachelor of Computer Science – Specialization: Data Management and Database Design, Technical University of The Hague, The Hague, Netherlands.

3. Director, CGI Federal. Senior level business and IT professional with over 18 years of experience in architecting and leading complex enterprise-wide solutions for Fortune 1000 companies and the federal government; an Expert in authorization and authentication, fraud and identity theft prevention; Devoted much of my time to studying, and devising solutions for these multifaceted problems; Knowledgeable in the computer Architecture Software and Information Security area.

4. I am familiar with the specification and pending claims of the present Application.

5. I have reviewed U.S. Patent No. 5,883,810 A to Franklin et al. ("*Franklin et al.*") and U.S. Patent Publication No. 2002/0069174 A1 by Fox et al. ("*Fox et al.*").

6. The temporary transaction number of *Franklin et al.* does not correspond to the dynamic SecureCode disclosed in U.S. Patent Application No. 12/210,926 and one of skill in the art upon reading both *Franklin et al.* and U.S. Patent Application No. 12/210,926 would NOT consider the dynamic SecureCode to be equivalent to the temporary transaction number. The temporary transaction number serves an entirely different purpose (i.e., to replace an actual credit card number to protect the actual credit card number from being exposed on the Internet during an online transaction) than the purpose served by the recited and disclosed dynamic SecureCode (*i.e.*, which is used to authenticate the individual); and one of skill in the art would understand this and therefore consider the dynamic code to be different than the temporary transaction number

7. U.S. Patent Publication No. 2002/0069174 A1 by Fox et al. ("*Fox et al.*") does not disclose anything equivalent to the disclosed and recited dynamic code in U.S. Patent Application No. 12/210,926 which dynamic SecureCode is during a transaction between the user and an External-Entity, which dynamic SecureCode is included in an authentication request and which dynamic SecureCode is used to authenticate the individual.

8. One of skill in the art of authentication would understand that the GRC of *Fox et al.* is not equivalent to the dynamic SecureCode of U.S. Patent Application No. 12/210,926 because in *Fox et al.* the GRC is not used to authenticate the individual, but rather ***a digitally signed GRC is used to authenticate the individual.*** This is a significant distinction.

9. Based on my review of *Fox et al., Fox et al.* employs a digital signature protocol to authenticate a user to a merchant during an online transaction. As is known by those of skill in the authentication art, a digital signature employs a matched pair of public and private encryption keys obtained by a user through an offline or out of band registration process, during which a user submits identification credentials (typically in person) and then later generates and registers the public-private key pair that is used to identify him.

10. In *Fox et al.*, a user digitally signs the user's GRC certificate using the user's private key and sends the digitally signed GRC to an institution over a communication network. The institution that holds user's public key can verify the digital signature using user's public key and thereby authenticate the user. In other words, the user can be authenticated because the institution can rely upon the fact that if the public key the institution holds that is associated with the user properly decrypts the GRC, then the user must have encrypted the GRC using the related private key. Thus, authentication is based on verifying that the public key matches the user.

11. One of skill in the art of authentication would understand that *Fox et al.* requires a digital signature and public key protocol to ensure that the user and the transaction signed by the user are authentic, or in other words the GRC was signed by a user that has access to the user's private key.

12. *Fox et al.* discloses that "*the digital signature is unique to the first party and includes both the public key and a private key, the private key being employed by the first party to transform the certificate, creating an encoded certificate, and the public key being employed by others to verify the encoded certificate.*" ¶ *[0011]*.

13. One of skill in the art of authentication would understand that in *Fox at al.* if a user does not digitally sign a GRC certificate, an entity that receives the user's GRC certificate would not be able to verify the user and the certificate. Thus, in *Fox et al.* authentication is based on a public-private key combination rather than the contents of the GRC.

14. One of skill in the art of authentication would understand that GRC certificate is useless as a means of identification to anyone who does not control the private key. A user digitally signs a GRC certificate with the user's private key before sending it to the merchant *Fox et al.*, ¶¶ [0009] and [0134]. The digitally signed GRC certificate indicates that the user and/or the transaction are authentic. *Fox et al.* discloses that "*the GRC is public information that can be sent with transaction packets, stored in online directories, and cached on distributed machines without concern that it might be accessed by unauthorized parties.*" ¶ [0071].

15. One of skill in the art of authentication would understand that digital signature and public key protocol is required in *Fox et al.* for authenticating various parties and eliminating this protocol from *Fox et al.* teaches away from the method specified by *Fox et al.*

16. One of skill in the art of authentication would understand that a modified system of *Franklin et al.* in view of *Fox et al.* would require a digital signature and public key protocol for authenticating a user. The *Fox et al.* workflow is conceptually bound to the public key and digital signature model of identification and authentication. As *Fox et al.* states, it implements a "meta-protocol", in the sense that it is a protocol built upon the pre-existing protocol public key and digital signature protocol. The contrasting key usages are listed below:

User Private Key (Fox et al.)	***User Public Key (Fox et al.)***
Secret	Not secret
Generated by user locally (simultaneously with the user public key) before user being involved in any transaction	Generated by user locally (simultaneously with the user private key) before user being involved in any transaction
Stored by user locally and kept private	Stored in the user certificate and made public
Used by the user for **SIGNING**, which requires possession of the user private key.	Used by Financial Institution or Seller for **VERIFYING SIGNATURE,** which confirms after the fact that the signer had possession of the user private key.

17. One of skill in the art of authentication would understand that a modified system of *Franklin et al.* in view of *Fox et al.* would require a user to satisfy GUMP's authentication policy. *Fox et al.* discloses that *GUMP's authentication policy requires the user to digitally sign a transaction instrument containing a freshness challenge, proving current control of the private signature key corresponding to the public key in the GRC (column 10, line 33-36).*

18. One of skill in the art of authentication would understand that *Kamrani* does not require a digital signature and public key protocol for authenticating the user but rather bases authentication of the user on a dynamic SecureCode.

19. One of skill in the authentication art would understand the difference between user authentication during online transaction in *Kamrani* that is based on dynamic SecureCode and user authentication in *Fox et al.* that is based on digital signature and public key protocol and users are required to satisfy *GUMP's authentication policy.*

20. With regard to the following statement, "Fox discloses that a financial institution issues upon a request a certificate which includes a one-time secret (OTS) to the buyer, to conduct the electronic transaction with the seller where the GRC corresponds to the recited dynamic code because it is issued to the client for one electronic transaction and includes the OTS" one of skill in the art of user authentication and electronic transactions would understand that this statement is inaccurate. The OTS in the GRC is only used to tie the client's public key to the GRC, and the OTS is an unsecret from the time the user receives digitally signed GRC certificate from the institution. Fox et al disclose that *the institution digitally signs and sends back a GRC binding the client's public signature key to the OTS. From this point on, the OTS becomes an unsecret (Column 3, line 1-7).* The Fox patent suggests that the OTS be derived from the user's financial account numbers, which are static. GRC does not correspond to recited dynamic SecureCode because GRC is public information and OTS is not a secret number from the time the user receives GRC from a financial institutions.

21. Also the statement "the GRC corresponds to the recited dynamic code" is inaccurate. In *Fox et al.* a financial institution verifies the identity of the user by verifying user's digital signature using user's public key. If a user does not digitally sign the GRC or any other document, the financial institution would not be able to verify the user and the

document (GRC). Therefore the statement "GRC correspond to dynamic code" is an invalid statement. *Kamrani* does not require a digital signature and public key protocol to verify a user. In *Kamrani*, a dynamic SecureCode authenticates a user whereas in *Fox* a GRC does not authenticate a user. In *Fox*, it is the user's digital signature and public key that verifies the user who controls the private key.

I affirm that all statements made herein of my own knowledge are true, and that all statements made herein on information and belief are believed to be true. I understand that willful false statements and the like are punishable by fine or imprisonment, or both (18 U.S.C. 1001), and may jeopardize the validity of the present patent application or any patent issuing thereon.

FURTHER AFFIANT SAYETH NOT.

It witness whereof,

____
Kamran Asghari-Kamrani

11/13/2011
Date

Certification Under 37 C.F.R. § 1.8

I hereby certify that on November 17, 2011 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: November 17, 2011 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 12/210,926

FILING DATE: September 15, 2008

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

ATTORNEY DOCKET: KAMR002US0

CONFIRMATION NO.: 7516

VIA ELECTRONIC FILING SYSTEM
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

AFFIDAVIT UNDER RULE 132

Applicants hereby submit this affidavit in support of their response to the Office Action mailed August 17, 2011 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 12/210,926 and pursuant to the provisions of 37 C.F.R. § 1.132. The witness hereby avers and testifies as follows:

1. I am Nader Asghari-Kamrani, one of the inventors listed in U.S. patent Application No. 12/210,926, which is the subject of the present proceeding.

2. I received a degree in computer science from Technical University of Vienna, in Vienna, Austria in 1993. I have been working in the field of authentication over communication networks since 2000. I am one of skill in the art of authentication and electrical transactions, including PKI and digital signature, online credit card payment as well as banking transactions.

3. In 2003, I obtained an Accredited ACH Professional certification from NACHA (The Electronic Payment Association). There are only approximately 3500 people with this certification in the United States.

4. I am familiar with the specification and pending claims of the present Application.

5. I have reviewed U.S. Patent No. 5,883,810 A to Franklin et al. ("*Franklin et al.*") and U.S. Patent Publication No. 2002/0069174 A1 by Fox et al. ("*Fox et al.*").

6. The temporary transaction number of *Franklin et al.* does not correspond to the dynamic SecureCode disclosed in U.S. Patent Application No. 12/210,926 and one of skill in the art upon reading both *Franklin et al.* and U.S. Patent Application No. 12/210,926 would NOT consider the dynamic SecureCode to be equivalent to the temporary transaction number., The temporary transaction number serves an entirely different purpose (i.e., to replace an actual credit card number to protect the actual credit card number from being exposed on the Internet during an online transaction) than the purpose served by the recited and disclosed dynamic SecureCode (*i.e.*, which is used to authenticate the individual); and one of skill in the art would understand this and therefore consider the dynamic code to be different than the temporary transaction number

7. U.S. Patent Publication No. 2002/0069174 A1 by Fox et al. ("*Fox et al.*") does not disclose anything equivalent to the disclosed and recited dynamic code in U.S. Patent Application No. 12/210,926 which dynamic SecureCode is during a transaction between the user and an External-Entity, which dynamic SecureCode is included in an authentication request and which dynamic SecureCode is used to authenticate the individual.

8. One of skill in the art of authentication would understand that the GRC of *Fox et al.* is not equivalent to the dynamic SecureCode of U.S. Patent Application No. 12/210,926 because in *Fox et al.* the GRC is not used to authenticate the individual, but rather ***a digitally signed GRC is used to authenticate the individual.*** This is a significant distinction.

9. Based on my review of *Fox et al., Fox et al.* employs a digital signature protocol to authenticate a user to a merchant during an online transaction. As is known by those of skill in the authentication art, a digital signature employs a matched pair of public and private encryption keys obtained by a user through an offline or out of band registration process, during which a user submits identification credentials (typically in person) and then later generates and registers the public-private key pair that is used to identify him.

10. In *Fox et al.*, a user digitally signs the user's GRC certificate using the user's private key and sends the digitally signed GRC to an institution over a communication network. The institution that holds user's public key can verify the digital signature using user's public key and thereby authenticate the user. In other words, the user can be authenticated because the institution can rely upon the fact that if the public key the institution holds that is associated with the user properly decrypts the GRC, then the user must have encrypted the GRC using the related private key. Thus, authentication is based on verifying that the public key matches the user.

11. One of skill in the art of authentication would understand that *Fox et al.* requires a digital signature and public key protocol to ensure that the user and the transaction signed by the user are authentic, or in other words the GRC was signed by a user that has access to the user's private key.

12. *Fox et al.* discloses that "*the digital signature is unique to the first party and includes both the public key and a private key, the private key being employed by the first party to transform the certificate, creating an encoded certificate, and the public key being employed by others to verify the encoded certificate.*" ¶ *[0011].*

13. One of skill in the art of authentication would understand that in *Fox at al.* if a user does not digitally sign a GRC certificate, an entity that receives the user's GRC certificate would not be able to verify the user and the certificate. Thus, in *Fox et al.* authentication is based on a public-private key combination rather than the contents of the GRC.

14. One of skill in the art of authentication would understand that GRC certificate is useless as a means of identification to anyone who does not control the private key. A user digitally signs a GRC certificate with the user's private key before sending it to the merchant *Fox et al.*, ¶¶ [0009] and [0134]. The digitally signed GRC certificate indicates that the user and/or the transaction are authentic. *Fox et al.* discloses that "*the GRC is public information that can be sent with transaction packets, stored in online directories, and cached on distributed machines without concern that it might be accessed by unauthorized parties.*" ¶ [0071].

15. One of skill in the art of authentication would understand that digital signature and public key protocol is required in *Fox et al.* for authenticating various parties and eliminating this protocol from *Fox et al.* teaches away from the method specified by *Fox et al.*

16. One of skill in the art of authentication would understand that a modified system of *Franklin et al.* in view of *Fox et al.* would require a digital signature and public key protocol for authenticating a user. The *Fox et al.* workflow is conceptually bound to the public key and digital signature model of identification and authentication. As *Fox et al.* states, it implements a "meta-protocol", in the sense that it is a protocol built upon the pre-existing protocol public key and digital signature protocol. The contrasting key usages are listed below:

User Private Key (Fox et al.)	***User Public Key (Fox et al.)***
Secret	Not secret
Generated by user locally (simultaneously with the user public key) before user being involved in any transaction	Generated by user locally (simultaneously with the user private key) before user being involved in any transaction
Stored by user locally and kept private	Stored in the user certificate and made public
Used by the user for **SIGNING,** which requires possession of the user private key.	Used by Financial Institution or Seller for **VERIFYING SIGNATURE,** which confirms after the fact that the signer had possession of the user private key.

17. One of skill in the art of authentication would understand that a modified system of *Franklin et al.* in view of *Fox et al.* would require a user to satisfy GUMP's authentication policy. *Fox et al.* discloses that *GUMP's authentication policy requires the user to digitally sign a transaction instrument containing a freshness challenge, proving current control of the private signature key corresponding to the public key in the GRC (column 10, line 33-36).*

18. One of skill in the art of authentication would understand that *Kamrani* does not require a digital signature and public key protocol for authenticating the user but rather bases authentication of the user on a dynamic SecureCode.

19. One of skill in the authentication art would understand the difference between user authentication during online transaction in *Kamrani* that is based on dynamic SecureCode and user authentication in *Fox et al.* that is based on digital signature and public key protocol and users are required to satisfy *GUMP's authentication policy.*

20. With regard to the following statement, "Fox discloses that a financial institution issues upon a request a certificate which includes a one-time secret (OTS) to the buyer, to conduct the electronic transaction with the seller where the GRC corresponds to the recited dynamic code because it is issued to the client for one electronic transaction and includes the OTS" one of skill in the art of user authentication and electronic transactions would understand that this statement is inaccurate. The OTS in the GRC is only used to tie the client's public key to the GRC, and the OTS is an unsecret from the time the user receives digitally signed GRC certificate from the institution. Fox et al disclose that *the institution digitally signs and sends back a GRC binding the client's public signature key to the OTS. From this point on, the OTS becomes an unsecret (Column 3, line 1-7).* The Fox patent suggests that the OTS be derived from the user's financial account numbers, which are static. GRC does not correspond to recited dynamic SecureCode because GRC is public information and OTS is not a secret number from the time the user receives GRC from a financial institutions.

21. Also the statement "the GRC corresponds to the recited dynamic code" is inaccurate. In *Fox et al.* a financial institution verifies the identity of the user by verifying user's digital signature using user's public key. If a user does not digitally sign the GRC or any other document, the financial institution would not be able to verify the user and the

document (GRC). Therefore the statement "GRC correspond to dynamic code" is an invalid statement. *Kamrani* does not require a digital signature and public key protocol to verify a user. In *Kamrani,* a dynamic SecureCode authenticates a user whereas in *Fox* a GRC does not authenticate a user. In *Fox*, it is the user's digital signature and public key that verifies the user who controls the private key.

I affirm that all statements made herein of my own knowledge are true, and that all statements made herein on information and belief are believed to be true. I understand that willful false statements and the like are punishable by fine or imprisonment, or both (18 U.S.C. 1001), and may jeopardize the validity of the present patent application or any patent issuing thereon.

FURTHER AFFIANT SAYETH NOT.

It witness whereof,

Nader Asghari-Kamrani

11/13/2011
Date

Certification Under 37 C.F.R. § 1.8

I hereby certify that on November 17, 2011 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: November 17, 2011 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 12/210,926

FILING DATE: September 15, 2008

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

ATTORNEY DOCKET: KAMR002US0

CONFIRMATION NO.: 7516

VIA ELECTRONIC FILING SYSTEM
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

AFFIDAVIT UNDER RULE 132

Applicants hereby submit this affidavit in support of their response to the Office Action mailed August 17, 2011 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 12/210,926 and pursuant to the provisions of 37 C.F.R. § 1.132. The witness hereby avers and testifies as follows:

1. I am Abolfazl Hosseinzadeh, with address of PO Box 3043, Bellevue, WA 98009.

2. I am an electrical engineer with more than 20 years of proven technical leadership and multi-disciplined experience in the area of systems engineering and development, program management, information security and e-commerce.

3. My experience includes working on e-commerce security and credit card processing projects; I also developed and implemented an online authentication system for secure delivery of policies documents over the internet.

4. I have reviewed U.S. Patent Application No. 12/210,926 ("*Kamrani*") which is the subject of this proceeding.

5. I am an expert in authentication systems and security related to online transactions, which are the fields to which the claimed invention relates.

6. I have reviewed U.S. Patent No. 5,883,810 A to Franklin et al. ("*Franklin et al.*").

7. The temporary transaction number of *Franklin et al.* does not correspond to the dynamic SecureCode disclosed in U.S. Patent Application No. 12/210,926 and one of skill in the art upon reading both *Franklin et al.* and U.S. Patent Application No. 12/210,926 would NOT consider the dynamic SecureCode to be equivalent to the temporary transaction number. The temporary transaction number serves an entirely different purpose (i.e., to replace an actual credit card number to protect the actual credit card number from being exposed on the Internet during an online transaction) than the purpose served by the recited and disclosed dynamic SecureCode (*i.e.*, which is used to authenticate the individual); and one of skill in the art would understand this and therefore consider the dynamic code to be different than the temporary transaction number

8. U.S. Patent Publication No. 2002/0069174 A1 by Fox et al. ("*Fox et al.*") does not disclose anything equivalent to the disclosed and recited dynamic code in U.S. Patent Application No. 12/210,926 which dynamic SecureCode is during a transaction between the user and an External-Entity, which dynamic SecureCode is included in an authentication request and which dynamic SecureCode is used to authenticate the individual.

9. One of skill in the art of authentication would understand that the GRC of *Fox et al.* is not equivalent to the dynamic SecureCode of U.S. Patent Application No. 12/210,926 because in *Fox et al.* the GRC is not used to authenticate the individual, but rather ***a digitally signed GRC is used to authenticate the individual.*** This is a significant distinction.

10. Based on my review of *Fox et al.*. *Fox et al.* employs a digital signature protocol to authenticate a user to a merchant during an online transaction. As is known by those of skill in the authentication art, a digital signature employs a matched pair of public and private encryption keys obtained by a user through an offline or out of band registration process, during which a user submits identification credentials (typically in person) and then later generates and registers the public-private key pair that is used to identify him.

11. In *Fox et al.*, a user digitally signs the user's GRC certificate using the user's private key and sends the digitally signed GRC to an institution over a communication network. The institution that holds user's public key can verify the digital signature using user's public key and thereby authenticate the user. In other words, the user can be authenticated because the institution can rely upon the fact that if the public key the institution holds that is associated with the user properly decrypts the GRC, then the user must have encrypted the GRC using the related private key. Thus, authentication is based on verifying that the public key matches the user.

12. One of skill in the art of authentication would understand that *Fox et al.* requires a digital signature and public key protocol to ensure that the user and the transaction signed by the user are authentic, or in other words the GRC was signed by a user that has access to the user's private key.

13. *Fox et al.* discloses that "*the digital signature is unique to the first party and includes both the public key and a private key, the private key being employed by the first party to transform the certificate, creating an encoded certificate, and the public key being employed by others to verify the encoded certificate.*" ¶ *[0011]*.

14. One of skill in the art of authentication would understand that in *Fox at al.* if a user does not digitally sign a GRC certificate, an entity that receives the user's GRC certificate would not be able to verify the user and the certificate. Thus, in *Fox et al.* authentication is based on a public-private key combination rather than the contents of the GRC.

15. One of skill in the art of authentication would understand that GRC certificate is useless as a means of identification to anyone who does not control the private key. A user digitally signs a GRC certificate with the user's private key before sending it to the merchant *Fox et al.*, ¶¶ [0009] and [0134]. The digitally signed GRC certificate indicates that the user and/or the transaction are authentic. *Fox et al.* discloses that "*the GRC is public information that can be sent with transaction packets, stored in online directories, and cached on distributed machines without concern that it might be accessed by unauthorized parties.*" ¶ [0071].

16. One of skill in the art of authentication would understand that digital signature and public key protocol is required in *Fox et al.* for authenticating various parties and eliminating this protocol from *Fox et al.* teaches away from the method specified by *Fox et al.*

17. One of skill in the art of authentication would understand that a modified system of *Franklin et al.* in view of *Fox et al.* would require a digital signature and public key protocol for authenticating a user. The *Fox et al.* workflow is conceptually bound to the public key and digital signature model of identification and authentication. As *Fox et al.* states, it implements a "meta-protocol", in the sense that it is a protocol built upon the pre-existing protocol public key and digital signature protocol. The contrasting key usages are listed below:

User Private Key (Fox et al.)	***User Public Key (Fox et al.)***
Secret	Not secret
Generated by user locally (simultaneously with the user public key) before user being involved in any transaction	Generated by user locally (simultaneously with the user private key) before user being involved in any transaction
Stored by user locally and kept private	Stored in the user certificate and made public
Used by the user for **SIGNING,** which requires possession of the user private key.	Used by Financial Institution or Seller for **VERIFYING SIGNATURE,** which confirms after the fact that the signer had possession of the user private key.

18. One of skill in the art of authentication would understand that a modified system of *Franklin et al.* in view of *Fox et al.* would require a user to satisfy GUMP's authentication policy. *Fox et al.* discloses that *GUMP's authentication policy requires the user to digitally sign a transaction instrument containing a freshness challenge, proving current control of the private signature key corresponding to the public key in the GRC (column 10, line 33-36).*

19. One of skill in the art of authentication would understand that *Kamrani* does not require a digital signature and public key protocol for authenticating the user but rather bases authentication of the user on a dynamic SecureCode.

20. One of skill in the authentication art would understand the difference between user authentication during online transaction in *Kamrani* that is based on dynamic SecureCode and user authentication in *Fox et al.* that is based on digital signature and public key protocol and users are required to satisfy *GUMP's authentication policy*.

21. With regard to the following statement, "Fox discloses that a financial institution issues upon a request a certificate which includes a one-time secret (OTS) to the buyer, to conduct the electronic transaction with the seller where the GRC corresponds to the recited dynamic code because it is issued to the client for one electronic transaction and includes the OTS" one of skill in the art of user authentication and electronic transactions would understand that this statement is inaccurate. The OTS in the GRC is only used to tie the client's public key to the GRC, and the OTS is an unsecret from the time the user receives digitally signed GRC certificate from the institution. Fox et al disclose that *the institution digitally signs and sends back a GRC binding the client's public signature key to the OTS. From this point on, the OTS becomes an unsecret (Column 3, line 1-7).* The Fox patent suggests that the OTS be derived from the user's financial account numbers, which are static. GRC does not correspond to recited dynamic SecureCode because GRC is public information and OTS is not a secret number from the time the user receives GRC from a financial institutions.

22. Also the statement "the GRC corresponds to the recited dynamic code" is inaccurate. In *Fox et al.* a financial institution verifies the identity of the user by verifying user's digital signature using user's public key. If a user does not digitally sign the GRC or any other document, the financial institution would not be able to verify the user and the

document (GRC). Therefore the statement "GRC correspond to dynamic code" is an invalid statement. *Kamrani* does not require a digital signature and public key protocol to verify a user. In *Kamrani*, a dynamic SecureCode authenticates a user whereas in *Fox* a GRC does not authenticate a user. In *Fox*, it is the user's digital signature and public key that verifies the user who controls the private key.

I affirm that all statements made herein of my own knowledge are true, and that all statements made herein on information and belief are believed to be true. I understand that willful false statements and the like are punishable by fine or imprisonment, or both (18 U.S.C. 1001), and may jeopardize the validity of the present patent application or any patent issuing thereon.

FURTHER AFFIANT SAYETH NOT.

It witness whereof,

Abolfazl Hosseinzadeh

11-13-11
Date

Certification Under 37 C.F.R. § 1.8

I hereby certify that on November 17, 2011 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: November 17, 2011 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 12/210,926

FILING DATE: September 15, 2008

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

ATTORNEY DOCKET: KAMR002US0

CONFIRMATION NO.: 7516

VIA ELECTRONIC FILING SYSTEM
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

AFFIDAVIT UNDER RULE 132

Applicants hereby submit this affidavit in support of their response to the Office Action mailed August 17, 2011 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 12/210,926 and pursuant to the provisions of 37 C.F.R. § 1.132. The witness hereby avers and testifies as follows:

1. I am James Hewitt, residing at 12587 Fair Lakes Circle, #202, Fairfax, Virginia 22033.

2. I received a Bachelors of Arts in Philosophy from Vassar College in 1983.

3. I have been a Certified Information System Security Professional since 2001. My certification number is #21060 per ISC2.org.

4. From 1998-2002, I was Director of Professional Services at CertCo, Inc. in Cambridge, Massachusetts. During this time, I produced cryptographic systems used by Tier 1 banks for authentication of users, machines and financial transactions.

5. From 2002-2003, I was Secure Messaging Project Manager for the Commonwealth of Massachusetts Information Technology Division. During this period, I implemented a system for securing healthcare-related messages for the state.

6. Since 2004 I have been Director of Security Governance for CGI Federal in Fairfax, Virginia. In this position, I design, implement and manage the security of large-scale applications for government and commercial clients.

7. I have reviewed U.S. Patent Application No. 12/210,926 ("*Kamrani*") which is the subject of this proceeding.

8. I am an expert in authentication systems and security related to online transactions, which are the fields to which the claimed invention relates.

9. Due to my extensive experience in the field of authentication systems and security related to online transactions, I am familiar with the level of skill of one of ordinary skill in the art of authentication systems and security related to online transactions as of August 29, 2001, which is the earliest filing date of the present application.

10. I have reviewed U.S. Patent No. 5,883,810 A to Franklin et al. ("*Franklin et al.*").

11. The temporary transaction number of *Franklin et al.* does not correspond to the dynamic SecureCode disclosed in U.S. Patent Application No. 12/210,926 and one of skill in the art upon reading both *Franklin et al.* and U.S. Patent Application No. 12/210,926 would NOT consider the dynamic SecureCode to be equivalent to the temporary transaction number. The temporary transaction number serves an entirely different purpose (i.e., to replace an actual credit card number to protect the actual credit card number from being exposed on the Internet during an online transaction) than the purpose served by the recited and disclosed dynamic SecureCode (*i.e.*, which is used to authenticate the individual); and one of skill in the art would understand this and therefore consider the dynamic code to be different than the temporary transaction number

12. U.S. Patent Publication No. 2002/0069174 A1 by Fox et al. ("*Fox et al.*") does not disclose anything equivalent to the disclosed and recited dynamic code in U.S. Patent Application No. 12/210,926 which dynamic SecureCode is during a transaction between the user and an External-Entity, which dynamic SecureCode is included in an authentication request and which dynamic SecureCode is used to authenticate the individual.

13. One of skill in the art of authentication would understand that the GRC of *Fox et al.* is not equivalent to the dynamic SecureCode of U.S. Patent Application No. 12/210,926 because in *Fox et al.* the GRC is not used to authenticate the individual, but rather ***a digitally signed GRC is used to authenticate the individual.*** This is a significant distinction.

14. Based on my review of *Fox et al.*, *Fox et al.* employs a digital signature protocol to authenticate a user to a merchant during an online transaction. As is known by those of skill in the authentication art, a digital signature employs a matched pair of public and private encryption keys obtained by a user through an offline or out of band registration

process, during which a user submits identification credentials (typically in person) and then later generates and registers the public-private key pair that is used to identify him.

15. In *Fox et al.*, a user digitally signs the user's GRC certificate using the user's private key and sends the digitally signed GRC to an institution over a communication network. The institution that holds user's public key can verify the digital signature using user's public key and thereby authenticate the user. In other words, the user can be authenticated because the institution can rely upon the fact that if the public key the institution holds that is associated with the user properly decrypts the GRC, then the user must have encrypted the GRC using the related private key. Thus, authentication is based on verifying that the public key matches the user.

16. One of skill in the art of authentication would understand that *Fox et al.* requires a digital signature and public key protocol to ensure that the user and the transaction signed by the user are authentic, or in other words the GRC was signed by a user that has access to the user's private key.

17. *Fox et al.* discloses that *"the digital signature is unique to the first party and includes both the public key and a private key, the private key being employed by the first party to transform the certificate, creating an encoded certificate, and the public key being employed by others to verify the encoded certificate." ¶ [0011].*

18. One of skill in the art of authentication would understand that in *Fox at al.* if a user does not digitally sign a GRC certificate, an entity that receives the user's GRC certificate would not be able to verify the user and the certificate. Thus, in *Fox et al.* authentication is based on a public-private key combination rather than the contents of the GRC.

19. One of skill in the art of authentication would understand that GRC certificate is useless as a means of identification to anyone who does not control the private key. A user

digitally signs a GRC certificate with the user's private key before sending it to the merchant *Fox et al.*, ¶¶ [0009] and [0134]. The digitally signed GRC certificate indicates that the user and/or the transaction are authentic. *Fox et al.* discloses that "*the GRC is public information that can be sent with transaction packets, stored in online directories, and cached on distributed machines without concern that it might be accessed by unauthorized parties.*" ¶ [0071].

20. One of skill in the art of authentication would understand that digital signature and public key protocol is required in *Fox et al.* for authenticating various parties and eliminating this protocol from *Fox et al.* teaches away from the method specified by *Fox et al.*

21. One of skill in the art of authentication would understand that a modified system of *Franklin et al.* in view of *Fox et al.* would require a digital signature and public key protocol for authenticating a user. The *Fox et al.* workflow is conceptually bound to the public key and digital signature model of identification and authentication. As *Fox et al.* states, it implements a "meta-protocol", in the sense that it is a protocol built upon the pre-existing protocol public key and digital signature protocol. The contrasting key usages are listed below:

User Private Key (Fox et al.)	***User Public Key (Fox et al.)***
Secret	Not secret
Generated by user locally (simultaneously with the user public key) before user being involved in any transaction	Generated by user locally (simultaneously with the user private key) before user being involved in any transaction
Stored by user locally and kept private	Stored in the user certificate and made public
Used by the user for **SIGNING**, which requires possession of the user private key.	Used by Financial Institution or Seller for **VERIFYING SIGNATURE**, which confirms after the fact that the signer had possession of the user private key.

22. One of skill in the art of authentication would understand that a modified system of *Franklin et al.* in view of *Fox et al.* would require a user to satisfy GUMP's authentication policy. *Fox et al.* discloses that *GUMP's authentication policy requires the user to digitally sign a transaction instrument containing a freshness challenge, proving current control of the private signature key corresponding to the public key in the GRC (column 10, line 33-36).*

23. One of skill in the art of authentication would understand that *Kamrani* does not require a digital signature and public key protocol for authenticating the user but rather bases authentication of the user on a dynamic SecureCode.

24. One of skill in the authentication art would understand the difference between user authentication during online transaction in *Kamrani* that is based on dynamic SecureCode and user authentication in *Fox et al.* that is based on digital signature and public key protocol and users are required to satisfy *GUMP's authentication policy.*

25. With regard to the following statement, "Fox discloses that a financial institution issues upon a request a certificate which includes a one-time secret (OTS) to the buyer, to conduct the electronic transaction with the seller where the GRC corresponds to the recited dynamic code because it is issued to the client for one electronic transaction and includes the OTS" one of skill in the art of user authentication and electronic transactions would understand that this statement is inaccurate. The OTS in the GRC is only used to tie the client's public key to the GRC, and the OTS is an unsecret from the time the user receives digitally signed GRC certificate from the institution. Fox et al disclose that *the institution digitally signs and sends back a GRC binding the client's public signature key to the OTS. From this point on, the OTS becomes an unsecret (Column 3, line 1-7).* The Fox patent

suggests that the OTS be derived from the user's financial account numbers, which are static. GRC does not correspond to recited dynamic SecureCode because GRC is public information and OTS is not a secret number from the time the user receives GRC from a financial institutions.

26. Also the statement "the GRC corresponds to the recited dynamic code" is inaccurate. In *Fox et al.* a financial institution verifies the identity of the user by verifying user's digital signature using user's public key. If a user does not digitally sign the GRC or any other document, the financial institution would not be able to verify the user and the document (GRC). Therefore the statement "GRC correspond to dynamic code" is an invalid statement. *Kamrani* does not require a digital signature and public key protocol to verify a user. In *Kamrani*, a dynamic SecureCode authenticates a user whereas in *Fox* a GRC does not authenticate a user. In *Fox*, it is the user's digital signature and public key that verifies the user who controls the private key.

I affirm that all statements made herein of my own knowledge are true, and that all statements made herein on information and belief are believed to be true. I understand that willful false statements and the like are punishable by fine or imprisonment, or both (18 U.S.C. 1001), and may jeopardize the validity of the present patent application or any patent issuing thereon.

FURTHER AFFIANT SAYETH NOT.

It witness whereof,

James Hewitt

Nov. 12, 2011
Date

Electronic Patent Application Fee Transmittal

Application Number:	12210926
Filing Date:	15-Sep-2008
Title of Invention:	Centralized Identification and Authentication System and Method
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Filer:	Michael P. Fortkort
Attorney Docket Number:	KAMR002US0

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	11	30	330
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
	Total in USD ($)			**330**

Electronic Acknowledgement Receipt

EFS ID:	11428967
Application Number:	12210926
International Application Number:	
Confirmation Number:	7516
Title of Invention:	Centralized Identification and Authentication System and Method
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Customer Number:	58293
Filer:	Michael P. Fortkort
Filer Authorized By:	
Attorney Docket Number:	KAMR002US0
Receipt Date:	17-NOV-2011
Filing Date:	15-SEP-2008
Time Stamp:	13:06:43
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$330
RAM confirmation Number	10619
Deposit Account	503776
Authorized User	FORTKORT,MICHAEL P
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	Amendment/Req. Reconsideration-After Non-Final Reject	12210926_Response_to_Office_Action_Mailed_081711_filed_111711.pdf	94212 8925dbc8bdff2508311255da486dffbb28422307	no	24
Warnings:					
Information:					
2	Rule 130, 131 or 132 Affidavits	Affidavit_Kamran_Kamrani_12210926_filed_111711.pdf	1666651 5641088b47d50f242f3b99576c2d67020b43f8f2	no	7
Warnings:					
Information:					
3	Rule 130, 131 or 132 Affidavits	Affidavit_Nader_Kamrani_12210926_filed_111711.pdf	1711738 12538fead49b6f18f6fd6c778970acec2a28ace5	no	7
Warnings:					
Information:					
4	Rule 130, 131 or 132 Affidavits	Affidavit_Hosseinzadeh_12210926_filed_111711.pdf	221072 2177548571fc5d87b347e351a4eae8eb5a6e447c	no	7
Warnings:					
Information:					
5	Rule 130, 131 or 132 Affidavits	Affidavit_Hewitt_12210926_filed_111711.pdf	4470666 993116bc03ae95608b3bc54d3a3da41c6806b729	no	7
Warnings:					
Information:					
6	Fee Worksheet (SB06)	fee-info.pdf	29889 ecc1416b9b2f388234ba2eebcaf486626c69f64a	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	8194228		

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.

Certification Under 37 C.F.R. § 1.8

I hereby certify that on November 17, 2011 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: November 17, 2011 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 12/210,926

FILING DATE: September 15, 2008

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

ATTORNEY DOCKET: KAMR002US0

CONFIRMATION NO.: 7516

VIA ELECTRONIC FILING SYSTEM
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

Sir:

INTERVIEW SUMMARY

The Applicants wish to thank Examiner Abdulhakim Nobahar for participating in a telephonic interview with their representative on October 28, 2011. During the interview, the undersigned discussed the differences between the prior art and the claims. The Applicants brought an expert in authentication and online transactions, Mr. James Hewitt who explained how the system disclosed by *Fox et al.* operates and highlighted the differences between the claims at issue and the prior art of *Fox et al.* and *Franklin et al.* Certain proposed claim amendments were discussed to attempt to obtain allowance, but no agreement was reached.

CONCLUSION

The Applicant respectfully submits this application is in condition for allowance and requests issuance of a Notice of Allowance.

Although not believed necessary, the Office is hereby authorized to charge any fees required under 37 C.F.R. § 1.16 or § 1.17 or credit any overpayments to the deposit account of MICHAEL P FORTKORT PC, Deposit Account No. 50-3776.

In the event the prosecution of this Application can be efficiently advanced by a phone discussion, it is requested that the undersigned attorney be called at (703) 435-9390.

Respectfully submitted,

By /Michael P. Fortkort/ Date: November 17, 2011
Michael P. Fortkort (Reg. No. 35,141)

MICHAEL P FORTKORT PC
The International Law Center
13164 Lazy Glen Lane
Oak Hill, Virginia 20171

Please direct telephone calls to:
Michael P. Fortkort
703-435-9390
703-435-8857 (facsimile)

Electronic Acknowledgement Receipt

EFS ID:	11431360
Application Number:	12210926
International Application Number:	
Confirmation Number:	7516
Title of Invention:	Centralized Identification and Authentication System and Method
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Customer Number:	58293
Filer:	Michael P. Fortkort
Filer Authorized By:	
Attorney Docket Number:	KAMR002US0
Receipt Date:	17-NOV-2011
Filing Date:	15-SEP-2008
Time Stamp:	15:20:18
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	Applicant summary of interview with examiner	Interview_Summary_12210926_111711.pdf	20599 ed9ffbb72e2c1d66d0b3b266dbe3e05db5794610	no	2

Warnings:

Information:

Total Files Size (in bytes):	20599

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 (07-06)
Approved for use through 1/31/2007. 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 12/210,926	Filing Date 09/15/2008	□ To be Mailed

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	
□ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
□ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			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 $250 ($125 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			TOTAL	

APPLICATION AS AMENDED – PART II

		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
AMENDMENT	**11/17/2011**	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 70	Minus	** 62	= 8	X $30 =	240	OR	X $ =	
	Independent (37 CFR 1.16(h))	* 4	Minus	***4	= 0	X $125 =	0	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	**240**	OR	TOTAL ADD'L FEE	

		(Column 1)		(Column 2)	(Column 3)					
AMENDMENT		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 number found in the appropriate box in column 1.

Legal Instrument Examiner:
/GOIGA DUCKETT/

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.
12/210,926	09/15/2008	Nader Asghari-Kamrani	KAMR002US0	7516

58293 7590 11/03/2011
FORTKORT & HOUSTON P.C.
9442 N. CAPITAL OF TEXAS HIGHWAY
ARBORETUM PLAZA ONE, SUITE 500
AUSTIN, TX 78759

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	**PAPER NUMBER**
2432	

NOTIFICATION DATE	DELIVERY MODE
11/03/2011	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):

58293@foholaw.com
rbernfeld@foholaw.com

Applicant-Initiated Interview Summary	**Application No.** 12/210,926	**Applicant(s)** ASGHARI-KAMRANI ET AL.	
	Examiner ABDULHAKIM NOBAHAR	**Art Unit** 2432	

All participants (applicant, applicant's representative, PTO personnel):

(1) *ABDULHAKIM NOBAHAR*.

(2) *Mr. Michael P. Fortkort, Reg. No. 35,141*.

(3) *Mr. Kamran Asghari-Kamrani*.

(4) *Mr. Nader Asghari-Kamrani*

(5) Mr. James Hewit.

Date of Interview: *28 October 2011*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☒103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *1*.

Identification of prior art discussed: *2002/0069174*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Claim 1 in view of the prior art Fox et al (2002/0069174) was discussed. Mr. Fortkort pointed out the difference between the authentication process of the instant invention and the authentication process of the prior art Fox et al. Applicants are going to amend the claims to make them futher different from the teachings of the prior art of record.

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.

☐ Attachment

/Abdulhakim Nobahar/ Examiner, Art Unit 2432	

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:

- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:

1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

Doc Code: M865 or FAI.REQ.INTV

PTOL-413A (08-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Applicant Initiated Interview Request Form

Application No.: 12/210,926 First Named Applicant: Asghari-Kamrani, Nader et al.
Examiner: Mr. Abdulhakim Nobahar Art Unit: 2432 Status of Application: Non-Final Issued

Tentative Participants:
(1) Michael P. Fortkort **(2)** Nader Asghari-Kamrani

(3) Kamran Asghari-Kamrani **(4)** Mr. James Hewitt

Proposed Date of Interview: October 28, 2011 **Proposed Time:** 11:00 a.m. **(AM/PM)**

Type of Interview Requested:
(1) [ ] Telephonic (2) [✓] Personal (3) [ ] Video Conference

Exhibit To Be Shown or Demonstrated: [ ] YES [✓] NO
If yes, provide brief description:

Issues To Be Discussed

Issues (Rej., Obj., etc)	**Claims/ Fig. #s**	**Prior Art**	**Discussed**	**Agreed**	**Not Agreed**
(1) Rej	All	Franklin/Fox	[ ]	[ ]	[ ]
(2)			[ ]	[ ]	[ ]
(3)			[ ]	[ ]	[ ]
(4)			[ ]	[ ]	[ ]

[ ] Continuation Sheet Attached [ ] Proposed Amendment or Arguments Attached

Brief Description of Arguments to be Presented: Distinction between Fox and claims and combination of Franklin and Fox vis-a-vis claims

An interview was conducted on the above-identified application on

<u>NOTE</u>: This form should be completed and filed by applicant in advance of the interview (see MPEP § 713.01). If this form is signed by a registered practitioner not of record, the Office will accept this as an indication that he or she is authorized to conduct an interview on behalf of the principal (37 CFR 1.32(a)(3)) pursuant to 37 CFR 1.34. This is not a power of attorney to any above named practitioner. See the Instruction Sheet for this form, which is incorporated by reference. By signing this form, applicant or practitioner is certifying that he or she has read the Instruction Sheet. After the interview is conducted, applicant is advised to file a statement of the substance of this interview (37 CFR 1.133(b)) as soon as possible. This application will not be delayed from issue because of applicant's failure to submit a written record of this interview.

/Michael P. Fortkort/
Applicant/Applicant's Representative Signature

Examiner/SPE Signature

Michael P. Fortkort
Typed/Printed Name of Applicant or Representative

35,141
Registration Number, if applicable

This collection of information is required by 37 CFR 1.133. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 24 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.

PTOL-413A (08-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Instruction Sheet for:
APPLICANT INITIATED INTERVIEW REQUEST FORM

(Not to be Submitted to the USPTO)

1. If this form is signed by a registered practitioner not of record, the authority to submit the Applicant Initiated Interview Request Form is pursuant to limited authority to act in a representative capacity under 37 CFR 1.34 and further proof of authority to act in a representative capacity may be required. *See* 37 CFR 1.34.

   The Office will accept the signed form as an indication that the registered practitioner not of record is authorized to conduct an interview on behalf of the principal in pursuant to 37 CFR 1.34.

   For more information, see the “Conducting an Interview with a Registered Practitioner Acting in a Representative Capacity” notice which is available on the USPTO Web site at: http://www.uspto.gov/patents/law/notices/2010.jsp.

2. This is not a power of attorney to any named practitioner. Accordingly, any registered practitioner not of record named on the form does not have authority to sign a request to change the correspondence address, a request for express abandonment, a disclaimer, a power of attorney, or other document requiring the signature of the applicant, assignee of the entire interest or an attorney of record. If appropriate, a separate power of attorney to the named practitioner should be executed and filed in the US Patent and Trademark Office.

3. Any interview concerning an unpublished application under 35 U.S.C. § 122(b) with a registered practitioner not of record, pursuant to 37 CFR 1.34, will be conducted based on the information and files supplied by the practitioner in view of the confidentiality requirements of 35 U.S.C. § 122(a).

Privacy Act Statement

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

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

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

Electronic Acknowledgement Receipt

EFS ID:	11227147
Application Number:	12210926
International Application Number:	
Confirmation Number:	7516
Title of Invention:	Centralized Identification and Authentication System and Method
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Customer Number:	58293
Filer:	Michael P. Fortkort
Filer Authorized By:	
Attorney Docket Number:	KAMR002US0
Receipt Date:	20-OCT-2011
Filing Date:	15-SEP-2008
Time Stamp:	12:19:22
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	Letter Requesting Interview with Examiner	Interview_request_102011_in_12210926.pdf	421585 5adeb189452c6f3dd62bd91d14df45a6787206a3	no	3

Warnings:

Information:

Total Files Size (in bytes):	421585

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 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.
12/210,926	09/15/2008	Nader Asghari-Kamrani	KAMR002US0	7516

58293 7590 08/17/2011
FORTKORT & HOUSTON P.C.
9442 N. CAPITAL OF TEXAS HIGHWAY
ARBORETUM PLAZA ONE, SUITE 500
AUSTIN, TX 78759

EXAMINER	
NOBAHAR, ABDULHAKIM	

ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
08/17/2011	PAPER

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

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

Office Action Summary	**Application No.** 12/210,926	**Applicant(s)** ASGHARI-KAMRANI ET AL.	
	Examiner ABDULHAKIM NOBAHAR	**Art Unit** 2432	

-- 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* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, 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 *Pre-Appeal Brief on 04/14/2011*.

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

3)□ 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

4)☒ Claim(s) *1-4,12-24,32-41,43-48,50-55,58,60 and 63-80* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4, 12-24, 32-41, 43-48, 50-55, 58, 60 and 63-80* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ 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).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

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).

a)□ All b)□ Some * c)□ None of:

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) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This office action is in response to applicants' Pre-Appeal Brief Conference request on 04/14/2011.

2. Claims 1-4, 12-24, 32-41, 43-48, 50-55, 58, 60 and 63-80 are pending.

Response to Arguments

Applicant's arguments with respect to the rejections of claims under 35 USC § 102 have been fully considered and are persuasive. Therefore, the rejections have been withdrawn. However, upon further consideration of the claims, a new ground(s) of rejection is made.

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 1-4, 12-24, 32-41, 43, 45-48, 50-55, 58, 60 and 63-80 are rejected under 35 U.S.C. 103(a) as being unpatentable over Franklin et al (US 5,883,810 A), hereinafter Franklin in view of Fox et al. (US 2002/0069174 A1), hereinafter Fox.

Regarding claims 1, 21, 50, 52 and 74, Franklin discloses:

A method for authenticating a user during an electronic transaction between the user and an External-Entity (see, e.g., col. 8, lines 15-56), the method comprising:

receiving electronically a request for a dynamic SecureCode for the user by a Central-Entity during the transaction between the user and the External-Entity (see, e.g., col. 8, lines 37-42 and col. 9, lines 30-46, where the temporary transaction number corresponds to the recited dynamic SecureCode);

generating during the transaction a dynamic SecureCode for the user in response to the request (see, e.g., col. 8, lines 57-67);

providing said generated SecureCode to the user during the transaction (see, e.g., col. 10, line 6-10),

Franklin, however, does not expressly disclose:

receiving electronically by a Central-Entity a request for authenticating the user based on a digital identity during the transaction, which digital identity includes the SecureCode; and

authenticating by the Central-Entity the user during the transaction if the digital identity is valid.

Fox discloses a method for an electronic transaction (i.e., e-commerce or online business transaction) between a buyer and a seller (see, e.g., [0017]). Fox discloses that a financial institution issues upon request a certificate which includes a one-time secret (OTS) to the buyer to conduct the electronic transaction with the seller (see, e.g., [0077], [0079], [0133] and [0139] where the GRC corresponds to the recited dynamic code because it is issued to the client for one electronic transaction and includes the OTS). Fox further discloses that the seller receives the GRC from the client (i.e., buyer) and forwards the GRC to its associated financial bank, an advising bank. The advising bank verifies the authenticity of the GRC by receiving a confirmation from an opening bank which is the client's financial institution (see, e.g., [0142]-[0144], [0160] and Fig. 11, step 167).

It would have been obvious to a person of ordinary skill in the art at the time of the invention was made to modify the system of Franklin to authenticate a user by verifying the user's one-time certificate (i.e., dynamic code) because it would facilitate two-party financial transactions between trusted and non-anonymous trading partners (see Fox, [0008]).

Regarding claims 2 and 22, Franklin discloses:

A method as recited in claim 1, wherein said user has a pre-existing relationship with the External-Entity (see, e.g., col. 8, line 15+, where before the transaction phase the customer has opened an account with the bank).

Regarding claims 3 and 23, Franklin discloses:

A method as recited in claim 1, wherein said user has no pre-existing relationship with the External-Entity (see, e.g., col. 5, line 23+, where before the registration phase the customer did not have an account with the bank).

Regarding claims 4, 24 and 43, Franklin discloses:

combining said generated SecureCode with a user-specific information using a predetermined algorithm to form a combined Secure-Code and user specific information (see, e.g., col. 8, line 60+, The account manager 60 associates the transaction number with the customer account number in a data record on the customer database 64; col. 11, lines 7-31: “transaction records”);

maintaining the combined Secure-Code and user specific information at the Central-Entity (see, e.g., Fig. 2, customer database 64 and col. 8, line 60+):

using the predetermined algorithm to combine received user specific information received by the Central-Entity with a received SecureCode received by the Central-Entity to form a combined received SecureCode and received user specific information (see, e.g., col. 11, lines 7-31);

comparing the combined Secure-Code and user specific information with the combined received SecureCode and received user specific information to validate the user (see, e.g., col. 11, lines 11-21).

Regarding claims 12 and 32, Franklin discloses:

A method as recited in claim 1, wherein the External-Entity receives the user’s digital identity (see, e.g., col. 8, lines 24-36).

Regarding claims 13 and 33, Franklin discloses:

A method as recited in claim 1, wherein said External-Entity submits a digital identity to the Central-Entity (see, e.g., col. 10, lines 61-67).

Regarding claims 14, 34, 65 and 66, Franklin does not expressly discloses:

The method of claim 1, wherein said digital identity includes a user-specific information.

Fox, however discloses:

The computer implemented method of claim 26, wherein said digital identity includes a user-specific information (see, e.g., [0071], [0139] and [0140], where the GRC includes information associated with the user).

It would have been obvious to a person of ordinary skill in the art at the time of the invention was made to modify the system of Franklin to include the user information with the dynamic code for verifying the identity of the user because it would provide the required assurance of authenticity, privacy and non-repudiation (see Fox, [0008]).

Regarding claims 15, 35, 48, 78 and 79, Franklin discloses:

The method of claim 14, wherein the user-specific information comprises one or more of the following: an alphanumeric name, an ID, a login name, and an identification phrase, wherein said identification phrase comprises one or more of the following: an account number, a telephone number, an IP address, a hardware key, a software key, a session ID, a token and serial number (see, e.g., col. 6, lines 25-32).

Regarding claims 16 and 36, Franklin discloses:

The method of claim 1, wherein the transaction corresponds to a financial transaction (see, e.g., col. 3, lines 34-47).

Regarding claims 17 and 37, Franklin discloses:

The method of claim 1, wherein the transaction corresponds to a non-financial transaction (see, e.g., col. 1, lines 19-25, order goods and/or services, where services may include non-financial transaction such as accessing secured information, application, web sites or other resources).

Regarding claims 18 and 38, Franklin discloses:

The method of claim 1, wherein the transaction corresponds to access to restricted web-site or restricted computer/server (see, e.g., col. 1, lines 19-25, order goods and/or services, where services may include non-financial transaction such as accessing secured information, application , web sites or other resources).

Regarding claims 19 and 39, Franklin discloses:

The method of claim 1, wherein said transaction occurs over a communication network, wherein said communication network comprises one or more of the following: an Internet, a wireless network, a mobile network, a satellite, and a private network (see, e.g., Fig. 1).

Regarding claims 20, 40, 51, 53-55 and 58, Franklin discloses:

The method of claim 1, wherein said transaction occurs over a communication network to which is coupled said user, said Central-Entity, and said External-Entity (see, e.g., Fig. 1).

Regarding claim 41, Franklin discloses:

A method as recited in claim 4, wherein said External-Entity is using said algorithmically combined SecureCode to authenticate a user's identity (see, e.g., col. 8, lines 24-36, the order form is a combination of the transaction number and other user's related information).

Regarding claims 45 and 75, Franklin discloses:

The method as recited in claim 1, wherein said SecureCode becomes invalid after being used for authentication (see, e.g., col. 2, lines 12-20, for a single transaction).

Regarding claims 46 and 76, Franklin discloses:

The method as recited in claim 1, wherein the SecureCode becomes invalid when a predefined period of time passes (see, e.g., col. 2, lines 12-20, where “a short expiration term" corresponds to the recited predefined period of time).

Regarding claims 47 and 77, Franklin discloses:

The method as recited in claim 1, wherein said Central-Entity generates SecureCode with dependence on one or more alphanumeric values (see, e.g., col. 4, lines 48-55, where the transaction number is associated with other information means that the transaction number is dependent on some alphanumeric values).

Regarding claim 60, Franklin discloses:

The method as recited in claim 58, wherein said request is initiated by a user through a standard interface provided to said user (see, e.g., col. 5, lines 55-60).

Regarding claim 63, Franklin discloses:

The apparatus according to claim 21, wherein said first Central-Entity computer and said second Central-Entity computer are the same (see, e.g., col. 10, lines 61-67 and Fig. 5).

Regarding claim 64, Franklin discloses:

The apparatus according to claim 21, wherein said first Central-Entity computer and said second Central-Entity computer are different (see, e.g., col. 10, lines 48-60, where the computer of the merchants acquiring bank is different from the computer of the issuing bank).

Regarding claims 67, 68, 71 and 72, Franklin discloses:

A method as recited in claim 1, wherein said digital identity is invalid if the SecureCode is invalid (see, e.g., col. 2, lines 52-55, col. 10, lines 61-67).

Regarding claims 69, 70, 73 and 80, Franklin discloses:

A method as recited in claim 1, wherein said External-Entity authenticates the user upon receiving an affirmation authentication message from the Central-Entity (see, e.g., col. 11, lines 40-45).

Claim 44 is rejected under 35 U.S.C. 103(a) as being unpatentable over Franklin et al (US 5,883,810 A); hereinafter Franklin in view of Fox as applied to claims 1-4, 12-24, 32-41, 43, 45-48, 50-55, 58, 60 and 63-80 above and further in view of the examiner Official Notice.

Regarding claim 44, Franklin-Fox does not expressly disclose:

wherein said External-Entity and said Central-Entity are the same entity.

Official Notice is taken that it is old and well-known practice in the art that some institutions such as banks that maintain users' accounts, the providers of email services to users and some the department stores which provide their own credit cards to the customers, directly authenticate the users when the users requires services or accessing their web sites, without receiving authentication services from a third party. Whenever users and customers logging on to their banks web sites, or their provider's website for email services or a customer purchasing goods using a department store's credit card, the users and customers are authenticated by the respective institution independent from a. In this case the Central-Entity and the External-Entity are the same institution that having an account for the user or the customer. Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to modify the system of Franklin-Fox to have one entity to be as the same Central-Entity and External-Entity. The deployment of one entity to issue a SecurCode to a user and also to authenticate the user when using the SecurCode would make the system of Franklin a versatile and a flexible system, in another word a scalable system.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See attached PTO-892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ABDULHAKIM NOBAHAR whose telephone number is (571)272-3808. The examiner can normally be reached on M-F 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. 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.

/Abdulhakim Nobahar/
Examiner, Art Unit 2432

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432

Notice of References Cited

Application/Control No. 12/210,926	Applicant(s)/Patent Under Reexamination ASGHARI-KAMRANI ET AL.	
Examiner ABDULHAKIM NOBAHAR	Art Unit 2432	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2002/0069174 A1	06-2002	FOX et al.	705/52
*	B	US-6,338,140 B1	01-2002	Owens et al.	713/168
*	C	US-5,732,137 A	03-1998	Aziz, Ashar	713/155
*	D	US-6,715,082 B1	03-2004	Chang et al.	726/8
*	E	US-5,535,276 A	07-1996	Ganesan, Ravi	713/155
	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	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.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12210926	ASGHARI-KAMRANI ET AL.
	Examiner	**Art Unit**
	ABDULHAKIM NOBAHAR	2432

SEARCHED

Class	Subclass	Date	Examiner
726	2-5,212,5,8,18,27,28	7/26/2011	AN
713	182-186	7/26/2011	AN
705	64,67,72,76,78	7/26/2011	AN
	See attached report		

SEARCH NOTES

Search Notes	Date	Examiner
East Inventors names search (see attached report)	7/6/2009 9/23/2009	AN
EAST text search only (see attached report)		AN
PALM inventors names search	9/23/2009	AN

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner
726	2-5,21	9/23/2021	AN
713	155,168,170	9/23/2009	AN
705	35,39,44,50,64,67	9/23/2009	AN
	See attached report		

/A. N./
Examiner.Art Unit 2432

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S41	15707	(713/182-186).ccls. (726/2,5,8,18,27,28).ccls. (705/64,67,72,76,78).ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/26 10:11
S42	2811	S41 and (dynamic$4 tempora $4 time transi$5 temp) adj2 (key password code seed PIN pincode secret)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/26 10:18
S43	980	S42 and (dynamic$4 tempora $4 time transi$5 temp) adj2 (key password code seed PIN pincode secret) with (authenticat$3 verification verif $4 valid$5)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/26 10:21
S44	853	S43 and (authenticat$3 verification verifying validation validity) near2 (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper trader entity member party pay$2 spender partner counterpart)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/26 10:23
S45	435	S44 and (dynamic$4 tempora $4 time transi$5 temp) adj2 (key password code seed PIN pincode secret) with (authenticat$3 verification verif $4 valid$5) same (authenticat $3 verification verifying validation validity) near2 (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper trader entity member party pay$2 spender partner counterpart)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/26 10:24
S48	345	S45 and (online Internet electronic$4 web website digital cyber network) near3 (bank$3 shop$4 commerc$3 purchas$3 buy$3 trad$3 business retail$3 sell$3 transact $3 communicat$3 financ$4 vend$3 procur$5 exchang$3)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/26 10:44

S49	324	S48 and (dynamic$4 tempora $4 time transi$5 temp) adj2 (key password code seed PIN pincode secret) with (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper trader entity member party pay$2 spender partner counterpart)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/26 10:45
S50	168	S49 and (dynamic$4 tempora $4 time transi$5 temp) adj2 (key password code seed PIN pincode secret) same (authenticat$3 authoriz$5 verify $3 verification valid$4 validat $3 match$3 compar$5) same (authority trust$3 bank issuing institution organization authenticator center$3 central $5 centre centralization or broker$4 authoritative or authorized official)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/26 10:47
S51	111	S50 and (dynamic$4 tempora $4 time transi$5 temp) adj2 (key password code seed PIN pincode secret) with (authority trust$3 bank issuing institution organization authenticator center$3 central$5 centre centralization or broker$4 authoritative or authorized official)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/26 10:51
S52	58	("5887065" "6148404" "6199113" "5657388" "20010037466" "5809144" "20020188574" "6324525" "5974148" "20020013900" "6016476" "6205437" "6955299" "20010037308" "6202151" "6698947" "20040230807" "20020124176" "6505193" "6715082" "6148404" "5889863" "6209091" "5535276" "5737523" "5815573" "5887065" "6105133" "20010016915" "20030105964").pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/26 14:04

S55	17	S52 and (dynamic$4 tempora $4 time transi$5 temp interim transi$4 short single) adj2 (key password code seed PIN pincode secret passcode passphrase phrase ID secureID securePIN securecode identification identify$3 identity)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/26 14:14
S56	11	S52 and (variable time-depend $4 changeable changing unpredictable nonpredictable non-predictable onetime provision$4) adj2 (key password code seed PIN pincode secret passcode passphrase phrase ID secureID securePIN securecode identification identify$3 identity)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/26 14:14
S57	20	S55 S56	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/26 14:15
S58	38	S52 and (authenticat$3 verification verifying validation validity) near2 (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper trader entity member party pay$2 spender partner counterpart)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/26 14:34
S59	13	S58 and (dynamic$4 tempora $4 time transi$5 temp interim transi$4 short single timebased) adj2 (key password code seed PIN pincode secret passcode passphrase phrase ID secureID securePIN securecode identification identify$3 identity)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/26 14:35
S60	8	S58 and (variable time-depend $4 timewise changeable changing unpredictable nonpredictable non-predictable onetime provision$4) adj2 (key password code seed PIN pincode secret passcode passphrase phrase ID secureID securePIN securecode identification identify$3 identity)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/26 14:36

S61	16	S59 S60	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/26 14:36
S62	15707	(713/182-186).ccls. (726/2,5,8,18,27,28).ccls. (705/64,67,72,76,78).ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/26 22:58
S63	264	S62 and FOB	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/26 22:58
S64	105	S63 and FOB same authenticat $3	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/26 22:59
S65	71	S63 and FOB same (authenticat $3 verification verifying validation validity) near2 (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper trader entity member party pay$2 spender partner counterpart)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/26 23:01
S66	69	S65 and (online Internet electronic$4 web website digital cyber network) with (bank$3 shop$4 commerc$3 purchas$3 buy$3 trad$3 business retail$3 sell$3 transact $3 communicat$3 financ$4 vend$3 procur$5 exchang$3)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/26 23:03
S67	65	S66 and (online Internet electronic$4 web website digital cyber network) near5 (bank$3 shop$4 commerc$3 purchas$3 buy$3 trad$3 business retail$3 sell$3 transact $3 communicat$3 financ$4 vend$3 procur$5 exchang$3)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/26 23:03
S68	9190	FOB	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/26 23:04
S69	1060	S68 and FOB same (authenticat $3 verification verifying validation validity)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/26 23:04

S70	400	S69 and FOB same (authenticat$3 verification verifying validation validity) near2 (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper trader entity member party pay$2 spender partner counterpart)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/26 23:04
S71	348	S70 and (online Internet electronic$4 web website digital cyber network) near5 (bank$3 shop$4 commerc$3 purchas$3 buy$3 trad$3 business retail$3 sell$3 transact$3 communicat$3 financ$4 vend$3 procur$5 exchang$3)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/26 23:05
S72	180	S71 and FOB with (authenticat$3 verification verifying validation validity) near2 (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper trader entity member party pay$2 spender partner counterpart)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/26 23:06
S73	166	S72 and (online Internet electronic$4 web website digital cyber network) near2 (bank$3 shop$4 commerc$3 purchas$3 buy$3 trad$3 business retail$3 sell$3 transact$3 communicat$3 financ$4 vend$3 procur$5 exchang$3)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/26 23:10
S74	13	S73 and FOB with (authenticat$3 verification verifying validation validity) near2 (user client person individual subscriber member consumer customer request$2 buyer purchaser shopper trader entity member party pay$2 spender partner counterpart) same (online Internet electronic$4 web website digital cyber network) near2 (bank$3 shop$4 commerc$3 purchas$3 buy$3 trad$3 business retail$3 sell$3 transact$3 communicat$3 financ$4 vend$3 procur$5 exchang$3)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/26 23:13

8/11/2011 1:11:36 PM
H:\EAST\Workspaces\11333400_12210926.wsp

Index of Claims	**Application/Control No.** 12210926	**Applicant(s)/Patent Under Reexamination** ASGHARI-KAMRANI ET AL.
	Examiner ABDULHAKIM NOBAHAR	**Art Unit** 2432

✓	**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	07/06/2009	11/20/2009	04/28/2010	09/12/2010	01/11/2011	08/11/2011			
	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.** 12210926	**Applicant(s)/Patent Under Reexamination** ASGHARI-KAMRANI ET AL.
	Examiner ABDULHAKIM NOBAHAR	**Art Unit** 2432

✓	**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	07/06/2009	11/20/2009	04/28/2010	09/12/2010	01/11/2011	08/11/2011			
	37	✓	✓	✓	✓	✓	✓			
	38	✓	✓	✓	✓	✓	✓			
	39	✓	✓	✓	✓	✓	✓			
	40	✓	✓	✓	✓	✓	✓			
	41	✓	✓	✓	✓	✓	✓			
	42	✓	-	✓	-	-	-			
	43	✓	✓	✓	✓	✓	✓			
	44	✓	✓	✓	✓	✓	✓			
	45	✓	✓	✓	✓	✓	✓			
	46	✓	✓	✓	✓	✓	✓			
	47	✓	✓	✓	✓	✓	✓			
	48	✓	✓	✓	✓	✓	✓			
	49	✓	-	-	-	-	-			
	50	✓	✓	✓	✓	✓	✓			
	51	✓	✓	✓	✓	✓	✓			
	52	✓	✓	✓	✓	✓	✓			
	53	✓	✓	✓	✓	✓	✓			
	54	✓	✓	✓	✓	✓	✓			
	55	✓	✓	✓	✓	✓	✓			
	56	✓	-	-	-	-	-			
	57	✓	-	-	-	-	-			
	58	✓	✓	✓	✓	✓	✓			
	59	✓	-	-	-	-	-			
	60	✓	✓	✓	✓	✓	✓			
	61	✓	-	-	-	-	-			
	62	✓	-	-	-	-	-			
	63				✓	✓	✓			
	64				✓	✓	✓			
	65				✓	✓	✓			
	66				✓	✓	✓			
	67				✓	✓	✓			
	68				✓	✓	✓			
	69				✓	✓	✓			
	70				✓	✓	✓			
	71				✓	✓	✓			
	72				✓	✓	✓			

Index of Claims	**Application/Control No.** 12210926	**Applicant(s)/Patent Under Reexamination** ASGHARI-KAMRANI ET AL.
	Examiner ABDULHAKIM NOBAHAR	**Art Unit** 2432

✓	**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	07/06/2009	11/20/2009	04/28/2010	09/12/2010	01/11/2011	08/11/2011			
	73				✓	✓	✓			
	74				✓	✓	✓			
	75				✓	✓	✓			
	76				✓	✓	✓			
	77				✓	✓	✓			
	78				✓	✓	✓			
	79				✓	✓	✓			
	80				✓	✓	✓			

Certification Under 37 C.F.R. § 1.8

I hereby certify that on July 6, 2011 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: July 6, 2011 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 12/210,926

FILING DATE: September 15, 2008

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

ATTORNEY DOCKET: KAMR002US0

CONFIRMATION NO.: 7516

VIA ELECTRONIC FILING SYSTEM
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

Sir:

INTERVIEW SUMMARY

The Applicants wish to thank Examiner Abdulhakim Nobahar for participating in a telephonic interview with their representative on June 24, 2011. During the interview, the undersigned discussed the status of the application following the remand resulting from the pre-appeal conference, as well as the differences between the prior art and the claims. The Examiner indicated he was planning to conduct another search.

CONCLUSION

The Applicant respectfully submits this application is in condition for allowance and requests issuance of a Notice of Allowance.

Although not believed necessary, the Office is hereby authorized to charge any fees required under 37 C.F.R. § 1.16 or § 1.17 or credit any overpayments to the deposit account of MICHAEL P FORTKORT PC, Deposit Account No. 50-3776.

In the event the prosecution of this Application can be efficiently advanced by a phone discussion, it is requested that the undersigned attorney be called at (703) 435-9390.

Respectfully submitted,

By /Michael P. Fortkort/ Date: July 6, 2011
Michael P. Fortkort (Reg. No. 35,141)

MICHAEL P FORTKORT PC
The International Law Center
13164 Lazy Glen Lane
Oak Hill, Virginia 20171

Please direct telephone calls to:
Michael P. Fortkort
703-435-9390
703-435-8857 (facsimile)

Electronic Acknowledgement Receipt

EFS ID:	10459386
Application Number:	12210926
International Application Number:	
Confirmation Number:	7516
Title of Invention:	Centralized Identification and Authentication System and Method
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Customer Number:	58293
Filer:	Michael P. Fortkort
Filer Authorized By:	
Attorney Docket Number:	KAMR002US0
Receipt Date:	06-JUL-2011
Filing Date:	15-SEP-2008
Time Stamp:	13:15:32
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	Applicant summary of interview with examiner	Interview_Summary_12210926_070611.pdf	17823 8464bf11101eb7411005086d5c0ea61ce694e491	no	2

Warnings:

Information:

Total Files Size (in bytes):	17823

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.
12/210,926	09/15/2008	Nader Asghari-Kamrani	KAMR002US0	7516

58293 7590 07/01/2011

FORTKORT & HOUSTON P.C.
9442 N. CAPITAL OF TEXAS HIGHWAY
ARBORETUM PLAZA ONE, SUITE 500
AUSTIN, TX 78759

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	**PAPER NUMBER**
2432	

MAIL DATE	DELIVERY MODE
07/01/2011	PAPER

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

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

Interview Summary	Application No. 12/210,926	Applicant(s) ASGHARI-KAMRANI ET AL.	
	Examiner ABDULHAKIM NOBAHAR	Art Unit 2432	

All participants (applicant, applicant's representative, PTO personnel):

(1) *ABDULHAKIM NOBAHAR*. (3) *Mr. Nader Asghari-Kamrani*.

(2) *Mr. Michael Fortkort, Reg. No. 35,141*. (4)_____.

Date of Interview: *27 June 2011*.

Type: a)☒ Telephonic b)☐ Video Conference
c)☐ Personal [copy given to: 1)☐ applicant 2)☐ applicant's representative]

Exhibit shown or demonstration conducted: d)☐ Yes e)☒ No.
If Yes, brief description: _____.

Claim(s) discussed: *1*.

Identification of prior art discussed: *N/A*.

Agreement with respect to the claims f)☐ was reached. g)☒ was not reached. h)☐ N/A.

Substance of Interview including description of the general nature of what was agreed to if an agreement was reached, or any other comments: *Mr. Fortkort discussed the unique features of the pending claims and their allowability over the prior arts of record especially authenticating a user based on a digital identity that includes a dynamic secure code associated to the user. Examiner stated that a new search must be conducted at this stage to check whether any priot art(s) exist to read on the claims' features*.

(A fuller description, if necessary, and a copy of the amendments which the examiner agreed would render the claims allowable, if available, must be attached. Also, where no copy of the amendments that would render the claims allowable is available, a summary thereof must be attached.)

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. See Summary of Record of Interview requirements on reverse side or on attached sheet.

/Abdulhakim Nobahar/ Examiner, Art Unit 2432	/Gilberto Barron Jr./ Supervisory Patent Examiner, Art Unit 2432

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

———

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:

- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:

1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

Doc Code: M865 or FAI.REQ.INTV

PTOL-413A (08-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Applicant Initiated Interview Request Form

Application No.: 12/210,926 First Named Applicant: NADER ASGHARI-KAMRANI
Examiner: ABDULHAKIM NOBAHAR Art Unit: 2432 Status of Application: PENDING

Tentative Participants:
(1) MICHAEL P. FORTKORT (2) NADER ASGHARI-KAMRANI

(3) __________ (4) __________

Proposed Date of Interview: June 27, 2011 **Proposed Time:** 11:00 am **(AM/PM)**

Type of Interview Requested:
(1) [✓] Telephonic (2) [ ] Personal (3) [ ] Video Conference

Exhibit To Be Shown or Demonstrated: [ ] YES [✓] NO
If yes, provide brief description: __________

Issues To Be Discussed

Issues (Rej., Obj., etc)	Claims/ Fig. #s	Prior Art	Discussed	Agreed	Not Agreed
(1)	Indep.		[✓]	[ ]	[ ]
(2)			[ ]	[ ]	[ ]
(3)			[ ]	[ ]	[ ]
(4)			[ ]	[ ]	[ ]

[ ] Continuation Sheet Attached [ ] Proposed Amendment or Arguments Attached

Brief Description of Arguments to be Presented: Status of claims after remand from pre-appeal conference.

An interview was conducted on the above-identified application on __________

NOTE: This form should be completed and filed by applicant in advance of the interview (see MPEP § 713.01). If this form is signed by a registered practitioner not of record, the Office will accept this as an indication that he or she is authorized to conduct an interview on behalf of the principal (37 CFR 1.32(a)(3)) pursuant to 37 CFR 1.34. This is not a power of attorney to any above named practitioner. See the Instruction Sheet for this form, which is incorporated by reference. By signing this form, applicant or practitioner is certifying that he or she has read the Instruction Sheet. After the interview is conducted, applicant is advised to file a statement of the substance of this interview (37 CFR 1.133(b)) as soon as possible. This application will not be delayed from issue because of applicant's failure to submit a written record of this interview.

/Michael P. Fortkort/
Applicant/Applicant's Representative Signature

____
Examiner/SPE Signature

Michael P. Fortkort
Typed/Printed Name of Applicant or Representative

35,141
Registration Number, if applicable

This collection of information is required by 37 CFR 1.133. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 24 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.

PTOL-413A (08-10)
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 displays a valid OMB control number.

Instruction Sheet for:
APPLICANT INITIATED INTERVIEW REQUEST FORM

(Not to be Submitted to the USPTO)

1. If this form is signed by a registered practitioner not of record, the authority to submit the Applicant Initiated Interview Request Form is pursuant to limited authority to act in a representative capacity under 37 CFR 1.34 and further proof of authority to act in a representative capacity may be required. *See* 37 CFR 1.34.

   The Office will accept the signed form as an indication that the registered practitioner not of record is authorized to conduct an interview on behalf of the principal in pursuant to 37 CFR 1.34.

   For more information, see the "Conducting an Interview with a Registered Practitioner Acting in a Representative Capacity" notice which is available on the USPTO Web site at: http://www.uspto.gov/patents/law/notices/2010.jsp.

2. This is not a power of attorney to any named practitioner. Accordingly, any registered practitioner not of record named on the form does not have authority to sign a request to change the correspondence address, a request for express abandonment, a disclaimer, a power of attorney, or other document requiring the signature of the applicant, assignee of the entire interest or an attorney of record. If appropriate, a separate power of attorney to the named practitioner should be executed and filed in the US Patent and Trademark Office.

3. Any interview concerning an unpublished application under 35 U.S.C. § 122(b) with a registered practitioner not of record, pursuant to 37 CFR 1.34, will be conducted based on the information and files supplied by the practitioner in view of the confidentiality requirements of 35 U.S.C. § 122(a).

Privacy Act Statement

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

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

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

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.
12/210,926	09/15/2008	Nader Asghari-Kamrani	KAMR002US0	7516

58293 7590 05/31/2011
FORTKORT & HOUSTON P.C.
9442 N. CAPITAL OF TEXAS HIGHWAY
ARBORETUM PLAZA ONE, SUITE 500
AUSTIN, TX 78759

EXAMINER	
NOBAHAR, ABDULHAKIM	

ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
05/31/2011	PAPER

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

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

Notice of Panel Decision from Pre-Appeal Brief Review	**Application/Control No.** 12/210,926	**Applicant(s)/Patent under Reexamination** ASGHARI-KAMRANI ET AL.	
	GILBERTO BARRON JR	**Art Unit** 2432	

This is in response to the Pre-Appeal Brief Request for Review filed 14 April 2011.

1. □ **Improper Request** – The Request is improper and a conference will not be held for the following reason(s):

   □ The Notice of Appeal has not been filed concurrent with the Pre-Appeal Brief Request.
   □ The request does not include reasons why a review is appropriate.
   □ A proposed amendment is included with the Pre-Appeal Brief request.
   □ Other: .

   The time period for filing a response continues to run from the receipt date of the Notice of Appeal or from the mail date of the last Office communication, if no Notice of Appeal has been received.

2. □ **Proceed to Board of Patent Appeals and Interferences** – A Pre-Appeal Brief conference has been held. The application remains under appeal because there is at least one actual issue for appeal. Applicant is required to submit an appeal brief in accordance with 37 CFR 41.37. The time period for filing an appeal brief will be reset to be one month from mailing this decision, or the balance of the two-month time period running from the receipt of the notice of appeal, whichever is greater. Further, the time period for filing of the appeal brief is extendible under 37 CFR 1.136 based upon the mail date of this decision or the receipt date of the notice of appeal, as applicable.

   □ The panel has determined the status of the claim(s) is as follows:
   Claim(s) allowed: _____.
   Claim(s) objected to: _____.
   Claim(s) rejected: _____.
   Claim(s) withdrawn from consideration: _____.

3. □ **Allowable application** – A conference has been held. The rejection is withdrawn and a Notice of Allowance will be mailed. Prosecution on the merits remains closed. No further action is required by applicant at this time.

4. ☒ **Reopen Prosecution** – A conference has been held. The rejection is withdrawn and a new Office action will be mailed. No further action is required by applicant at this time.

All participants:

(1) GILBERTO BARRON JR.

(2) _____.

(3) Abdulhakim Nobahar, Examiner, Art Unit 2432.

(4) Benjamin Lanier, Primary Examiner, Art Unit 2432.

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432

Certification Under 37 C.F.R. § 1.8

I hereby certify that on April 14, 2011 this correspondence is being electronically filed with the U.S. Patent Office.

Date: April 14, 2011 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI
SERIAL NO.: 12/210,926
FILING DATE: September 15, 2008
EXAMINER: Mr. Abdulhakim Nobahar
ART UNIT: 2432
TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD
ATTORNEY DOCKET: KAMR002US0

APPLICANTS' REMARKS IN SUPPORT OF PRE-APPEAL REQUEST

The claims at issue stand rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,883,810 A to *Franklin et al.* ("*Franklin*"). Yet, this reference fails to include at least: (1) a request for authentication that includes a SecureCode (all claims); (2) authentication based on a valid SecureCode (all claims); and (3) an alphanumeric SecureCode (claims 50 and 52). The Office Action includes at least four major points of legal error and flawed logic.

1. Mere Conjecture Cannot Refute Evidence

The Office Action asserts that "authentication and authorization are not two mutually exclusive operations and generally a person needs to be authenticated first in order to be authorized to use or access a resource under certain or no restrictions." This statement remains unsupported and unsubstantiated by any evidence from the record and is directly opposed by six affidavits from the Applicants and four independent experts. *See Aff. Hosseinzadeh and others, ¶5.* This evidence shows that *Franklin* neither expressly nor inherently discloses authentication merely by authorizing the credit card transaction. Inherency can only be established if a feature is necessarily present, even though it is not explicitly disclosed by a reference. *In re Rijckaert*, 9 F.3d 1531, 1534 (Fed. Cir.

1993). Inherency may not be established by probabilities or possibilities. *See,* MPEP § 2112(IV). The mere fact that a certain thing may result from a given set of circumstances is not sufficient. *In re Robertson,* 169 F.3d 743, 745 (Fed. Cir. 1999). As the evidence shows that credit card *authorization* can occur without *authentication*, then *authentication* is NOT inherently disclosed merely by credit card *authorization*. Performing credit card authorization is NOT authenticating the cardholder and has never been viewed as user authentication by those of skill in the art. *See Aff. Hosseinzadeh and others,¶5-14; and Aff. Laing, ¶5-14 and pp. 4-5.* To use credit card authorization as a proxy for cardholder authentication is improper and would be seen as improper by those of skill in the art. *Id.*

The only relevant point is whether the transaction in *Franklin* comprises authentication of the customer based on the temporary transaction number. All the evidence in the record unequivocally supports the Applicants' position that there is no user authentication in *Franklin* based on the temporary transaction number. *Id.* It does not matter whether authentication and authorization are mutually exclusive operations, but rather whether these operations are the same or not. The weight of the evidence establishes they are not the same. The only evidence on the record comprises the Applicants' affidavits buttressed by four affidavits from independent experts in the field, whereas there remains no evidence supporting the Office Action's position on this point but rather only mere conjecture. As such, the weight of the evidence falls incontrovertibly on the side of Applicants' position.

2. Argument in Office Action Includes False Assumptions

Further, the Office Action cites a portion from *Franklin* at col. 8, lines 57-58 which states "the bank computer 32 receives the signed request and immediately <u>verifies the identity and authenticity of the customer.</u>" (emphasis by Examiner) in an attempt to establish that this reference teaches a request for authentication that includes a SecureCode as recited in the claims.

Remarkably, this request in *Franklin* does not contain the temporary transaction number, which the Examiner had equated to the recited SecureCode! Thus, this citation fails to disclose the claimed limitation. This request uses a digital certificate to sign the request for a temporary transaction number. *Id.* This request for authentication from *Franklin* CANNOT include the temporary transaction number because it is a request for a temporary transaction number. As the temporary transaction number does not yet exist, this citation cannot form the basis for the claim element of a request for authentication that includes a SecureCode, and basing the rejection on this teaching constitutes reversible error.

The Office Action continues to cite a series of steps from *Franklin* and states:

> The aforesaid steps are performed for a single transaction and in a short duration. The temporary transaction number is issued to a user after the user is authenticated by the bank.... The confirmation of the short life, single use (temporary) transaction number by the bank is as though the customer is authenticated to the merchant by the bank, because the steps of the entire transaction are carried out in one online session and in a short period. Therefore, Franklin teaches an online transaction between a customer, a merchant and a bank(s) that is functionally equivalent to the same steps of the instant invention recited in the claims.
> *Office Action mailed January 28, 2011, p.4.*

While also admitting the absence of key claim elements, this flawed logic assumes that the merchant knows the credit card number submitted by the customer is a temporary transaction number that was just obtained by the customer during an authenticated session between the customer and the bank. Yet, *Franklin* specifically states that the temporary transaction number looks just like a credit card number and is treated by all as a credit card number. *See Franklin, col. 10, lines 39 et seq.* Thus, the merchant cannot determine the difference between a credit card number and the temporary transaction number and so the merchant cannot rely on the normal credit card approval for any more information than what the normal credit card approval provides, which is NOT authentication. Since the merchant does not receive any more information from the bank than the merchant normally receives during a credit card authorization, the merchant cannot rely on the mere credit card authorization approval by the bank as cardholder authentication. *Id.* Therefore, the Office Action's argument contains flawed logic because it relies on false assumptions, which leads to false conclusions.

3. Argument Fails to Show Each Claim Element Arranged as in the Claims

The Examiner's penultimate statement regarding *Franklin* is that this reference teaches an online transaction that is "functionally equivalent" to the claimed invention. Yet, the law on anticipation requires more than this. *See, Old Reliable Wholesale Inc v. Cornell Corp.*, No. 2010-1247 ___ F.3d. ___ (Fed. Cir., March 16, 2011), which states:

> "Anticipation requires that all of the claim elements and their limitations are shown in a single prior art reference." *In re Skvorecz*, 580 F.3d 1262, 1266 (Fed. Cir. 2009); *see also Advanced Display Sys., Inc. v. Kent State Univ.*, 212 F.3d 1272, 1282 (Fed. Cir. 2000) (explaining that "invalidity by anticipation requires that the four corners of a single, prior art document describe every element of the claimed invention, either expressly or inherently"). Regardless of whether the VT-2 and the commercial embodiment of the '950 patent did "[e]xactly the same thing," there could be no anticipation unless the VT-2 disclosed, either expressly or inherently, all the structural limitations contained in the asserted apparatus claims. *See ... Applied Med. Res. Corp. v. United States Surgical Corp.*, 147 F.3d 1374, 1380 (Fed. Cir. 1998) (emphasizing that a prior art device does not anticipate "simply by possessing identically named parts, unless these parts also have the same structure or otherwise satisfy the claim limitations"); *In re Ruskin*, 347 F.2d 843, 846 (CCPA 1965) (Even where a prior art device is the "functional equivalent" of a patented product, it does not anticipate unless it discloses the structure required by the asserted claims.) (emphasis supplied).

To anticipate a claim, the prior art reference must teach every claim element ***arranged as in the claims.*** *Finisar v. DirecTV*, 523 F.3d 1323, 1334 (Fed. Cir. 2008) (emphasis supplied). But, the Examiner is admitting that there remains something different between *Franklin* and the claimed invention because he is using the phrase "functionally equivalent." Simply put, there is no teaching of a request for authentication that includes a SecureCode and no teaching of authentication based on a SecureCode in *Franklin. See Aff.Kamrani, ¶5-16.* Where are these claim elements in *Franklin* ARRANGED AS RECITED IN THE CLAIMS? The only request for authentication in *Franklin* does not include the temporary transaction number. The authorization of the transaction using the temporary transaction number is not an authentication of the user, hence these claims elements are simply not taught by *Franklin* nor are these claim elements arranged as in the claims at issue. Thus, Applicants respectfully submit that the claims at issue are not anticipated by *Franklin.*

4. Claims 50 and 52 Cannot be Anticipated by Franklin

The Examiner rejected claims 50 and 52 which include the claim element that the SecureCode is alphanumeric. Yet, in a previous Office Action, the Examiner admitted that *Franklin* does not expressly disclose that the SecureCode is alphanumeric and cited another reference for this missing teaching. *See Office Action mailed 09/17/10, p.10.* Therefore, this admission precludes these claims being anticipated by *Franklin.* Moreover, *Franklin* specifically states that the temporary transaction number "has the same format and number of digits as a regular credit card." *Col. 2, lines 21-23.* As such, it remains impossible for the temporary transaction number of *Franklin* to include alphanumeric values because it must be processed by traditional credit card processing systems that can only process numeric values. *See Aff. Hosseinzadeh,¶15 and others, ¶15.* Therefore, these claims cannot be anticipated by *Franklin.* Reconsideration and withdrawal of the rejection of these claims is respectfully requested.

Respectfully submitted,

By /Michael P. Fortkort/ Date: April 14, 2011

Michael P. Fortkort (Reg. No. 35,141)
13164 Lazy Glen Lane
Oak Hill, Virginia 20171
703-435-9390 (please direct all telephone calls to this number)

Doc Code: AP.PRE.REQ

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 displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional)
KAMR002US0

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]

on ______________________

Signature______________________

Typed or printed name ______________________

Application Number 12/210,926	Filed SEPTEMBER 15, 2008
First Named Inventor NADER ASGHARI-KAMRANI ET AL.	
Art Unit 2432	Examiner ABDULHAKIM NOBAHAR

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

□ applicant/inventor.

□ assignee of record of the entire interest.
See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)

☑ attorney or agent of record.
Registration number 35,141.

□ attorney or agent acting under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34 ______________

/Michael P. Fortkort/
Signature

MICHAEL P. FORTKORT
Typed or printed name

703-435-9390
Telephone number

APRIL 14, 2011
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☑ *Total of 1 forms are submitted.

This collection of information is required by 35 U.S.C. 132. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. 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: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Privacy Act Statement

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

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

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

Electronic Patent Application Fee Transmittal

Application Number:	12210926
Filing Date:	15-Sep-2008
Title of Invention:	Centralized Identification and Authentication System and Method
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Filer:	Michael P. Fortkort
Attorney Docket Number:	KAMR002US0

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:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Notice of appeal	2401	1	270	270
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**270**

Electronic Acknowledgement Receipt

EFS ID:	9881727
Application Number:	12210926
International Application Number:	
Confirmation Number:	7516
Title of Invention:	Centralized Identification and Authentication System and Method
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Customer Number:	58293
Filer:	Michael P. Fortkort
Filer Authorized By:	
Attorney Docket Number:	KAMR002US0
Receipt Date:	14-APR-2011
Filing Date:	15-SEP-2008
Time Stamp:	15:30:12
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$270
RAM confirmation Number	1860
Deposit Account	503776
Authorized User	FORTKORT,MICHAEL P

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	Notice of Appeal Filed	12210926_Notice_of_Appeal_041411.pdf	246426 0e808fd8d4c20a806fcee875265e71366817ec6e	no	2
Warnings:					
Information:					
2	Pre-Brief Conference request	12210926_Brief_in_Support_of_Pre-Appeal_Request_041411.pdf	49228 091a95d704d02d92893fa6885ff6c4f8f1626834	no	5
Warnings:					
Information:					
3	Pre-Brief Conference request	12210926_Pre-Appeal_Request_041411.pdf	239139 cecb9aaab75531d54948105a6f7e6f53f7cf8527	no	2
Warnings:					
Information:					
4	Fee Worksheet (PTO-875)	fee-info.pdf	29915 675595a51b2cbffafdbfe1e0bb889d305b6a9f26	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	564708		

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.

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.

NOTICE OF APPEAL FROM THE EXAMINER TO THE BOARD OF PATENT APPEALS AND INTERFERENCES	Docket Number (Optional) KAMR002US0

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]

on ______________________

Signature______________________

Typed or printed name ______________________

In re Application of NADER ASGHARI-KAMRANI ET AL.	
Application Number 12/210,926	Filed SEPTEMBER 15, 2008
For CENTRALIZED IDENTIFICATION AND...	
Art Unit 2432	Examiner ABDULHAKIM NOBAHAR

Applicant hereby **appeals** to the Board of Patent Appeals and Interferences from the last decision of the examiner.

The fee for this Notice of Appeal is (37 CFR 41.20(b)(1)) $ 540

☑ Applicant claims small entity status. See 37 CFR 1.27. Therefore, the fee shown above is reduced by half, and the resulting fee is: $ 270

□ A check in the amount of the fee is enclosed.

☑ Payment by credit card. Form PTO-2038 is attached.

☑ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. 503776 .

□ A petition for an extension of time under 37 CFR 1.136(a) (PTO/SB/22) is enclosed.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

□ applicant/inventor.

□ assignee of record of the entire interest.
See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)

☑ attorney or agent of record.
Registration number 35,141 .

□ attorney or agent acting under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34. ______________

/Michael P. Fortkort/
Signature

MICHAEL P. FORTKORT
Typed or printed name

703-435-9390
Telephone number

APRIL 14, 2011
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☑ *Total of 1 forms are submitted.

This collection of information is required by 37 CFR 41.31. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. 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.

Privacy Act Statement

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

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

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

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.
12/210,926	09/15/2008	Nader Asghari-Kamrani	KAMR002US0	7516

58293 7590 04/07/2011
FORTKORT & HOUSTON P.C.
9442 N. CAPITAL OF TEXAS HIGHWAY
ARBORETUM PLAZA ONE, SUITE 500
AUSTIN, TX 78759

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	PAPER NUMBER
2432	
MAIL DATE	DELIVERY MODE
04/07/2011	PAPER

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

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

Advisory Action Before the Filing of an Appeal Brief	**Application No.** *12/210,926*	**Applicant(s)** ASGHARI-KAMRANI ET AL.	
	Examiner ABDULHAKIM NOBAHAR	**Art Unit** 2432	

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

THE REPLY FILED 15 March 2011 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:

a) ☒ The period for reply expires *3* months from the mailing date of the final rejection.

b) □ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. □ The Notice of Appeal was filed on ______. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. □ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because

(a) □ They raise new issues that would require further consideration and/or search (see NOTE below);

(b) □ They raise the issue of new matter (see NOTE below);

(c) □ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or

(d) □ They present additional claims without canceling a corresponding number of finally rejected claims.

NOTE: ______. (See 37 CFR 1.116 and 41.33(a)).

4. □ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).

5. □ Applicant's reply has overcome the following rejection(s): ______.

6. □ Newly proposed or amended claim(s) ______ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).

7. ☒ For purposes of appeal, the proposed amendment(s): a) □ will not be entered, or b) ☒ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.

The status of the claim(s) is (or will be) as follows:
Claim(s) allowed: ______.
Claim(s) objected to: ______.
Claim(s) rejected: *1-4,12-24,32-41,43-48,50-55,58,60 and 63-80*.
Claim(s) withdrawn from consideration: ______.

AFFIDAVIT OR OTHER EVIDENCE

8. □ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).

9. □ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).

10. ☒ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Continuation Sheet.

12. □ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). ______

13. □ Other: ______.

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432

/Abdulhakim Nobahar/
Examiner, Art Unit 2432

Continuation of 11. does NOT place the application in condition for allowance because: The applicants arguments and the affidavits filed on 15 March 2011 are not pursvasive. The prior art Franklin et al. teaches foundamentally and substantially the same as the claimed invention. Franklin et al. teaches an online transaction system (see, e.g., Fig. 1) in which an issuing bank generates a temporary transaction number having a short life and valid for a single transaction (corresponding to the recited dynamic code) upon a customer request (see, e.g., col. 2, lines 12-17 and col. 9, lines 43-46). The customer fills out an order form to purchase a desired product from a merchant (col. 8, lines 32-33) and enters a password to be identified (i.e., authenticated) as prompted (col. 8, lines 45-46). The merchant computer submits a request for authorization over a payment network to the issuing bank computing center (col. 10, lines 48-50). The issuing bank computer receives the authorization request and it first examines the transaction number to determine whether it is a valid number (corresponding to the recited authentication of the customer) (col. 10, lines 61-63). These steps are taken for a single transaction in one online session and are functionally equivalent to the same steps of the instant invention. Therefore, the teachings of Franklin et al. meet the limitations of the instant invention.

Certification Under 37 C.F.R. § 1.8

I hereby certify that on March 15, 2011 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: March 15, 2011 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 12/210,926

FILING DATE: September 15, 2008

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

ATTORNEY DOCKET: KAMR002US0

CONFIRMATION NO.: 7516

VIA ELECTRONIC FILING SYSTEM
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

RESPONSE TO FINAL OFFICE ACTION

Sir:

In response to the final Office Action mailed January 28, 2011, the Applicants hereby respectfully submit the following amendments and remarks:

Amendments to the Claims begin on page 2.

Remarks begin on page 14.

OK to enter
/a.n./ 04/01/2011

Certification Under 37 C.F.R. § 1.8

I hereby certify that on March 15, 2011 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: March 15, 2011 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 12/210,926

FILING DATE: September 15, 2008

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

ATTORNEY DOCKET: KAMR002US0

CONFIRMATION NO.: 7516

VIA ELECTRONIC FILING SYSTEM
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

AFFIDAVIT UNDER RULE 132

Applicants hereby submit this affidavit in support of their response to the Office Action mailed January 28, 2011 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 12/210,926, and pursuant to the provisions of 37 C.F.R. § 1.132. The witness hereby avers and testifies as follows:

1. I am Majid (Mike) Shahbazi – 11501 Vale Road Oakton, VA 22124.

OK to enter
/a. n./ 04/04/2011

Certification Under 37 C.F.R. § 1.8

I hereby certify that on March 15, 2011 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: March 15, 2011 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 12/210,926

FILING DATE: September 15, 2008

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

ATTORNEY DOCKET: KAMR002US0

CONFIRMATION NO.: 7516

VIA ELECTRONIC FILING SYSTEM
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

AFFIDAVIT UNDER RULE 132

Applicants hereby submit this affidavit in support of their response to the Office Action mailed January 28, 2011 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 12/210,926, and pursuant to the provisions of 37 C.F.R. § 1.132. The witness hereby avers and testifies as follows:

1. I am Abolfazl Hosseinzadeh, with address of PO Box 3043, Bellevue, WA 98009.

OK to enter
/a. n./ 04/04/2011

Certification Under 37 C.F.R. § 1.8

I hereby certify that on March 15, 2011 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: March 15, 2011 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 12/210,926

FILING DATE: September 15, 2008

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

ATTORNEY DOCKET: KAMR002US0

CONFIRMATION NO.: 7516

VIA ELECTRONIC FILING SYSTEM
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

AFFIDAVIT UNDER RULE 132

Applicants hereby submit this affidavit in support of their response to the Office Action mailed January 28, 2011 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 12/210,926, and pursuant to the provisions of 37 C.F.R. § 1.132. The witness hereby avers and testifies as follows:

OK to enter
/a. n./ 04/04/2011

Certification Under 37 C.F.R. § 1.8

I hereby certify that on March 15, 2011 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: March 15, 2011 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 12/210,926

FILING DATE: September 15, 2008

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

ATTORNEY DOCKET: KAMR002US0

CONFIRMATION NO.: 7516

VIA ELECTRONIC FILING SYSTEM
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

AFFIDAVIT UNDER RULE 132

Applicants hereby submit this affidavit in support of their response to the Office Action mailed January 28, 2011 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 12/210,926, and pursuant to the provisions of 37 C.F.R. § 1.132. The witness hereby avers and testifies as follows:

OK to enter
/a. n./ 04/04/2011

Certification Under 37 C.F.R. § 1.8

I hereby certify that on March 15, 2011 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: March 15, 2011 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 12/210,926

FILING DATE: September 15, 2008

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

ATTORNEY DOCKET: KAMR002US0

CONFIRMATION NO.: 7516

VIA ELECTRONIC FILING SYSTEM
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

AFFIDAVIT UNDER RULE 132

Applicants hereby submit this affidavit in support of their response to the Office Action mailed January 28, 2011 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 12/210,926, and pursuant to the provisions of 37 C.F.R. § 1.132. The witness hereby avers and testifies as follows:

OK to enter
/a. n./ 04/04/2011

Certification Under 37 C.F.R. § 1.8

I hereby certify that on March 15, 2011 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: March 15, 2011 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 12/210,926

FILING DATE: September 15, 2008

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

ATTORNEY DOCKET: KAMR002US0

CONFIRMATION NO.: 7516

VIA ELECTRONIC FILING SYSTEM
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

AFFIDAVIT UNDER RULE 132

Applicants hereby submit this affidavit in support of their response to the Office Action mailed January 28, 2011 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 12/210,926, and pursuant to the provisions of 37 C.F.R. § 1.132. The witness hereby avers and testifies as follows:

1. I am Fred Laing, II

OK to enter
/a. n./ 04/04/2011

Certification Under 37 C.F.R. § 1.8

I hereby certify that on March 17, 2011 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: March 17, 2011 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 12/210,926

FILING DATE: September 15, 2008

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

ATTORNEY DOCKET: KAMR002US0

CONFIRMATION NO.: 7516

VIA ELECTRONIC FILING SYSTEM
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

Sir:

INTERVIEW SUMMARY

The Applicants wish to thank Examiner Abdulhakim Nobahar for participating in a telephonic interview with their representative on February 22, 2011. During the interview, the undersigned discussed the difference between the primary reference (*Franklin et al.*) and the claims at issue. In particular, the undersigned discussed that *Franklin et al.* does not authenticate the individual using the recited SecureCode but rather authenticates the customer using a digital certificate. No final agreement was reached regarding the claims and the rejections.

CONCLUSION

The Applicant respectfully submits this application is in condition for allowance and requests issuance of a Notice of Allowance.

Although not believed necessary, the Office is hereby authorized to charge any fees required under 37 C.F.R. § 1.16 or § 1.17 or credit any overpayments to the deposit account of MICHAEL P FORTKORT PC, Deposit Account No. 50-3776.

In the event the prosecution of this Application can be efficiently advanced by a phone discussion, it is requested that the undersigned attorney be called at (703) 435-9390.

Respectfully submitted,

By /Michael P. Fortkort/ Date: March 17, 2011
Michael P. Fortkort (Reg. No. 35,141)

MICHAEL P FORTKORT PC
The International Law Center
13164 Lazy Glen Lane
Oak Hill, Virginia 20171

Please direct telephone calls to:
Michael P. Fortkort
703-435-9390
703-435-8857 (facsimile)

Electronic Acknowledgement Receipt

EFS ID:	9677004
Application Number:	12210926
International Application Number:	
Confirmation Number:	7516
Title of Invention:	Centralized Identification and Authentication System and Method
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Customer Number:	58293
Filer:	Michael P. Fortkort
Filer Authorized By:	
Attorney Docket Number:	KAMR002US0
Receipt Date:	17-MAR-2011
Filing Date:	15-SEP-2008
Time Stamp:	09:51:32
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	Applicant summary of interview with examiner	12210926_Interview_Summary_filed_031711.pdf	20258 b175cfbe629d0568a48f10ced0b91ca9bc9c31fb	no	2

Warnings:

Information:

Total Files Size (in bytes):	20258

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.

Certification Under 37 C.F.R. § 1.8

I hereby certify that on March 15, 2011 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: March 15, 2011 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 12/210,926

FILING DATE: September 15, 2008

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

ATTORNEY DOCKET: KAMR002US0

CONFIRMATION NO.: 7516

VIA ELECTRONIC FILING SYSTEM
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

RESPONSE TO FINAL OFFICE ACTION

Sir:

In response to the final Office Action mailed January 28, 2011, the Applicants hereby respectfully submit the following amendments and remarks:

Amendments to the Claims begin on page 2.

Remarks begin on page 14.

Certification Under 37 C.F.R. § 1.8

I hereby certify that on March 15, 2011 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: March 15, 2011 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 12/210,926

FILING DATE: September 15, 2008

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

ATTORNEY DOCKET: KAMR002US0

CONFIRMATION NO.: 7516

VIA ELECTRONIC FILING SYSTEM
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

RESPONSE TO FINAL OFFICE ACTION

Sir:

In response to the final Office Action mailed January 28, 2011, the Applicants hereby respectfully submit the following amendments and remarks:

Amendments to the Claims begin on page 2.

Remarks begin on page 14.

In the Claims:

Please amend the claims as follows:

1. (Previously Presented) A method for authenticating a user during an electronic transaction between the user and an External-Entity, the method comprising:

receiving electronically a request for a dynamic SecureCode for the user by a Central-Entity during the transaction between the user and the External-Entity;

generating during the transaction a dynamic SecureCode for the user in response to the request;

providing said generated SecureCode to the user during the transaction;

receiving electronically by a Central-Entity a request for authenticating the user based on a digital identity during the transaction, which digital identity includes the SecureCode; and

authenticating by the Central-Entity the user during the transaction if the digital identity is valid.

2. (Original) A method as recited in claim 1, wherein said user has a pre-existing relationship with the External-Entity.

3. (Original) A method as recited in claim 1, wherein said user has no pre-existing relationship with the External-Entity.

4. (Previously Presented) A method as recited in claim 1, further comprising:

combining said generated SecureCode with a user-specific information using a

predetermined algorithm to form a combined Secure-Code and user specific information;

maintaining the combined Secure-Code and user specific information at the Central-Entity;

using the predetermined algorithm to combine received user specific information received by the Central-Entity with a received SecureCode received by the Central-Entity to form a combined received SecureCode and received user specific information;

comparing the combined Secure-Code and user specific information with the combined received SecureCode and received user specific information to validate the user.

5-11. (Cancelled)

12. (Previously Presented) A method as recited in claim 1, wherein said External-Entity receives the user's digital identity.

13. (Previously Presented) A method as recited in claim 1, wherein said External-Entity submits a digital identity to the Central-Entity.

14. (Previously Presented) The method of claim 1, wherein said digital identity includes a user-specific information.

15. (Previously Presented) The method of claim 14, wherein the user specific information comprises one or more of the following: an alphanumeric name, an ID, a login name, and an identification phrase, wherein said identification phrase comprises one or more of the following:

an account number, a telephone number, an IP address, a hardware key, a software key, a session ID, a token and a serial number.

16. (Original) The method of claim 1, wherein the transaction corresponds to a financial transaction.

17. (Original) The method of claim 1, wherein the transaction corresponds to a non-financial transaction.

18. (Previously Presented) The method of claim 1, wherein the transaction corresponds to access to restricted web-site or restricted computer/server.

19. (Previously Presented) The method of claim 1, wherein said transaction occurs over a communication network, wherein said communication network comprises one or more of the following: an Internet, a wireless network, a mobile network, a satellite network, and a private network.

20. (Previously Presented) The method of claim 1, wherein said transaction occurs over a communication network to which is coupled said user, said Central-Entity, and said External-Entity.

21. (Previously Presented) An apparatus for authenticating a user during an electronic transaction with an External-Entity, the apparatus comprising:

a first Central-Entity computer adapted to:

generate a dynamic SecureCode for the user in response to a request during the transaction; and

provide said SecureCode to the user;

a second Central-Entity computer adapted to validate a digital identity, which includes said SecureCode, and authenticate the user if the digital identity is valid.

22. (Previously Presented) The apparatus as recited in claim 21, wherein said user has a pre-existing relationship with the External-Entity.

23. (Previously Presented) The apparatus as recited in claim 21, wherein said user has no pre-existing relationship with the External-Entity.

24. (Previously Presented) The apparatus as recited in claim 21, wherein said External-Entity and said Central-Entity use a SecureCode that is algorithmically combined with said user-specific information.

25-31. (Cancelled)

32. (Previously Presented) The apparatus as recited in claim 21, wherein the user submits a digital identity to the External-Entity.

33. (Previously Presented) The apparatus as recited in claim 21, wherein the External-

Entity submits a digital identity to the Central-Entity.

34. (Previously Presented) The apparatus of claim 21, wherein the digital identity includes a user-specific information.

35. (Previously Presented) The apparatus of claim 34, wherein the user specific information comprises one or more of the following; an alphanumeric name, an ID, a login name, and an identification phrase, wherein said identification phrase comprises one or more of the following: an account number, a telephone number, an IP address, a hardware key, a software key, a session ID, or token, and a serial number.

36. (Previously Presented) The apparatus of claim 21, wherein the transaction corresponds to a financial transaction.

37. (Previously Presented) The apparatus of claim 21, wherein the transaction corresponds to a non-financial transaction.

38. (Previously Presented) The apparatus of claim 21, wherein the transaction corresponds to access to restricted web-site or restricted computer/server.

39. (Previously Presented) The apparatus of claim 21, wherein said transaction occurs over a communication network and wherein said communication network comprises one or more of the following; an Internet, a wireless network, a mobile network, a satellite network, and a

private network.

40. (Previously Presented) The apparatus of claim 21, wherein said transaction occurs over a communication network to which is coupled said user, said Central-Entity, and said External-Entity.

41. (Previously Presented) A method as recited in claim 4, wherein said External-Entity is using said algorithmically combined SecureCode to authenticate a user's identity.

42. (Cancelled)

43. (Previously Presented) A method as recited in claim 4, wherein said Central-Entity is using said algorithmically combined SecureCode to authenticate a user's identity.

44. (Original) A method as recited in claim 1, wherein said External-Entity and said Central-Entity are the same entity.

45. (Previously Presented) The method as recited in claim 1, wherein said SecureCode becomes invalid after being used for authentication.

46. (Previously Presented) The method as recited in claim 1, wherein the SecureCode becomes invalid when a predefined period of time passes.

47. (Original) The method as recited in claim 1, wherein said Central-Entity generates SecureCode with dependence on one or more alphanumeric values.

48. (Previously Presented) The method as recited in claim 47, wherein said one or more alphanumeric values comprise one or more of the following: an unique key, an ID, a login name, a password, and an identification phrase, wherein said identification phrase comprises an account number, a telephone number, an IP address, a Hardware key, a software key a session ID, a token, a seed, and a serial number.

49. (Cancelled)

50. (Currently Amended) A method for authenticating a user during an electronic transaction between the user and an External-Entity, the method comprising:

receiving electronically a request for a dynamic SecureCode for the user by a Central-Entity during the transaction between the user and the External-Entity;

generating during the transaction a dynamic SecureCode for the user in response to the request;

providing said generated SecureCode to the user during the transaction;

receiving electronically by a Central-Entity a request for authenticating the user based on a digital identity during the transaction, which digital identity includes the SecureCode; and

authenticating by the Central-Entity the user during the transaction if the digital identity is valid ~~The method as recited in claim 1~~, wherein said SecureCode is alphanumeric.

51. (Original) The method as recited in claim 1, wherein said user communicates with said Central-Entity over a communication network.

52. (Currently Amended) An apparatus for authenticating a user during an electronic transaction with an External-Entity, the apparatus comprising:

a first Central-Entity computer adapted to:

generate a dynamic SecureCode for the user in response to a request during the transaction; and

provide said SecureCode to the user;

a second Central-Entity computer adapted to validate a digital identity, which includes said SecureCode, and authenticate the user if the digital identity is valid ~~The apparatus as recited in claim 21~~, wherein said SecureCode is alphanumeric.

53. (Original) The method as recited in claim 1, wherein said user communicates with said External-Entity over a communication network.

54. (Previously Presented) The apparatus as recited in claim 21, wherein said user communicates with said Central-Entity over a communication network.

55. (Previously Presented) The apparatus as recited in claim 21, wherein said user communicates with said External-Entity over a communication network.

56-57. (Cancelled)

58. (Previously Presented) The method as recited in claim 1, wherein said SecureCode is generated based on a request submitted by said user over a communication network.

59. (Cancelled)

60. (Previously Presented) The method as recited in claim 58, wherein said request is initiated by said user through a standard interface provided to said user.

61-62. (Cancelled)

63. (Previously Presented) The apparatus according to claim 21, wherein said first Central-Entity computer and said second Central-Entity computer are the same.

64. (Previously Presented) The apparatus according to claim 21, wherein said first Central-Entity computer and said second Central-Entity computer are different.

65. (Previously Presented) A method as recited in claim 1, wherein said digital identity comprises the SecureCode and a user-specific information.

66. (Previously Presented) A method as recited in claim 1, wherein said digital identity comprises the SecureCode.

67. (Previously Presented) A method as recited in claim 1, wherein said digital identity is invalid if the SecureCode is invalid.

68. (Previously Presented) A method as recited in claim 1, wherein said digital identity is valid if at least the SecureCode is valid.

69. (Previously Presented) A method as recited in claim 1, wherein said External-Entity authenticates the user upon receiving an affirmation authentication message from the Central-Entity.

70. (Previously Presented) A method as recited in claim 1, wherein said External-Entity authenticates the user if said Central-Entity authenticates the user based on the SecureCode.

71. (Previously Presented) The apparatus of claim 21, wherein said digital identity is invalid if the SecureCode is invalid.

72. (Previously Presented) The apparatus of claim 21, wherein said digital identity is valid if at least the SecureCode is valid.

73. (Previously Presented) The apparatus of claim 21, wherein said External-Entity authenticates the user upon receiving an affirmation authentication message from the Central-Entity.

74. (Previously Presented) The apparatus of claim 21, wherein said digital identity comprises the SecureCode.

75. (Previously Presented) The apparatus of claim 21, wherein said SecureCode becomes invalid after being used for authentication.

76. (Previously Presented) The apparatus of claim 21, wherein the SecureCode becomes invalid when a predefined period of time passes.

77. (Previously Presented) The apparatus of claim 21, wherein said Central-Entity generates the SecureCode based on one or more alphanumeric values.

78. (Previously Presented) The apparatus of claim 78, wherein said one or more alphanumeric values comprise one or more of the following: an unique key, an ID, a login name, a password, and an identification phrase, wherein said identification phrase comprises an account number, a telephone number, an IP address, a Hardware key, a software key, a session id or token, a seed and a serial number.

79. (Previously Presented) The method of claim 65, wherein the user specific information comprises one or more of the following: an alphanumeric name, an ID, a login name, and an identification phrase, wherein said identification phrase comprises one or more of the following: an account number, a telephone number, an IP address, a hardware key, a software key, a session

id or token and a serial number.

80. (Previously Presented) The apparatus of claim 21, wherein said External-Entity authenticates the user if said Central-Entity authenticates the user based on the SecureCode.

REMARKS

Claims 1-4, 12-24, 32-41, 43-48, 50-55, 58, 60 and 63-80 were previously pending. Claims 5-11, 25-31, 42, 49, 56-57, 59 and 61-62 have been previously cancelled without disclaimer of or prejudice to the subject matter contained therein. Claims 50 and 52 have been rewritten in independent form to include all limitations of their previous base claims. No other amendments have been made. Claims 1-4, 12-24, 32-41, 43-48, 50-55, 58, 60 and 63-80 remain pending.

ALL CLAIMS REMAIN PATENTABLE OVER *FRANKLIN ET AL.*

The Office Action rejected claims 1-4, 12-24, 32-41, 43, 45-48, 51-55, 58, 60 and 63-80 under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,883,810 to *Franklin et al.* [hereinafter "*Franklin et al.*"]. Notably, claim 50 is not mentioned in the summary section, but is included in the remarks; however, the Applicants will address claim 50 as if included with the rejection of all other claims.

Because this rejection arises under 35 U.S.C. § 102(b), the Office Action must contend that *Franklin et al.* discloses all of the elements of the claims at issue. The Applicants respectfully disagree with the Office Action's characterization of these references vis-à-vis the claims at issue and respectfully request reconsideration and withdrawal of the rejection in light of the following remarks. At a minimum, the cited prior art reference fails to include at least the following claim elements: (1) a request for authentication that includes a SecureCode (all claims); (2) authentication based on a valid SecureCode (all claims); and (3) an alphanumeric SecureCode (claims 50 and 52). The Applicants will discuss in detail these features that are missing from the cited reference.

Response to Examiner's Remarks

The Office Action includes at least four major points of legal error and flawed logic in its arguments in support of the 102 rejection. First, the Office Action employs mere conjecture to refute ***evidence*** submitted by the Applicant. In and of itself, this constitutes legal error. Second, the Office Action employs false assumptions in its argument that *Franklin et al.* discloses the functional equivalent of the claimed invention, thereby leading to a false conclusion. Third, the Office Action argument fails to rigorously adhere to Federal Circuit precedent regarding anticipation. Finally, with regard to claims 50 and 52, the Office Action contradicts a position taken in prior office actions regarding the plain teachings of *Franklin et al.* to now reject these claims.

1. Mere Conjecture Cannot Refute Evidence

In response to Applicants' Rule 132 Affidavit stating that authentication of a person is different from a credit card authorization, the Office Action asserts that "authentication and authorization are not two mutually exclusive operations and generally a person needs to be authenticated first in order to be authorized to use or access a resource under certain or no restrictions." This statement remains unsupported and unsubstantiated by any evidence from the record and is directly opposed by the Rule 132 Affidavit previously submitted by the Applicants, and the Exhibits attached thereto, as well as six additional affidavits filed concurrently herewith. *See Aff. Hosseinzadeh,¶5; Aff. Hewitt, ¶5; Aff. N.Kamrani, ¶6; Aff. K.Kamrani, ¶5; Aff. Shahbazi, ¶5; and Aff. Laing, ¶5.* The Applicants respectfully request that the Examiner support this statement by *evidence* rather than personal opinion or belief because the Applicants and four independent experts

respectfully submit that this statement is not accurate. *Id.* Online credit card transactions are approved or authorized daily without any authentication. *See Aff. Hosseinzadeh,¶5; Aff. Hewitt, ¶5; Aff. N.Kamrani, ¶6; Aff. K.Kamrani, ¶5; Aff. Shahbazi, ¶5; and Aff. Laing, ¶5.* Therefore, approval or authorization of a credit card payment occurs without authentication of the user.

Notably, this means that *Franklin et al.* neither expressly nor inherently discloses authentication merely by authorizing the credit card transaction. Inherency can only be established if a feature is necessarily present, even though it is not explicitly disclosed by a reference. *In re Rijckaert*, 9 F.3d 1531, 1534 (Fed. Cir. 1993). Inherency may not be established by probabilities or possibilities. *See,* MPEP § 2112(IV). The mere fact that a certain thing may result from a given set of circumstances is not sufficient. *In re Robertson,* 169 F.3d 743, 745, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999) (emphasis supplied). Stated another way, the doctrine of inherency requires that the missing descriptive matter MUST be present, and if there is another way of performing a missing descriptive function, then the missing descriptive function is NOT inherently disclosed. As the evidence shows that *authorization* can occur without *authentication*, then *authentication* is NOT inherently disclosed merely by *authorization*.

Authentication of a credit card user in an online transaction remains a key problem today and is one problem solved by the present invention. *See Aff. Laing, pp. 4-5. Franklin et al.* does not use a temporary transaction number to authenticate the user but rather a digital certificate installed by the user on his computer from a manual registration process during a separate process between the user and a bank, of which the merchant is not part and is not aware. *See Aff. Hosseinzadeh,¶11; Aff. Hewitt, ¶11; Aff. N.Kamrani, ¶12; Aff. K.Kamrani, ¶11; Aff. Shahbazi, ¶11; and Aff. Laing, ¶11.* As opposed to *Franklin et al.*, the claimed invention avoids authentication employing a digital certificate, which is notoriously cumbersome to obtain and

use. Online transactions pose difficult problems for merchants precisely because the customers are not authenticated during the online transaction. *See Aff. Hosseinzadeh,¶6; Aff. Hewitt, ¶6; Aff. N.Kamrani, ¶7; Aff. K.Kamrani, ¶6; Aff. Shahbazi, ¶6; and Aff. Laing, ¶6 and pp. 4-5.* During a face to face transaction, the merchant can request the customer provide a driver's license or other picture identification along with the physical credit card to authenticate the customer before submitting the credit card for approval. *See, Aff. Laing, pp. 4-5.* In contrast, during an online transaction, the merchant cannot compare a picture of the customer from a government-issued identification to the actual customer. *Id. at p. 4.* Thus, during an online transaction, the credit card payment is authorized without similar authentication first occurring. *See Aff. Hosseinzadeh,¶5-14; Aff. Hewitt, ¶5-14; Aff. N.Kamrani, ¶6-16; Aff. K.Kamrani, ¶5-14; Aff. Shahbazi, ¶5-14; and Aff. Laing, ¶5-14 and pp. 4-5.* It remains irrelevant whether authentication and payment authorization are mutually exclusive operations. They are simply not the same operation. Performing payment authorization is NOT authenticating one and has never been viewed as authentication by those of skill in the art. *See Aff. Hosseinzadeh,¶5-14; Aff. Hewitt, ¶5-14; Aff. N.Kamrani, ¶5-14; Aff. K.Kamrani, ¶6-16; Aff. Shahbazi, ¶5-14; and Aff. Laing, ¶5-14 and pp. 4-5.* To use payment authorization as a proxy for authentication is improper and would be seen as improper by those of skill in the art. *Id.*

The only relevant point is whether the transaction in *Franklin et al.* comprises authentication of the customer based on the temporary transaction number. All the evidence in the record unequivocally supports the Applicants' position that there is no authentication in *Franklin et al.* based on the temporary transaction number. *Id.* It does not matter whether authentication and authorization are mutually exclusive operations, but rather whether these operations are the same or not. The weight of the evidence shows they are not the same.

The Applicants have submitted six Rule 132 Affidavits in support of this argument. *See Aff. Hosseinzadeh; Aff. Hewitt; Aff. N.Kamrani; Aff. K.Kamrani; Aff. Shahbazi; and Aff. Laing.* Thus, the only evidence on the record comprises the Applicants' affidavits buttressed by four affidavits from independent experts in the field, along with previously filed Exhibits from the industry supporting these experts' opinions, whereas there remains no evidence supporting the Office Action's position on this point but rather only mere conjecture. As such, the weight of the evidence falls incontrovertibly on the side of Applicants' position. Failing to weigh the evidence on this point constitutes reversible error.

2. Argument in Office Action Includes False Assumptions

Further in the Examiner's remarks, the Office Action cites a portion from *Franklin et al.* at col. 8, lines 57-58 which states "the bank computer 32 receives the signed request and immediately <u>verifies the identity and authenticity of the customer.</u>" (emphasis supplied by the Examiner) in an attempt to establish that this reference teaches a request for authentication that includes a SecureCode as recited in the claims. However, this request in *Frannklin et al.* does not contain the temporary transaction number, which the Examiner had equated to the recited SecureCode! Rather, this request uses a digital certificate to sign the request for a temporary transaction number. *See Aff. Hosseinzadeh,¶5; Aff. Hewitt, ¶5; Aff. N.Kamrani, ¶5; Aff. K.Kamrani, ¶6; Aff. Shahbazi, ¶5; and Aff. Laing, ¶5.* This request for authentication from *Franklin et al.* CANNOT include the temporary transaction number because it is a request for a temporary transaction number. As the temporary transaction number does not yet exist, this citation cannot form the basis for the claim element of a request for authentication that includes a SecureCode. This authentication request of *Franklin et al.* does not teach the claimed

authentication request that includes a SecureCode and basing the rejection on this teaching constitutes reversible error.

The Office Action continues to cite a series of steps from *Franklin et al.* and states:

> The aforesaid steps are performed for a single transaction and in a short duration. The temporary transaction number is issued to a user after the user is authenticated by the bank. The customer enters the temporary transaction number in the order form of the merchant while filing out the form. The merchant receives the temporary transaction number and all the necessary information related to the customer via the order form. The merchant immediately sends the temporary transaction number to the bank for verification. The confirmation of the short life, single use (temporary) transaction number by the bank is as though the customer is authenticated to the merchant by the bank, because the steps of the entire transaction are carried out in one online session and in a short period. Therefore, Franklin teaches an online transaction between a customer, a merchant and a bank(s) that is functionally equivalent to the same steps of the instant invention recited in the claims.

Office Action mailed January 28, 2011, p.4.

This flawed logic assumes that the merchant knows the credit card number submitted by the customer is a temporary transaction number that was just obtained by the customer during an authenticated session between the customer and the bank. Yet, *Franklin et al.* specifically states that the temporary transaction number looks just like a credit card number and is treated by all as a credit card number. *See Franklin et al., col. 10, lines 39 et seq. and see Aff. Hosseinzadeh,¶12; Aff. Hewitt, ¶12; Aff. N.Kamrani, ¶14; Aff. K.Kamrani, ¶12; Aff. Shahbazi, ¶12; and Aff. Laing, ¶12.* Thus, the merchant cannot determine the difference and relying upon the customer to tell the merchant that the number is a temporary transaction number that was just obtained would defeat the purpose as it would be allowing the customer to self-authenticate himself to the merchant. *See Aff. Hosseinzadeh,¶12-14; Aff. Hewitt, ¶12-14; Aff. N.Kamrani, ¶14-15; Aff. K.Kamrani, ¶12-14; Aff. Shahbazi, ¶12-14; and Aff. Laing, ¶12-14.*

First, the online transaction between the customer and the bank in *Franklin et al.* is separate from the online transaction between the customer and the merchant. *See col. 8, lines 37 et seq.* The user invokes a tool previously installed on his browser to generate an online transaction with the bank to obtain a temporary transaction number during which the user is authenticated to the bank using the previously installed digital certificate. *Id.* The merchant is completely unaware of this transaction between the customer and the bank because the merchant is not part of this transaction, and this transaction occurs separate and apart from the transaction between the customer and the merchant. *Id.* Moreover, once the temporary transaction number is issued by the bank to the customer, the customer must enter this temporary transaction number into the merchant's form where the credit card number is to be entered. *Id.* The merchant remains completely unaware that the credit card number is actually a temporary transaction number just issued. *See Franklin et al., col. 10, lines 39-47* ("Rather, the merchant computer 30 treats the transaction number of the online commerce card no differently than it treats a standard credit card number. In fact, the merchant computer 30 most likely will not be able to distinguish between the two types of numbers."). When the bank replies to the merchant it substitutes the actual account number with the temporary transaction number, hence the merchant never knows the difference between the temporary transaction number and the actual account number. *Franklin et al., col. 11, lines 32-40.*

Yet, the Office Action's argument inherently assumes that the merchant knows that the customer is using a temporary transaction number and thus when the online credit card transaction is approved the customer is therefore authenticated to the merchant. Therein lays the flaw in the Office Action's logic. Without knowing that the customer has just obtained the temporary transaction number from an online authenticated session, the merchant cannot rely on

the normal credit card approval for any more information than what the normal credit card approval provides, which is NOT authentication. *See Aff. Hosseinzadeh,¶5-14; Aff. Hewitt, ¶5-14; Aff. N.Kamrani, ¶6-16; Aff. K.Kamrani, ¶5-14; Aff. Shahbazi, ¶5-14; and Aff. Laing, ¶5-14 and pp. 4-5.* The merchant has no way of knowing the difference between a temporary transaction number being used by a customer and a regular credit card. *Id.* Since the merchant does not receive any more information from the customer or the bank than the merchant normally receives during a credit card authorization, the merchant cannot rely on the mere approval by the bank as authentication. *Id.* Therefore, the Office Action's argument contains flawed logic because it relies on false assumptions, which can only lead to false conclusions.

3. Argument Fails to Show Each Claim Element Arranged as in the Claims

The Examiner's penultimate statement regarding *Franklin et al.* is that this reference teaches an online transaction that is "functionally equivalent" to the claimed invention. Yet, the law on anticipation requires more than this. The *Finisar* case cited in prior responses requires that to anticipate a claim, the prior art reference must teach every claim element ***arranged as in the claims.*** *Finisar v. DirecTV*, 523 F.3d 1323, 1334 (Fed. Cir. 2008). But, the Examiner is admitting that there remains something different between *Franklin et al.* and the claimed invention because he is using the phrase "functionally equivalent." Simply put, there is no teaching of a request for authentication that includes a SecureCode and no teaching of authentication based on a valid SecureCode in *Franklin et al. See Aff.Kamrani, ¶5-16.* Where are these claim elements in *Franklin et al.* ARRANGED AS RECITED IN THE CLAIMS? The only request for authentication in *Franklin et al.* does not include the temporary transaction number. The authorization of the transaction using the temporary transaction number is not an

authentication of the user, hence these claims elements are simply not taught by *Franklin et al.* nor are these claim elements arranged as in the claims at issue. *See Aff. Hosseinzadeh,¶5-14; Aff. Hewitt, ¶5-14; Aff. N.Kamrani, ¶6-16; Aff. K.Kamrani, ¶5-114; Aff. Shahbazi, ¶5-14; and Aff. Laing, ¶5-14 and pp. 4-5.* Thus, for at least these three reasons the Applicants respectfully submit that the claims at issue are neither anticipated by nor rendered obvious by *Franklin et al.* Reconsideration and withdrawal of the rejection of these claims is respectfully requested.

4. Claims 50 and 52 Cannot be Anticipated by Franklin et al.

The Examiner rejected claims 50 and 52 which include the claim element that the SecureCode is alphanumeric. Yet, in a previous Office Action, the Examiner admitted that *Franklin et al.* does not expressly disclose that the SecureCode is alphanumeric and cited a reference by Johnson (U.S. Patent Application Publication No. 2005/0222963 A1) for this missing teaching. *See Office Action mailed September 17, 2010, p.10.* Therefore, this admission precludes these claims being anticipated by *Franklin et al.* Moreover, *Frankin et al.* specifically states that the temporary transaction number "has the same format and number of digits as a regular credit card." *See Franklin et al., col. 2, lines 21-23.* As such, it remains impossible for the temporary transaction number of *Franklin et al.* to include alphanumeric values because it must be processed by traditional credit card processing systems that can only process numeric values. *See Aff. Hosseinzadeh,¶15; Aff. Hewitt, ¶15; Aff. N.Kamrani, ¶17; Aff. K.Kamrani, ¶15; Aff. Shahbazi, ¶15; and Aff. Laing, ¶15.* Therefore, these claims cannot be anticipated by *Franklin et al.* Reconsideration and withdrawal of the rejection of these claims is respectfully requested. These claims have been written in independent form without additional changes to expedite the issuance of a patent.

ALL CLAIMS REMAIN PATENTABLE OVER *FRANKLIN ET AL.* AND CERTAIN OFFICIAL NOTICE

The Office Action rejected claim 44 under 35 U.S.C. § 103(a) as being unpatentable over *Franklin et al.* and further in view of certain Official Notice. The Office Action contends that *Franklin et al.* discloses all of the elements of the claim at issue, except for "wherein said Eternal-Entity and said Central-Entity are the same entity," for which the Office Action provides certain Official Notice. The Office Action takes Official Notice for this teaching missing from *Franklin et al.* Even assuming *arguendo* that the Office Action's citation of Official Notice is proper, because claim 44 directly depends from independent claim 1, which has been shown to be patentable over *Franklin et al.*, claim 44 remains patentable over *Franklin et al.* for at least the same reasons discussed above. The Applicants therefore respectfully request reconsideration and withdrawal of the rejection of this claim.

CONCLUSION

The Applicants respectfully submit that the Final Office Action includes multiple instances of reversible error and earnestly requests reconsideration and solicits issuance of a Notice of Allowance to avoid the delay and costs associated with an appeal to the Board of Patent Appeals & Interferences.

Although not believed necessary, the Office is hereby authorized to charge any fees required under 37 C.F.R. § 1.16 or § 1.17 or credit any overpayments to the deposit account of MICHAEL P FORTKORT PC, Deposit Account No. 50-3776, including but not limited to any fees for additional independent claims.

In the event the prosecution of this Application can be efficiently advanced by a phone discussion, it is requested that the undersigned attorney be called at (703) 435-9390.

Respectfully submitted,

By /Michael P. Fortkort/ Date: March 15, 2011

Michael P. Fortkort (Reg. No. 35,141)

MICHAEL P FORTKORT PC
The International Law Center
13164 Lazy Glen Lane
Oak Hill, Virginia 20171

Please direct telephone calls to:
Michael P. Fortkort
703-435-9390
703-435-8857 (facsimile)

Certification Under 37 C.F.R. § 1.8

I hereby certify that on March 15, 2011 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: March 15, 2011 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 12/210,926

FILING DATE: September 15, 2008

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

ATTORNEY DOCKET: KAMR002US0

CONFIRMATION NO.: 7516

VIA ELECTRONIC FILING SYSTEM
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

RESPONSE TO FINAL OFFICE ACTION

Sir:

In response to the final Office Action mailed January 28, 2011, the Applicants hereby respectfully submit the following amendments and remarks:

Amendments to the Claims begin on page 2.

Remarks begin on page 14.

In the Claims:

Please amend the claims as follows:

1. (Previously Presented) A method for authenticating a user during an electronic transaction between the user and an External-Entity, the method comprising:

receiving electronically a request for a dynamic SecureCode for the user by a Central-Entity during the transaction between the user and the External-Entity;

generating during the transaction a dynamic SecureCode for the user in response to the request;

providing said generated SecureCode to the user during the transaction;

receiving electronically by a Central-Entity a request for authenticating the user based on a digital identity during the transaction, which digital identity includes the SecureCode; and

authenticating by the Central-Entity the user during the transaction if the digital identity is valid.

2. (Original) A method as recited in claim 1, wherein said user has a pre-existing relationship with the External-Entity.

3. (Original) A method as recited in claim 1, wherein said user has no pre-existing relationship with the External-Entity.

4. (Previously Presented) A method as recited in claim 1, further comprising:

combining said generated SecureCode with a user-specific information using a

predetermined algorithm to form a combined Secure-Code and user specific information;

maintaining the combined Secure-Code and user specific information at the Central-Entity;

using the predetermined algorithm to combine received user specific information received by the Central-Entity with a received SecureCode received by the Central-Entity to form a combined received SecureCode and received user specific information;

comparing the combined Secure-Code and user specific information with the combined received SecureCode and received user specific information to validate the user.

5-11. (Cancelled)

12. (Previously Presented) A method as recited in claim 1, wherein said External-Entity receives the user's digital identity.

13. (Previously Presented) A method as recited in claim 1, wherein said External-Entity submits a digital identity to the Central-Entity.

14. (Previously Presented) The method of claim 1, wherein said digital identity includes a user-specific information.

15. (Previously Presented) The method of claim 14, wherein the user specific information comprises one or more of the following: an alphanumeric name, an ID, a login name, and an identification phrase, wherein said identification phrase comprises one or more of the following:

an account number, a telephone number, an IP address, a hardware key, a software key, a session ID, a token and a serial number.

16. (Original) The method of claim 1, wherein the transaction corresponds to a financial transaction.

17. (Original) The method of claim 1, wherein the transaction corresponds to a non-financial transaction.

18. (Previously Presented) The method of claim 1, wherein the transaction corresponds to access to restricted web-site or restricted computer/server.

19. (Previously Presented) The method of claim 1, wherein said transaction occurs over a communication network, wherein said communication network comprises one or more of the following: an Internet, a wireless network, a mobile network, a satellite network, and a private network.

20. (Previously Presented) The method of claim 1, wherein said transaction occurs over a communication network to which is coupled said user, said Central-Entity, and said External-Entity.

21. (Previously Presented) An apparatus for authenticating a user during an electronic transaction with an External-Entity, the apparatus comprising:

a first Central-Entity computer adapted to:

generate a dynamic SecureCode for the user in response to a request during the transaction; and

provide said SecureCode to the user;

a second Central-Entity computer adapted to validate a digital identity, which includes said SecureCode, and authenticate the user if the digital identity is valid.

22. (Previously Presented) The apparatus as recited in claim 21, wherein said user has a pre-existing relationship with the External-Entity.

23. (Previously Presented) The apparatus as recited in claim 21, wherein said user has no pre-existing relationship with the External-Entity.

24. (Previously Presented) The apparatus as recited in claim 21, wherein said External-Entity and said Central-Entity use a SecureCode that is algorithmically combined with said user-specific information.

25-31. (Cancelled)

32. (Previously Presented) The apparatus as recited in claim 21, wherein the user submits a digital identity to the External-Entity.

33. (Previously Presented) The apparatus as recited in claim 21, wherein the External-

Entity submits a digital identity to the Central-Entity.

34. (Previously Presented) The apparatus of claim 21, wherein the digital identity includes a user-specific information.

35. (Previously Presented) The apparatus of claim 34, wherein the user specific information comprises one or more of the following; an alphanumeric name, an ID, a login name, and an identification phrase, wherein said identification phrase comprises one or more of the following: an account number, a telephone number, an IP address, a hardware key, a software key, a session ID, or token, and a serial number.

36. (Previously Presented) The apparatus of claim 21, wherein the transaction corresponds to a financial transaction.

37. (Previously Presented) The apparatus of claim 21, wherein the transaction corresponds to a non-financial transaction.

38. (Previously Presented) The apparatus of claim 21, wherein the transaction corresponds to access to restricted web-site or restricted computer/server.

39. (Previously Presented) The apparatus of claim 21, wherein said transaction occurs over a communication network and wherein said communication network comprises one or more of the following; an Internet, a wireless network, a mobile network, a satellite network, and a

private network.

40. (Previously Presented) The apparatus of claim 21, wherein said transaction occurs over a communication network to which is coupled said user, said Central-Entity, and said External-Entity.

41. (Previously Presented) A method as recited in claim 4, wherein said External-Entity is using said algorithmically combined SecureCode to authenticate a user's identity.

42. (Cancelled)

43. (Previously Presented) A method as recited in claim 4, wherein said Central-Entity is using said algorithmically combined SecureCode to authenticate a user's identity.

44. (Original) A method as recited in claim 1, wherein said External-Entity and said Central-Entity are the same entity.

45. (Previously Presented) The method as recited in claim 1, wherein said SecureCode becomes invalid after being used for authentication.

46. (Previously Presented) The method as recited in claim 1, wherein the SecureCode becomes invalid when a predefined period of time passes.

47. (Original) The method as recited in claim 1, wherein said Central-Entity generates SecureCode with dependence on one or more alphanumeric values.

48. (Previously Presented) The method as recited in claim 47, wherein said one or more alphanumeric values comprise one or more of the following: an unique key, an ID, a login name, a password, and an identification phrase, wherein said identification phrase comprises an account number, a telephone number, an IP address, a Hardware key, a software key a session ID, a token, a seed, and a serial number.

49. (Cancelled)

50. (Currently Amended) A method for authenticating a user during an electronic transaction between the user and an External-Entity, the method comprising:

receiving electronically a request for a dynamic SecureCode for the user by a Central-Entity during the transaction between the user and the External-Entity;

generating during the transaction a dynamic SecureCode for the user in response to the request;

providing said generated SecureCode to the user during the transaction;

receiving electronically by a Central-Entity a request for authenticating the user based on a digital identity during the transaction, which digital identity includes the SecureCode; and

authenticating by the Central-Entity the user during the transaction if the digital identity is valid ~~The method as recited in claim 1~~, wherein said SecureCode is alphanumeric.

51. (Original) The method as recited in claim 1, wherein said user communicates with said Central-Entity over a communication network.

52. (Currently Amended) An apparatus for authenticating a user during an electronic transaction with an External-Entity, the apparatus comprising:

a first Central-Entity computer adapted to:

generate a dynamic SecureCode for the user in response to a request during the transaction; and

provide said SecureCode to the user;

a second Central-Entity computer adapted to validate a digital identity, which includes said SecureCode, and authenticate the user if the digital identity is valid ~~The apparatus as recited in claim 21~~, wherein said SecureCode is alphanumeric.

53. (Original) The method as recited in claim 1, wherein said user communicates with said External-Entity over a communication network.

54. (Previously Presented) The apparatus as recited in claim 21, wherein said user communicates with said Central-Entity over a communication network.

55. (Previously Presented) The apparatus as recited in claim 21, wherein said user communicates with said External-Entity over a communication network.

56-57. (Cancelled)

58. (Previously Presented) The method as recited in claim 1, wherein said SecureCode is generated based on a request submitted by said user over a communication network.

59. (Cancelled)

60. (Previously Presented) The method as recited in claim 58, wherein said request is initiated by said user through a standard interface provided to said user.

61-62. (Cancelled)

63. (Previously Presented) The apparatus according to claim 21, wherein said first Central-Entity computer and said second Central-Entity computer are the same.

64. (Previously Presented) The apparatus according to claim 21, wherein said first Central-Entity computer and said second Central-Entity computer are different.

65. (Previously Presented) A method as recited in claim 1, wherein said digital identity comprises the SecureCode and a user-specific information.

66. (Previously Presented) A method as recited in claim 1, wherein said digital identity comprises the SecureCode.

67. (Previously Presented) A method as recited in claim 1, wherein said digital identity is invalid if the SecureCode is invalid.

68. (Previously Presented) A method as recited in claim 1, wherein said digital identity is valid if at least the SecureCode is valid.

69. (Previously Presented) A method as recited in claim 1, wherein said External-Entity authenticates the user upon receiving an affirmation authentication message from the Central-Entity.

70. (Previously Presented) A method as recited in claim 1, wherein said External-Entity authenticates the user if said Central-Entity authenticates the user based on the SecureCode.

71. (Previously Presented) The apparatus of claim 21, wherein said digital identity is invalid if the SecureCode is invalid.

72. (Previously Presented) The apparatus of claim 21, wherein said digital identity is valid if at least the SecureCode is valid.

73. (Previously Presented) The apparatus of claim 21, wherein said External-Entity authenticates the user upon receiving an affirmation authentication message from the Central-Entity.

74. (Previously Presented) The apparatus of claim 21, wherein said digital identity comprises the SecureCode.

75. (Previously Presented) The apparatus of claim 21, wherein said SecureCode becomes invalid after being used for authentication.

76. (Previously Presented) The apparatus of claim 21, wherein the SecureCode becomes invalid when a predefined period of time passes.

77. (Previously Presented) The apparatus of claim 21, wherein said Central-Entity generates the SecureCode based on one or more alphanumeric values.

78. (Previously Presented) The apparatus of claim 78, wherein said one or more alphanumeric values comprise one or more of the following: an unique key, an ID, a login name, a password, and an identification phrase, wherein said identification phrase comprises an account number, a telephone number, an IP address, a Hardware key, a software key, a session id or token, a seed and a serial number.

79. (Previously Presented) The method of claim 65, wherein the user specific information comprises one or more of the following: an alphanumeric name, an ID, a login name, and an identification phrase, wherein said identification phrase comprises one or more of the following: an account number, a telephone number, an IP address, a hardware key, a software key, a session

id or token and a serial number.

80. (Previously Presented) The apparatus of claim 21, wherein said External-Entity authenticates the user if said Central-Entity authenticates the user based on the SecureCode.

REMARKS

Claims 1-4, 12-24, 32-41, 43-48, 50-55, 58, 60 and 63-80 were previously pending. Claims 5-11, 25-31, 42, 49, 56-57, 59 and 61-62 have been previously cancelled without disclaimer of or prejudice to the subject matter contained therein. Claims 50 and 52 have been rewritten in independent form to include all limitations of their previous base claims. No other amendments have been made. Claims 1-4, 12-24, 32-41, 43-48, 50-55, 58, 60 and 63-80 remain pending.

ALL CLAIMS REMAIN PATENTABLE OVER *FRANKLIN ET AL.*

The Office Action rejected claims 1-4, 12-24, 32-41, 43, 45-48, 51-55, 58, 60 and 63-80 under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,883,810 to *Franklin et al.* [hereinafter "*Franklin et al.*"]. Notably, claim 50 is not mentioned in the summary section, but is included in the remarks; however, the Applicants will address claim 50 as if included with the rejection of all other claims.

Because this rejection arises under 35 U.S.C. § 102(b), the Office Action must contend that *Franklin et al.* discloses all of the elements of the claims at issue. The Applicants respectfully disagree with the Office Action's characterization of these references vis-à-vis the claims at issue and respectfully request reconsideration and withdrawal of the rejection in light of the following remarks. At a minimum, the cited prior art reference fails to include at least the following claim elements: (1) a request for authentication that includes a SecureCode (all claims); (2) authentication based on a valid SecureCode (all claims); and (3) an alphanumeric SecureCode (claims 50 and 52). The Applicants will discuss in detail these features that are missing from the cited reference.

Response to Examiner's Remarks

The Office Action includes at least four major points of legal error and flawed logic in its arguments in support of the 102 rejection. First, the Office Action employs mere conjecture to refute ***evidence*** submitted by the Applicant. In and of itself, this constitutes legal error. Second, the Office Action employs false assumptions in its argument that *Franklin et al.* discloses the functional equivalent of the claimed invention, thereby leading to a false conclusion. Third, the Office Action argument fails to rigorously adhere to Federal Circuit precedent regarding anticipation. Finally, with regard to claims 50 and 52, the Office Action contradicts a position taken in prior office actions regarding the plain teachings of *Franklin et al.* to now reject these claims.

1. Mere Conjecture Cannot Refute Evidence

In response to Applicants' Rule 132 Affidavit stating that authentication of a person is different from a credit card authorization, the Office Action asserts that "authentication and authorization are not two mutually exclusive operations and generally a person needs to be authenticated first in order to be authorized to use or access a resource under certain or no restrictions." This statement remains unsupported and unsubstantiated by any evidence from the record and is directly opposed by the Rule 132 Affidavit previously submitted by the Applicants, and the Exhibits attached thereto, as well as six additional affidavits filed concurrently herewith. *See Aff. Hosseinzadeh,¶5; Aff. Hewitt, ¶5; Aff. N.Kamrani, ¶6; Aff. K.Kamrani, ¶5; Aff. Shahbazi, ¶5; and Aff. Laing, ¶5.* The Applicants respectfully request that the Examiner support this statement by *evidence* rather than personal opinion or belief because the Applicants and four independent experts

respectfully submit that this statement is not accurate. *Id.* Online credit card transactions are approved or authorized daily without any authentication. *See Aff. Hosseinzadeh,¶5; Aff. Hewitt, ¶5; Aff. N.Kamrani, ¶6; Aff. K.Kamrani, ¶5; Aff. Shahbazi, ¶5; and Aff. Laing, ¶5.* Therefore, approval or authorization of a credit card payment occurs without authentication of the user.

Notably, this means that *Franklin et al.* neither expressly nor inherently discloses authentication merely by authorizing the credit card transaction. Inherency can only be established if a feature is necessarily present, even though it is not explicitly disclosed by a reference. *In re Rijckaert*, 9 F.3d 1531, 1534 (Fed. Cir. 1993). Inherency may not be established by probabilities or possibilities. *See,* MPEP § 2112(IV). The mere fact that a certain thing may result from a given set of circumstances is not sufficient. *In re Robertson,* 169 F.3d 743, 745, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999) (emphasis supplied). Stated another way, the doctrine of inherency requires that the missing descriptive matter MUST be present, and if there is another way of performing a missing descriptive function, then the missing descriptive function is NOT inherently disclosed. As the evidence shows that *authorization* can occur without *authentication*, then *authentication* is NOT inherently disclosed merely by *authorization*.

Authentication of a credit card user in an online transaction remains a key problem today and is one problem solved by the present invention. *See Aff. Laing, pp. 4-5. Franklin et al.* does not use a temporary transaction number to authenticate the user but rather a digital certificate installed by the user on his computer from a manual registration process during a separate process between the user and a bank, of which the merchant is not part and is not aware. *See Aff. Hosseinzadeh,¶11; Aff. Hewitt, ¶11; Aff. N.Kamrani, ¶12; Aff. K.Kamrani, ¶11; Aff. Shahbazi, ¶11; and Aff. Laing, ¶11.* As opposed to *Franklin et al.*, the claimed invention avoids authentication employing a digital certificate, which is notoriously cumbersome to obtain and

use. Online transactions pose difficult problems for merchants precisely because the customers are not authenticated during the online transaction. *See Aff. Hosseinzadeh,¶6; Aff. Hewitt, ¶6; Aff. N.Kamrani, ¶7; Aff. K.Kamrani, ¶6; Aff. Shahbazi, ¶6; and Aff. Laing, ¶6 and pp. 4-5.* During a face to face transaction, the merchant can request the customer provide a driver's license or other picture identification along with the physical credit card to authenticate the customer before submitting the credit card for approval. *See, Aff. Laing, pp. 4-5.* In contrast, during an online transaction, the merchant cannot compare a picture of the customer from a government-issued identification to the actual customer. *Id. at p. 4.* Thus, during an online transaction, the credit card payment is authorized without similar authentication first occurring. *See Aff. Hosseinzadeh,¶5-14; Aff. Hewitt, ¶5-14; Aff. N.Kamrani, ¶6-16; Aff. K.Kamrani, ¶5-14; Aff. Shahbazi, ¶5-14; and Aff. Laing, ¶5-14 and pp. 4-5.* It remains irrelevant whether authentication and payment authorization are mutually exclusive operations. They are simply not the same operation. Performing payment authorization is NOT authenticating one and has never been viewed as authentication by those of skill in the art. *See Aff. Hosseinzadeh,¶5-14; Aff. Hewitt, ¶5-14; Aff. N.Kamrani, ¶5-14; Aff. K.Kamrani, ¶6-16; Aff. Shahbazi, ¶5-14; and Aff. Laing, ¶5-14 and pp. 4-5.* To use payment authorization as a proxy for authentication is improper and would be seen as improper by those of skill in the art. *Id.*

The only relevant point is whether the transaction in *Franklin et al.* comprises authentication of the customer based on the temporary transaction number. All the evidence in the record unequivocally supports the Applicants' position that there is no authentication in *Franklin et al.* based on the temporary transaction number. *Id.* It does not matter whether authentication and authorization are mutually exclusive operations, but rather whether these operations are the same or not. The weight of the evidence shows they are not the same.

The Applicants have submitted six Rule 132 Affidavits in support of this argument. *See Aff. Hosseinzadeh; Aff. Hewitt; Aff. N.Kamrani; Aff. K.Kamrani; Aff. Shahbazi; and Aff. Laing.* Thus, the only evidence on the record comprises the Applicants' affidavits buttressed by four affidavits from independent experts in the field, along with previously filed Exhibits from the industry supporting these experts' opinions, whereas there remains no evidence supporting the Office Action's position on this point but rather only mere conjecture. As such, the weight of the evidence falls incontrovertibly on the side of Applicants' position. Failing to weigh the evidence on this point constitutes reversible error.

2. Argument in Office Action Includes False Assumptions

Further in the Examiner's remarks, the Office Action cites a portion from *Franklin et al.* at col. 8, lines 57-58 which states "the bank computer 32 receives the signed request and immediately <u>verifies the identity and authenticity of the customer.</u>" (emphasis supplied by the Examiner) in an attempt to establish that this reference teaches a request for authentication that includes a SecureCode as recited in the claims. However, this request in *Frannklin et al.* does not contain the temporary transaction number, which the Examiner had equated to the recited SecureCode! Rather, this request uses a digital certificate to sign the request for a temporary transaction number. *See Aff. Hosseinzadeh,¶5; Aff. Hewitt, ¶5; Aff. N.Kamrani, ¶5; Aff. K.Kamrani, ¶6; Aff. Shahbazi, ¶5; and Aff. Laing, ¶5.* This request for authentication from *Franklin et al.* CANNOT include the temporary transaction number because it is a request for a temporary transaction number. As the temporary transaction number does not yet exist, this citation cannot form the basis for the claim element of a request for authentication that includes a SecureCode. This authentication request of *Franklin et al.* does not teach the claimed

authentication request that includes a SecureCode and basing the rejection on this teaching constitutes reversible error.

The Office Action continues to cite a series of steps from *Franklin et al.* and states:

> The aforesaid steps are performed for a single transaction and in a short duration. The temporary transaction number is issued to a user after the user is authenticated by the bank. The customer enters the temporary transaction number in the order form of the merchant while filing out the form. The merchant receives the temporary transaction number and all the necessary information related to the customer via the order form. The merchant immediately sends the temporary transaction number to the bank for verification. The confirmation of the short life, single use (temporary) transaction number by the bank is as though the customer is authenticated to the merchant by the bank, because the steps of the entire transaction are carried out in one online session and in a short period. Therefore, Franklin teaches an online transaction between a customer, a merchant and a bank(s) that is functionally equivalent to the same steps of the instant invention recited in the claims.

Office Action mailed January 28, 2011, p.4.

This flawed logic assumes that the merchant knows the credit card number submitted by the customer is a temporary transaction number that was just obtained by the customer during an authenticated session between the customer and the bank. Yet, *Franklin et al.* specifically states that the temporary transaction number looks just like a credit card number and is treated by all as a credit card number. *See Franklin et al., col. 10, lines 39 et seq. and see Aff. Hosseinzadeh,¶12; Aff. Hewitt, ¶12; Aff. N.Kamrani, ¶14; Aff. K.Kamrani, ¶12; Aff. Shahbazi, ¶12; and Aff. Laing, ¶12.* Thus, the merchant cannot determine the difference and relying upon the customer to tell the merchant that the number is a temporary transaction number that was just obtained would defeat the purpose as it would be allowing the customer to self-authenticate himself to the merchant. *See Aff. Hosseinzadeh,¶12-14; Aff. Hewitt, ¶12-14; Aff. N.Kamrani, ¶14-15; Aff. K.Kamrani, ¶12-14; Aff. Shahbazi, ¶12-14; and Aff. Laing, ¶12-14.*

First, the online transaction between the customer and the bank in *Franklin et al.* is separate from the online transaction between the customer and the merchant. *See col. 8, lines 37 et seq.* The user invokes a tool previously installed on his browser to generate an online transaction with the bank to obtain a temporary transaction number during which the user is authenticated to the bank using the previously installed digital certificate. *Id.* The merchant is completely unaware of this transaction between the customer and the bank because the merchant is not part of this transaction, and this transaction occurs separate and apart from the transaction between the customer and the merchant. *Id.* Moreover, once the temporary transaction number is issued by the bank to the customer, the customer must enter this temporary transaction number into the merchant's form where the credit card number is to be entered. *Id.* The merchant remains completely unaware that the credit card number is actually a temporary transaction number just issued. *See Franklin et al., col. 10, lines 39-47* ("Rather, the merchant computer 30 treats the transaction number of the online commerce card no differently than it treats a standard credit card number. In fact, the merchant computer 30 most likely will not be able to distinguish between the two types of numbers."). When the bank replies to the merchant it substitutes the actual account number with the temporary transaction number, hence the merchant never knows the difference between the temporary transaction number and the actual account number. *Franklin et al., col. 11, lines 32-40.*

Yet, the Office Action's argument inherently assumes that the merchant knows that the customer is using a temporary transaction number and thus when the online credit card transaction is approved the customer is therefore authenticated to the merchant. Therein lays the flaw in the Office Action's logic. Without knowing that the customer has just obtained the temporary transaction number from an online authenticated session, the merchant cannot rely on

the normal credit card approval for any more information than what the normal credit card approval provides, which is NOT authentication. *See Aff. Hosseinzadeh,¶5-14; Aff. Hewitt, ¶5-14; Aff. N.Kamrani, ¶6-16; Aff. K.Kamrani, ¶5-14; Aff. Shahbazi, ¶5-14; and Aff. Laing, ¶5-14 and pp. 4-5.* The merchant has no way of knowing the difference between a temporary transaction number being used by a customer and a regular credit card. *Id.* Since the merchant does not receive any more information from the customer or the bank than the merchant normally receives during a credit card authorization, the merchant cannot rely on the mere approval by the bank as authentication. *Id.* Therefore, the Office Action's argument contains flawed logic because it relies on false assumptions, which can only lead to false conclusions.

3. Argument Fails to Show Each Claim Element Arranged as in the Claims

The Examiner's penultimate statement regarding *Franklin et al.* is that this reference teaches an online transaction that is "functionally equivalent" to the claimed invention. Yet, the law on anticipation requires more than this. The *Finisar* case cited in prior responses requires that to anticipate a claim, the prior art reference must teach every claim element ***arranged as in the claims.*** *Finisar v. DirecTV*, 523 F.3d 1323, 1334 (Fed. Cir. 2008). But, the Examiner is admitting that there remains something different between *Franklin et al.* and the claimed invention because he is using the phrase "functionally equivalent." Simply put, there is no teaching of a request for authentication that includes a SecureCode and no teaching of authentication based on a valid SecureCode in *Franklin et al. See Aff.Kamrani, ¶5-16.* Where are these claim elements in *Franklin et al.* ARRANGED AS RECITED IN THE CLAIMS? The only request for authentication in *Franklin et al.* does not include the temporary transaction number. The authorization of the transaction using the temporary transaction number is not an

authentication of the user, hence these claims elements are simply not taught by *Franklin et al.* nor are these claim elements arranged as in the claims at issue. *See Aff. Hosseinzadeh,¶5-14; Aff. Hewitt, ¶5-14; Aff. N.Kamrani, ¶6-16; Aff. K.Kamrani, ¶5-114; Aff. Shahbazi, ¶5-14; and Aff. Laing, ¶5-14 and pp. 4-5.* Thus, for at least these three reasons the Applicants respectfully submit that the claims at issue are neither anticipated by nor rendered obvious by *Franklin et al.* Reconsideration and withdrawal of the rejection of these claims is respectfully requested.

4. Claims 50 and 52 Cannot be Anticipated by Franklin et al.

The Examiner rejected claims 50 and 52 which include the claim element that the SecureCode is alphanumeric. Yet, in a previous Office Action, the Examiner admitted that *Franklin et al.* does not expressly disclose that the SecureCode is alphanumeric and cited a reference by Johnson (U.S. Patent Application Publication No. 2005/0222963 A1) for this missing teaching. *See Office Action mailed September 17, 2010, p.10.* Therefore, this admission precludes these claims being anticipated by *Franklin et al.* Moreover, *Frankin et al.* specifically states that the temporary transaction number "has the same format and number of digits as a regular credit card." *See Franklin et al., col. 2, lines 21-23.* As such, it remains impossible for the temporary transaction number of *Franklin et al.* to include alphanumeric values because it must be processed by traditional credit card processing systems that can only process numeric values. *See Aff. Hosseinzadeh,¶15; Aff. Hewitt, ¶15; Aff. N.Kamrani, ¶17; Aff. K.Kamrani, ¶15; Aff. Shahbazi, ¶15; and Aff. Laing, ¶15.* Therefore, these claims cannot be anticipated by *Franklin et al.* Reconsideration and withdrawal of the rejection of these claims is respectfully requested. These claims have been written in independent form without additional changes to expedite the issuance of a patent.

ALL CLAIMS REMAIN PATENTABLE OVER *FRANKLIN ET AL.* AND CERTAIN OFFICIAL NOTICE

The Office Action rejected claim 44 under 35 U.S.C. § 103(a) as being unpatentable over *Franklin et al.* and further in view of certain Official Notice. The Office Action contends that *Franklin et al.* discloses all of the elements of the claim at issue, except for "wherein said Eternal-Entity and said Central-Entity are the same entity," for which the Office Action provides certain Official Notice. The Office Action takes Official Notice for this teaching missing from *Franklin et al.* Even assuming *arguendo* that the Office Action's citation of Official Notice is proper, because claim 44 directly depends from independent claim 1, which has been shown to be patentable over *Franklin et al.*, claim 44 remains patentable over *Franklin et al.* for at least the same reasons discussed above. The Applicants therefore respectfully request reconsideration and withdrawal of the rejection of this claim.

CONCLUSION

The Applicants respectfully submit that the Final Office Action includes multiple instances of reversible error and earnestly requests reconsideration and solicits issuance of a Notice of Allowance to avoid the delay and costs associated with an appeal to the Board of Patent Appeals & Interferences.

Although not believed necessary, the Office is hereby authorized to charge any fees required under 37 C.F.R. § 1.16 or § 1.17 or credit any overpayments to the deposit account of MICHAEL P FORTKORT PC, Deposit Account No. 50-3776, including but not limited to any fees for additional independent claims.

In the event the prosecution of this Application can be efficiently advanced by a phone discussion, it is requested that the undersigned attorney be called at (703) 435-9390.

Respectfully submitted,

By /Michael P. Fortkort/ Date: March 15, 2011
Michael P. Fortkort (Reg. No. 35,141)

MICHAEL P FORTKORT PC
The International Law Center
13164 Lazy Glen Lane
Oak Hill, Virginia 20171

Please direct telephone calls to:
Michael P. Fortkort
703-435-9390
703-435-8857 (facsimile)

In the Claims:

Please amend the claims as follows:

1. (Previously Presented) A method for authenticating a user during an electronic transaction between the user and an External-Entity, the method comprising:

receiving electronically a request for a dynamic SecureCode for the user by a Central-Entity during the transaction between the user and the External-Entity;

generating during the transaction a dynamic SecureCode for the user in response to the request;

providing said generated SecureCode to the user during the transaction;

receiving electronically by a Central-Entity a request for authenticating the user based on a digital identity during the transaction, which digital identity includes the SecureCode; and

authenticating by the Central-Entity the user during the transaction if the digital identity is valid.

2. (Original) A method as recited in claim 1, wherein said user has a pre-existing relationship with the External-Entity.

3. (Original) A method as recited in claim 1, wherein said user has no pre-existing relationship with the External-Entity.

4. (Previously Presented) A method as recited in claim 1, further comprising:

combining said generated SecureCode with a user-specific information using a

predetermined algorithm to form a combined Secure-Code and user specific information;

maintaining the combined Secure-Code and user specific information at the Central-Entity;

using the predetermined algorithm to combine received user specific information received by the Central-Entity with a received SecureCode received by the Central-Entity to form a combined received SecureCode and received user specific information;

comparing the combined Secure-Code and user specific information with the combined received SecureCode and received user specific information to validate the user.

5-11. (Cancelled)

12. (Previously Presented) A method as recited in claim 1, wherein said External-Entity receives the user's digital identity.

13. (Previously Presented) A method as recited in claim 1, wherein said External-Entity submits a digital identity to the Central-Entity.

14. (Previously Presented) The method of claim 1, wherein said digital identity includes a user-specific information.

15. (Previously Presented) The method of claim 14, wherein the user specific information comprises one or more of the following: an alphanumeric name, an ID, a login name, and an identification phrase, wherein said identification phrase comprises one or more of the following:

an account number, a telephone number, an IP address, a hardware key, a software key, a session ID, a token and a serial number.

16. (Original) The method of claim 1, wherein the transaction corresponds to a financial transaction.

17. (Original) The method of claim 1, wherein the transaction corresponds to a non-financial transaction.

18. (Previously Presented) The method of claim 1, wherein the transaction corresponds to access to restricted web-site or restricted computer/server.

19. (Previously Presented) The method of claim 1, wherein said transaction occurs over a communication network, wherein said communication network comprises one or more of the following: an Internet, a wireless network, a mobile network, a satellite network, and a private network.

20. (Previously Presented) The method of claim 1, wherein said transaction occurs over a communication network to which is coupled said user, said Central-Entity, and said External-Entity.

21. (Previously Presented) An apparatus for authenticating a user during an electronic transaction with an External-Entity, the apparatus comprising:

a first Central-Entity computer adapted to:

generate a dynamic SecureCode for the user in response to a request during the transaction; and

provide said SecureCode to the user;

a second Central-Entity computer adapted to validate a digital identity, which includes said SecureCode, and authenticate the user if the digital identity is valid.

22. (Previously Presented) The apparatus as recited in claim 21, wherein said user has a pre-existing relationship with the External-Entity.

23. (Previously Presented) The apparatus as recited in claim 21, wherein said user has no pre-existing relationship with the External-Entity.

24. (Previously Presented) The apparatus as recited in claim 21, wherein said External-Entity and said Central-Entity use a SecureCode that is algorithmically combined with said user-specific information.

25-31. (Cancelled)

32. (Previously Presented) The apparatus as recited in claim 21, wherein the user submits a digital identity to the External-Entity.

33. (Previously Presented) The apparatus as recited in claim 21, wherein the External-

Entity submits a digital identity to the Central-Entity.

34. (Previously Presented) The apparatus of claim 21, wherein the digital identity includes a user-specific information.

35. (Previously Presented) The apparatus of claim 34, wherein the user specific information comprises one or more of the following; an alphanumeric name, an ID, a login name, and an identification phrase, wherein said identification phrase comprises one or more of the following: an account number, a telephone number, an IP address, a hardware key, a software key, a session ID, or token, and a serial number.

36. (Previously Presented) The apparatus of claim 21, wherein the transaction corresponds to a financial transaction.

37. (Previously Presented) The apparatus of claim 21, wherein the transaction corresponds to a non-financial transaction.

38. (Previously Presented) The apparatus of claim 21, wherein the transaction corresponds to access to restricted web-site or restricted computer/server.

39. (Previously Presented) The apparatus of claim 21, wherein said transaction occurs over a communication network and wherein said communication network comprises one or more of the following; an Internet, a wireless network, a mobile network, a satellite network, and a

private network.

40. (Previously Presented) The apparatus of claim 21, wherein said transaction occurs over a communication network to which is coupled said user, said Central-Entity, and said External-Entity.

41. (Previously Presented) A method as recited in claim 4, wherein said External-Entity is using said algorithmically combined SecureCode to authenticate a user's identity.

42. (Cancelled)

43. (Previously Presented) A method as recited in claim 4, wherein said Central-Entity is using said algorithmically combined SecureCode to authenticate a user's identity.

44. (Original) A method as recited in claim 1, wherein said External-Entity and said Central-Entity are the same entity.

45. (Previously Presented) The method as recited in claim 1, wherein said SecureCode becomes invalid after being used for authentication.

46. (Previously Presented) The method as recited in claim 1, wherein the SecureCode becomes invalid when a predefined period of time passes.

47. (Original) The method as recited in claim 1, wherein said Central-Entity generates SecureCode with dependence on one or more alphanumeric values.

48. (Previously Presented) The method as recited in claim 47, wherein said one or more alphanumeric values comprise one or more of the following: an unique key, an ID, a login name, a password, and an identification phrase, wherein said identification phrase comprises an account number, a telephone number, an IP address, a Hardware key, a software key a session ID, a token, a seed, and a serial number.

49. (Cancelled)

50. (Currently Amended) A method for authenticating a user during an electronic transaction between the user and an External-Entity, the method comprising:

receiving electronically a request for a dynamic SecureCode for the user by a Central-Entity during the transaction between the user and the External-Entity;

generating during the transaction a dynamic SecureCode for the user in response to the request;

providing said generated SecureCode to the user during the transaction;

receiving electronically by a Central-Entity a request for authenticating the user based on a digital identity during the transaction, which digital identity includes the SecureCode; and

authenticating by the Central-Entity the user during the transaction if the digital identity is valid ~~The method as recited in claim 1~~, wherein said SecureCode is alphanumeric.

51. (Original) The method as recited in claim 1, wherein said user communicates with said Central-Entity over a communication network.

52. (Currently Amended) An apparatus for authenticating a user during an electronic transaction with an External-Entity, the apparatus comprising:

a first Central-Entity computer adapted to:

generate a dynamic SecureCode for the user in response to a request during the transaction; and

provide said SecureCode to the user;

a second Central-Entity computer adapted to validate a digital identity, which includes said SecureCode, and authenticate the user if the digital identity is valid ~~The apparatus as recited in claim 21~~, wherein said SecureCode is alphanumeric.

53. (Original) The method as recited in claim 1, wherein said user communicates with said External-Entity over a communication network.

54. (Previously Presented) The apparatus as recited in claim 21, wherein said user communicates with said Central-Entity over a communication network.

55. (Previously Presented) The apparatus as recited in claim 21, wherein said user communicates with said External-Entity over a communication network.

56-57. (Cancelled)

58. (Previously Presented) The method as recited in claim 1, wherein said SecureCode is generated based on a request submitted by said user over a communication network.

59. (Cancelled)

60. (Previously Presented) The method as recited in claim 58, wherein said request is initiated by said user through a standard interface provided to said user.

61-62. (Cancelled)

63. (Previously Presented) The apparatus according to claim 21, wherein said first Central-Entity computer and said second Central-Entity computer are the same.

64. (Previously Presented) The apparatus according to claim 21, wherein said first Central-Entity computer and said second Central-Entity computer are different.

65. (Previously Presented) A method as recited in claim 1, wherein said digital identity comprises the SecureCode and a user-specific information.

66. (Previously Presented) A method as recited in claim 1, wherein said digital identity comprises the SecureCode.

67. (Previously Presented) A method as recited in claim 1, wherein said digital identity is invalid if the SecureCode is invalid.

68. (Previously Presented) A method as recited in claim 1, wherein said digital identity is valid if at least the SecureCode is valid.

69. (Previously Presented) A method as recited in claim 1, wherein said External-Entity authenticates the user upon receiving an affirmation authentication message from the Central-Entity.

70. (Previously Presented) A method as recited in claim 1, wherein said External-Entity authenticates the user if said Central-Entity authenticates the user based on the SecureCode.

71. (Previously Presented) The apparatus of claim 21, wherein said digital identity is invalid if the SecureCode is invalid.

72. (Previously Presented) The apparatus of claim 21, wherein said digital identity is valid if at least the SecureCode is valid.

73. (Previously Presented) The apparatus of claim 21, wherein said External-Entity authenticates the user upon receiving an affirmation authentication message from the Central-Entity.

74. (Previously Presented) The apparatus of claim 21, wherein said digital identity comprises the SecureCode.

75. (Previously Presented) The apparatus of claim 21, wherein said SecureCode becomes invalid after being used for authentication.

76. (Previously Presented) The apparatus of claim 21, wherein the SecureCode becomes invalid when a predefined period of time passes.

77. (Previously Presented) The apparatus of claim 21, wherein said Central-Entity generates the SecureCode based on one or more alphanumeric values.

78. (Previously Presented) The apparatus of claim 78, wherein said one or more alphanumeric values comprise one or more of the following: an unique key, an ID, a login name, a password, and an identification phrase, wherein said identification phrase comprises an account number, a telephone number, an IP address, a Hardware key, a software key, a session id or token, a seed and a serial number.

79. (Previously Presented) The method of claim 65, wherein the user specific information comprises one or more of the following: an alphanumeric name, an ID, a login name, and an identification phrase, wherein said identification phrase comprises one or more of the following: an account number, a telephone number, an IP address, a hardware key, a software key, a session

id or token and a serial number.

80. (Previously Presented) The apparatus of claim 21, wherein said External-Entity authenticates the user if said Central-Entity authenticates the user based on the SecureCode.

REMARKS

Claims 1-4, 12-24, 32-41, 43-48, 50-55, 58, 60 and 63-80 were previously pending. Claims 5-11, 25-31, 42, 49, 56-57, 59 and 61-62 have been previously cancelled without disclaimer of or prejudice to the subject matter contained therein. Claims 50 and 52 have been rewritten in independent form to include all limitations of their previous base claims. No other amendments have been made. Claims 1-4, 12-24, 32-41, 43-48, 50-55, 58, 60 and 63-80 remain pending.

ALL CLAIMS REMAIN PATENTABLE OVER *FRANKLIN ET AL.*

The Office Action rejected claims 1-4, 12-24, 32-41, 43, 45-48, 51-55, 58, 60 and 63-80 under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,883,810 to *Franklin et al.* [hereinafter "*Franklin et al.*"]. Notably, claim 50 is not mentioned in the summary section, but is included in the remarks; however, the Applicants will address claim 50 as if included with the rejection of all other claims.

Because this rejection arises under 35 U.S.C. § 102(b), the Office Action must contend that *Franklin et al.* discloses all of the elements of the claims at issue. The Applicants respectfully disagree with the Office Action's characterization of these references vis-à-vis the claims at issue and respectfully request reconsideration and withdrawal of the rejection in light of the following remarks. At a minimum, the cited prior art reference fails to include at least the following claim elements: (1) a request for authentication that includes a SecureCode (all claims); (2) authentication based on a valid SecureCode (all claims); and (3) an alphanumeric SecureCode (claims 50 and 52). The Applicants will discuss in detail these features that are missing from the cited reference.

Response to Examiner's Remarks

The Office Action includes at least four major points of legal error and flawed logic in its arguments in support of the 102 rejection. First, the Office Action employs mere conjecture to refute ***evidence*** submitted by the Applicant. In and of itself, this constitutes legal error. Second, the Office Action employs false assumptions in its argument that *Franklin et al.* discloses the functional equivalent of the claimed invention, thereby leading to a false conclusion. Third, the Office Action argument fails to rigorously adhere to Federal Circuit precedent regarding anticipation. Finally, with regard to claims 50 and 52, the Office Action contradicts a position taken in prior office actions regarding the plain teachings of *Franklin et al.* to now reject these claims.

1. Mere Conjecture Cannot Refute Evidence

In response to Applicants' Rule 132 Affidavit stating that authentication of a person is different from a credit card authorization, the Office Action asserts that "authentication and authorization are not two mutually exclusive operations and generally a person needs to be authenticated first in order to be authorized to use or access a resource under certain or no restrictions." This statement remains unsupported and unsubstantiated by any evidence from the record and is directly opposed by the Rule 132 Affidavit previously submitted by the Applicants, and the Exhibits attached thereto, as well as six additional affidavits filed concurrently herewith. *See Aff. Hosseinzadeh,¶5; Aff. Hewitt, ¶5; Aff. N.Kamrani, ¶6; Aff. K.Kamrani, ¶5; Aff. Shahbazi, ¶5; and Aff. Laing, ¶5.* The Applicants respectfully request that the Examiner support this statement by *evidence* rather than personal opinion or belief because the Applicants and four independent experts

respectfully submit that this statement is not accurate. *Id.* Online credit card transactions are approved or authorized daily without any authentication. *See Aff. Hosseinzadeh,¶5; Aff. Hewitt, ¶5; Aff. N.Kamrani, ¶6; Aff. K.Kamrani, ¶5; Aff. Shahbazi, ¶5; and Aff. Laing, ¶5.* Therefore, approval or authorization of a credit card payment occurs without authentication of the user.

Notably, this means that *Franklin et al.* neither expressly nor inherently discloses authentication merely by authorizing the credit card transaction. Inherency can only be established if a feature is necessarily present, even though it is not explicitly disclosed by a reference. *In re Rijckaert*, 9 F.3d 1531, 1534 (Fed. Cir. 1993). Inherency may not be established by probabilities or possibilities. *See,* MPEP § 2112(IV). The mere fact that a certain thing may result from a given set of circumstances is not sufficient. *In re Robertson,* 169 F.3d 743, 745, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999) (emphasis supplied). Stated another way, the doctrine of inherency requires that the missing descriptive matter MUST be present, and if there is another way of performing a missing descriptive function, then the missing descriptive function is NOT inherently disclosed. As the evidence shows that *authorization* can occur without *authentication*, then *authentication* is NOT inherently disclosed merely by *authorization*.

Authentication of a credit card user in an online transaction remains a key problem today and is one problem solved by the present invention. *See Aff. Laing, pp. 4-5. Franklin et al.* does not use a temporary transaction number to authenticate the user but rather a digital certificate installed by the user on his computer from a manual registration process during a separate process between the user and a bank, of which the merchant is not part and is not aware. *See Aff. Hosseinzadeh,¶11; Aff. Hewitt, ¶11; Aff. N.Kamrani, ¶12; Aff. K.Kamrani, ¶11; Aff. Shahbazi, ¶11; and Aff. Laing, ¶11.* As opposed to *Franklin et al.*, the claimed invention avoids authentication employing a digital certificate, which is notoriously cumbersome to obtain and

use. Online transactions pose difficult problems for merchants precisely because the customers are not authenticated during the online transaction. *See Aff. Hosseinzadeh,¶6; Aff. Hewitt, ¶6; Aff. N.Kamrani, ¶7; Aff. K.Kamrani, ¶6; Aff. Shahbazi, ¶6; and Aff. Laing, ¶6 and pp. 4-5.* During a face to face transaction, the merchant can request the customer provide a driver's license or other picture identification along with the physical credit card to authenticate the customer before submitting the credit card for approval. *See, Aff. Laing, pp. 4-5.* In contrast, during an online transaction, the merchant cannot compare a picture of the customer from a government-issued identification to the actual customer. *Id. at p. 4.* Thus, during an online transaction, the credit card payment is authorized without similar authentication first occurring. *See Aff. Hosseinzadeh,¶5-14; Aff. Hewitt, ¶5-14; Aff. N.Kamrani, ¶6-16; Aff. K.Kamrani, ¶5-14; Aff. Shahbazi, ¶5-14; and Aff. Laing, ¶5-14 and pp. 4-5.* It remains irrelevant whether authentication and payment authorization are mutually exclusive operations. They are simply not the same operation. Performing payment authorization is NOT authenticating one and has never been viewed as authentication by those of skill in the art. *See Aff. Hosseinzadeh,¶5-14; Aff. Hewitt, ¶5-14; Aff. N.Kamrani, ¶5-14; Aff. K.Kamrani, ¶6-16; Aff. Shahbazi, ¶5-14; and Aff. Laing, ¶5-14 and pp. 4-5.* To use payment authorization as a proxy for authentication is improper and would be seen as improper by those of skill in the art. *Id.*

The only relevant point is whether the transaction in *Franklin et al.* comprises authentication of the customer based on the temporary transaction number. All the evidence in the record unequivocally supports the Applicants' position that there is no authentication in *Franklin et al.* based on the temporary transaction number. *Id.* It does not matter whether authentication and authorization are mutually exclusive operations, but rather whether these operations are the same or not. The weight of the evidence shows they are not the same.

The Applicants have submitted six Rule 132 Affidavits in support of this argument. *See Aff. Hosseinzadeh; Aff. Hewitt; Aff. N.Kamrani; Aff. K.Kamrani; Aff. Shahbazi; and Aff. Laing.* Thus, the only evidence on the record comprises the Applicants' affidavits buttressed by four affidavits from independent experts in the field, along with previously filed Exhibits from the industry supporting these experts' opinions, whereas there remains no evidence supporting the Office Action's position on this point but rather only mere conjecture. As such, the weight of the evidence falls incontrovertibly on the side of Applicants' position. Failing to weigh the evidence on this point constitutes reversible error.

2. Argument in Office Action Includes False Assumptions

Further in the Examiner's remarks, the Office Action cites a portion from *Franklin et al.* at col. 8, lines 57-58 which states "the bank computer 32 receives the signed request and immediately <u>verifies the identity and authenticity of the customer.</u>" (emphasis supplied by the Examiner) in an attempt to establish that this reference teaches a request for authentication that includes a SecureCode as recited in the claims. However, this request in *Frannklin et al.* does not contain the temporary transaction number, which the Examiner had equated to the recited SecureCode! Rather, this request uses a digital certificate to sign the request for a temporary transaction number. *See Aff. Hosseinzadeh,¶5; Aff. Hewitt, ¶5; Aff. N.Kamrani, ¶5; Aff. K.Kamrani, ¶6; Aff. Shahbazi, ¶5; and Aff. Laing, ¶5.* This request for authentication from *Franklin et al.* CANNOT include the temporary transaction number because it is a request for a temporary transaction number. As the temporary transaction number does not yet exist, this citation cannot form the basis for the claim element of a request for authentication that includes a SecureCode. This authentication request of *Franklin et al.* does not teach the claimed

authentication request that includes a SecureCode and basing the rejection on this teaching constitutes reversible error.

The Office Action continues to cite a series of steps from *Franklin et al.* and states:

> The aforesaid steps are performed for a single transaction and in a short duration. The temporary transaction number is issued to a user after the user is authenticated by the bank. The customer enters the temporary transaction number in the order form of the merchant while filing out the form. The merchant receives the temporary transaction number and all the necessary information related to the customer via the order form. The merchant immediately sends the temporary transaction number to the bank for verification. The confirmation of the short life, single use (temporary) transaction number by the bank is as though the customer is authenticated to the merchant by the bank, because the steps of the entire transaction are carried out in one online session and in a short period. Therefore, Franklin teaches an online transaction between a customer, a merchant and a bank(s) that is functionally equivalent to the same steps of the instant invention recited in the claims.

Office Action mailed January 28, 2011, p.4.

This flawed logic assumes that the merchant knows the credit card number submitted by the customer is a temporary transaction number that was just obtained by the customer during an authenticated session between the customer and the bank. Yet, *Franklin et al.* specifically states that the temporary transaction number looks just like a credit card number and is treated by all as a credit card number. *See Franklin et al., col. 10, lines 39 et seq. and see Aff. Hosseinzadeh,¶12; Aff. Hewitt, ¶12; Aff. N.Kamrani, ¶14; Aff. K.Kamrani, ¶12; Aff. Shahbazi, ¶12; and Aff. Laing, ¶12.* Thus, the merchant cannot determine the difference and relying upon the customer to tell the merchant that the number is a temporary transaction number that was just obtained would defeat the purpose as it would be allowing the customer to self-authenticate himself to the merchant. *See Aff. Hosseinzadeh,¶12-14; Aff. Hewitt, ¶12-14; Aff. N.Kamrani, ¶14-15; Aff. K.Kamrani, ¶12-14; Aff. Shahbazi, ¶12-14; and Aff. Laing, ¶12-14.*

First, the online transaction between the customer and the bank in *Franklin et al.* is separate from the online transaction between the customer and the merchant. *See col. 8, lines 37 et seq.* The user invokes a tool previously installed on his browser to generate an online transaction with the bank to obtain a temporary transaction number during which the user is authenticated to the bank using the previously installed digital certificate. *Id.* The merchant is completely unaware of this transaction between the customer and the bank because the merchant is not part of this transaction, and this transaction occurs separate and apart from the transaction between the customer and the merchant. *Id.* Moreover, once the temporary transaction number is issued by the bank to the customer, the customer must enter this temporary transaction number into the merchant's form where the credit card number is to be entered. *Id.* The merchant remains completely unaware that the credit card number is actually a temporary transaction number just issued. *See Franklin et al., col. 10, lines 39-47* ("Rather, the merchant computer 30 treats the transaction number of the online commerce card no differently than it treats a standard credit card number. In fact, the merchant computer 30 most likely will not be able to distinguish between the two types of numbers."). When the bank replies to the merchant it substitutes the actual account number with the temporary transaction number, hence the merchant never knows the difference between the temporary transaction number and the actual account number. *Franklin et al., col. 11, lines 32-40.*

Yet, the Office Action's argument inherently assumes that the merchant knows that the customer is using a temporary transaction number and thus when the online credit card transaction is approved the customer is therefore authenticated to the merchant. Therein lays the flaw in the Office Action's logic. Without knowing that the customer has just obtained the temporary transaction number from an online authenticated session, the merchant cannot rely on

the normal credit card approval for any more information than what the normal credit card approval provides, which is NOT authentication. *See Aff. Hosseinzadeh,¶5-14; Aff. Hewitt, ¶5-14; Aff. N.Kamrani, ¶6-16; Aff. K.Kamrani, ¶5-14; Aff. Shahbazi, ¶5-14; and Aff. Laing, ¶5-14 and pp. 4-5.* The merchant has no way of knowing the difference between a temporary transaction number being used by a customer and a regular credit card. *Id.* Since the merchant does not receive any more information from the customer or the bank than the merchant normally receives during a credit card authorization, the merchant cannot rely on the mere approval by the bank as authentication. *Id.* Therefore, the Office Action's argument contains flawed logic because it relies on false assumptions, which can only lead to false conclusions.

3. Argument Fails to Show Each Claim Element Arranged as in the Claims

The Examiner's penultimate statement regarding *Franklin et al.* is that this reference teaches an online transaction that is "functionally equivalent" to the claimed invention. Yet, the law on anticipation requires more than this. The *Finisar* case cited in prior responses requires that to anticipate a claim, the prior art reference must teach every claim element ***arranged as in the claims.*** *Finisar v. DirecTV*, 523 F.3d 1323, 1334 (Fed. Cir. 2008). But, the Examiner is admitting that there remains something different between *Franklin et al.* and the claimed invention because he is using the phrase "functionally equivalent." Simply put, there is no teaching of a request for authentication that includes a SecureCode and no teaching of authentication based on a valid SecureCode in *Franklin et al. See Aff.Kamrani, ¶5-16.* Where are these claim elements in *Franklin et al.* ARRANGED AS RECITED IN THE CLAIMS? The only request for authentication in *Franklin et al.* does not include the temporary transaction number. The authorization of the transaction using the temporary transaction number is not an

authentication of the user, hence these claims elements are simply not taught by *Franklin et al.* nor are these claim elements arranged as in the claims at issue. *See Aff. Hosseinzadeh,¶5-14; Aff. Hewitt, ¶5-14; Aff. N.Kamrani, ¶6-16; Aff. K.Kamrani, ¶5-114; Aff. Shahbazi, ¶5-14; and Aff. Laing, ¶5-14 and pp. 4-5.* Thus, for at least these three reasons the Applicants respectfully submit that the claims at issue are neither anticipated by nor rendered obvious by *Franklin et al.* Reconsideration and withdrawal of the rejection of these claims is respectfully requested.

4. Claims 50 and 52 Cannot be Anticipated by Franklin et al.

The Examiner rejected claims 50 and 52 which include the claim element that the SecureCode is alphanumeric. Yet, in a previous Office Action, the Examiner admitted that *Franklin et al.* does not expressly disclose that the SecureCode is alphanumeric and cited a reference by Johnson (U.S. Patent Application Publication No. 2005/0222963 A1) for this missing teaching. *See Office Action mailed September 17, 2010, p.10.* Therefore, this admission precludes these claims being anticipated by *Franklin et al.* Moreover, *Frankin et al.* specifically states that the temporary transaction number "has the same format and number of digits as a regular credit card." *See Franklin et al., col. 2, lines 21-23.* As such, it remains impossible for the temporary transaction number of *Franklin et al.* to include alphanumeric values because it must be processed by traditional credit card processing systems that can only process numeric values. *See Aff. Hosseinzadeh,¶15; Aff. Hewitt, ¶15; Aff. N.Kamrani, ¶17; Aff. K.Kamrani, ¶15; Aff. Shahbazi, ¶15; and Aff. Laing, ¶15.* Therefore, these claims cannot be anticipated by *Franklin et al.* Reconsideration and withdrawal of the rejection of these claims is respectfully requested. These claims have been written in independent form without additional changes to expedite the issuance of a patent.

ALL CLAIMS REMAIN PATENTABLE OVER *FRANKLIN ET AL.* AND CERTAIN OFFICIAL NOTICE

The Office Action rejected claim 44 under 35 U.S.C. § 103(a) as being unpatentable over *Franklin et al.* and further in view of certain Official Notice. The Office Action contends that *Franklin et al.* discloses all of the elements of the claim at issue, except for "wherein said Eternal-Entity and said Central-Entity are the same entity," for which the Office Action provides certain Official Notice. The Office Action takes Official Notice for this teaching missing from *Franklin et al.* Even assuming *arguendo* that the Office Action's citation of Official Notice is proper, because claim 44 directly depends from independent claim 1, which has been shown to be patentable over *Franklin et al.*, claim 44 remains patentable over *Franklin et al.* for at least the same reasons discussed above. The Applicants therefore respectfully request reconsideration and withdrawal of the rejection of this claim.

CONCLUSION

The Applicants respectfully submit that the Final Office Action includes multiple instances of reversible error and earnestly requests reconsideration and solicits issuance of a Notice of Allowance to avoid the delay and costs associated with an appeal to the Board of Patent Appeals & Interferences.

Although not believed necessary, the Office is hereby authorized to charge any fees required under 37 C.F.R. § 1.16 or § 1.17 or credit any overpayments to the deposit account of MICHAEL P FORTKORT PC, Deposit Account No. 50-3776, including but not limited to any fees for additional independent claims.

In the event the prosecution of this Application can be efficiently advanced by a phone discussion, it is requested that the undersigned attorney be called at (703) 435-9390.

Respectfully submitted,

By /Michael P. Fortkort/ Date: March 15, 2011
Michael P. Fortkort (Reg. No. 35,141)

MICHAEL P FORTKORT PC
The International Law Center
13164 Lazy Glen Lane
Oak Hill, Virginia 20171

Please direct telephone calls to:
Michael P. Fortkort
703-435-9390
703-435-8857 (facsimile)

Certification Under 37 C.F.R. § 1.8

I hereby certify that on March 15, 2011 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: March 15, 2011 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 12/210,926

FILING DATE: September 15, 2008

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

ATTORNEY DOCKET: KAMR002US0

CONFIRMATION NO.: 7516

VIA ELECTRONIC FILING SYSTEM
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

AFFIDAVIT UNDER RULE 132

Applicants hereby submit this affidavit in support of their response to the Office Action mailed January 28, 2011 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 12/210,926, and pursuant to the provisions of 37 C.F.R. § 1.132. The witness hereby avers and testifies as follows:

1. I am Kamran A. Kamrani, 6547 Palisades Drive, Centreville VA 20121.

2. Bachelor of Computer Science – Specialization: Data Management & Database Design, Technical University of The Hague, The Hague, Netherlands

3. Director, CGI Federal. Senior-level business and IT professional with over 18 years of experience in architecting and leading complex enterprise-wide solutions for Fortune 1000 companies and the federal government; An expert in authorization and authentication, fraud and identity theft prevention; Devoted his time to studying, and devising solutions for these multifaceted problems; Excellent analytical skills and knowledge of patent laws in the Computer Architecture Software and Information Security area, the patent search, investigation and examination process.

4. I have reviewed U.S. Patent No. 5,883,810 (*Franklin et al.*).

5. With regard to the following statement, "authentication and authorization are not two mutually exclusive operations and generally a person needs to be authenticated first in order to be authorized to use or access a resource under certain or no restrictions," one of skill in the art of user authentication and credit card transactions would understand that this statement is inaccurate. Online credit card transactions occur daily during which credit card payments are authorized without first authenticating the user. These transactions are similar to the online transactions as described in *Franklin et al.*

6. One of skill in the field of credit card transactions would understand that "card not present" transactions occurring online involve payments that are not guaranteed to the merchant. No guarantee is provided primarily because the payers are not authenticated in online transactions, thereby allowing many risks to accompany the "card not present" transactions. Such

risks involve issues such as chargeback of payment transactions to online merchants and fraud for both merchants and cardholders.

7. One of skill in the authentication art would understand that authentication of a user involves determining whether a user is, in fact, who he or she claims to be.

8. In contrast, one of skill in the art of authentication would understand the difference between user authentication during online transactions and credit card authorization that occurs during a credit card payment transaction, which involves receiving a user's credit card information for payment and sending the customer's credit card and order information to the customer's issuing bank for payment approval before deciding whether or not to fulfill a user's order.

9. One of skill in the art of authentication would understand that the temporary transaction number of *Franklin et al.* is not used for authentication of the user but rather for authorization of payment. The authorization transaction of *Franklin et al.* does not include an authentication.

10. One of skill in the art of authentication and credit card authorization would understand that the electronic online commerce card of Franklin has not been developed for verification of user's identity since the merchants treat the transaction number the same manner they process credit card transactions.

11. *Franklin et al.* does not disclose a request for authentication of an online customer that includes the temporary transaction number. *Franklin et al.* uses a digital certificate during an online session between a bank and the customer to obtain a temporary transaction number. But, the temporary transaction number is not used for authentication of the customer.

12. The merchant in *Franklin et al.* cannot rely upon mere authorization of a credit card payment as authentication of the customer. In *Franklin et al.* the merchant cannot distinguish between a recently obtained temporary transaction number and a normal credit card number.

14. Franklin does not provide any assurance to the merchant that the payer is authenticated. No assurance is provided because the merchant never receives any message from issuing bank that the user is authentic.

15. The temporary transaction number of *Franklin et al.* is not alphanumeric in format because it must have the same format and digits as a regular credit card number, which is not alphanumeric. Moreover, one of skill in the art would not change the temporary transaction number of *Franklin et al.* to an alphanumeric value because the system of *Franklin et al.* would no longer function as the temporary transaction number is designed to be processed by existing credit card processing systems that expect all numerical values in the format of a credit card number.

I affirm that all statements made herein of my own knowledge are true, and that all statements made herein on information and belief are believed to be true. I understand that willful false statements and the like are punishable by fine or imprisonment, or both (18 U.S.C. 1001), and may jeopardize the validity of the present patent application or any patent issuing thereon.

FURTHER AFFIANT SAYETH NOT.

It witness whereof,

Kamran

3/11/2011
Date

Certification Under 37 C.F.R. § 1.8

I hereby certify that on March 15, 2011 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: March 15, 2011 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 12/210,926

FILING DATE: September 15, 2008

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

ATTORNEY DOCKET: KAMR002US0

CONFIRMATION NO.: 7516

VIA ELECTRONIC FILING SYSTEM
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

AFFIDAVIT UNDER RULE 132

Applicants hereby submit this affidavit in support of their response to the Office Action mailed January 28, 2011 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 12/210,926, and pursuant to the provisions of 37 C.F.R. § 1.132. The witness hereby avers and testifies as follows:

1. I am James Hewitt, 12587 Fair Lakes Circle, #202, Fairfax VA 22033.

2. BA Philosophy, Vassar College, 1983, Certified Information System Security Professional since 2001, cert. #21060, per ISC2.org.

3. Selected professional background:

- 1998-2002 Director of Professional Services at CertCo, Inc., Cambridge MA CertCo. Produced cryptographic systems used by Tier I banks for authentication of users, machines and financial transactions.
- 2002-2003 Secure Messaging Project Manager for the Commonwealth of Massachusetts Information Technology Division. Implemented a system for securing healthcare-related transactions statewide.
- 2004-2011 Director of Security Governance, CGI Federal, Fairfax VA. Design, implement and manage the security of large-scale applications for government and commercial clients.

4. I have reviewed U.S. Patent No. 5,883,810 (*Franklin et al.*).

5. With regard to the following statement, "authentication and authorization are not two mutually exclusive operations and generally a person needs to be authenticated first in order to be authorized to use or access a resource under certain or no restrictions," one of skill in the art of user authentication and credit card transactions would understand that this statement is inaccurate. Online credit card transactions occur daily during which credit card payments are authorized without first authenticating the user. These transactions are similar to the online transactions as described in *Franklin et al.*

6. One of skill in the field of credit card transactions would understand that "card not present" transactions occurring online involve payments that are not guaranteed to the merchant.

No guarantee is provided primarily because the payers are not authenticated in online transactions, thereby allowing many risks to accompany the "card not present" transactions. Such risks involve issues such as chargeback of payment transactions to online merchants and fraud for both merchants and cardholders.

7. One of skill in the authentication art would understand that authentication of a user involves determining whether a user is, in fact, who he or she claims to be.

8. In contrast, one of skill in the art of authentication would understand the difference between user authentication during online transactions and credit card authorization that occurs during a credit card payment transaction, which involves receiving a user's credit card information for payment and sending the customer's credit card and order information to the customer's issuing bank for payment approval before deciding whether or not to fulfill a user's order.

9. One of skill in the art of authentication would understand that the temporary transaction number of *Franklin et al.* is not used for authentication of the user but rather for authorization of payment. The authorization transaction of *Franklin et al.* does not include an authentication.

10. One of skill in the art of authentication and credit card authorization would understand that the electronic online commerce card of Franklin has not been developed for verification of user's identity since the merchants treat the transaction number the same manner they process credit card transactions.

11. *Franklin et al.* does not disclose a request for authentication of an online customer that includes the temporary transaction number. *Franklin et al.* uses a digital certificate during an online session between a bank and the customer to obtain a temporary transaction number. But, the temporary transaction number is not used for authentication of the customer.

12. The merchant in *Franklin et al.* cannot rely upon mere authorization of a credit card payment as authentication of the customer. In *Franklin et al.* the merchant cannot distinguish between a recently obtained temporary transaction number and a normal credit card number.

14. Franklin does not provide any assurance to the merchant that the payer is authenticated. No assurance is provided because the merchant never receives any message from issuing bank that the user is authentic.

15. The temporary transaction number of *Franklin et al.* is not alphanumeric in format because it must have the same format and digits as a regular credit card number, which is not alphanumeric. Moreover, one of skill in the art would not change the temporary transaction number of *Franklin et al.* to an alphanumeric value because the system of *Franklin et al.* would no longer function as the temporary transaction number is designed to be processed by existing credit card processing systems that expect all numerical values in the format of a credit card number.

I affirm that all statements made herein of my own knowledge are true, and that all statements made herein on information and belief are believed to be true. I understand that willful false statements and the like are punishable by fine or imprisonment, or both (18 U.S.C. 1001), and may jeopardize the validity of the present patent application or any patent issuing thereon.

FURTHER AFFIANT SAYETH NOT.

It witness whereof,

James Hewitt

3-11-2011
Date

Certification Under 37 C.F.R. § 1.8

I hereby certify that on March 15, 2011 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: March 15, 2011 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 12/210,926

FILING DATE: September 15, 2008

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

ATTORNEY DOCKET: KAMR002US0

CONFIRMATION NO.: 7516

VIA ELECTRONIC FILING SYSTEM
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

AFFIDAVIT UNDER RULE 132

Applicants hereby submit this affidavit in support of their response to the Office Action mailed January 28, 2011 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 12/210,926, and pursuant to the provisions of 37 C.F.R. § 1.132. The witness hereby avers and testifies as follows:

1. I am Nader Asghari-Kamrani, one of the inventors listed in U.S. Patent Application No. 12/210,926, which is the subject of the present proceeding.

2. I received a degree in computer science from the Technical University of Vienna, in Vienna, Austria in 1993. I have been working in the field of authentication over communication networks since 2000. I am one of skill in the art of authentication and electronic transactions, including online credit card and banking transactions.

3. In 2003, I obtained an Accredited ACH Professional certification from NACHA (The Electronic Payment Association). There are only approximately 3500 professionals with this certification in the United States.

4. I am familiar with the specification and claims of the present Application as pending and as amended in accordance with a response filed concurrently herewith.

5. I have reviewed the art cited by the Examiner in the present proceeding and in particular, U.S. Patent No. 5,883,810 (*Franklin et al.*). I have also reviewed the final Office Action in the present application and in particular the Examiner's comments therein.

6. In his comments, the Examiner asserts "authentication and authorization are not two mutually exclusive operations and generally a person needs to be authenticated first in order to be authorized to use or access a resource under certain or no restrictions." One of skill in the art of user authentication and credit card transactions would understand that this statement is inaccurate for online credit card payments. Online credit card transactions occur daily during which credit card payments are authorized without first authenticating the user. These transactions are similar to the online transactions as described in *Franklin et al.*

7. One of skill in the world of credit card would understand that "Card not present" transactions occurring online involve payments that are not guaranteed to the merchant. No guarantee is provided primarily because the payers are not authenticated in online transactions, thereby allowing many risks to accompany the "card not present" transactions.

Such risks involve issues such as chargeback of payment transactions to online merchants and fraud for both merchants and cardholders.

8. One of skill in the authentication art would understand that authentication of a user involves determining whether a user is, in fact, who he or she claims to be. This is supported by, for example, Exhibit A to this Affidavit, which is from a recent publication by Hitachi ID Systems that that defines authentication as "Authentication is any process by which a system verifies the identity of a User who wishes to access it."

9. In contrast, one of skill in the art of authentication would understand the difference between user authentication during online transactions and credit card authorization that occurs during a credit card payment transaction, which involves receiving a user's credit card information for payment and sending the customer's credit card and order information to the customer's issuing bank for payment approval before deciding whether or not to fulfill a user's order. Exhibit B to this Affidavit describes credit card authorization as "An authorization is an approval on a cardholder account for a sale amount." Exhibit C to this Affidavit states: "The term "credit card authorization" refers to the process of verifying with a prepaid card issuer that an account has sufficient funds available and is in good standing. When a prepaid debit card transaction is 'authorized,' the available balance of the account is reduced by the authorized amount."

10. One of skill in the art of authentication would understand that the temporary transaction number of *Franklin et al.* is not used for authentication of the user but rather for authorization of payment. The authorization transaction of *Franklin et al.* does not include an authentication.

11. One of skill in the art of authentication and credit card authorization would understand that the electronic online commerce card of Franklin has not been developed for

verification of user's identity since the merchants treat the transaction number the same manner they process credit card transactions.

12. *Franklin et al.* does not disclose a request for authentication of an online customer that includes something equivalent to the SecureCode recited in the claims at issue. *Franklin et al.* uses a digital certificate during an online session between a bank and the customer to obtain a temporary transaction number. But, the temporary transaction number is not used for authentication of the customer.

13. *Franklin et al.* does not authenticate the user based on something equivalent to the recited SecureCode during an online transaction between a merchant and a customer.

14. The merchant in *Franklin et al.* cannot rely upon mere authorization of a credit card payment as authentication of the customer. In *Franklin et al.* the merchant cannot distinguish between a recently obtained temporary transaction number and a normal credit card number.

15. Franklin does not provide any assurance to the merchant that the payer is authenticated. No assurance is provided because the merchant never receives any message from issuing bank that the user is authentic.

16. The statement "*Franklin [et al.]* teaches an online transaction between a customer, a merchant and a bank(s) that is functionally equivalent to the same steps of the instant invention recited in the claims" is not accurate because among other things there is no request for authentication of the customer that includes anything equivalent to the recited SecureCode nor authentication of the customer based on a valid SecureCode. The transaction in *Franklin et al.* is simply not functionally equivalent to the claimed transaction and one of skill in the authentication field would not consider them to be functionally equivalent.

17. The temporary transaction number of *Franklin et al.* is not alphanumeric in format because it must have the same format and digits as a regular credit card number, which is not alphanumeric. Moreover, one of skill in the art would not change the temporary transaction

number of *Franklin et al.* to an alphanumeric value because the system of *Franklin et al.* would no longer function as the temporary transaction number is designed to be processed by existing credit card processing systems that expect all numerical values in the format of a credit card number.

I affirm that all statements made herein of my own knowledge are true, and that all statements made herein on information and belief are believed to be true. I understand that willful false statements and the like are punishable by fine or imprisonment, or both (18 U.S.C. 1001), and may jeopardize the validity of the present patent application or any patent issuing thereon.

FURTHER AFFIANT SAYETH NOT.

In witness whereof,

Nader Asghari-Kamrani

03/14/2011
Date

Certification Under 37 C.F.R. § 1.8

I hereby certify that on March 15, 2011 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: March 15, 2011 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 12/210,926

FILING DATE: September 15, 2008

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

ATTORNEY DOCKET: KAMR002US0

CONFIRMATION NO.: 7516

VIA ELECTRONIC FILING SYSTEM
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

AFFIDAVIT UNDER RULE 132

Applicants hereby submit this affidavit in support of their response to the Office Action mailed January 28, 2011 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 12/210,926, and pursuant to the provisions of 37 C.F.R. § 1.132. The witness hereby avers and testifies as follows:

1. I am Fred Laing, II

2. I have a BA degree in Economics from Moorhead State College, Moorhead, MN. I'm an Accredited ACH Professional (AAP) and a Certified Cash Manager (CCM).

3. I've been the President of the Upper Midwest Automated Clearing House Association for over 26 years. Prior to that I was a Cash Management Officer for Norwest Bank MN, now Wells Fargo. I'm the chairman of NACHA's Internet Council and head of the ACH Security Group within that organization. Since all of this experience revolves around payments, most of them electronic, the concepts of authorization and authentication are central to my job.

4. I have reviewed U.S. Patent No. 5,883,810 (*Franklin et al.*).

5. With regard to the following statement, "authentication and authorization are not two mutually exclusive operations and generally a person needs to be authenticated first in order to be authorized to use or access a resource under certain or no restrictions," one of skill in the art of user authentication and credit card transactions would understand that this statement is inaccurate. Online credit card transactions occur daily during which credit card payments are authorized without first authenticating the user. These transactions are similar to the online transactions as described in *Franklin et al.*

6. One of skill in the field of credit card transactions would understand that "card not present" transactions occurring online involve payments that are not guaranteed to the merchant. No guarantee is provided primarily because the payers are not authenticated in online transactions, thereby allowing many risks to accompany the "card not present" transactions. Such risks involve issues such as chargeback of payment transactions to online merchants and fraud for both merchants and cardholders.

7. One of skill in the authentication art would understand that authentication of a user involves determining whether a user is, in fact, who he or she claims to be.

8. In contrast, one of skill in the art of authentication would understand the difference between user authentication during online transactions and credit card authorization that occurs during a credit card payment transaction, which involves receiving a user's credit card information for payment and sending the customer's credit card and order information to the customer's issuing bank for payment approval before deciding whether or not to fulfill a user's order.

9. One of skill in the art of authentication would understand that the temporary transaction number of *Franklin et al.* is not used for authentication of the user but rather for authorization of payment which is designed to safeguard the users account number. The authorization transaction of *Franklin et al.* does not include, and is not intended to supply authentication.

10. One of skill in the art of authentication and credit card authorization would understand that the electronic online commerce card of Franklin has not been developed for verification of user's identity since the merchants treat the transaction number the same manner they process credit card transactions.

11. *Franklin et al.* does not disclose a request for authentication of an online customer that includes the temporary transaction number. *Franklin et al.* uses a digital certificate during an online session between a bank and the customer to obtain a temporary transaction number. But, the temporary transaction number is not used for authentication of the customer.

12. The merchant in *Franklin et al.* cannot rely upon mere authorization of a credit card payment as authentication of the customer. In *Franklin et al.* the merchant cannot distinguish between a recently obtained temporary transaction number and a normal credit card number.

14. Franklin does not provide any assurance to the merchant that the payer is authenticated. No assurance is provided because the merchant never receives any message from issuing bank that the user is authentic.

15. The temporary transaction number of *Franklin et al.* is not alphanumeric in format because it must have the same format and digits as a regular credit card number, which is not alphanumeric. Moreover, one of skill in the art would not change the temporary transaction number of *Franklin et al.* to an alphanumeric value because the system of *Franklin et al.* would no longer function as the temporary transaction number is designed to be processed by existing credit card processing systems that expect all numerical values in the format of a credit card number.

User Authentication And Credit Card Authorization

Virtually every payment network is faced with the issues surrounding how to authenticate an individual or company before allowing that transaction to be authorized. Let's start in the paper world. The signature on the check authorizes that check to be presented but it does not authenticate the individual that wrote the check, that's done at the point of sale by asking for some form of ID, usually a drivers license.

In a card-based face to face transaction the credit card authorization is done when the card is swiped and a data base is accessed to be sure the consumer either has the money in their account for debit, or has not hit their credit limit for a credit card. The authentication is done when the clerk compares the signature on the receipt with that on the card. A company can make the decision not to check that signature but they take the risk if they don't. In a "Card not present" situation (online transactions) the company taking the card is at risk because there is no reasonable way today to authenticate the customer. Therefore "Card not present" transactions occurring online involve payments that are not guaranteed to the company. No guarantee is provided primarily because the payers are not authenticated in online transactions, thereby allowing many risks to accompany the "card not present" transactions. Such risks involve issues such as chargeback of payment transactions to online merchants, fraud for both merchants and cardholders, increased exception item processing expenses for banks, and an increased perception that buying goods and services online is not safe and secure, which may keep some consumers from buying online.

To reduce fraud credit card issuing companies such as Visa and MasterCard developed a system to generate a random and temporary credit card numbers for customers. A temporary credit card number looks like a real credit card number. It has numeric value and online business process it the same manner they process a real credit card number. The system has not been developed for verification of user's identity and businesses have no idea if the card number given by the customer is an actual credit card number or a temporary number.

The electronic online commerce card of Franklin (U.S. Patent No. 5,883,810, *Franklin et al.*) has not been developed for verification of user's identity to the merchant either. The merchant has no idea if the numeric number given by a customer is a real credit card number or a temporary transaction number. The merchant process the temporary transaction number the same manner as it process the real credit card number and authorization response is also the same. The merchant never receives any message from issuing bank that the customer is authentic.

In today's market an invention that enables online businesses to verify users' identity would be of great benefit specially during online purchase transactions. By enabling online businesses to verify user's identity online businesses would be able to reduce risk associated with fraud, disputes, retrievals and credit card chargeback, and increases users' trust which subsequently will increase online transactions.

I affirm that all statements made herein of my own knowledge are true, and that all statements made herein on information and belief are believed to be true. I understand that willful false statements and the like are punishable by fine or imprisonment, or both (18 U.S.C. 1001), and may jeopardize the validity of the present patent application or any patent issuing thereon.

FURTHER AFFIANT SAYETH NOT.

It witness whereof,

Name

March 14, 2011
Date

Certification Under 37 C.F.R. § 1.8

I hereby certify that on March 15, 2011 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: March 15, 2011 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 12/210,926

FILING DATE: September 15, 2008

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

ATTORNEY DOCKET: KAMR002US0

CONFIRMATION NO.: 7516

VIA ELECTRONIC FILING SYSTEM
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

AFFIDAVIT UNDER RULE 132

Applicants hereby submit this affidavit in support of their response to the Office Action mailed January 28, 2011 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 12/210,926, and pursuant to the provisions of 37 C.F.R. § 1.132. The witness hereby avers and testifies as follows:

1. I am Majid (Mike) Shahbazi – 11501 Vale Road Oakton, VA 22124.

2. Educational background: Master of Science in Computer Science.

3. Work experience related to authentication and electronic transactions: With over 23 years experience in the areas of Enterprise Security, Identity Management, Single Sign-on authentication, Mobile, wireless security and biometrics solutions. Supporting commercial and government agencies in different initiatives such as Homeland Security Presidential Directive 12 (HSPD-12), HIPPA, System Infrastructure, security governance. Holds multiple patents and prestigious industry accolades in the area of enterprise security, policy management and mobile security.

4. I have reviewed U.S. Patent No. 5,883,810 (*Franklin et al.*).

5. With regard to the following statement, "authentication and authorization are not two mutually exclusive operations and generally a person needs to be authenticated first in order to be authorized to use or access a resource under certain or no restrictions," one of skill in the art of credit card transactions would understand that this statement is inaccurate. Online transactions occur daily during which credit card payments are authorized without first authenticating the user. These transactions are similar to the online transactions as described in *Franklin et al.*

6. One of skill in the field of credit card transactions would understand that "card not present" transactions occurring online involve payments that are not guaranteed to the merchant. No guarantee is provided primarily because the payers are not authenticated in online transactions, thereby allowing many risks to accompany the "card not present" transactions. Such risks involve issues such as chargeback of payment transactions to online merchants and fraud for both merchants and cardholders.

7. One of skill in the authentication art would understand that authentication of a user involves determining whether a user is, in fact, who he or she claims to be.

8. In contrast, one of skill in the art of authentication would understand the difference between user authentication during online transactions and credit card authorization during a a credit card payment transaction. Credit card authorization involves receiving a user's credit card information for payment and sending the customer's credit card and order information to the customer's issuing bank for payment approval before deciding whether or not to fulfill a user's order.

9. One of skill in the art of authentication would understand that the temporary transaction number of *Franklin et al.* is not used for authentication of the user but rather for authorization of payment. The authorization transaction of *Franklin et al.* does not include an authentication.

10. One of skill in the art of authentication and credit card authorization would understand that the electronic online commerce card of Franklin has not been developed for verification of user's identity since the merchants treat the transaction number the same manner they process credit card transactions.

11. *Franklin et al.* does not disclose a request for authentication of an online customer that includes the temporary transaction number. *Franklin et al.* uses a digital certificate during an online session between a bank and the customer to obtain a temporary transaction number. But, the temporary transaction number is not used for authentication of the customer.

12. The merchant in *Franklin et al.* cannot rely upon mere authorization of a credit card payment as authentication of the customer. In *Franklin et al.* the merchant cannot distinguish between a recently obtained temporary transaction number and a normal credit card number.

14. Franklin does not provide any assurance to the merchant that the payer is authenticated. No assurance is provided because the merchant never receives any message from issuing bank that the user is authentic.

15. The temporary transaction number of *Franklin et al.* is not alphanumeric in format because it must have the same format and digits as a regular credit card number, which is not alphanumeric. Moreover, one of skill in the art would not change the temporary transaction number of *Franklin et al.* to an alphanumeric value because the system of *Franklin et al.* would no longer function as the temporary transaction number is designed to be processed by existing credit card processing systems that expect all numerical values in the format of a credit card number.

I affirm that all statements made herein of my own knowledge are true, and that all statements made herein on information and belief are believed to be true. I understand that willful false statements and the like are punishable by fine or imprisonment, or both (18 U.S.C. 1001), and may jeopardize the validity of the present patent application or any patent issuing thereon.

FURTHER AFFIANT SAYETH NOT.

In witness whereof,

Majid/Mike Shahbazi

3/14/11
Date

Certification Under 37 C.F.R. § 1.8

I hereby certify that on March 15, 2011 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: March 15, 2011 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 12/210,926

FILING DATE: September 15, 2008

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

ATTORNEY DOCKET: KAMR002US0

CONFIRMATION NO.: 7516

VIA ELECTRONIC FILING SYSTEM
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

AFFIDAVIT UNDER RULE 132

Applicants hereby submit this affidavit in support of their response to the Office Action mailed January 28, 2011 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 12/210,926, and pursuant to the provisions of 37 C.F.R. § 1.132. The witness hereby avers and testifies as follows:

1. I am Abolfazl Hosseinzadeh, with address of PO Box 3043, Bellevue, WA 98009.

2. I am an electrical engineer with more than 20 years of proven technical leadership and multi-disciplined experience in the areas of systems engineering and development, program management, information security and e-commerce.

3. My experience includes working on e-commerce security and credit card processing projects; I also developed and implemented an online authentication system for secure delivery of policies documents over the Internet.

4. I have reviewed U.S. Patent No. 5,883,810 (*Franklin et al.*).

5. With regard to the following statement, "authentication and authorization are not two mutually exclusive operations and generally a person needs to be authenticated first in order to be authorized to use or access a resource under certain or no restrictions," one of skill in the art of user authentication and credit card transactions would understand that this statement is inaccurate. Online credit card transactions occur daily during which credit card payments are authorized without first authenticating the user. These transactions are similar to the online transactions as described in *Franklin et al.*

6. One of skill in the field of credit card transactions would understand that "card not present" transactions occurring online involve payments that are not guaranteed to the merchant. No guarantee is provided primarily because the payers are not authenticated in online transactions, thereby allowing many risks to accompany the "card not present" transactions. Such risks involve issues such as chargeback of payment transactions to online merchants and fraud for both merchants and cardholders.

7. One of skill in the authentication art would understand that authentication of a user involves determining whether a user is, in fact, who he or she claims to be.

8. In contrast, one of skill in the art of authentication would understand the difference between user authentication during online transactions and credit card authorization that occurs during a credit card payment transaction, which involves receiving a user's credit card

information for payment and sending the customer's credit card and order information to the customer's issuing bank for payment approval before deciding whether or not to fulfill a user's order.

9. One of skill in the art of authentication would understand that the temporary transaction number of *Franklin et al.* is not used for authentication of the user but rather for authorization of payment. The authorization transaction of *Franklin et al.* does not include an authentication.

10. One of skill in the art of authentication and credit card authorization would understand that the electronic online commerce card of Franklin has not been developed for verification of user's identity since the merchants treat the transaction number the same manner they process credit card transactions.

11. *Franklin et al.* does not disclose a request for authentication of an online customer that includes the temporary transaction number. *Franklin et al.* uses a digital certificate during an online session between a bank and the customer to obtain a temporary transaction number. But, the temporary transaction number is not used for authentication of the customer.

12. The merchant in *Franklin et al.* cannot rely upon mere authorization of a credit card payment as authentication of the customer. In *Franklin et al.* the merchant cannot distinguish between a recently obtained temporary transaction number and a normal credit card number.

14. Franklin does not provide any assurance to the merchant that the payer is authenticated. No assurance is provided because the merchant never receives any message from issuing bank that the user is authentic.

15. The temporary transaction number of *Franklin et al.* is not alphanumeric in format because it must have the same format and digits as a regular credit card number, which is not alphanumeric. Moreover, one of skill in the art would not change the temporary transaction

number of *Franklin et al.* to an alphanumeric value because the system of *Franklin et al.* would no longer function as the temporary transaction number is designed to be processed by existing credit card processing systems that expect all numerical values in the format of a credit card number.

I affirm that all statements made herein of my own knowledge are true, and that all statements made herein on information and belief are believed to be true. I understand that willful false statements and the like are punishable by fine or imprisonment, or both (18 U.S.C. 1001), and may jeopardize the validity of the present patent application or any patent issuing thereon.

FURTHER AFFIANT SAYETH NOT.

It witness whereof,

3-9-11
Date

Electronic Acknowledgement Receipt

EFS ID:	9666572
Application Number:	12210926
International Application Number:	
Confirmation Number:	7516
Title of Invention:	Centralized Identification and Authentication System and Method
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Customer Number:	58293
Filer:	Michael P. Fortkort
Filer Authorized By:	
Attorney Docket Number:	KAMR002US0
Receipt Date:	15-MAR-2011
Filing Date:	15-SEP-2008
Time Stamp:	19:31:15
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	Amendment After Final	12210926_Response_to_OA_mailed_012811_filed_031511.pdf	101090 85f070b7820f2f0cdba6887a2f51e6b3e0d2100d	no	24

Warnings:

Information:

2	Rule 130, 131 or 132 Affidavits	12210926_132_Affidavit_K_Kamrani_031511.pdf	1999388 341c50bbf05c970c1c9573f07560347659490feb	no	4
Warnings:					
Information:					
3	Rule 130, 131 or 132 Affidavits	12210926_132_Affidavit_Hewitt_031511.pdf	1471046 814b3e32349b01cb3430e78bd7feda6e19297a01	no	4
Warnings:					
Information:					
4	Rule 130, 131 or 132 Affidavits	12210926_132_Affidavit_N_Kamrani_031511.pdf	6166905 be659ee31513c6d0dc946701e735d094cee8d31d	no	5
Warnings:					
Information:					
5	Rule 130, 131 or 132 Affidavits	12210926_132_Affidavit_Fred_Laing_031511.pdf	142254 8881f6c7323a6a4076bd306ca0fe85aa1ebf398a	no	6
Warnings:					
Information:					
6	Rule 130, 131 or 132 Affidavits	12210926_132_Affidavit_MikeShahbazi_031511.pdf	49541 9a8eeb56970f8d71dd8a9429918ec5916293b346	no	4
Warnings:					
Information:					
7	Rule 130, 131 or 132 Affidavits	12210926_132_Affidavit_Hosseinzadeh_031511.pdf	143160 200ae50848b3281e8e9d2e070615974d529f4e18	no	4
Warnings:					
Information:					
		Total Files Size (in bytes):	10073384		

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 (07-06)
Approved for use through 1/31/2007. 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 12/210,926	Filing Date 09/15/2008	□ To be Mailed

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	
□ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
□ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			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 $250 ($125 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			TOTAL	

APPLICATION AS AMENDED – PART II

		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
AMENDMENT	**03/15/2011**	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 59	Minus	** 62	= 0	X $26 =	0	OR	X $ =	
	Independent (37 CFR 1.16(h))	* 4	Minus	***3	= 1	X $110 =	110	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	**110**	OR	TOTAL ADD'L FEE	

		(Column 1)		(Column 2)	(Column 3)					
AMENDMENT		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 number found in the appropriate box in column 1.

Legal Instrument Examiner:
/DORIS M. KING/

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 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.
12/210,926	09/15/2008	Nader Asghari-Kamrani	KAMR002US0	7516

58293 7590 02/28/2011
FORTKORT & HOUSTON P.C.
9442 N. CAPITAL OF TEXAS HIGHWAY
ARBORETUM PLAZA ONE, SUITE 500
AUSTIN, TX 78759

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	PAPER NUMBER
2432	
MAIL DATE	DELIVERY MODE
02/28/2011	PAPER

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

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

Interview Summary	Application No. 12/210,926	Applicant(s) ASGHARI-KAMRANI ET AL.	
	Examiner ABDULHAKIM NOBAHAR	Art Unit 2432	

All participants (applicant, applicant's representative, PTO personnel):

(1) ABDULHAKIM NOBAHAR. (3)_____.

(2) Mr. Michael P. Fortkort. (4)_____.

Date of Interview: 22 February 2011.

Type: a)☒ Telephonic b)□ Video Conference
c)□ Personal [copy given to: 1)□ applicant 2)□ applicant's representative]

Exhibit shown or demonstration conducted: d)□ Yes e)☒ No.
If Yes, brief description: _____.

Claim(s) discussed: 1.

Identification of prior art discussed: US 5883810 A.

Agreement with respect to the claims f)□ was reached. g)□ was not reached. h)☒ N/A.

Substance of Interview including description of the general nature of what was agreed to if an agreement was reached, or any other comments: Mr. Fortkort explained that the prior art Franklin does not authorize the user based on the authentication of user using a secure code upon the merchant's request in an online transaction. Examiner will consider this applicants' argument when filed in response to the Final Office Action mailed on 01/28/2011.

(A fuller description, if necessary, and a copy of the amendments which the examiner agreed would render the claims allowable, if available, must be attached. Also, where no copy of the amendments that would render the claims allowable is available, a summary thereof must be attached.)

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. See Summary of Record of Interview requirements on reverse side or on attached sheet.

/Abdulhakim Nobahar/
Examiner, Art Unit 2432

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:
1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

PTOL-413A (08-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Applicant Initiated Interview Request Form

Application No.: 12/210,926 First Named Applicant: ASGHARI-KAMRANI, NADER
Examiner: MR. ABDUL-HAKIM NOBAHAR Art Unit: 2432 Status of Application: FINAL REJECTION

Tentative Participants:
(1) MICHAEL P. FORTKORT (2)________
(3)________ (4)________

Proposed Date of Interview: February 21, 2011 **Proposed Time:** 2:00 p.m. **(AM/PM)**

Type of Interview Requested:
(1) [✓] Telephonic (2) [ ] Personal (3) [ ] Video Conference

Exhibit To Be Shown or Demonstrated: [ ] YES [ ] NO
If yes, provide brief description:________

Issues To Be Discussed

Issues (Rej., Obj., etc)	Claims/ Fig. #s	Prior Art	Discussed	Agreed	Not Agreed
(1) Rejection	All	Franklin et al.	[ ]	[ ]	[ ]
(2)			[ ]	[ ]	[ ]
(3)			[ ]	[ ]	[ ]
(4)			[ ]	[ ]	[ ]

[ ] Continuation Sheet Attached [ ] Proposed Amendment or Arguments Attached

Brief Description of Arguments to be Presented: Authorization of transaction is not based on authentication of user using a secure code, but rather the authentication of the user in Franklin is done by digital certificate -- not as arranged as in claims.

An interview was conducted on the above-identified application on ________

NOTE: This form should be completed and filed by applicant in advance of the interview (see MPEP § 713.01). If this form is signed by a registered practitioner not of record, the Office will accept this as an indication that he or she is authorized to conduct an interview on behalf of the principal (37 CFR 1.32(a)(3)) pursuant to 37 CFR 1.34. This is not a power of attorney to any above named practitioner. See the Instruction Sheet for this form, which is incorporated by reference. By signing this form, applicant or practitioner is certifying that he or she has read the Instruction Sheet. After the interview is conducted, applicant is advised to file a statement of the substance of this interview (37 CFR 1.133(b)) as soon as possible. This application will not be delayed from issue because of applicant's failure to submit a written record of this interview.

/Michael P. Fortkort/
Applicant/Applicant's Representative Signature

____
Examiner/SPE Signature

MICHAEL P. FORTKORT
Typed/Printed Name of Applicant or Representative

35,141
Registration Number, if applicable

This collection of information is required by 37 CFR 1.133. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 24 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.

PTOL-413A (08-10)
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 displays a valid OMB control number.

Instruction Sheet for:
APPLICANT INITIATED INTERVIEW REQUEST FORM

(Not to be Submitted to the USPTO)

1. If this form is signed by a registered practitioner not of record, the authority to submit the Applicant Initiated Interview Request Form is pursuant to limited authority to act in a representative capacity under 37 CFR 1.34 and further proof of authority to act in a representative capacity may be required. *See* 37 CFR 1.34.

   The Office will accept the signed form as an indication that the registered practitioner not of record is authorized to conduct an interview on behalf of the principal in pursuant to 37 CFR 1.34.

   For more information, see the "Conducting an Interview with a Registered Practitioner Acting in a Representative Capacity" notice which is available on the USPTO Web site at: http://www.uspto.gov/patents/law/notices/2010.jsp.

2. This is not a power of attorney to any named practitioner. Accordingly, any registered practitioner not of record named on the form does not have authority to sign a request to change the correspondence address, a request for express abandonment, a disclaimer, a power of attorney, or other document requiring the signature of the applicant, assignee of the entire interest or an attorney of record. If appropriate, a separate power of attorney to the named practitioner should be executed and filed in the US Patent and Trademark Office.

3. Any interview concerning an unpublished application under 35 U.S.C. § 122(b) with a registered practitioner not of record, pursuant to 37 CFR 1.34, will be conducted based on the information and files supplied by the practitioner in view of the confidentiality requirements of 35 U.S.C. § 122(a).

Page 2

Privacy Act Statement

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

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

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

Doc Code: M865 or FAI.REQ.INTV

PTOL-413A (08-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Applicant Initiated Interview Request Form

Application No.: 12/210,926 First Named Applicant: NADER ASGHARI-KAMRANI ET AL.
Examiner: ABDULHAKIM NOBAHAR Art Unit: 2432 Status of Application: FINAL REJECTION MAILED

Tentative Participants:
(1) MICHAEL P. FORTKORT (2) ______
(3) ______ (4) ______

Proposed Date of Interview: FRIDAY, FEBRUARY 18, 2011 **Proposed Time:** 10:00 AM **(AM/PM)**

Type of Interview Requested:
(1) [✓] Telephonic (2) [ ] Personal (3) [ ] Video Conference

Exhibit To Be Shown or Demonstrated: [ ] YES [ ] NO
If yes, provide brief description: ______

Issues To Be Discussed

Issues (Rej., Obj., etc)	**Claims/ Fig. #s**	**Prior Art**	**Discussed**	**Agreed**	**Not Agreed**
(1) REJECTION	ALL	Franklin	[ ]	[ ]	[ ]
(2)			[ ]	[ ]	[ ]
(3)			[ ]	[ ]	[ ]
(4)			[ ]	[ ]	[ ]

[ ] Continuation Sheet Attached [ ] Proposed Amendment or Arguments Attached
Brief Description of Arguments to be Presented: Franklin uses digital certificate for authentication not the claimed secure code

An interview was conducted on the above-identified application on ______

NOTE: This form should be completed and filed by applicant in advance of the interview (see MPEP § 713.01). If this form is signed by a registered practitioner not of record, the Office will accept this as an indication that he or she is authorized to conduct an interview on behalf of the principal (37 CFR 1.32(a)(3)) pursuant to 37 CFR 1.34. This is not a power of attorney to any above named practitioner. See the Instruction Sheet for this form, which is incorporated by reference. By signing this form, applicant or practitioner is certifying that he or she has read the Instruction Sheet. After the interview is conducted, applicant is advised to file a statement of the substance of this interview (37 CFR 1.133(b)) as soon as possible. This application will not be delayed from issue because of applicant's failure to submit a written record of this interview.

/Michael P. Fortkort/
Applicant/Applicant's Representative Signature

Examiner/SPE Signature

Michael P. Fortkort
Typed/Printed Name of Applicant or Representative

35,141
Registration Number, if applicable

This collection of information is required by 37 CFR 1.133. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 24 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.

Instruction Sheet for:
APPLICANT INITIATED INTERVIEW REQUEST FORM

(Not to be Submitted to the USPTO)

1. If this form is signed by a registered practitioner not of record, the authority to submit the Applicant Initiated Interview Request Form is pursuant to limited authority to act in a representative capacity under 37 CFR 1.34 and further proof of authority to act in a representative capacity may be required. *See* 37 CFR 1.34.

   The Office will accept the signed form as an indication that the registered practitioner not of record is authorized to conduct an interview on behalf of the principal in pursuant to 37 CFR 1.34.

   For more information, see the “Conducting an Interview with a Registered Practitioner Acting in a Representative Capacity” notice which is available on the USPTO Web site at: http://www.uspto.gov/patents/law/notices/2010.jsp.

2. This is not a power of attorney to any named practitioner. Accordingly, any registered practitioner not of record named on the form does not have authority to sign a request to change the correspondence address, a request for express abandonment, a disclaimer, a power of attorney, or other document requiring the signature of the applicant, assignee of the entire interest or an attorney of record. If appropriate, a separate power of attorney to the named practitioner should be executed and filed in the US Patent and Trademark Office.

3. Any interview concerning an unpublished application under 35 U.S.C. § 122(b) with a registered practitioner not of record, pursuant to 37 CFR 1.34, will be conducted based on the information and files supplied by the practitioner in view of the confidentiality requirements of 35 U.S.C. § 122(a).

Privacy Act Statement

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

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

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

Electronic Acknowledgement Receipt

EFS ID:	9430433
Application Number:	12210926
International Application Number:	
Confirmation Number:	7516
Title of Invention:	Centralized Identification and Authentication System and Method
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Customer Number:	58293
Filer:	Michael P. Fortkort
Filer Authorized By:	
Attorney Docket Number:	KAMR002US0
Receipt Date:	11-FEB-2011
Filing Date:	15-SEP-2008
Time Stamp:	17:01:27
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	Letter Requesting Interview with Examiner	Interview_Request_for_021811.pdf	419953 7e589d71c3553d5601d7c3f0ba63a9d1add97155	no	3

Warnings:

Information:

Total Files Size (in bytes):	419953

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.
12/210,926	09/15/2008	Nader Asghari-Kamrani	KAMR002US0	7516

58293 7590 01/28/2011
FORTKORT & HOUSTON P.C.
9442 N. CAPITAL OF TEXAS HIGHWAY
ARBORETUM PLAZA ONE, SUITE 500
AUSTIN, TX 78759

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	PAPER NUMBER
2432	
MAIL DATE	DELIVERY MODE
01/28/2011	PAPER

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

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

Office Action Summary	**Application No.** 12/210,926	**Applicant(s)** ASGHARI-KAMRANI ET AL.	
	Examiner ABDULHAKIM NOBAHAR	**Art Unit** 2432	

-- 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* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, 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 November 2010*.

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

3)□ 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

4)☒ Claim(s) *1-4,12-24,32-41,43-48,50-55,58,60 and 63-80* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4, 12-24, 32-41, 43-48, 50-55, 58, 60 and 63-80* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ 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).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

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).

a)□ All b)□ Some * c)□ None of:

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) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This office action is in response to applicants' amendment filed on 11/12/2010.

2. Claims 1-4, 12-24, 32-41, 43-48, 50-55, 58, 60 and 63-80 are pending.

Response to Arguments

Applicant's arguments have been fully considered but they are not persuasive.

Applicants have filed an Affidavit under rule 132, which states that an authentication of a person is different from a credit card authorization. While in the particular case of a credit card authorization for subtracting certain amount from the cardholder account may not need authentication of the person, but examiner asserts that authentication and authorization are not two mutually exclusive operations and generally a person needs to be authenticated first in order to be authorized to use or access a resource under certain or no restrictions.

On pages 15 and 16 of the remark applicants argue that the Franklin's temporary transaction number is not a code and therefore cannot be the recited SecureCode and alphanumerical code.

Examiner respectfully disagrees and asserts that Franklin discloses: "When the customer desires to conduct an online transaction, the customer sends a request to the issuing institution to issue a transaction number for a single transaction. The issuing institution generates a temporary transaction number and associates it with the permanent account number in a data record (see, e.g., col. 2, lines 12-17) and "The transaction number is designed to have a finite life, as determined by the issuing bank.

The shorter the duration, the less likelihood of fraud resulting from the transaction number being stolen and reused prior to the end of its life (see, e.g., col. 9, lines 43-46)." A number is the same as a code unless a different definition for the code is provided in the specification. Furthermore, based on own applicants' definition recited in the claim 48 an alphanumeric value can also be a telephone number, an IP address or a serial number that are numbers. Therefore, the Franklin transaction number that is used for a single transaction or has a short finite life is the same as a dynamic, non-predictable and time dependent alphanumeric code, secret code, PIN or other code and accordingly, the temporary transaction number of Franklin is equivalent to the SecureCode recited in the instant claims and is alphanumeric.

Applicants also on page 15 of the remark argue that in Franklin there is no request for authentication that includes anything akin to the recited SecureCode and that Franklin does not authenticate the user based on the temporary transaction number.

Examiner respectfully disagrees and asserts that Franklin discloses: "As part of the process, the customer 22 requests a transaction number from the bank 26 to be used in the commerce transaction (col. 8, lines 38-20)", "The customer fills out the order form 70 to purchase a desired product from the merchant (col. 8, lines 32-33)", "The customer is prompted by the dialog box to input a password for identification purposes (col. 8, lines 45-46)", "The bank computer 32 receives the signed request and immediately verifies the identity and authenticity of the customer…(col. 8, lines 57-58)", "the merchant computer submits a request for authorization over a payment network 36 to the bank computing center 32 (col. 10, lines 48-50)", "When the bank computer 32 receives the authorization request, it first examines the transaction number to determine whether it is a valid number (col. 10, lines 61-63)" and "After the request is processed, the processing system 92 returns an authorization response to the account manager 60 (col. 11, lines 32-33)". The aforesaid steps are performed for a single transaction and in a short duration. A temporary transaction number is issued to a user after the user is authenticated by the bank. The customer enters the temporary transaction number in the order form of the merchant while filling out the form. The merchant receives the temporary transaction number and all the necessary information related to the customer via the order form. The merchant immediately sends the temporary transaction number to the bank for verification. The confirmation of the short life, single-use (temporary) transaction number by the bank is as though the customer is authenticated to the merchant by the bank, because the steps of the entire transaction are carried out in one online session and in a short period. Therefore, Franklin teaches an online transaction between a customer, a merchants and a bank(s) that is functionally equivalent to the same steps of the instant invention recited in the claims.

Examiner, however, in light of the above submission maintains the previous rejections as follows:

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-4, 12-24, 32-41, 43, 45-48, 51-55, 58, 60 and 63-80 are rejected under 35 U.S.C. 102(b) as being anticipated by Franklin et al (US 5,883,810 A), hereinafter Franklin.

Regarding claims 1, 21 and 74, Franklin discloses:

A method for authenticating a user during an electronic transaction between the user and an External-Entity (see, e.g., col. 8, lines 15-56), the method comprising:

receiving electronically a request for a dynamic SecureCode for the user by a Central-Entity during the transaction between the user and the External-Entity (see, e.g., col. 8, lines 37-42 and col. 9, lines 30-46, where the temporary transaction number corresponds to the recited dynamic SecureCode);

generating during the transaction a dynamic SecureCode for the user in response to the request (see, e.g., col. 8, lines 57-67);

providing said generated SecureCode to the user during the transaction (see, e.g., col. 10, line 6-10),

receiving electronically by a Central-Entity a request for authenticating the user based on a digital identity during the transaction, which digital identity includes the SecureCode (see, e.g., col. 8, lines 24-36, the order form and col. 10, lines 14-20, where the order form which includes the transaction number and other user's information corresponds to the recited digital identity); and authenticating by the Central-Entity the user during the transaction if the digital identity is valid (see, e.g., col. 10, lines 61-63 and col. 11, lines 31-40).

Regarding claims 2 and 22, Franklin discloses:

A method as recited in claim 1, wherein said user has a pre-existing relationship with the External-Entity (see, e.g., col. 8, line 15+, where before the transaction phase the customer has opened an account with the bank).

Regarding claims 3 and 23, Franklin discloses:

A method as recited in claim 1, wherein said user has no pre-existing relationship with the External-Entity (see, e.g., col. 5, line 23+, where before the registration phase the customer did not have an account with the bank).

Regarding claims 4, 24 and 43, Franklin discloses:

A method as recited in claim 1, further comprising:

combining said generated SecureCode with a user-specific information using a predetermined algorithm to form a combined Secure-Code and user specific information (see, e.g., col. 8, line 60+, The account manager 60 associates the transaction number with the customer account number in a data record on the customer database 64);

maintaining the combined Secure-Code and user specific information at the Central-Entity (see, e.g., Fig. 2, customer database 64 and col. 8, line 60+):

using the predetermined algorithm to combine received user specific information received by the Central-Entity with a received SecureCode received by the Central-Entity to form a combined received SecureCode and received user specific information (see, e.g., col. 11, lines 7-31);

comparing the combined Secure-Code and user specific information with the combined received SecureCode and received user specific information to validate the user (see, e.g., col. 11, lines 11-21).

Regarding claims 12 and 32, Franklin discloses:

A method as recited in claim 1, wherein the External-Entity receives the user's digital identity (see, e.g., col. 8, lines 24-36).

Regarding claims 13 and 33, Franklin discloses:

A method as recited in claim 1, wherein said External-Entity submits a digital identity to the Central-Entity (see, e.g., col. 10, lines 61-67).

Regarding claims 14, 34, 65 and 66, Franklin discloses:

The method of claim 1, wherein said digital identity includes a user-specific information (see, e.g., col. 8, lines 24-36, where the order form contains the user's specific information).

Regarding claims 15, 35, 48, 78 and 79, Franklin discloses:

The method of claim 14, wherein the user-specific information comprises one or more of the following: an alphanumeric name, an ID, a login name, and an identification phrase, wherein said identification phrase comprises one or more of the following: an account number, a telephone number, an IP address, a hardware key, a software key, a session ID, a token and serial number (see, e.g., col. 6, lines 25-32).

Regarding claims 16 and 36, Franklin discloses:

The method of claim 1, wherein the transaction corresponds to a financial transaction (see, e.g., col. 3, lines 34-47).

Regarding claims 17 and 37, Franklin discloses:

The method of claim 1, wherein the transaction corresponds to a non-financial transaction (see, e.g., col. 1, lines 19-25, order goods and/or services, where services may include non-financial transaction such as accessing secured information, application, web sites or other resources).

Regarding claims 18 and 38, Franklin discloses:

The method of claim 1, wherein the transaction corresponds to access to restricted web-site or restricted computer/server (see, e.g., col. 1, lines 19-25, order goods and/or services, where services may include non-financial transaction such as accessing secured information, application , web sites or other resources).

Regarding claims 19 and 39, Franklin discloses:

The method of claim 1, wherein said transaction occurs over a communication network, wherein said communication network comprises one or more of the following: an Internet, a wireless network, a mobile network, a satellite, and a private network (see, e.g., Fig. 1).

Regarding claims 20, 40, 51, 53-55 and 58, Franklin discloses:

The method of claim 1, wherein said transaction occurs over a communication network to which is coupled said user, said Central-Entity, and said External-Entity (see, e.g., Fig. 1).

Regarding claim 41, Franklin discloses:

A method as recited in claim 4, wherein said External-Entity is using said algorithmically combined SecureCode to authenticate a user's identity (see, e.g., col. 8, lines 24-36, <u>the order form is a combination of the transaction number and other user's related information</u>).

Regarding claims 45 and 75, Franklin discloses:

The method as recited in claim 1, wherein said SecureCode becomes invalid after being used for authentication (see, e.g., col. 2, lines 12-20, <u>for a single transaction</u>).

Regarding claims 46 and 76, Franklin discloses:

The method as recited in claim 1, wherein the SecureCode becomes invalid when a predefined period of time passes (see, e.g., col. 2, lines 12-20, where “a short expiration term" corresponds to the recited predefined period of time).

Regarding claims 47 and 77, Franklin discloses:

The method as recited in claim 1, wherein said Central-Entity generates SecureCode with dependence on one or more alphanumeric values (see, e.g., col. 4, lines 48-55, where the transaction number is associated with other information means that the transaction number is dependent on some alphanumeric values).

Regarding claims 50 and 52, Franklin discloses:

The method as recited in claim 1, wherein said SecureCode is alphanumeric (see, e.g., col. 2, lines 12-20, where the temporary transaction number is an alphanumeric code and corresponds to the recited SecureCode).

Regarding claim 60, Franklin discloses:

The method as recited in claim 58, wherein said request is initiated by a user through a standard interface provided to said user (see, e.g., col. 5, lines 55-60).

Regarding claim 63, Franklin discloses:

The apparatus according to claim 21, wherein said first Central-Entity computer and said second Central-Entity computer are the same (see, e.g., col. 10, lines 61-67 and Fig. 5).

Regarding claim 64, Franklin discloses:

The apparatus according to claim 21, wherein said first Central-Entity computer and said second Central-Entity computer are different (see, e.g., col. 10, lines 48-60, where the computer of the merchants acquiring bank is different from the computer of the issuing bank).

Regarding claims 67, 68, 71 and 72, Franklin discloses:

A method as recited in claim 1, wherein said digital identity is invalid if the SecureCode is invalid (see, e.g., col. 2, lines 52-55, col. 10, lines 61-67).

Regarding claims 69, 70, 73 and 80, Franklin discloses:

A method as recited in claim 1, wherein said External-Entity authenticates the user upon receiving an affirmation authentication message from the Central-Entity (see, e.g., col. 11, lines 40-45).

Claim Rejections - 35 USC § 103

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

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, 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.

Claim 44 is rejected under 35 U.S.C. 103(a) as being unpatentable over Franklin et al (US 5,883,810 A); hereinafter Franklin in view of the examiner Official Notice.

Regarding claim 44, Franklin does not expressly disclose:

wherein said External-Entity and said Central-Entity are the same entity.

Official Notice is taken that it is old and well-known practice in the art that some institutions such as banks that maintain users' accounts, the providers of email services to users and some the department stores which provide their own credit cards to the customers, directly authenticate the users when the users requires services or accessing their web sites, without receiving authentication services from a third party. Whenever users and customers logging on to their banks web sites, or their provider's website for email services or a customer purchasing goods using a department store's credit card, the users and customers are authenticated by the respective institution independent from a. In this case the Central-Entity and the External-Entity are the same institution that having an account for the user or the customer. Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to modify the system of Franklin to have one entity to be as the same Central-Entity and External-Entity. The deployment of one entity to issue a SecurCode to a user and also to authenticate the user when using the SecurCode would make the system of Franklin a versatile and a flexible system, in another word a scalable system.

Conclusion

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 ABDULHAKIM NOBAHAR whose telephone number is (571)272-3808. The examiner can normally be reached on M-T 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. 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.

Abdulhakim Nobahar
Examiner
Art Unit 2432

/A. N./
Examiner, Art Unit 2432

/Jung Kim/
Primary Examiner, AU 2432

Index of Claims	**Application/Control No.** 12210926	**Applicant(s)/Patent Under Reexamination** ASGHARI-KAMRANI ET AL.
	Examiner ABDULHAKIM NOBAHAR	**Art Unit** 2432

✓	**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	07/06/2009	11/20/2009	04/28/2010	09/12/2010	01/11/2011				
	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.	Applicant(s)/Patent Under Reexamination
	12210926	ASGHARI-KAMRANI ET AL.
	Examiner	**Art Unit**
	ABDULHAKIM NOBAHAR	2432

✓	**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	07/06/2009	11/20/2009	04/28/2010	09/12/2010	01/11/2011				
	37	✓	✓	✓	✓	✓				
	38	✓	✓	✓	✓	✓				
	39	✓	✓	✓	✓	✓				
	40	✓	✓	✓	✓	✓				
	41	✓	✓	✓	✓	✓				
	42	✓	-	✓	-	-				
	43	✓	✓	✓	✓	✓				
	44	✓	✓	✓	✓	✓				
	45	✓	✓	✓	✓	✓				
	46	✓	✓	✓	✓	✓				
	47	✓	✓	✓	✓	✓				
	48	✓	✓	✓	✓	✓				
	49	✓	-	-	-	-				
	50	✓	✓	✓	✓	✓				
	51	✓	✓	✓	✓	✓				
	52	✓	✓	✓	✓	✓				
	53	✓	✓	✓	✓	✓				
	54	✓	✓	✓	✓	✓				
	55	✓	✓	✓	✓	✓				
	56	✓	-	-	-	-				
	57	✓	-	-	-	-				
	58	✓	✓	✓	✓	✓				
	59	✓	-	-	-	-				
	60	✓	✓	✓	✓	✓				
	61	✓	-	-	-	-				
	62	✓	-	-	-	-				
	63				✓	✓				
	64				✓	✓				
	65				✓	✓				
	66				✓	✓				
	67				✓	✓				
	68				✓	✓				
	69				✓	✓				
	70				✓	✓				
	71				✓	✓				
	72				✓	✓				

Index of Claims	**Application/Control No.** 12210926	**Applicant(s)/Patent Under Reexamination** ASGHARI-KAMRANI ET AL.
	Examiner ABDULHAKIM NOBAHAR	**Art Unit** 2432

✓	**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	07/06/2009	11/20/2009	04/28/2010	09/12/2010	01/11/2011				
	73				✓	✓				
	74				✓	✓				
	75				✓	✓				
	76				✓	✓				
	77				✓	✓				
	78				✓	✓				
	79				✓	✓				
	80				✓	✓				

Certification Under 37 C.F.R. § 1.8

I hereby certify that on November 18, 2010 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: November 18, 2010 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 12/210,926

FILING DATE: September 15, 2008

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

ATTORNEY DOCKET: KAMR002US0

CONFIRMATION NO.: 7516

VIA ELECTRONIC FILING SYSTEM
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

Sir:

INTERVIEW SUMMARY

The Applicants wish to thank Examiner Abdulhakim Nobahar for meeting with them and their representative on November 10, 2010 as part of an Interview. During the interview, the Applicants described the development of their invention and discussed the applicability of the main reference, Franklin et al., to the claims at issue. The Applicants noted that the Franklin et al. reference does not relate to authentication of an individual but rather to authorization of a credit card transaction, and thus the claims were not anticipated by Franklin et al. No final agreement was reached regarding the claims and the rejections.

CONCLUSION

The Applicant respectfully submits this application is in condition for allowance and requests issuance of a Notice of Allowance.

Although not believed necessary, the Office is hereby authorized to charge any fees required under 37 C.F.R. § 1.16 or § 1.17 or credit any overpayments to the deposit account of MICHAEL P FORTKORT PC, Deposit Account No. 50-3776.

In the event the prosecution of this Application can be efficiently advanced by a phone discussion, it is requested that the undersigned attorney be called at (703) 435-9390.

Respectfully submitted,

By /Michael P. Fortkort/ Date: November 18, 2010
Michael P. Fortkort (Reg. No. 35,141)

MICHAEL P FORTKORT PC
The International Law Center
13164 Lazy Glen Lane
Oak Hill, Virginia 20171

Please direct telephone calls to:
Michael P. Fortkort
703-435-9390
703-435-8857 (facsimile)

Electronic Acknowledgement Receipt

EFS ID:	8870688
Application Number:	12210926
International Application Number:	
Confirmation Number:	7516
Title of Invention:	Centralized Identification and Authentication System and Method
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Customer Number:	58293
Filer:	Michael P. Fortkort
Filer Authorized By:	
Attorney Docket Number:	KAMR002US0
Receipt Date:	18-NOV-2010
Filing Date:	15-SEP-2008
Time Stamp:	17:53:32
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	Applicant summary of interview with examiner	Interview_Summary_111810.pdf	18111 61be724ee4458127d69118934e789015549612a3	no	2

Warnings:

Information:

Total Files Size (in bytes):	18111

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.
12/210,926	09/15/2008	Nader Asghari-Kamrani	KAMR002US0	7516

58293 7590 11/17/2010
FORTKORT & HOUSTON P.C.
9442 N. CAPITAL OF TEXAS HIGHWAY
ARBORETUM PLAZA ONE, SUITE 500
AUSTIN, TX 78759

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	PAPER NUMBER
2432	
MAIL DATE	DELIVERY MODE
11/17/2010	PAPER

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

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

Interview Summary	**Application No.** 12/210,926	**Applicant(s)** ASGHARI-KAMRANI ET AL.
	Examiner ABDULHAKIM NOBAHAR	**Art Unit** 2432

All participants (applicant, applicant's representative, PTO personnel):

(1) *ABDULHAKIM NOBAHAR*.

(2) *Mr. Michael Fortkort, Reg. No. 35,141*.

(3)*Mr. Nader Asghari-Kamrani*.

(4)*Mr. Kamran Asghari-Kamrani*.

Date of Interview: *10 November 2010*.

Type: a)□ Telephonic b)□ Video Conference
c)☒ Personal [copy given to: 1)□ applicant 2)□ applicant's representative]

Exhibit shown or demonstration conducted: d)□ Yes e)☒ No.
If Yes, brief description: _____.

Claim(s) discussed: *1*.

Identification of prior art discussed: *5,883,810*.

Agreement with respect to the claims f)□ was reached. g)□ was not reached. h)☒ N/A.

Substance of Interview including description of the general nature of what was agreed to if an agreement was reached, or any other comments: *The limitations of claim 1 in view of the applied prior art Franklin et al in the rejection of claims were discussed. Mr. Fortkort stated that the differences between the instant invention and the prior art will be further explained in the applicans' response to the Office Action*.

(A fuller description, if necessary, and a copy of the amendments which the examiner agreed would render the claims allowable, if available, must be attached. Also, where no copy of the amendments that would render the claims allowable is available, a summary thereof must be attached.)

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. See Summary of Record of Interview requirements on reverse side or on attached sheet.

/A. N./
Examiner, Art Unit 2432

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:

- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:

1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

Certification Under 37 C.F.R. § 1.8

I hereby certify that on November 12, 2010 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: November 12, 2010 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 12/210,926

FILING DATE: September 15, 2008

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

ATTORNEY DOCKET: KAMR002US0

CONFIRMATION NO.: 7516

VIA ELECTRONIC FILING SYSTEM
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

RESPONSE TO OFFICE ACTION

Sir:

In response to the Office Action mailed September 17, 2010, the Applicants hereby respectfully submit the following amendments and remarks:

Amendments to the Claims begin on page 2.

Remarks begin on page 13.

In the Claims:

Please amend the claims as follows:

1. (Previously Presented) A method for authenticating a user during an electronic transaction between the user and an External-Entity, the method comprising:

receiving electronically a request for a dynamic SecureCode for the user by a Central-Entity during the transaction between the user and the External-Entity;

generating during the transaction a dynamic SecureCode for the user in response to the request;

providing said generated SecureCode to the user during the transaction;

receiving electronically by a Central-Entity a request for authenticating the user based on a digital identity during the transaction, which digital identity includes the SecureCode; and

authenticating by the Central-Entity the user during the transaction if the digital identity is valid.

2. (Original) A method as recited in claim 1, wherein said user has a pre-existing relationship with the External-Entity.

3. (Original) A method as recited in claim 1, wherein said user has no pre-existing relationship with the External-Entity.

4. (Previously Presented) A method as recited in claim 1, further comprising:

combining said generated SecureCode with a user-specific information using a

predetermined algorithm to form a combined Secure-Code and user specific information;

maintaining the combined Secure-Code and user specific information at the Central-Entity;

using the predetermined algorithm to combine received user specific information received by the Central-Entity with a received SecureCode received by the Central-Entity to form a combined received SecureCode and received user specific information;

comparing the combined Secure-Code and user specific information with the combined received SecureCode and received user specific information to validate the user.

5-11. (Cancelled)

12. (Previously Presented) A method as recited in claim 1, wherein said External-Entity receives the user's digital identity.

13. (Previously Presented) A method as recited in claim 1, wherein said External-Entity submits a digital identity to the Central-Entity.

14. (Previously Presented) The method of claim 1, wherein said digital identity includes a user-specific information.

15. (Previously Presented) The method of claim 14, wherein the user specific information comprises one or more of the following: an alphanumeric name, an ID, a login name, and an identification phrase, wherein said identification phrase comprises one or more of the following:

an account number, a telephone number, an IP address, a hardware key, a software key, a session ID, a token and a serial number.

16. (Original) The method of claim 1, wherein the transaction corresponds to a financial transaction.

17. (Original) The method of claim 1, wherein the transaction corresponds to a non-financial transaction.

18. (Previously Presented) The method of claim 1, wherein the transaction corresponds to access to restricted web-site or restricted computer/server.

19. (Previously Presented) The method of claim 1, wherein said transaction occurs over a communication network, wherein said communication network comprises one or more of the following: an Internet, a wireless network, a mobile network, a satellite network, and a private network.

20. (Previously Presented) The method of claim 1, wherein said transaction occurs over a communication network to which is coupled said user, said Central-Entity, and said External-Entity.

21. (Previously Presented) An apparatus for authenticating a user during an electronic transaction with an External-Entity, the apparatus comprising:

a first Central-Entity computer adapted to:

generate a dynamic SecureCode for the user in response to a request during the transaction; and

provide said SecureCode to the user;

a second Central-Entity computer adapted to validate a digital identity, which includes said SecureCode, and authenticate the user if the digital identity is valid.

22. (Previously Presented) The apparatus as recited in claim 21, wherein said user has a pre-existing relationship with the External-Entity.

23. (Previously Presented) The apparatus as recited in claim 21, wherein said user has no pre-existing relationship with the External-Entity.

24. (Previously Presented) The apparatus as recited in claim 21, wherein said External-Entity and said Central-Entity use a SecureCode that is algorithmically combined with said user-specific information.

25-31. (Cancelled)

32. (Previously Presented) The apparatus as recited in claim 21, wherein the user submits a digital identity to the External-Entity.

33. (Previously Presented) The apparatus as recited in claim 21, wherein the External-

Entity submits a digital identity to the Central-Entity.

34. (Previously Presented) The apparatus of claim 21, wherein the digital identity includes a user-specific information.

35. (Previously Presented) The apparatus of claim 34, wherein the user specific information comprises one or more of the following; an alphanumeric name, an ID, a login name, and an identification phrase, wherein said identification phrase comprises one or more of the following: an account number, a telephone number, an IP address, a hardware key, a software key, a session ID, or token, and a serial number.

36. (Previously Presented) The apparatus of claim 21, wherein the transaction corresponds to a financial transaction.

37. (Previously Presented) The apparatus of claim 21, wherein the transaction corresponds to a non-financial transaction.

38. (Previously Presented) The apparatus of claim 21, wherein the transaction corresponds to access to restricted web-site or restricted computer/server.

39. (Previously Presented) The apparatus of claim 21, wherein said transaction occurs over a communication network and wherein said communication network comprises one or more of the following; an Internet, a wireless network, a mobile network, a satellite network, and a

private network.

40. (Currently Amended) The apparatus of claim 21, wherein said transaction occurs over ~~a a communication network~~ a communication network to which is coupled said user, said Central-Entity, and said External-Entity.

41. (Previously Presented) A method as recited in claim 4, wherein said External-Entity is using said algorithmically combined SecureCode to authenticate a user's identity.

42. (Cancelled)

43. (Previously Presented) A method as recited in claim 4, wherein said Central-Entity is using said algorithmically combined SecureCode to authenticate a user's identity.

44. (Original) A method as recited in claim 1, wherein said External-Entity and said Central-Entity are the same entity.

45. (Previously Presented) The method as recited in claim 1, wherein said SecureCode becomes invalid after being used for authentication.

46. (Previously Presented) The method as recited in claim 1, wherein the SecureCode becomes invalid when a predefined period of time passes.

47. (Original) The method as recited in claim 1, wherein said Central-Entity generates SecureCode with dependence on one or more alphanumeric values.

48. (Previously Presented) The method as recited in claim 47, wherein said one or more alphanumeric values comprise one or more of the following: an unique key, an ID, a login name, a password, and an identification phrase, wherein said identification phrase comprises an account number, a telephone number, an IP address, a Hardware key, a software key a session ID, a token, a seed, and a serial number.

49. (Cancelled)

50. (Previously Presented) The method as recited in claim 1, wherein said SecureCode is alphanumeric.

51. (Original) The method as recited in claim 1, wherein said user communicates with said Central-Entity over a communication network.

52. (Previously Presented) The apparatus as recited in claim 21, wherein said SecureCode is alphanumeric.

53. (Original) The method as recited in claim 1, wherein said user communicates with said External-Entity over a communication network.

54. (Previously Presented) The apparatus as recited in claim 21, wherein said user communicates with said Central-Entity over a communication network.

55. (Previously Presented) The apparatus as recited in claim 21, wherein said user communicates with said External-Entity over a communication network.

56-57. (Cancelled)

58. (Previously Presented) The method as recited in claim 1, wherein said SecureCode is generated based on a request submitted by said user over a communication network.

59. (Cancelled)

60. (Previously Presented) The method as recited in claim 58, wherein said request is initiated by said user through a standard interface provided to said user.

61-62. (Cancelled)

63. (Previously Presented) The apparatus according to claim 21, wherein said first Central-Entity computer and said second Central-Entity computer are the same.

64. (Previously Presented) The apparatus according to claim 21, wherein said first Central-Entity computer and said second Central-Entity computer are different.

65. (Previously Presented) A method as recited in claim 1, wherein said digital identity comprises the SecureCode and a user-specific information.

66. (Previously Presented) A method as recited in claim 1, wherein said digital identity comprises the SecureCode.

67. (Previously Presented) A method as recited in claim 1, wherein said digital identity is invalid if the SecureCode is invalid.

68. (Previously Presented) A method as recited in claim 1, wherein said digital identity is valid if at least the SecureCode is valid.

69. (Previously Presented) A method as recited in claim 1, wherein said External-Entity authenticates the user upon receiving an affirmation authentication message from the Central-Entity.

70. (Previously Presented) A method as recited in claim 1, wherein said External-Entity authenticates the user if said Central-Entity authenticates the user based on the SecureCode.

71. (Previously Presented) The apparatus of claim 21, wherein said digital identity is invalid if the SecureCode is invalid.

72. (Previously Presented) The apparatus of claim 21, wherein said digital identity is valid if at least the SecureCode is valid.

73. (Previously Presented) The apparatus of claim 21, wherein said External-Entity authenticates the user upon receiving an affirmation authentication message from the Central-Entity.

74. (Previously Presented) The apparatus of claim 21, wherein said digital identity comprises the SecureCode.

75. (Previously Presented) The apparatus of claim 21, wherein said SecureCode becomes invalid after being used for authentication.

76. (Previously Presented) The apparatus of claim 21, wherein the SecureCode becomes invalid when a predefined period of time passes.

77. (Previously Presented) The apparatus of claim 21, wherein said Central-Entity generates the SecureCode based on one or more alphanumeric values.

78. (Previously Presented) The apparatus of claim 78, wherein said one or more alphanumeric values comprise one or more of the following: an unique key, an ID, a login name, a password, and an identification phrase, wherein said identification phrase comprises an account

number, a telephone number, an IP address, a Hardware key, a software key, a session id or token, a seed and a serial number.

79. (Previously Presented) The method of claim 65, wherein the user specific information comprises one or more of the following: an alphanumeric name, an ID, a login name, and an identification phrase, wherein said identification phrase comprises one or more of the following: an account number, a telephone number, an IP address, a hardware key, a software key, a session id or token and a serial number.

80. (Previously Presented) The apparatus of claim 21, wherein said External-Entity authenticates the user if said Central-Entity authenticates the user based on the SecureCode.

REMARKS

Claims 1-4, 12-24, 32-41, 43-48, 50-55, 58, 60 and 63-80 were previously pending. Claims 5-11, 25-31, 42, 49, 56-57, 59 and 61-62 have been previously cancelled without disclaimer of or prejudice to the subject matter contained therein. Claim 40 has been amended to correct a typographical error. Claims 1-4, 12-24, 32-41, 43-48, 50-55, 58, 60 and 63-80 remain pending.

CLAIMS REMAIN PATENTABLE OVER *FRANKLIN ET AL.*

The Office Action rejected claims 1-4, 12-24, 32-41, 43, 45-48, 51, 53-55, 58, 60 and 63-80 under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,883,810 to *Franklin et al.* [hereinafter "*Franklin et al.*"]. The Office Action contends that *Franklin et al.* discloses all of the elements of the claims at issue. The Applicants respectfully disagree with the Office Action's characterization of these references vis-à-vis the claims at issue and respectfully request reconsideration and withdrawal of the rejection in light of the following remarks.

Background on Anticipation

To anticipate a claim, a single prior art reference must expressly or inherently disclose each claim limitation. But disclosure of each claim element is not quite enough ... anticipation requires the presence in a single prior art disclosure of all elements of a claimed invention *arranged as in the claims*. *Finisar v. DirecTV*, 523 F.3d 1323, 1334 (Fed. Cir. 2008) (emphasis supplied).

The reference must enable one to make the claimed invention without further research or experimentation. *In re Hall*, 781 F.2d 897, 899 (Fed. Cir. 1986). The disclosure in an assertedly anticipating reference must be adequate to enable possession of the desired subject matter. *It is insufficient to name or describe the desired subject matter*, if it cannot be produced without undue experimentation. *Elan Pharmaceuticals, Inc. v. Mayo Foundation for Medical Educ. and Research*, 346 F.3d 1051, 1055 (Fed. Cir. 2003) (emphasis supplied).

Inherency

With regard to inherency, inherency can only be established if a feature is necessarily present, even though it is not explicitly disclosed by a reference. Inherency may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient. As stated in MPEP § 2112(IV):

> The fact that a certain result or characteristic may occur or be present in the prior art is not sufficient to establish the inherency of that result or characteristic. *In re Rijckaert*, 9 F.3d 1531, 1534, 28 USPQ2d 1955, 1957 (Fed. Cir. 1993) (emphasis supplied)..." To establish inherency, the extrinsic evidence 'must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill. Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient.'" *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999) (emphasis supplied).

Stated another way, the doctrine of inherency requires that the missing descriptive matter MUST be present, and if there is another way of performing a missing descriptive function, then the missing descriptive function is NOT inherently disclosed.

***Franklin et al.* Does not Expressly or Inherently Disclose Each Element of the Claims Arranged as in the Claims**

Franklin et al. fails to disclose each element of the claims arranged as in the claims for at least three reasons. First, *Franklin et al.* does not disclose the SecureCode that is recited in independent claims 1 and 21, from which the remaining claims ultimately depend. The Office Action cites the temporary transaction number as being the claimed SecureCode (see Office Action, page 2, last line to page 3, first line). At paragraph [0016], the specification of the present application states that the term "SecureCode" is used herein to denote any dynamic, non-predictable and time dependent alphanumeric code, secret code, PIN or other code, which may be broadcast to the user over a communication network, and may be used as part of a digital identity to identify a user as an authorized user." The temporary transaction number of *Franklin et al.* is simply not a "code," but merely a numerical value that looks like a credit card number. Thus, the temporary transaction number of *Franklin et al.* is simply not the recited SecureCode.

Second, claim 1 recites "receiving ... a request for authenticating the user based on a digital identity during the transaction, which digital identity includes the SecureCode." Simply put, in *Franklin et al.* there is no request for authentication that includes anything akin to the recited SecureCode. *Franklin et al.* does not use the temporary transaction number to AUTHENTICATE the user. *See Aff. Kamrani, ¶ 8.* Rather, the system of *Franklin et al.* uses the temporary transaction number to AUTHORIZE a credit card transaction with the bank. *See Aff. Kamrani, ¶ 8.* Authentication is an entirely different process than credit card authorization. *See Aff. Kamrani, ¶ 6-7.* Credit card authorization merely confirms that the temporary transaction number is a valid account number and there are sufficient funds to pay the desired transaction. *See Aff. Kamrani, ¶ 7.* In contrast, authentication is a process by which the authenticator states that the individual is who the individual says he is. *See Aff. Kamrani, ¶ 6.* Thus, *Franklin et al.* fails to disclose receiving a request for authentication that includes the SecureCode as recited in claim 1.

Third, claim 1 recites "authenticating ... the user during the transaction if the digital identity is valid." The digital identity is recited to include the SecureCode. *Franklin et al.* does not authenticate the user based on the temporary transaction number, hence *Franklin et al.* also fails to disclose this claim element, which also appears in independent claim 21.

Thus, for at least these three reasons the Applicants respectfully submit that the claims at issue are neither anticipated by nor rendered obvious by *Franklin et al.* Reconsideration and withdrawal of the rejection of these claims is respectfully requested.

CLAIMS ARE PATENTABLE OVER *FRANKLIN ET AL.* AND *JOHNSON*

The Office Action rejected claims 50 and 52 under 35 U.S.C. § 103(a) as being unpatentable over *Franklin et al.* in view of U.S. Patent Application Publication No. 2005/0222963 A1 [hereinafter "*Johnson*"]. The Office Action contends that *Franklin et al.* discloses all of the elements of the claims at issue, except that the SecureCode is alphanumeric, for which the Office Action cites *Johnson* and then argues that "it would have been obvious to one of ordinary skill in the art at the time of the invention to utilize an alphanumerical ID for the online transactions as taught in Johnson in the system of Franklin because it would uniquely identifies [sic] the web customer (see Johnson, [0024])." The Applicants respectfully disagree with the Office Action's characterization of these references vis-à-vis the claims at issue.

The transaction number used in *Franklin et al.* cannot be alphanumerical because it must look exactly like a credit card number. *See, e.g.*, *Franklin et al.*, Abstract "The transaction number looks like a real card number and the merchant handles the transaction number in the same manner as any regular credit card number." Therefore, the transaction number of *Franklin et al.* cannot be replaced with an alphanumeric value because an alphanumeric value would not look like a real credit card number and could not be processed by the merchant in the same manner as any regular credit card number. Thus, *Johnson* and *Franklin et al.* cannot be combined in the manner suggested by the Office Action; hence the claims at issue remain patentable over these two references. Thus, the combination of *Franklin et al.* and *Johnson* also fails to present a *prima facie* case of obviousness. The Applicants therefore respectfully request reconsideration and withdrawal of the rejection of these claims.

CLAIMS ARE PATENTABLE OVER *FRANKLIN ET AL.* AND CERTAIN OFFICIAL NOTICE

The Office Action rejected claim 44 under 35 U.S.C. § 103(a) as being unpatentable over *Franklin et al.* and further in view of certain Official Notice. The Office Action contends that *Franklin et al.* discloses all of the elements of the claim at issue, except for "wherein said Eternal-Entity and said Central-Entity are the same entity," for which the Office Action provides certain Official Notice. The Office Action takes Official Notice for this teaching missing from *Franklin et al.* Even assuming *arguendo* that the Office Action's citation of Official Notice is proper, because claim 44 directly depends from independent claim 1, which has been shown to be patentable over *Franklin et al.*, claim 44 remains patentable over *Franklin et al.* for at least the same reasons discussed above. The Applicants therefore respectfully request reconsideration and withdrawal of the rejection of this claim.

CONCLUSION

The Applicant respectfully submits this application is in condition for allowance and requests issuance of a Notice of Allowance.

Although not believed necessary, the Office is hereby authorized to charge any fees required under 37 C.F.R. § 1.16 or § 1.17 or credit any overpayments to the deposit account of MICHAEL P FORTKORT PC, Deposit Account No. 50-3776.

In the event the prosecution of this Application can be efficiently advanced by a phone discussion, it is requested that the undersigned attorney be called at (703) 435-9390.

Respectfully submitted,

By /Michael P. Fortkort/ Date: November 12, 2010
Michael P. Fortkort (Reg. No. 35,141)

MICHAEL P FORTKORT PC
The International Law Center
13164 Lazy Glen Lane
Oak Hill, Virginia 20171

Please direct telephone calls to:
Michael P. Fortkort
703-435-9390
703-435-8857 (facsimile)

Certification Under 37 C.F.R. § 1.8

I hereby certify that on November 12, 2010 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: November 12, 2010 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 12/210,926

FILING DATE: September 15, 2008

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

ATTORNEY DOCKET: KAMR002US0

CONFIRMATION NO.: 7516

VIA ELECTRONIC FILING SYSTEM
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

AFFIDAVIT UNDER RULE 132

Applicants hereby submit this affidavit in support of their response to the Office Action mailed September 17, 2010 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 12/210,926, and pursuant to the provisions of 37 C.F.R. § 1.132. The witness hereby avers and testifies as follows:

1. I am Nader Asghari-Kamrani, one of the inventors listed in U.S. Patent Application No. 12/210,926, which is the subject of the present proceeding.

2. I received a degree in computer science from the Technical University of Vienna, in Vienna, Austria in 1993. I have been working in the field of authentication over communication networks since 2000. I am one of skill in the art of authentication and electronic transactions.

3. In 2003, I obtained an Accredited ACH Professional certification from NACHA (The Electronic Payment Association). There are only approximately 3500 professionals with this certification in the United States.

4. I am familiar with the specification and claims of the present Application as pending and as amended in accordance with a response filed concurrently herewith.

5. I have reviewed the art cited by the Examiner in the present proceeding and in particular, U.S. Patent No. 5,883,810 (*Franklin et al.*).

6. One of skill in the authentication art would understand that authentication of a user involves determining whether a user is, in fact, who he or she claims to be. This is supported by, for example, Exhibit A to this Affidavit, which is from a recent publication by Hitachi ID Systems that that defines authentication as "Authentication is any process by which a system verifies the identity of a User who wishes to access it."

7. In contrast, one of skill in the art of authentication would understand the difference between authentication and credit card authorization that occurs during a credit card payment transaction, which involves receiving a user's credit card information for payment and sending the customer's credit card and order information to the customer's issuing bank for payment approval before deciding whether or not to fulfill a user's order. Exhibit B to this Affidavit describes authorization as "An authorization is an approval on a cardholder account for a sale amount." Exhibit C to this Affidavit states: "The term "authorization" refers to the

process of verifying with a prepaid card issuer that an account has sufficient funds available and is in good standing. When a prepaid debit card transaction is 'authorized,' the available balance of the account is reduced by the authorized amount."

8. One of skill in the art of authentication would understand that the temporary transaction number of *Franklin et al.* is not used for authentication of the user but rather for authorization of payment.

I affirm that all statements made herein of my own knowledge are true, and that all statements made herein on information and belief are believed to be true. I understand that willful false statements and the like are punishable by fine or imprisonment, or both (18 U.S.C. 1001), and may jeopardize the validity of the present patent application or any patent issuing thereon.

FURTHER AFFIANT SAYETH NOT.

It witness whereof,

11/12/2010

Nader Asghari-Kamrani

Date

EXHIBIT A

Definition of Authentication

Authentication is any process by which a system verifies the identity of a User who wishes to access it. Since Access Control is normally based on the identity of the User who requests access to a resource, Authentication is essential to effective Security.

Authentication may be implemented using Credentials, each of which is composed of a User ID and Password. Alternately, Authentication may be implemented with Smart Cards, an Authentication Server or even a Public Key Infrastructure.

Users are frequently assigned (with or without their knowledge) Tickets, which are used to track their Authentication state. This helps various systems manage Access Control without frequently asking for new Authentication information.

Hitachi ID Systems, Inc.

500, 1401 - 1 Street SE, Calgary AB Canada T2G 2J3 Tel: 1.403.233.0740 Fax: 1.403.233.0735 E-Mail: sales@Hitachi-ID.com

www.Hitachi-ID.com

EXHIBIT B

Authorizations

An authorization is an approval on a cardholder account for a sale amount. An authorization hold is a reduction of the cardholder's credit line for the amount of the sale. This hold can remain on the cardholder's account for up to 30 days, depending upon the issuing bank policy.

When you're conducting a transaction and you need an authorization, remember that the authorization must be for the identical sale amount. If you receive an authorization for the wrong amount, delete the incorrect authorization, and re-authorize for the exact dollar amount. However, you can pre-authorize for a different amount than the sale amount if you're in any of these industries: car rental, hotel, mail/telephone order, or restaurant.

Here are some typical authorization methods, followed by some common response codes and what you should do in each case.

Authorization methods

- **Terminal:** Obtained electronically through your terminal by magnetically swipe reading or manually entering the credit card number.
- **Voice:** Obtained when a when contact is made with our authorization center, either through the automated system or when speaking to a representative at the authorization center.
- **Direct solutions/Autobats:** Obtained when you compile your sales at the end of the day and transmit them to Wells Fargo Merchant Services electronically. Wells Fargo Merchant Services will then authorize and process the merchant sales.
- **Tape authorizations:** Obtained through a personal computer or a terminal. Works in the same manner as a terminal authorization.
- **Tape ECR (Electronic Cash Register):** Works in the same manner as a terminal authorization.

Response codes

Approved. Normally followed by a 2 to 6 digit code.

Declined. If you receive this response you should never accept the card. Request another form of payment. If you receive an authorization from an alternate source, such as the issuing bank, after receiving a decline message through the terminal or VRU, you may be subject to chargebacks and cancellation of your sales agreement.

If a foreign card gets a referral message, the authorization center should contact the issuing bank for further information. Due to the time differences to reach these countries, it may take up to two business days to get an authorization response. An authorization representative will contact you with the response when it's received. Wait before processing the transaction — or providing the customer with the merchandise. If the response is a referral response or an authorization by phone, the authorization/transaction must be force entered.

Referral. This response indicates the card issuer is requesting direct contact with the business in order to authorize the sale. Contact the Wells Fargo Merchant Services authorization center for Visa®, MasterCard®, and Discover® Network. For American Express, contact the appropriate authorization center.

Hold card/Call center. Indicates that the card issuer is requesting the card be removed from circulation. Never accept the credit card for payment when this response is received.

Call center. This response indicates the card issuer is requesting direct contact with the business in order to authorize the sale. Contact the Wells Fargo Merchant Services authorization center for Visa®, MasterCard®, and Discover® Network. For American Express, contact the appropriate authorization center.

EXHIBIT C

getdebit | Helping you choose and use the right prepaid debit card.

GIFT CARDS PREPA

Prepaid Debit Card > Debit Card Glossary > Authorization

Authorization

The term "authorization" refers to the process of verifying with a prepaid card issuer that an account has sufficient funds available and is in good standing. When a prepaid debit card transaction is "authorized", the available balance of the account is reduced by the authorized amount.

In some types of prepaid debit card transactions (such as "pay at the pump" gasoline purchases, hotel room transactions, or car rental transactions), an authorization hold may be placed on the account which is larger than the actual transaction amount.

C
E
C
A
C
B

More Filed under: Glossary

Other Prepaid Card Terms & Information You Should Know:

Skimming
Network Branded Prepaid Cards
Settlement bank
Automated Teller Machine (ATM)
Rebate Card

About

About Us
Contact Info
Advertisers
Affiliate Program
Privacy and Terms

Prepaid Cards

Best Prepaid Cards
Prepaid Visa Cards
Prepaid MasterCards
Prepaid Discover Cards
Prepaid American Express Cards
Visa Gift Cards
Tax Refund Cards

Learn

Debit Card News
Debit Card Rights
Debit Card Fees
Gift Card Balance
Prepaid Glossary
Learning Center

Electronic Acknowledgement Receipt

EFS ID:	8828715
Application Number:	12210926
International Application Number:	
Confirmation Number:	7516
Title of Invention:	Centralized Identification and Authentication System and Method
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Customer Number:	58293
Filer:	Michael P. Fortkort
Filer Authorized By:	
Attorney Docket Number:	KAMR002US0
Receipt Date:	12-NOV-2010
Filing Date:	15-SEP-2008
Time Stamp:	16:21:29
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	Amendment/Req. Reconsideration-After Non-Final Reject	12210926_Response_to_OA_mailed_091710_filed_111210.pdf	74520 1838adbe5e89b165de109d5b095bb7675d9f612f	no	18

Warnings:

Information:

2	Rule 130, 131 or 132 Affidavits	12210926_132_Affidavit_filed_111210.pdf	4108879 69031a57e2bfb7bcd0c86b62908a4ab363d3d156	no	7
Warnings:					
Information:					
		Total Files Size (in bytes):	4183399		

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 (07-06)
Approved for use through 1/31/2007. 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 12/210,926	Filing Date 09/15/2008	□ To be Mailed

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	
□ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
□ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			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 $250 ($125 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			TOTAL	

APPLICATION AS AMENDED – PART II

		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
AMENDMENT	**11/12/2010**	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 60	Minus	** 62	= 0	X $26 =	0	OR	X $ =	
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $110 =	0	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	**0**	OR	TOTAL ADD'L FEE	

		(Column 1)		(Column 2)	(Column 3)					
AMENDMENT		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 number found in the appropriate box in column 1.

Legal Instrument Examiner:
/LINDA WISE/

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.

Doc Code: M865 or FAI.REQ.INTV

PTOL-413A (08-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Applicant Initiated Interview Request Form

Application No.: 12/210,926 First Named Applicant: NADER ASGHARI-KAMRANI
Examiner: NOBAHAR, ABDULHAKIM Art Unit: 2432 Status of Application: NON-FINAL REJECTION MAILED

Tentative Participants:
(1) MICHAEL P. FORTKORT (2) NADER ASGHARAI-KAMRANI

(3) KAMRAN ASCHARI-KAMRANI (4) ____________________

Proposed Date of Interview: NOVEMBER 10, 2010 **Proposed Time:** 11:00 A.M. **(AM/PM)**

Type of Interview Requested:
(1) [ ] Telephonic (2) [✓] Personal (3) [ ] Video Conference

Exhibit To Be Shown or Demonstrated: [ ] YES [✓] NO
If yes, provide brief description: ____________________

Issues To Be Discussed

Issues (Rej., Obj., etc)	**Claims/ Fig. #s**	**Prior Art**	**Discussed**	**Agreed**	**Not Agreed**
(1) REJECTION	ALL	FRANKLIN AND JOHNSON	[✓]	[ ]	[ ]
(2)			[ ]	[ ]	[ ]
(3)			[ ]	[ ]	[ ]
(4)			[ ]	[ ]	[ ]

[ ] Continuation Sheet Attached [ ] Proposed Amendment or Arguments Attached
Brief Description of Arguments to be Presented: DIFFERENCES BETWEEN CLAIMS AND CITED ART

An interview was conducted on the above-identified application on NOVEMBER 10, 2010

__NOTE__: This form should be completed and filed by applicant in advance of the interview (see MPEP § 713.01). If this form is signed by a registered practitioner not of record, the Office will accept this as an indication that he or she is authorized to conduct an interview on behalf of the principal (37 CFR 1.32(a)(3)) pursuant to 37 CFR 1.34. This is not a power of attorney to any above named practitioner. See the Instruction Sheet for this form, which is incorporated by reference. By signing this form, applicant or practitioner is certifying that he or she has read the Instruction Sheet. After the interview is conducted, applicant is advised to file a statement of the substance of this interview (37 CFR 1.133(b)) as soon as possible. This application will not be delayed from issue because of applicant's failure to submit a written record of this interview.

/MICHAEL P. FORTKORT/
Applicant/Applicant's Representative Signature

Examiner/SPE Signature

MICHAEL P. FORTKORT
Typed/Printed Name of Applicant or Representative

35,141
Registration Number, if applicable

This collection of information is required by 37 CFR 1.133. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 24 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.

Electronic Acknowledgement Receipt

EFS ID:	8756879
Application Number:	12210926
International Application Number:	
Confirmation Number:	7516
Title of Invention:	Centralized Identification and Authentication System and Method
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Customer Number:	58293
Filer:	Michael P. Fortkort
Filer Authorized By:	
Attorney Docket Number:	KAMR002US0
Receipt Date:	03-NOV-2010
Filing Date:	15-SEP-2008
Time Stamp:	08:50:32
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	Letter Requesting Interview with Examiner	Interview_Request_110310_12210926.pdf	302737 65eb05215ed7c1773dc23c39f6f6a649f72499fe	no	1

Warnings:

Information:

Total Files Size (in bytes):	302737

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.
12/210,926	09/15/2008	Nader Asghari-Kamrani	KAMR002US0	7516

58293 7590 09/17/2010

FORTKORT & HOUSTON P.C.
9442 N. CAPITAL OF TEXAS HIGHWAY
ARBORETUM PLAZA ONE, SUITE 500
AUSTIN, TX 78759

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	PAPER NUMBER
2432	
MAIL DATE	DELIVERY MODE
09/17/2010	PAPER

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

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

Office Action Summary	**Application No.** 12/210,926	**Applicant(s)** ASGHARI-KAMRANI ET AL.	
	Examiner ABDULHAKIM NOBAHAR	**Art Unit** 2432	

-- 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* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, 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 *24 August 2010*.

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

3)☐ 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

4)☒ Claim(s) *1-4,12-24,32-41,43-48,50-55,58,60 and 63-80* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4, 12-24, 32-41, 43-48, 50-55, 58, 60 and 63-80* is/are rejected.

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

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

Application Papers

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

10)☐ 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).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

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).

a)☐ All b)☐ Some * c)☐ None of:

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) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

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

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to applicant's amendment filed on 08/24/2010.

2. Claims 1-4, 12-24, 32-41, 43-48, 50-55, 58, 60 and 63-80 are pending.

Response to Arguments

1. Applicant's arguments filed on 08/05/2010 have been fully considered but they are not persuasive.

2. Applicant on pages 15 and 16 of remarks argues that the prior art Franklin does not relate to an authentication process, but rather merely a way to avoid using the actual account number in financial transactions over a public network.

Examiner respectfully disagrees because Franklin discloses that "The certificate request contains the public/private key pair and the temporary PIN, which serves as a baseline authentication of the customer requesting the certificate" (see col. 7, lines 29-32) and "The bank computer 32 receives the signed request and immediately verifies the identity and authenticity of the customer by applying the customer's public key to the digital signature and examining the certificate" (see col. 8, lines 57-60).

3. Applicant on pages 16 and 17 of remarks argues that the digital certificate of the prior art Franklin is not capable of being generated dynamically and then being used during an online transaction to authenticate the user to the External-Entity.

Examiner respectfully disagrees and asserts that Franklin discloses a digital certificate received during the registration phase to be used by the user to request a temporary transaction number for a single use that corresponds to the recited dynamic

SecureCode during a transaction phase (see col. 2, lines 12-21, col. 7, lines 6-17 and col. 7, line 62-col. 8, line 5). Franklin further discloses that the temporary transaction number is generated upon the user request for an online transaction during the transaction (see, e.g., col. 8, lines 15-23 and col. 8, lines 37-56).

4. The applicant's arguments on page 19 that the references cannot be combined in the manner suggested by the Examiner to arrive at the claimed invention have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-4, 12-24, 32-41, 43, 45-48, 51, 53-55, 58, 60 and 63-80 are rejected under 35 U.S.C. 102(b) as being anticipated by Franklin et al (US 5,883,810 A), hereinafter Franklin.

Regarding claims 1, 21 and 74, Franklin discloses:

A method for authenticating a user during an electronic transaction between the user and an External-Entity (see, e.g., col. 8, lines 15-56), the method comprising:

receiving electronically a request for a dynamic SecureCode for the user by a Central-Entity during the transaction between the user and the External-Entity (see, e.g., col. 8, lines 37-42 and col. 9, lines 30-46, where the temporary transaction number corresponds to the recited dynamic SecureCode);

generating during the transaction a dynamic SecureCode for the user in response to the request (see, e.g., col. 8, lines 57-67);

providing said generated SecureCode to the user during the transaction (see, e.g., col. 10, line 6-10),

receiving electronically by a Central-Entity a request for authenticating the user based on a digital identity during the transaction, which digital identity includes the SecureCode (see, e.g., col. 8, lines 24-36, the order form and col. 10, lines 14-20, where the order form which includes the transaction number and other user's information corresponds to the recited digital identity); and

authenticating by the Central-Entity the user during the transaction if the digital identity is valid (see, e.g., col. 10, lines 61-63 and col. 11, lines 31-40).

Regarding claims 2 and 22, Franklin discloses:

A method as recited in claim 1, wherein said user has a pre-existing relationship with the External-Entity (see, e.g., col. 8, line 15+, where before the transaction phase the customer has opened an account with the bank).

Regarding claims 3 and 23, Franklin discloses:

A method as recited in claim 1, wherein said user has no pre-existing relationship with the External-Entity (see, e.g., col. 5, line 23+, where before the registration phase the customer did not have an account with the bank).

Regarding claims 4, 24 and 43, Franklin discloses:

A method as recited in claim 1, further comprising:

combining said generated SecureCode with a user-specific information using a predetermined algorithm to form a combined Secure-Code and user specific information (see, e.g., col. 8, line 60+, The account manager 60 associates the transaction number with the customer account number in a data record on the customer database 64);

maintaining the combined Secure-Code and user specific information at the Central-Entity (see, e.g., Fig. 2, customer database 64 and col. 8, line 60+):

using the predetermined algorithm to combine received user specific information received by the Central-Entity with a received SecureCode received by the Central-Entity to form a combined received SecureCode and received user specific information (see, e.g., col. 11, lines 7-31);

comparing the combined Secure-Code and user specific information with the combined received SecureCode and received user specific information to validate the user (see, e.g., col. 11, lines 11-21).

Regarding claims 12 and 32, Franklin discloses:

A method as recited in claim 1, wherein the External-Entity receives the user's digital identity (see, e.g., col. 8, lines 24-36).

Regarding claims 13 and 33, Franklin discloses:

A method as recited in claim 1, wherein said External-Entity submits a digital identity to the Central-Entity (see, e.g., col. 10, lines 61-67).

Regarding claims 14, 34, 65 and 66, Franklin discloses:

The method of claim 1, wherein said digital identity includes a user-specific information (see, e.g., col. 8, lines 24-36, where the order form contains the user's specific information).

Regarding claims 15, 35, 48, 78 and 79, Franklin discloses:

The method of claim 14, wherein the user-specific information comprises one or more of the following: an alphanumeric name, an ID, a login name, and an identification phrase, wherein said identification phrase comprises one or more of the following: an account number, a telephone number, an IP address, a hardware key, a software key, a session ID, a token and serial number (see, e.g., col. 6, lines 25-32).

Regarding claims 16 and 36, Franklin discloses:

The method of claim 1, wherein the transaction corresponds to a financial transaction (see, e.g., col. 3, lines 34-47).

Regarding claims 17 and 37, Franklin discloses:

The method of claim 1, wherein the transaction corresponds to a non-financial transaction (see, e.g., col. 1, lines 19-25, order goods and/or services, where services may include non-financial transaction such as accessing secured information, application, web sites or other resources).

Regarding claims 18 and 38, Franklin discloses:

The method of claim 1, wherein the transaction corresponds to access to restricted web-site or restricted computer/server (see, e.g., col. 1, lines 19-25, order goods and/or services, where services may include non-financial transaction such as accessing secured information, application , web sites or other resources).

Regarding claims 19 and 39, Franklin discloses:

The method of claim 1, wherein said transaction occurs over a communication network, wherein said communication network comprises one or more of the following: an Internet, a wireless network, a mobile network, a satellite, and a private network (see, e.g., Fig. 1).

Regarding claims 20, 40, 51, 53-55 and 58, Franklin discloses:

The method of claim 1, wherein said transaction occurs over a communication network to which is coupled said user, said Central-Entity, and said External-Entity (see, e.g., Fig. 1).

Regarding claim 41, Franklin discloses:

A method as recited in claim 4, wherein said External-Entity is using said algorithmically combined SecureCode to authenticate a user's identity (see, e.g., col. 8, lines 24-36, the order form is a combination of the transaction number and other user's related information).

Regarding claims 45 and 75, Franklin discloses:

The method as recited in claim 1, wherein said SecureCode becomes invalid after being used for authentication (see, e.g., col. 2, lines 12-20, for a single transaction).

Regarding claims 46 and 76, Franklin discloses:

The method as recited in claim 1, wherein the SecureCode becomes invalid when a predefined period of time passes (see, e.g., col. 2, lines 12-20, where “a short expiration term" corresponds to the recited predefined period of time).

Regarding claims 47 and 77, Franklin discloses:

The method as recited in claim 1, wherein said Central-Entity generates SecureCode with dependence on one or more alphanumeric values (see, e.g., col. 4, lines 4855, where the transaction number is associated with other information means that the transaction number is dependent on some alphanumeric values).

Regarding claim 60, Franklin discloses:

The method as recited in claim 58, wherein said request is initiated by a user through a standard interface provided to said user (see, e.g., col. 5, lines 55-60).

Regarding claim 63, Franklin discloses:

The apparatus according to claim 21, wherein said first Central-Entity computer and said second Central-Entity computer are the same (see, e.g., col. 10, lines 61-67 and Fig. 5).

Regarding claim 64, Franklin discloses:

The apparatus according to claim 21, wherein said first Central-Entity computer and said second Central-Entity computer are different (see, e.g., col. 10, lines 48-60, where the computer of the merchants acquiring bank is different from the computer of the issuing bank).

Regarding claims 67, 68, 71 and 72, Franklin discloses:

A method as recited in claim 1, wherein said digital identity is invalid if the SecureCode is invalid (see, e.g., col. 2, lines 52-55, col. 10, lines 61-67).

Regarding claims 69, 70, 73 and 80, Franklin discloses:

A method as recited in claim 1, wherein said External-Entity authenticates the user upon receiving an affirmation authentication message from the Central-Entity (see, e.g., col. 11, lines 40-45).

Claim Rejections - 35 USC § 103

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

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, 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.

Claims 50 and 52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Franklin et al (US 5,883,810 A), hereinafter Franklin in view of Johnson (US 2005/0222963 A1).

Regarding claims 50 and 52, Franklin does not expressly disclose that the SecureCode is alphanumeric. Johnson, however, discloses that the ID that the web customer receives from his bank to conduct e-commerce transaction is alphanumerical. Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to utilize an alphanumerical ID for the online transactions as taught in Johnson in the system of Franklin because it would uniquely identifies the web customer (see Johnson, [0024]).

Claim 44 is rejected under 35 U.S.C. 103(a) as being unpatentable over Franklin et al (US 5,883,810 A); hereinafter Franklin in view of the examiner Official Notice.

Regarding claim 44, Franklin does not expressly disclose:
wherein said External-Entity and said Central-Entity are the same entity.

Official Notice is taken that it is old and well-known practice in the art that some institutions such as banks that maintain users' accounts, the providers of email services to users and some the department stores which provide their own credit cards to the customers, directly authenticate the users when the users requires services or accessing their web sites, without receiving authentication services from a third party. Whenever users and customers logging on to their banks web sites, or their provider's website for email services or a customer purchasing goods using a department store's credit card, the users and customers are authenticated by the respective institution independent from a. In this case the Central-Entity and the External-Entity are the same institution that having an account for the user or the customer. Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to modify the system of Franklin to have one entity to be as the same Central-Entity and External-Entity. The deployment of one entity to issue a SecurCode to a user and also to authenticate the user when using the SecurCode would make the system of Franklin a versatile and a flexible system, in another word a scalable system.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ABDULHAKIM NOBAHAR whose telephone number is (571)272-3808. The examiner can normally be reached on M-T 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. 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.

Abdulhakim Nobahar
Examiner
Art Unit 2432

/A. N./
Examiner, Art Unit 2432

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432

Index of Claims	**Application/Control No.** 12210926	**Applicant(s)/Patent Under Reexamination** ASGHARI-KAMRANI ET AL.
	Examiner ABDULHAKIM NOBAHAR	**Art Unit** 2432

✓	**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	07/06/2009	11/20/2009	04/28/2010	09/12/2010					
	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.** 12210926	**Applicant(s)/Patent Under Reexamination** ASGHARI-KAMRANI ET AL.
	Examiner ABDULHAKIM NOBAHAR	**Art Unit** 2432

✓	**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	07/06/2009	11/20/2009	04/28/2010	09/12/2010					
	37	✓	✓	✓	✓					
	38	✓	✓	✓	✓					
	39	✓	✓	✓	✓					
	40	✓	✓	✓	✓					
	41	✓	✓	✓	✓					
	42	✓	-	✓	-					
	43	✓	✓	✓	✓					
	44	✓	✓	✓	✓					
	45	✓	✓	✓	✓					
	46	✓	✓	✓	✓					
	47	✓	✓	✓	✓					
	48	✓	✓	✓	✓					
	49	✓	-	-	-					
	50	✓	✓	✓	✓					
	51	✓	✓	✓	✓					
	52	✓	✓	✓	✓					
	53	✓	✓	✓	✓					
	54	✓	✓	✓	✓					
	55	✓	✓	✓	✓					
	56	✓	-	-	-					
	57	✓	-	-	-					
	58	✓	✓	✓	✓					
	59	✓	-	-	-					
	60	✓	✓	✓	✓					
	61	✓	-	-	-					
	62	✓	-	-	-					
	63				✓					
	64				✓					
	65				✓					
	66				✓					
	67				✓					
	68				✓					
	69				✓					
	70				✓					
	71				✓					
	72				✓					

Index of Claims	Application/Control No. 12210926	Applicant(s)/Patent Under Reexamination ASGHARI-KAMRANI ET AL.
	Examiner ABDULHAKIM NOBAHAR	Art Unit 2432

✓	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	07/06/2009	11/20/2009	04/28/2010	09/12/2010					
	73				✓					
	74				✓					
	75				✓					
	76				✓					
	77				✓					
	78				✓					
	79				✓					
	80				✓					

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	12/210,926	Filing Date	2008-09-15	Docket Number (if applicable)	KAMR002US0	Art Unit	2432
First Named Inventor	NADER ASGHARI-KAMRANI			Examiner Name	MR. ABDULHAKIM NOBAHAR		

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, 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 AMENDMENT AND AFFIDAVIT UNDER RULE 132 FILED AUGUST 5, 2010

□ 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 503776

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature
□ Applicant Signature

Doc code: RCEX
Doc description: Request for Continued Examination (RCE)

PTO/SB/30EFS (07-09)
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.

Signature of Registered U.S. Patent Practitioner

Signature	/Michael P. Fortkort/	Date (YYYY-MM-DD)	2010-08-24
Name	MICHAEL P. FORTKORT	Registration Number	35141

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 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.

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.

Electronic Patent Application Fee Transmittal

Application Number:	12210926
Filing Date:	15-Sep-2008
Title of Invention:	Centralized Identification and Authentication System and Method
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Filer:	Michael P. Fortkort
Attorney Docket Number:	KAMR002US0

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	38	26	988
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 1 month with $0 paid	2251	1	65	65
Miscellaneous:				
Request for continued examination	2801	1	405	405
			Total in USD ($)	**1458**

Electronic Acknowledgement Receipt

EFS ID:	8275395
Application Number:	12210926
International Application Number:	
Confirmation Number:	7516
Title of Invention:	Centralized Identification and Authentication System and Method
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Customer Number:	58293
Filer:	Michael P. Fortkort
Filer Authorized By:	
Attorney Docket Number:	KAMR002US0
Receipt Date:	24-AUG-2010
Filing Date:	15-SEP-2008
Time Stamp:	08:06:30
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$1458
RAM confirmation Number	7707
Deposit Account	503776
Authorized User	FORTKORT,JOHN A
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	Request for Continued Examination (RCE)	RCE_12210926_filed_082410.pdf	798077 2975e98a8186c2ac2f24efb30c9a36d183baa595	no	3
Warnings:					
Information:					
2	Fee Worksheet (PTO-875)	fee-info.pdf	33619 f70b24b39d1376b1b01eb38d0cedf62cadf3d1ec	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	831696	

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.

Electronic Acknowledgement Receipt

EFS ID:	8275395
Application Number:	12210926
International Application Number:	
Confirmation Number:	7516
Title of Invention:	Centralized Identification and Authentication System and Method
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Customer Number:	58293
Filer:	Michael P. Fortkort
Filer Authorized By:	
Attorney Docket Number:	KAMR002US0
Receipt Date:	24-AUG-2010
Filing Date:	15-SEP-2008
Time Stamp:	08:06:30
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$1458
RAM confirmation Number	7707
Deposit Account	503776
Authorized User	FORTKORT,JOHN A

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	Request for Continued Examination (RCE)	RCE_12210926_filed_082410.pdf	798077 2975e98a8186c2ac2f24efb30c9a36d183baa595	no	3
Warnings:					
Information:					
2	Fee Worksheet (PTO-875)	fee-info.pdf	33619 f70b24b39d1376b1b01eb38d0cedf62cadf3d1ec	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	831696		

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 (07-06)
Approved for use through 1/31/2007. 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 12/210,926	Filing Date 09/15/2008	□ To be Mailed

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	
□ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
□ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			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 $250 ($125 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			TOTAL	

APPLICATION AS AMENDED – PART II

		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
AMENDMENT	**08/24/2010**	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 59	Minus	** 62	= 0	X $26 =	0	OR	X $ =	
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $110 =	0	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	**0**	OR	TOTAL ADD'L FEE	

		(Column 1)		(Column 2)	(Column 3)					
AMENDMENT		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 number found in the appropriate box in column 1.

Legal Instrument Examiner:
/FRANCES Y. FIELDS/

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.
12/210,926	09/15/2008	Nader Asghari-Kamrani	KAMR002US0	7516

58293 7590 08/20/2010

FORTKORT & HOUSTON P.C.
9442 N. CAPITAL OF TEXAS HIGHWAY
ARBORETUM PLAZA ONE, SUITE 500
AUSTIN, TX 78759

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	**PAPER NUMBER**
2432	
MAIL DATE	**DELIVERY MODE**
08/20/2010	PAPER

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

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

Advisory Action Before the Filing of an Appeal Brief	**Application No.** *12/210,926*	**Applicant(s)** ASGHARI-KAMRANI ET AL.	
	Examiner ABDULHAKIM NOBAHAR	**Art Unit** 2432	

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

THE REPLY FILED 05 August 2010 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:

   a) ☒ The period for reply expires *3* months from the mailing date of the final rejection.

   b) □ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

   Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. □ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☒ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because

   (a) ☒ They raise new issues that would require further consideration and/or search (see NOTE below);

   (b) □ They raise the issue of new matter (see NOTE below);

   (c) □ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or

   (d) ☒ They present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: *Claims 63-80 are added new claims and equal number of claims have not been cancelled via the proposed amendments. Claim 4 and the added new claims 63-80 also contain elements that are not included in the original and previously amended claims and thus requiring further consideration/search* . (See 37 CFR 1.116 and 41.33(a)).

4. □ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).

5. □ Applicant's reply has overcome the following rejection(s): _____.

6. □ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).

7. ☒ For purposes of appeal, the proposed amendment(s): a) ☒ will not be entered, or b) □ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.

   The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: _____.
   Claim(s) objected to: _____.
   Claim(s) rejected: *1-4,12-24,32-41,43-48,50-55,58 and 60*.
   Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☒ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).

9. □ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).

10. □ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. □ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: _____.

12. □ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). _____

13. □ Other: _____.

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432

/A. N./
Examiner, Art Unit 2432

Certification Under 37 C.F.R. § 1.8

I hereby certify that on August 5, 2010 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: August 5, 2010 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 12/210,926

FILING DATE: September 15, 2008

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

ATTORNEY DOCKET: KAMR002US0

CONFIRMATION NO.: 7516

VIA ELECTRONIC FILING SYSTEM
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

Do not enter
/a.n./ 08/18/2010

RESPONSE TO OFFICE ACTION

Sir:

In response to the Office Action mailed May 5, 2010, the Applicants hereby respectfully submit the following amendments and remarks:

Amendments to the Claims begin on page 2.

Remarks begin on page 15.

Certification Under 37 C.F.R. § 1.8

I hereby certify that on August 5, 2010 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: August 5, 2010 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 12/210,926

FILING DATE: September 15, 2008

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

ATTORNEY DOCKET: KAMR002US0

CONFIRMATION NO.: 7516

VIA ELECTRONIC FILING SYSTEM
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

RESPONSE TO OFFICE ACTION

Sir:

In response to the Office Action mailed May 5, 2010, the Applicants hereby respectfully submit the following amendments and remarks:

Amendments to the Claims begin on page 2.

Remarks begin on page 15.

In the Claims:

Please amend the claims as follows:

1. (Currently Amended) A method for authenticating a user ~~in~~ during an electronic ~~e-commerce~~ transaction between the user and an External-Entity ~~for a transaction based on a digital identity issued by a Central-Entity~~, the method comprising:

~~a. the user communicates with an External-Entity to perform a secure transaction with the External-Entity;~~

~~b. the External-Entity requires the user to authenticate itself by providing a valid digital identity before executing the transaction;~~

~~c.~~ receiving electronically a request for a dynamic SecureCode for the user ~~establishes communication with the~~ by a Central-Entity during the transaction between the user and the External-Entity ~~and submits a request for a dynamic SecureCode in response to the External-Entity's requirement~~;

~~d. the Central-Entity:~~

~~i. dynamically~~ generating ~~generates~~ during the transaction a dynamic SecureCode for the user in response to the ~~user~~ request;~~, wherein said SecureCode is alphanumeric;~~

~~ii. algorithmically combines said generated SecureCode with user-specific information before providing the SecureCode to the user;~~

~~iii. maintains a copy of said generated SecureCode; and~~

~~iv. provides~~ providing said generated SecureCode to the user during the transaction;~~,~~

~~e. the External-Entity receives a digital identity from the user, wherein the digital identity~~

~~comprises a UserName and said generated SecureCode, and forwards said digital identity to the Central-Entity for authentication of the user;~~

receiving electronically by a Central-Entity a request for authenticating the user based on a digital identity during the transaction, which digital identity includes the SecureCode; and

authenticating by the Central-Entity the user during the transaction if the digital identity is valid

~~f. the Central-Entity receives said digital identity, validates said digital identity based on said SecureCode maintained in its system, and if valid, then authenticates the user and sends an affirmation message to the External-Entity; and~~

~~g. upon receipt of an affirmation message from the Central-Entity, the External-Entity executes the transaction~~.

2. (Original) A method as recited in claim 1, wherein said user has a pre-existing relationship with the External-Entity.

3. (Original) A method as recited in claim 1, wherein said user has no pre-existing relationship with the External-Entity.

4. (Currently Amended) A method as recited in claim 1, further comprising:

combining said generated SecureCode with a user-specific information using a predetermined algorithm to form a combined Secure-Code and user specific information;

maintaining the combined Secure-Code and user specific information at the Central-Entity;

using the predetermined algorithm to combine received user specific information received by the Central-Entity with a received SecureCode received by the Central-Entity to form a combined received SecureCode and received user specific information;

comparing the combined Secure-Code and user specific information with the combined received SecureCode and received user specific information to validate the user

~~wherein said External-Entity and said Central-Entity use a SecureCode that is algorithmically combined with said user-specific information~~.

5-11. (Cancelled)

12. (Currently Amended) A method as recited in claim 1, wherein said External-Entity receives the user's digital identity ~~is based on a logical combination of the SecureCode and the user-specific information~~.

13. (Currently Amended) A method as recited in claim 1, wherein said External-Entity submits a digital identity to the Central-Entity ~~is based on the SecureCode and the user-specific information~~.

14. (Currently Amended) The method of claim 1, wherein said digital identity includes a ~~the~~ user-specific information ~~comprises UserName~~.

15. (Currently Amended) The method of claim 14, wherein the user specific information comprises ~~corresponds to a~~ one or more of the following: an alphanumeric name, an ID, a login

name, and an identification phrase, wherein said identification phrase comprises one or more of the following: ~~is~~ an account number, a telephone number, an IP address, a hardware key, a software key, a session ID, a token ~~or~~ and a serial number.

16. (Original) The method of claim 1, wherein the transaction corresponds to a financial transaction.

17. (Original) The method of claim 1, wherein the transaction corresponds to a non-financial transaction.

18. (Currently Amended) The method of claim 1, wherein the transaction corresponds to access to restricted web-site or restricted computer/server.

19. (Currently Amended) The method of claim 1, wherein said transaction ~~communication is done~~ ~~on~~ occurs over a communication network, wherein said communication network ~~is~~ comprises one or more of the following: an Internet, a wireless network, a mobile network, a satellite network, ~~or~~ and a private network.

20. (Currently Amended) The method of claim 1, wherein said transaction ~~communication is done on~~ occurs over a communication network to which is coupled ~~including~~ said user, said Central-Entity, and said External-Entity.

21. (Currently Amended) An apparatus ~~system~~ for authenticating a user during an

electronic ~~in e-commerce for a~~ transaction with an External-Entity ~~based on a digital identity issued by a Central-Entity~~, the apparatus ~~system~~ comprising:

~~a. the user in communication with an External-Entity to perform a secure transaction with the External-Entity;~~

~~b. the External-Entity requires the user to authenticate itself by providing a valid digital identity before executing the transaction;~~

~~c. the user in communication with the Central-Entity and with a request for a dynamic SecureCode in response to the External-Entity's requirement;~~

~~d. the~~ a first Central-Entity computer adapted to:

~~i. dynamically~~ generate a dynamic SecureCode for the user in response to ~~the user~~ a request during the transaction~~, wherein said SecureCode is alphanumeric~~;

~~ii. algorithmically combine said generated SecureCode with user-specific information before providing the SecureCode to the user;~~

~~iii. maintain a copy of said generated SecureCode;~~ and

~~iv.~~ provide said SecureCode to the user~~;~~

~~e. the External-Entity adapted to receive a digital identity from the user, wherein the digital identity comprises a UserName and said generated SecureCode, and to forward said digital identity to the Central-Entity to authenticate the user~~;

~~f.~~ a second ~~the~~ Central-Entity computer ~~further~~ adapted to validate ~~the received~~ a digital identity, which includes said SecureCode, and authenticate the user if the digital identity is valid ~~digital identity based on said SecureCode~~ ~~maintained in its system, and if valid, then to authenticate the user, and send an affirmation message to the External-Entity; and~~

~~g. the External-Entity further adapted to execute the transaction upon receipt of an~~

~~affirmation message from the Central-Entity~~.

22. (Currently Amended) ~~A system~~ The apparatus as recited in claim 21, wherein said user has a pre-existing relationship with the External-Entity.

23. (Currently Amended) ~~A system~~ The apparatus as recited in claim 21, wherein said user has no pre-existing relationship with the External-Entity.

24. (Currently Amended) ~~A system~~ The apparatus as recited in claim 21, wherein said External-Entity and said Central-Entity use a SecureCode that is algorithmically combined with said user-specific information.

25-31. (Cancelled)

32. (Currently Amended) ~~A system~~ The apparatus as recited in claim 21, wherein the user submits a ~~said~~ digital identity to the External-Entity ~~is based on a logical combination of the SecureCode and the user-specific information~~.

33. (Currently Amended) ~~A system~~ The apparatus as recited in claim 21, wherein the External-Entity submits a ~~said~~ digital identity to the Central-Entity ~~is based on the SecureCode and the user-specific information~~.

34. (Currently Amended) ~~A system~~ The apparatus of claim 21, wherein the digital identity

includes a user-specific information ~~comprises UserName~~.

35. (Currently Amended) ~~A system~~ The apparatus of claim 34, wherein the ~~UserName corresponds to~~ user specific information comprises one or more of the following; an alphanumeric name, an ID, a login name, and an identification phrase, wherein said identification phrase comprises one or more of the following: ~~is~~ an account number, a telephone number, an IP address, a hardware key, a software key, a session ID, or token, ~~or~~ and a serial number.

36. (Currently Amended) ~~A system~~ The apparatus of claim 21, wherein the transaction corresponds to a financial transaction.

37. (Currently Amended) ~~A system~~ The apparatus of claim 21, wherein the transaction corresponds to a non-financial transaction.

38. (Currently Amended) ~~A system~~ The apparatus of claim 21, wherein the transaction corresponds to access to restricted web-site or restricted computer/server.

39. (Currently Amended) ~~A system~~ The apparatus of claim 21, wherein said transaction ~~communication is done on~~ occurs over a communication network and wherein said communication network ~~is~~ comprises one or more of the following; an Internet, a wireless network, a mobile network, a satellite network, and a ~~or~~ private network.

40. (Currently Amended) ~~A system~~ The apparatus of claim 21, wherein said transaction

~~communication~~ occurs over a ~~is done on~~ a communication network ~~including~~ to which is coupled said user, said Central-Entity, and said External-Entity.

41. (Previously Presented) A method as recited in claim 4, wherein said External-Entity is using said algorithmically combined SecureCode to authenticate a user's identity.

42. (Cancelled)

43. (Previously Presented) A method as recited in claim 4, wherein said Central-Entity is using said algorithmically combined SecureCode to authenticate a user's identity.

44. (Original) A method as recited in claim 1, wherein said External-Entity and said Central-Entity are the same entity.

45. (Currently Amended) The method as recited in claim 1, wherein said ~~Central-Entity generates a~~ SecureCode ~~that~~ becomes invalid after being used for authentication ~~by one of a timer event and a validation event~~.

46. (Currently Amended) The method as recited in claim 1~~45~~, wherein the SecureCode becomes invalid when a predefined period of time passes.

47. (Original) The method as recited in claim 1, wherein said Central-Entity generates SecureCode with dependence on one or more alphanumeric values.

48. (Currently Amended) The method as recited in claim 47, wherein said one or more alphanumeric values ~~are~~ comprise one or more of the following: an unique key, an ID, a login name, a password, and an identification phrase, wherein said identification phrase ~~is~~ comprises an account number, a telephone number, an IP address, a Hardware key, a software key ~~or~~ a session ID, a token, a seed, and a serial number.

49. (Cancelled)

50. (Currently Amended) The method as recited in claim 1, wherein said ~~digital identity is a~~ SecureCode is alphanumeric.

51. (Original) The method as recited in claim 1, wherein said user communicates with said Central-Entity over a communication network.

52. (Currently Amended) ~~A system~~ The apparatus as recited in claim 21, wherein said ~~digital identity is a~~ SecureCode is alphanumeric.

53. (Original) The method as recited in claim 1, wherein said user communicates with said External-Entity over a communication network.

54. (Currently Amended) ~~A system~~ The apparatus as recited in claim 21, wherein said user communicates with said Central-Entity over a communication network.

55. (Currently Amended) ~~A system~~ The apparatus as recited in claim 21, wherein said user communicates with said External-Entity over a communication network.

56-57. (Cancelled)

58. (Previously Presented) The method as recited in claim 1, wherein said SecureCode is generated based on a request submitted by said user over a communication network.

59. (Cancelled)

60. (Previously Presented) The method as recited in claim 58, wherein said request is initiated by said user through a standard interface provided to said user.

61-62. (Cancelled)

63. (New) The apparatus according to claim 21, wherein said first Central-Entity computer and said second Central-Entity computer are the same.

64. (New) The apparatus according to claim 21, wherein said first Central-Entity computer and said second Central-Entity computer are different.

65. (New) A method as recited in claim 1, wherein said digital identity comprises the SecureCode and a user-specific information.

66. (New) A method as recited in claim 1, wherein said digital identity comprises the SecureCode.

67. (New) A method as recited in claim 1, wherein said digital identity is invalid if the SecureCode is invalid.

68. (New) A method as recited in claim 1, wherein said digital identity is valid if at least the SecureCode is valid.

69. (New) A method as recited in claim 1, wherein said External-Entity authenticates the user upon receiving an affirmation authentication message from the Central-Entity.

70. (New) A method as recited in claim 1, wherein said External-Entity authenticates the user if said Central-Entity authenticates the user based on the SecureCode.

71. (New) The apparatus of claim 21, wherein said digital identity is invalid if the SecureCode is invalid.

72. (New) The apparatus of claim 21, wherein said digital identity is valid if at least the SecureCode is valid.

73. (New) The apparatus of claim 21, wherein said External-Entity authenticates the user upon receiving an affirmation authentication message from the Central-Entity.

74. (New) The apparatus of claim 21, wherein said digital identity comprises the SecureCode.

75. (New) The apparatus of claim 21, wherein said SecureCode becomes invalid after being used for authentication.

76. (New) The apparatus of claim 21, wherein the SecureCode becomes invalid when a predefined period of time passes.

77. (New) The apparatus of claim 21, wherein said Central-Entity generates the SecureCode based on one or more alphanumeric values.

78. (New) The apparatus of claim 78, wherein said one or more alphanumeric values comprise one or more of the following: an unique key, an ID, a login name, a password, and an identification phrase, wherein said identification phrase comprises an account number, a telephone number, an IP address, a Hardware key, a software key, a session id or token, a seed and a serial number.

79. (New) The method of claim 65, wherein the user specific information comprises one

or more of the following: an alphanumeric name, an ID, a login name, and an identification phrase, wherein said identification phrase comprises one or more of the following: an account number, a telephone number, an IP address, a hardware key, a software key, a session id or token and a serial number.

80. (New) The apparatus of claim 21, wherein said External-Entity authenticates the user if said Central-Entity authenticates the user based on the SecureCode.

REMARKS

Claims 1-4, 12-24, 32-41, 43-48, 50-55, 58 and 60 were previously pending. Claims 5-11, 25-31, 42, 49, 56-57, 59 and 61-62 have been previously cancelled without disclaimer of or prejudice to the subject matter contained therein. Claims 1, 4, 12, 13, 14, 15, 18, 19, 20, 21-24, 32-40, 45, 46, 48, 50, 52, 54 and 55 have been amended to more particularly recite the claimed invention. Claims 63-80 have been added to further claim the present invention. Claims 1-4, 12-24, 32-41, 43-48, 50-55, 58, 60 and 63-80 remain pending.

CLAIMS ARE PATENTABLE OVER FRANKLIN ET AL. AND JOHNSON

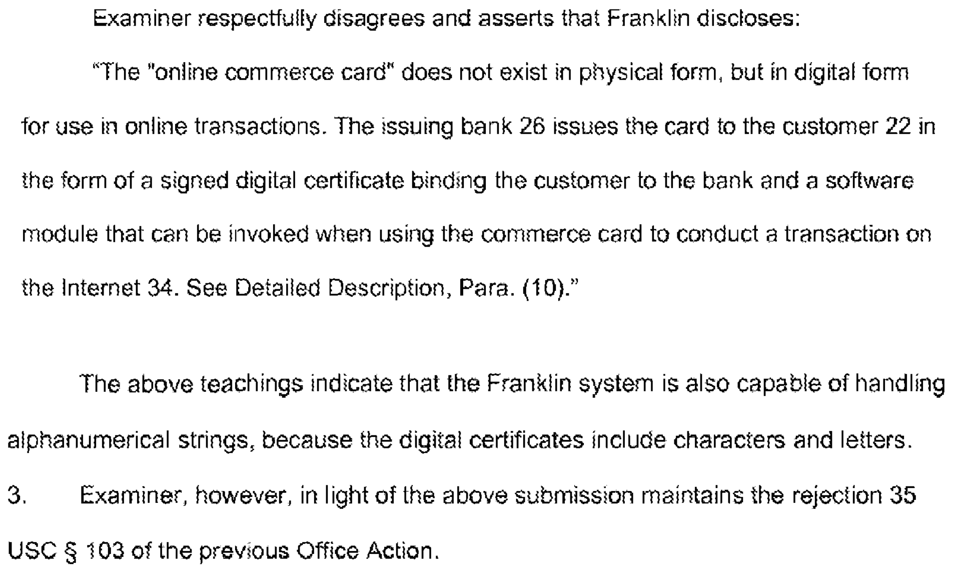
The Examiner rejected claims 1-4, 12-24, 32-39, 43, 45, 46, 50-55, 58 and 60 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,883,810 to *Franklin et al.* [hereinafter "*Franklin et al.*"] in view of U.S. Patent Application Publication No. 2005/0222963 A1) by *Johnson* [hereinafter "*Johnson*"]. The Examiner contends that *Franklin et al.* discloses all of the elements of the claims at issue, except that the SecureCode is alphanumeric, for which the Examiner cites *Johnson.* The Applicants respectfully disagree with the Examiner's characterization of these references vis-à-vis the claims at issue and respectfully request reconsideration and withdrawal of the rejection in light of the following remarks.

The Applicants respectfully submit that the suggested combination of *Franklin et al.* and *Johnson* fails to disclose the claimed invention, and furthermore, that these references cannot be combined in the manner suggested by the Examiner to arrive at the claims at issue because *inter alia* the teaching of *Franklin et al.* does not relate to an authentication process, but rather teaches the use of a temporary transaction number (rather than the actual account number) for payment relating to a financial transaction. *See Kamrani Aff., ¶7.* Simply put, *Franklin et al.* does not disclose an authentication process. *See Kamrani Aff., ¶ 5-13.*

Franklin et al. does not teach an authentication system but merely an online payment processing system that protects a user's actual account number by employing a proxy account number, which is quite different than an authentication process. *See Kamrani Aff., ¶ 6-7.* When authentication is necessary in the system of *Franklin et al.,* in fact, *Franklin et al.* details a rather cumbersome process for authenticating a user, thereby indicating its proxy credit card number technique is not capable of serving as an authentication process, but rather merely a way to avoid using the actual account number in financial transactions over a public network. *See Col. 4, lines 27-47.*

RESPONSE TO EXAMINER'S ARGUMENTS

For convenience of the reader, the Examiner's arguments are reproduced below:



Examiner respectfully disagrees and asserts that Franklin discloses:

"The "online commerce card" does not exist in physical form, but in digital form for use in online transactions. The issuing bank 26 issues the card to the customer 22 in the form of a signed digital certificate binding the customer to the bank and a software module that can be invoked when using the commerce card to conduct a transaction on the Internet 34. See Detailed Description, Para. (10)."

The above teachings indicate that the Franklin system is also capable of handling alphanumerical strings, because the digital certificates include characters and letters.

3. Examiner, however, in light of the above submission maintains the rejection 35 USC § 103 of the previous Office Action.

Digital Certificate of Franklin et al. is Not SecureCode as Disclosed and Claimed

As indicated in the Rule 132 Affidavit submitted herewith, the digital certificate mentioned in *Franklin et al.* is not capable of being generated dynamically and then being used during an online transaction to authenticate the user to the External-Entity. *See Kamrani Aff., ¶ 11-13.* As such, the digital certificate of *Franklin et al.* does not meet the elements of the SecureCode set forth in the claims at issue.

The claims (*e.g.*, claim 1) at issue specifically recite *inter alia* that "the Central-Entity generates a dynamic SecureCode for the user <u>during the transaction</u>" and the dynamic SecureCode is then used during the transaction for authentication of the user. The digital certificate of *Franklin et al.* is not the same as a dynamic SecureCode of the present invention since the dynamic SecureCode is generated during the transaction with the user and the digital certificate cannot be so generated. *See Kamrani Aff., ¶ 11-13.*

During the registration phase of *Franklin et al.*, a customer requests a certificate from an issuing bank. *See, Col. 7, Line 6.* This certificate is only used for conversations between customer and issuing bank. *See Col. 7, Line 62.* This means that the issuing bank uses a customer's certificate to authenticate customer's identity before issuing the transaction number. Moreover, this certificate cannot be generated during the transaction as is the recited SecureCode. *See Kamrani Aff., ¶ 11-13. Also a new certificate cannot be issued for each and every transaction as is the recited SecureCode.*

At column 8, line 43 clearly mentions that the software module installed on customer's computer sends customer's certificate to the issuing bank to request a transaction number. "transaction module 72 prepares a request for a transaction number, digitally signs the request using the customer's private key, and submits the signed request to the issuing bank's computer 32 via the Internet 34 (flow arrow 2 in FIG. 3). **The request contains the certificate originally issued by the bank.**" In other words, this digital certificate is not generated during the transaction, but done previously in a non-real time manner. Here are some citations from *Franklin et al.* that indicate the long and cumbersome process of obtaining the digital certificate, which the present invention seeks to overcome.

Column 5, Line 52:

> The operating system 48 includes a certificate store 50 to securely hold digital certificates. The certificate store 50 holds a signed certificate received from the issuing bank as part of the ***online commerce card***.

Column 7, Line 6:

> The customer receives a PIN mailer three to ten days following application submittal. Upon receiving the PIN, the customer invokes the registration module 56 and prepares a "request for a certificate" from the issuing bank. As part of creating the request for certificate, the customer is asked to enter a public key (or one can be provided automatically by the customer computer). The registration wizard 56 generates an associated private key using its own resources, or by calling a cryptographic services library resident on the customer computer. The cryptographic services perform such tasks as encryption, decryption, digital signing, authentication, and hash computations.

Column 7, Line 62:

> The certificate is deposited in the certificate store 50 on the customer computer 28. The certificate and customer's private key act as a password for all future authenticated conversations between customer and issuing bank. Along with the certificate, the issuing bank also downloads the button UI 54, which can be added to the browser's toolbar (and/or toolbars of other applications). The button UI 54 enables the customer to invoke the wizard to communicate with the issuing bank during future commerce transactions. At this point, the customer has been issued an "***online commerce card***".

Column 8, Line 43:

> Upon clicking the button UI 54, a dialog box appears on the display to inform the customer that they have requested a secure card number. The customer is prompted by the dialog box to input a password for identification purposes. This password might be the private key (if the customer knows the key value) or it may be a separate name or number created by the customer. The operating system 48 checks the password prior to allowing access to the certificate store 50. If the password is approved, the transaction module 72 prepares a request for a transaction number, digitally signs the request using the customer's private key, and submits the signed request to the issuing bank's computer 32 via the Internet 34 (flow arrow 2 in FIG. 3). **The request contains the certificate originally issued by the bank.**

Thus, the Applicants respectfully submit that the claims at issue are not obvious in view of *Franklin et al.* and *Johnson*, either taken alone or in combination. Moreover, the Applicants respectfully submit that these references cannot be combined in the manner suggested by the Examiner to arrive at the claimed invention for the reasons set forth above. Reconsideration and withdrawal of the rejection of these claims is respectfully requested.

CLAIMS ARE PATENTABLE
OVER FRANKLIN ET AL. AND JOHNSON AND CERTAIN OFFICIAL NOTICE

The Examiner rejected claims 41, 44, 47 and 48 under 35 U.S.C. § 103(a) as being unpatentable over *Franklin et al.* in view of *Johnson* and further in view of certain Official Notice. The Examiner contends that the aforementioned combination of *Franklin et al.* and *Johnson* discloses all of the elements of the claims at issue, except for "wherein said External-Entity is using said algorithmically combined SecureCode to authenticate a user's identity, and wherein said Eternal-Entity and said Central-Entity are the same entity," for which the Examiner provides certain Official Notice. The Examiner takes Official Notice that it is old and well-known practice in the art that some institutions such as providers of email services to users or some of the department.

While the Applicants respectfully disagree with the Examiner's characterization of these references vis-à-vis the claims at issue, the aforementioned combination of *Franklin et al.* and *Johnson* fails to result in the claimed invention for at least the reasons discussed above; hence these claims are allowable for the same reasons as above. The Applicants therefore respectfully request reconsideration and withdrawal of the rejection of these claims.

CONCLUSION

The Applicant respectfully submits this application is in condition for allowance and requests issuance of a Notice of Allowance.

Although not believed necessary, the Office is hereby authorized to charge any fees required under 37 C.F.R. § 1.16 or § 1.17 or credit any overpayments to the deposit account of MICHAEL P FORTKORT PC, Deposit Account No. 50-3776.

In the event the prosecution of this Application can be efficiently advanced by a phone discussion, it is requested that the undersigned attorney be called at (703) 435-9390.

Respectfully submitted,

By /Michael P. Fortkort/ Date: August 5, 2010
Michael P. Fortkort (Reg. No. 35,141)

MICHAEL P FORTKORT PC
The International Law Center
13164 Lazy Glen Lane
Oak Hill, Virginia 20171

Please direct telephone calls to:
Michael P. Fortkort
703-435-9390
703-435-8857 (facsimile)

Electronic Acknowledgement Receipt

EFS ID:	8165110
Application Number:	12210926
International Application Number:	
Confirmation Number:	7516
Title of Invention:	Centralized Identification and Authentication System and Method
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Customer Number:	58293
Filer:	Michael P. Fortkort
Filer Authorized By:	
Attorney Docket Number:	KAMR002US0
Receipt Date:	05-AUG-2010
Filing Date:	15-SEP-2008
Time Stamp:	17:25:39
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	Rule 130, 131 or 132 Affidavits	12201926_132_Affidavit_filed_080510.pdf	3012832 2c8434b0e45fc6c7ec5303e5989a95566079fc3a	no	4

Warnings:

Information:

2	Amendment After Final	12210926_Response_to_OA_mailed_050510_filed_080510.pdf	110237 340fecc486b5d6bb2bb08eaf6be0a89e95eacd3c	no	20
Warnings:					
Information:					
		Total Files Size (in bytes):	3123069		

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.

Certification Under 37 C.F.R. § 1.8

I hereby certify that on August 5, 2010 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: August 5, 2010 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 12/210,926

FILING DATE: September 15, 2008

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

ATTORNEY DOCKET: KAMR002US0

CONFIRMATION NO.: 7516

VIA ELECTRONIC FILING SYSTEM
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

AFFIDAVIT UNDER RULE 132

Applicants hereby submit this affidavit in support of their response to the Office Action mailed May 5, 2010 which finally rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 12/210,926, and pursuant to the provisions of 37 C.F.R. § 1.132. The witness hereby avers and testifies as follows:

1. I am Nader Asghari-Kamrani, one of the inventors listed in U.S. Patent Application No. 12/210,926, which is the subject of the present proceeding.

2. I have a degree in computer science from the Technical University of Vienna in 1993. I have been working in the field of authentication over communication networks since 2000. I am one of skill in the art of authentication and electronic transactions.

3. I am familiar with the specification and claims of the present Application as pending and as amended in accordance with a response filed concurrently herewith.

4. I have reviewed the art cited by the Examiner in the present proceeding and in particular, U.S. Patent No. 5,883,810 (*Franklin et al.*) and U.S. Patent Application Publication No. 2005/0222963 A1) by Johnson ("*Johnson*").

5. With respect to the Examiner's rejection of the pending claims under 35 U.S.C. § 103(a) as being obvious based on a combination of *Franklin et al.* and *Johnson*, I disagree that the claimed invention is disclosed by or rendered obvious in view of this combination of references for a variety of reasons, but at a minimum *Franklin et al.* and *Johnson* do not teach or suggest the use of a dynamic SecureCode generated for a user during a transaction between the user and an External-Entity, which SecureCode is then used authenticate the user to the External-Entity as disclosed and claimed in the present Application. Moreover, one of skill in the art of authentication would not combine these references in the manner suggested by the Examiner because of the reasons set forth below.

6. One of skill in the authentication art would understand that authentication involves determining whether a user is, in fact, who he or she claims to be. In contrast, one of skill in the art of authentication would understand the difference between authentication and an online credit card payment process, which involves receiving a user's credit card information for payment and sending the customer's credit card and order information to the customer's issuing bank for payment approval before deciding whether or not to fulfill a user's order.

7. One of skill in the art of authentication would understand that the electronic online commerce card of *Franklin et al.* is integrated with the existing card verification and settlement systems (*see column 1, line 62*) to improve security in the online credit card payment environment, and therefore requires that the transaction number be like a real credit card number because the transaction number is used for payment just like a credit card and not used as authentication of the user. One of skill in the art of authentication would understand that *Franklin et al.'s* online commerce card has been developed to secure online credit card payment, whereas the dynamic SecureCode of the present invention was created to enhance security in the authentication environment.

8. One of skill in the art of authentication would understand that the temporary transaction number of *Franklin et al.* is treated as regular credit card number (*see column 2, line* 23) because the temporary transaction number is actually used for payment, whereas the SecureCode of the present invention provides the basis of authentication.

9. One of skill in the art of authentication would understand that a credit card number or temporary credit card number as described in *Franklin et al.* would raise security and privacy issues if used for online authentication purposes. In contrast, one of skill in the art of authentication would understand that using the SecureCode of the present invention for login or identity authentication would reduce fraud and enhance security in an online environment, whereas requiring credit card information or proxy credit card information for login and identity authentication will decrease security and therefore would not be appropriate for authentication.

10. One of skill in the art of authentication would understand that credit card processing companies do not offer online authentication services, and in order to implement authentication services using *Franklin et al.* they would have to change their existing business model and infrastructure while accepting increased financial risk.

11. One of skill in the art of authentication would not consider a certificate or temporary credit card number as described in *Franklin et al.* to be the same or equivalent to a dynamic SecureCode as described in the present Application, as they are quite different. One of skill in the art of authentication would understand that the digital certificate mentioned in *Franklin et al.* is not capable of being generated dynamically and then being used during an online transaction to authenticate the user to the External-Entity.

12. One of skill in the art of authentication would understand that a certificate as described in *Franklin et al.* and *Johnson* cannot be issued in real time, as there are manual steps involved in creating a certificate, which prevents the issuance of such in real-time or while a user is in communication with another entity. One of skill in the art of authentication upon reading *Franklin et al.* and *Johnson* would understand that a certificate is not generated in real-time or during an online transaction and that obtaining a certificate requires a time delay.

13. One of skill in the art of authentication would understand that a certificate as described in *Franklin et al.* and *Johnson* must be installed in a user's computer, whereas a SecureCode as described in the present invention need not be installed.

I affirm that all statements made herein of my own knowledge are true, and that all statements made herein on information and belief are believed to be true. I understand that willful false statements and the like are punishable by fine or imprisonment, or both (18 U.S.C. 1001), and may jeopardize the validity of the present patent application or any patent issuing thereon.

It witness whereof,

08/05/10

Nader Asghari-Kamrani

Date

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. 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 12/210,926	Filing Date 09/15/2008	□ To be Mailed

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	
□ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
□ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			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 $250 ($125 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			TOTAL	

APPLICATION AS AMENDED – PART II

		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
	08/05/2010	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
AMENDMENT	Total (37 CFR 1.16(i))	* 59	Minus	** 62	= 0	X $26 =	0	OR	X $ =	
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $110 =	0	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	**0**	OR	TOTAL ADD'L FEE	

		(Column 1)		(Column 2)	(Column 3)					
		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
AMENDMENT	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 number found in the appropriate box in column 1.

Legal Instrument Examiner:
/PATSY ZIMMERMAN/

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
12/210,926	09/15/2008	Nader Asghari-Kamrani	6583P3445

CONFIRMATION NO. 7516

58293
FORTKORT & HOUSTON P.C.
9442 N. CAPITAL OF TEXAS HIGHWAY
ARBORETUM PLAZA ONE, SUITE 500
AUSTIN, TX 78759

POA ACCEPTANCE LETTER

OC000000041729801

Date Mailed: 05/21/2010

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 05/14/2010.

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

/llam/

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

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
12/210,926	09/15/2008	Nader Asghari-Kamrani	Kamrani-00001

CONFIRMATION NO. 7516

23504
WEISS & MOY PC
4204 NORTH BROWN AVENUE
SCOTTSDALE, AZ 85251

POWER OF ATTORNEY NOTICE

OC000000041729792

Date Mailed: 05/21/2010

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 05/14/2010.

- The Power of Attorney to you in this application has been revoked by the applicant. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

/llam/

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

page 1 of 1

PTO/SB/81 (01-09)
Approved for use through 11/30/2011. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

POWER OF ATTORNEY OR REVOCATION OF POWER OF ATTORNEY WITH A NEW POWER OF ATTORNEY AND CHANGE OF CORRESPONDENCE ADDRESS

Application Number	12/210,926
Filing Date	September 15, 2008
First Named Inventor	ASGHARI-KAMRANI, NADER
Title	CENTRALIZED IDENTIFICATION AND
Art Unit	2432
Examiner Name	NOBAHAR, A.
Attorney Docket Number	6583P3445

I hereby revoke all previous powers of attorney given in the above-identified application.

□ A Power of Attorney is submitted herewith.

OR

☒ I hereby appoint Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith: 58,293

OR

☒ I hereby appoint Practitioner(s) named below as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith:

Practitioner(s) Name	Registration Number
Michael P. Fortkort	35,141
John A. Fortkort	38,454

Please recognize or change the correspondence address for the above-identified application to:

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

OR

□ The address associated with Customer Number:

OR

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

I am the:

☒ Applicant/Inventor.

OR

□ Assignee of record of the entire interest. See 37 CFR 3.71.
Statement under 37 CFR 3.73(b) (Form PTO/SB/96) submitted herewith or filed on ____________.

SIGNATURE of Applicant or Assignee of Record

Signature		Date	MAY 14, 2010
Name	NADER ASGHARI-KAMRANI	Telephone	703-470-8030
Title and Company	INVENTOR		

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☒ *Total of 2 forms are submitted.

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

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

PTO/SB/81 (01-09)
Approved for use through 11/30/2011. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

POWER OF ATTORNEY OR REVOCATION OF POWER OF ATTORNEY WITH A NEW POWER OF ATTORNEY AND CHANGE OF CORRESPONDENCE ADDRESS

Application Number	12/210,926
Filing Date	September 15, 2008
First Named Inventor	ASGHARI-KAMRANI, NADER
Title	CENTRALIZED IDENTIFICATION AND
Art Unit	2432
Examiner Name	NOBAHAR, A.
Attorney Docket Number	6583P3445

I hereby revoke all previous powers of attorney given in the above-identified application.

□ A Power of Attorney is submitted herewith.

OR

☒ I hereby appoint Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith: 58,293

OR

☒ I hereby appoint Practitioner(s) named below as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith:

Practitioner(s) Name	Registration Number
Michael P. Fortkort	35,141
John A. Fortkort	38,454

Please recognize or change the correspondence address for the above-identified application to:

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

OR

□ The address associated with Customer Number:

OR

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

I am the:

☒ Applicant/Inventor.

OR

□ Assignee of record of the entire interest. See 37 CFR 3.71.
Statement under 37 CFR 3.73(b) (Form PTO/SB/96) submitted herewith or filed on ______________.

SIGNATURE of Applicant or Assignee of Record

Signature	Kamran	Date	MAY 14, 2010
Name	KAMRAN ASGHARI-KAMRANI	Telephone	703-220-3863
Title and Company	INVENTOR		

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☒ *Total of 2 forms are submitted.

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

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

Electronic Acknowledgement Receipt

EFS ID:	7617369
Application Number:	12210926
International Application Number:	
Confirmation Number:	7516
Title of Invention:	Centralized Identification and Authentication System and Method
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Customer Number:	23504
Filer:	Michael P. Fortkort
Filer Authorized By:	
Attorney Docket Number:	Kamrani-00001
Receipt Date:	14-MAY-2010
Filing Date:	15-SEP-2008
Time Stamp:	16:54:33
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Power of Attorney	POA_for_12210926.pdf	117615 ede1a470f9732e86ffca0ddc9c55533900c84cf2	no	2

Warnings:

Information:

Total Files Size (in bytes):	117615

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.
12/210,926	09/15/2008	Nader Asghari-Kamrani	Kamrani-00001	7516

23504 7590 05/05/2010

WEISS & MOY PC
4204 NORTH BROWN AVENUE
SCOTTSDALE, AZ 85251

EXAMINER	
NOBAHAR, ABDULHAKIM	

ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
05/05/2010	PAPER

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

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

Office Action Summary	**Application No.** 12/210,926	**Applicant(s)** ASGHARI-KAMRANI ET AL.	
	Examiner ABDULHAKIM NOBAHAR	**Art Unit** 2432	

-- 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* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, 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 *17 February 2010*.

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

3)□ 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

4)☒ Claim(s) *1-4,12-24,32-41,43-48,50-55,58 and 60* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4, 12-24, 32-41, 43-48, 50-55, 58 and 60* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ 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).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

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).

a)□ All b)□ Some * c)□ None of:

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) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This office action is in response to applicant's amendment filed on .

2. Claims 1-4, 12-24, 32-41, 43-48, 50-55, 58 and 60 are pending.

5. Claims 1 and 21 are amended.

Response to Arguments

1. Applicant's arguments with respect to the rejections of the pending claims under 35 USC § 102 have been fully considered and are persuasive. Therefore, the rejections have been withdrawn. However, upon further consideration of the amended claims, a new ground(s) of rejection is made.

2. With regard to claim rejection 35 USC § 103, applicants on page 15 of the remarks argue that the Franklin art cannot be modified to meet the applicants' invention. If the transaction number of Franklin is modified to include letters and numbers, then the transaction number will no longer appear as a credit card number and it will not be able to read by a merchant.

Examiner respectfully disagrees and asserts that Franklin discloses:

"The "online commerce card" does not exist in physical form, but in digital form for use in online transactions. The issuing bank 26 issues the card to the customer 22 in the form of a signed digital certificate binding the customer to the bank and a software module that can be invoked when using the commerce card to conduct a transaction on the Internet 34. See Detailed Description, Para. (10)."

The above teachings indicate that the Franklin system is also capable of handling alphanumerical strings, because the digital certificates include characters and letters.

3. Examiner, however, in light of the above submission maintains the rejection 35 USC § 103 of the previous Office Action.

Claim Rejections - 35 USC § 103

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

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, 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.

Claims 1-4, 12-24, 32-39, 43, 45, 46, 50-55, 58 and 60 are rejected under 35 U.S.C. 103(a) as being unpatentable over Franklin et al (US 5,883,810 A), hereinafter Franklin in view of Johnson (US 2005/0222963 A1).

Regarding claims 1, 21, 50-55 and 58, Franklin discloses:

A method for authenticating a user in e-commerce for a transaction based on a digital identity issued by a Central-Entity (see, e.g., Fig. 1, where issuing bank corresponds to the recited Central-Entity), the method comprising:

a. the user communicates with an External-Entity to perform a secure transaction with the External-Entity (see abstract, where the merchant corresponds to the recited External-Entity);

b. the External-Entity requires the user to authenticate itself by providing a valid digital identity before executing the transaction (see, e.g., abstract, where the merchant corresponds to the recited External-Entity);

c. the user establishes communication with the Central-Entity and submits a request for a dynamic SecureCode in response to the External-Entity's requirement (see, e.g., Fig. 1, col. 1, line 65-col. 2, line 20 where the card corresponds to the recited SecureCode; col. 4, line 49-col. 5, line 3, where the transaction number for only a single use and with a limited life corresponds to the recited dynamic SecureCode);

d. the Central-Entity:

i. dynamically generates a dynamic SecureCode for the user in response to the user request (see, e.g., Fig. 2; col. 4, line 59-col. 5, line 3, where the transaction number for only a single use and with a limited life corresponds to the recited dynamic SecureCode);

ii. algorithmically combines said generated SecureCode with user-specific information before providing the SecureCode to the user (see, e.g., col. 7, line 40-col. 8, line5);

iii. maintains a copy of said generated SecureCode (see, e.g., col. 7, line 40-col. 8, line5); and

iv. provides said generated SecureCode to the user (see, e.g., col. 7, line 40-col. 8, line5),

e. the External-Entity receives a digital identity from the user, wherein the digital identity comprises a UserName and said generated SecureCode, and forwards said digital identity to the Central-Entity for authentication of the user (see, e.g., col. 7, line 40-col. 8, line5);

f. the Central-Entity receives said digital identity, validates said digital identity based on said SecureCode maintained in its system, and if valid, then authenticates the user and sends an affirmation message to the External-Entity (see, e.g., col. 8, line 15+; col. 10, lines 15-50); and

g. upon receipt of an affirmation message from the Central-Entity, the External-Entity executes the transaction (see, e.g., col. 11, lines 32-44).

Franklin does not expressly disclose that the SecureCode is alphanumeric. Johnson, however, discloses that the ID that the web customer receives from his bank to conduct e-commerce transaction is alphanumerical. Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to utilize an alphanumerical ID for the online transactions as taught in Johnson in the system of Franklin because it would uniquely identifies the web customer (see Johnson, [0024]).

Regarding claims 2 and 22, Franklin discloses:

A method as recited in claim 1, wherein said user has a pre-existing relationship with the External-Entity (see, e.g., col. 8, line 15+, where before the transaction phase the customer has opened an account with the bank).

Regarding claims 3 and 23, Franklin discloses:

A method as recited in claim 1, wherein said user has no pre-existing relationship with the External-Entity (see, e.g., col. 5, line 23+, where before the registration phase the customer did not have an account with the bank).

Regarding claims 4 and 24, Franklin discloses:

A method as recited in claim 1, wherein said External-Entity and said Central-Entity use a SecureCode that is algorithmically combined with said user-specific information (see, e.g., col. 7, line 40-col. 8, line5).

Regarding claims 12 and 32, Franklin discloses:

A method as recited in claim 1, wherein said digital identity is based on a logical combination of the SecureCode and the user-specific information (see, e.g., col. 4, line 36+, where a certificate is a logical combination of information; col. 7, line 40-col. 8, line5).

Regarding claims 13 and 33, Franklin discloses:

A method as recited in claim 1, wherein said digital identity is based on the SecureCode and the user-specific information (see, e.g., col. 6, lines 25-32).

Regarding claims 14 and 34, Franklin discloses:

The method of claim 1, wherein the user-specific information comprises UserName (see, e.g., col. 6, lines 25-32).

Regarding claims 15 and 35, Franklin discloses:

The method of claim 14, wherein the UserName corresponds to a alphanumeric name, ID, login name, an identification phrase, wherein said identification phrase is an account number, phone number, IP address, hardware key, software key, or serial number (see, e.g., col. 6, lines 25-32).

Regarding claims 16 and 36, Franklin discloses:

The method of claim 1, wherein the transaction corresponds to a financial transaction (see, e.g., col. 3, lines 34-47).

Regarding claims 17 and 37, Franklin discloses:

The method of claim 1, wherein the transaction corresponds to a non-financial transaction (see, e.g., col. 1, lines 19-25, order goods and/or services, where services may include non-financial transaction such as accessing secured information, application, web sites or other resources).

Regarding claims 18 and 38, Franklin discloses:

The method of claim 1, wherein the transaction corresponds to access to restricted web-site (see, e.g., col. 1, lines 19-25, order goods and/or services, where services may include non-financial transaction such as accessing secured information, application , web sites or other resources).

Regarding claims 19 and 39, Franklin discloses:

The method of claim 1, wherein said communication is done on a communication network, wherein said communication network is Internet, wireless, mobile network, satellite, or private network (see, e.g., Fig. 1).

Regarding claims 20 and 40, Franklin discloses:

The method of claim 1, wherein said communication is done on a communication network including said user, said Central-Entity, and said External-Entity (see, e.g., Fig. 1).

Regarding claim 43, Franklin discloses:

A method as recited in claim 4, wherein said Central-Entity is using said algorithmically combined SecureCode to authenticate a user's identity (see, e.g., col. 11, lines 11-30, where the bank uses the the transaction number corresponding to the recited algorithmically combined SecureCode and other transaction information for authentication of the customer).

Regarding claim 45, Franklin discloses:

The method as recited in claim 1, wherein said Central-Entity generates a SecureCode that becomes invalid by one of a timer event and a validation event (see, e.g., col. 2, lines 12-20, where “for a single transaction” corresponds to the recited validation event and “a short expiration term" corresponds to the recited timer event).

Regarding claim 46, Franklin discloses:

The method as recited in claim 45, wherein the SecureCode becomes invalid when a predefined period of time passes (see, e.g., col. 2, lines 12-20, where “a short expiration term" corresponds to the recited predefined period of time).

Regarding claim 60, Franklin discloses:

The method as recited in claim 58, wherein said request is initiated by a user through a standard interface provided to said user (see, e.g., col. 5, lines 55-60).

Claims 41, 44, 47 and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Franklin et al (US 5,883,810 A); hereinafter Franklin in view of the examiner Official Notice.

Regarding claims 41 and 44, Franklin does not expressly disclose:

wherein said External-Entity is using said algorithmically combined SecureCode to authenticate a user's identity; and

wherein said External-Entity and said Central-Entity are the same entity.

Official Notice is taken that it is old and well-known practice in the art that some institutions such as providers of email services to users or some of the department stores providing their own credit cards to the customers directly authenticate, without receiving authentication services from a third party, the users and the customers whenever a user logging on to the provider's website for email service usage or a customer purchasing goods using a department store's credit card. In this case the Central-Entity and the External-Entity are the same institution that having an account for the user or the customer. Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to modify the system of Franklin to have one entity to be as the same Central-Entity and External-Entity. The deployment of one entity to issue a SecurCode to a user and also to authenticate the user when using the SecurCode would make the system of Franklin a versatile and a flexible system, in another word a scalable system.

Regarding claim 47, Franklin does not expressly disclose:

The method as recited in claim 1, wherein said Central-Entity generates SecureCode with dependence on one or more alphanumeric values.

Official Notice is taken that it is old and well-known practice in the art that an institution providing a service to a customer generates a key, passphrase, pass-code or a digital identifier made of a combination of numbers and characters (i.e., alphanumeric) for the customer. Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to implement a scheme in the Franklin system to generate alphanumeric digital identifier in order to make the system of Franklin a versatile and a flexible system.

Regarding claim 48, Franklin discloses:

The method as recited in claim 47, wherein said one or more alphanumeric values are one or more of the following: unique key, ID, login name, password, identification phrase, wherein said identification phrase is an account number, phone number, IP address, Hardware key, software key or serial number (see, e.g., col. 6, lines 25-62).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). 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 date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ABDULHAKIM NOBAHAR whose telephone number is (571)272-3808. The examiner can normally be reached on M-T 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. 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.

Abdulhakim Nobahar
Examiner
Art Unit 2432

/A. N./
Examiner, Art Unit 2432

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432

Notice of References Cited	Application/Control No. 12/210,926	Applicant(s)/Patent Under Reexamination ASGHARI-KAMRANI ET AL.
	Examiner ABDULHAKIM NOBAHAR	Art Unit 2432 | Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2005/0222963	10-2005	Johnson, Richard C.	705/067
	B	US-			
	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	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.** 12210926	**Applicant(s)/Patent Under Reexamination** ASGHARI-KAMRANI ET AL.
	Examiner ABDULHAKIM NOBAHAR	**Art Unit** 2432

✓	**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	07/06/2009	11/20/2009	04/28/2010						
	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.** 12210926	**Applicant(s)/Patent Under Reexamination** ASGHARI-KAMRANI ET AL.
	Examiner ABDULHAKIM NOBAHAR	**Art Unit** 2432

✓	**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	07/06/2009	11/20/2009	04/28/2010							
	37	✓	✓	✓							
	38	✓	✓	✓							
	39	✓	✓	✓							
	40	✓	✓	✓							
	41	✓	✓	✓							
	42	✓	-	✓							
	43	✓	✓	✓							
	44	✓	✓	✓							
	45	✓	✓	✓							
	46	✓	✓	✓							
	47	✓	✓	✓							
	48	✓	✓	✓							
	49	✓	-	-							
	50	✓	✓	✓							
	51	✓	✓	✓							
	52	✓	✓	✓							
	53	✓	✓	✓							
	54	✓	✓	✓							
	55	✓	✓	✓							
	56	✓	-	-							
	57	✓	-	-							
	58	✓	✓	✓							
	59	✓	-	-							
	60	✓	✓	✓							
	61	✓	-	-							
	62	✓	-	-							

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.
12/210,926	09/15/2008	Nader Asghari-Kamrani	Kamrani-00001	7516

23504 7590 03/02/2010
WEISS & MOY PC
4204 NORTH BROWN AVENUE
SCOTTSDALE, AZ 85251

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	**PAPER NUMBER**
2432	

MAIL DATE	DELIVERY MODE
03/02/2010	PAPER

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

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

Interview Summary	**Application No.** 12/210,926	**Applicant(s)** ASGHARI-KAMRANI ET AL.	
	Examiner ABDULHAKIM NOBAHAR	**Art Unit** 2432	

All participants (applicant, applicant's representative, PTO personnel):

(1) *ABDULHAKIM NOBAHAR*. (3)_____.

(2) *Ms. Veronica Cao, Reg. No. 52,694*. (4)_____.

Date of Interview: *16 February 2010*.

Type: a)☒ Telephonic b)□ Video Conference
c)□ Personal [copy given to: 1)□ applicant 2)□ applicant's representative]

Exhibit shown or demonstration conducted: d)☒ Yes e)□ No.
If Yes, brief description: *see attachment*.

Claim(s) discussed: *1 and 21*.

Identification of prior art discussed: *US 5,883,810*.

Agreement with respect to the claims f)□ was reached. g)☒ was not reached. h)□ N/A.

Substance of Interview including description of the general nature of what was agreed to if an agreement was reached, or any other comments: *The proposed amendment (see the attachment) to the claims 1 & 21 in view of the prior art Franklin et al. were discussed. Examiner suggested that the claims need to be amended further to ovecome the Franklin disclosure. Ms. Cao stated that the applicants will file a new set of amended claims in response to the last office action*.

(A fuller description, if necessary, and a copy of the amendments which the examiner agreed would render the claims allowable, if available, must be attached. Also, where no copy of the amendments that would render the claims allowable is available, a summary thereof must be attached.)

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. See Summary of Record of Interview requirements on reverse side or on attached sheet.

/A. N./ Examiner, Art Unit 2432	/Gilberto Barron Jr./ Supervisory Patent Examiner, Art Unit 2432

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

———

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:

- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:

1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

WEISS & MOY, P.C.

Attorneys and Counselors
4204 N. Brown Avenue
Scottsdale, Arizona 85251-3914
(480) 994-8888
Fax (480) 947-2663

E-Mail Address: patents@weissiplaw.com
Web Site: www.weissiplaw.com

Founder:
Harry M. Weiss* 1932-2008

Specializing in:
Patents, Trademarks & Copyrights
& Corporate Matters

Jeffrey L. Weiss*
Jeffrey D. Moy*
Farley I. Weiss
Mark H. Weiss
Craig R. Weiss*
Joshua S. Becker
Karen J. S. Fouts*
Veronica-Adele R. Cao*
Aaron C. Fong*

Of Counsel:
Jessica J. Weiss
Steven M. Rabin*
Robert H. Berdo, Jr.*
Phillip Avruch*
Allen Wood*

**Registered Patent Attorney*

Washington, D.C. Office
1101 14th Street, N.W.
Suite 500
Washington, D.C. 20005
(202) 682-1722
Fax (202) 682-1723

Las Vegas, Nevada Office
5851 W. Charleston
Las Vegas, Nevada 89146
(702) 878-7323
Fax (702) 878-4510

Our Ref. 6583P3445

TELECOPIER COVER LETTER

January 29, 2010

Please deliver the following pages to:

NAME:	Examiner Abdulhakim Nobahar
FIRM:	USPTO, Art Unit 2432
CITY:	Alexandria
FAX #:	(571) 273- 3808
FROM:	Veronica Cao

Total number of pages (including cover sheet): 15

MESSAGE: Examiner Interview and Proposed Amendment for Application No. 12/210,926

<u>CONFIDENTIALITY NOTICE</u>: The documents accompanying this facsimile transmission contain legally privileged, confidential information belonging to the sender and intended only for the use of the individual or entity named as receiver above. If you are not the intended receiver, you are hereby notified that disclosure, copying, distribution or the taking of any action in reliance upon the contents of this facsimile is strictly prohibited. If you have received this facsimile in error, please immediately notify us by telephone (call collect) to arrange for return of the documents to us.

Doc Code: M865 or FAI.REQ.INTV

PTOL-413A (10-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Applicant Initiated Interview Request Form

Application No.: 12/210,926 First Named Applicant: Nader Asghari-Kamrani
Examiner: Abdulhakim Nobahar Art Unit: 2432 Status of Application: Pending

Tentative Participants:
(1) Veronica-Adele R. Cao (2) ____________

(3) ____________ (4) ____________

Proposed Date of Interview: February 2, 2010 **Proposed Time:** 3:30 p.m. **(AM/PM)**

Type of Interview Requested:
(1) [✓] Telephonic (2) [ ] Personal (3) [ ] Video Conference

Exhibit To Be Shown or Demonstrated: [ ] YES [ ] NO
If yes, provide brief description: ____________

Issues To Be Discussed

Issues (Rej., Obj., etc)	Claims/ Fig. #s	Prior Art	Discussed	Agreed	Not Agreed
(1) 102 Rejections	1 and 21	Franklin et al.	[ ]	[ ]	[ ]
(2)			[ ]	[ ]	[ ]
(3)			[ ]	[ ]	[ ]
(4)			[ ]	[ ]	[ ]

[ ] Continuation Sheet Attached
[✓] Proposed Amendment or Arguments Attached
Brief Description of Arguments to be Presented:

Proposed amendment language should overcome the prior art because the Franklin reference dicloses a temporary transaction number that must be in the form of a credit card number. The Secure Code of Applicants' invention may be used for identification purposes: i.e. password, PIN number, etc.

An interview was conducted on the above-identified application on ____________.
NOTE: This form should be completed by applicant and submitted to the examiner in advance of the interview (see MPEP § 713.01).
This application will not be delayed from issue because of applicant's failure to submit a written record of this interview. Therefore, applicant is advised to file a statement of the substance of this interview (37 CFR 1.133(b)) as soon as possible.

/Veronica-Adele R. Cao/
Applicant/Applicant's Representative Signature

Examiner/SPE Signature

Veronica-Adele R. Cao
Typed/Printed Name of Applicant or Representative

52,694
Registration Number, if applicable

This collection of information is required by 37 CFR 1.133. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 21 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

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

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT:	ASGHARI-KAMRANI ET AL.	DOCKET NO:	6583P3445
SERIAL NO:	12/210,926	EXAMINER:	NOBAHAR, A.
FILED:	09/15/2008	ART UNIT:	2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

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

Weiss & Moy, P.C.
4204 N. Brown Ave.
Scottsdale, AZ 85251-3914

February ___, 2010

I hereby certify that on the ___ day of February, 2010, this correspondence is being filed electronically on EFS-Web.

/Veronica-Adele R. Cao/
Veronica-Adele R. Cao
Reg. No. 52,694

PROPOSED AMENDMENT

Dear Examiner Nobahar:

This is a response to the Office Action dated December 1, 2009 in connection with the above-identified patent application Please amend the subject patent application as follows:

CLAIM AMENDMENTS

1. (currently amended) A method for authenticating a user in e-commerce for a transaction based on a digital identity issued by a Central-Entity, the method comprising:

a. the user communicates with an External-Entity to perform a secure transaction with the External-Entity;

b. the External-Entity requires the user to authenticate itself by providing a valid digital identity before executing the transaction;

c. the user establishes communication with the Central-Entity and submits a request for a dynamic SecureCode in response to the External-Entity's requirement;

d. the Central-Entity:

i. dynamically generates a dynamic SecureCode for the user in response to the user request, wherein said SecureCode does not necessarily appear as a credit card number;

ii. algorithmically combines said generated SecureCode with user-specific information before providing the SecureCode to the user;

iii. maintains a copy of said generated SecureCode; and

iv. provides said generated SecureCode to the user,

e. the External-Entity receives a digital identity from the user, wherein the digital identity comprises a UserName and said

generated SecureCode, and forwards said digital identity to the Central-Entity for authentication of the user;

f. the Central-Entity receives said digital identity, validates said digital identity based on said SecureCode maintained in its system, and if valid, then authenticates the user and sends an affirmation message to the External-Entity; and

g. upon receipt of an affirmation message from the Central-Entity, the External-Entity executes the transaction.

2. (original) A method as recited in claim 1, wherein said user has a pre-existing relationship with the External-Entity.

3. (original) A method as recited in claim 1, wherein said user has no pre-existing relationship with the External-Entity.

4. (previously presented) A method as recited in claim 1, wherein said External-Entity and said Central-Entity use a SecureCode that is algorithmically combined with said user-specific information.

5-11. (canceled)

12. (original) A method as recited in claim 1, wherein said digital identity is based on a logical combination of the SecureCode and the user-specific information.

13. (original) A method as recited in claim 1, wherein said digital identity is based on the SecureCode and the user-specific information.

14. (original) The method of claim 1, wherein the user-specific information comprises UserName.

15. (previously presented) The method of claim 14, wherein the UserName corresponds to a alphanumeric name, ID, login name, an identification phrase, wherein said identification phrase is an account number, phone number, IP address, hardware key, software key, or serial number.

16. (original) The method of claim 1, wherein the transaction corresponds to a financial transaction.

17. (original) The method of claim 1, wherein the transaction corresponds to a non-financial transaction.

18. (original) The method of claim 1, wherein the transaction corresponds to access to restricted web-site.

19. (previously presented) The method of claim 1, wherein said communication is done on a communication network, wherein said communication network is Internet, wireless, mobile network, satellite, or private network.

20. (previously presented) The method of claim 1, wherein said communication is done on a communication network including said user, said Central-Entity, and said External-Entity.

21. (currently amended) A system for authenticating a user in e-commerce for a transaction based on a digital identity issued by a Central-Entity, the system comprising:

a. the user in communication with an External-Entity to perform a secure transaction with the External-Entity;

b. the External-Entity requires the user to authenticate itself by providing a valid digital identity before executing the transaction;

c. the user in communication with the Central-Entity and with a request for a dynamic SecureCode in response to the External-Entity's requirement;

d. the Central-Entity adapted to:

i. dynamically generate a dynamic SecureCode for the user in response to the user request, wherein said SecureCode does not necessarily appear as a credit card number;

ii. algorithmically combine said generated SecureCode with user-specific information before providing the SecureCode to the user;

iii. maintain a copy of said generated SecureCode; and

iv. provide said SecureCode to the user,

e. the External-Entity adapted to receive a digital identity from the user, wherein the digital identity comprises a UserName and said generated SecureCode, and to forward said digital identity to the Central-Entity to authenticate the user;

f. the Central-Entity further adapted to validate the received said digital identity based on said SecureCode maintained in its system, and if valid, then to authenticate the user, and send an affirmation message to the External-Entity; and

g. the External-Entity further adapted to execute the transaction upon receipt of an affirmation message from the Central-Entity.

22. (original) A system as recited in claim 21, wherein said user has a pre-existing relationship with the External-Entity.

23. (original) A system as recited in claim 21, wherein said user has no pre-existing relationship with the External-Entity.

24. (previously presented) A system as recited in claim 21, wherein said External-Entity and said Central-Entity use a SecureCode that is algorithmically combined with said user-specific information.

25-31. (canceled)

32. (original) A system as recited in claim 21, wherein said digital identity is based on a logical combination of the SecureCode and the user-specific information.

33. (original) A system as recited in claim 21, wherein said digital identity is based on the SecureCode and the user-specific information.

34. (original) The system of claim 21, wherein the user-specific information comprises UserName.

35. (previously presented) The system of claim 34, wherein the UserName corresponds to a alphanumeric name, ID, login name, identification phrase, wherein said identification phrase is an account number, phone number, IP address, hardware key, software key, or serial number.

36. (original) The system of claim 21, wherein the transaction corresponds to a financial transaction.

37. (original) The system of claim 21, wherein the transaction corresponds to a non-financial transaction.

38. (original) The system of claim 21, wherein the transaction corresponds to access to restricted web-site.

39. (previously presented) The system of claim 21, wherein said communication is done on a communication network and wherein said communication network is Internet, wireless, mobile network, satellite, or private network.

40. (previously presented) The system of claim 21, wherein said communication is done on a communication network including said user, said Central-Entity, and said External-Entity.

41. (previously presented) A method as recited in claim 4, wherein said External-Entity is using said algorithmically combined SecureCode to authenticate a user's identity.

42. (canceled)

43. (previously presented) A method as recited in claim 4, wherein said Central-Entity is using said algorithmically combined SecureCode to authenticate a user's identity.

44. (original) A method as recited in claim 1, wherein said External-Entity and said Central-Entity are the same entity.

45. (previously presented) The method as recited in claim 1, wherein said Central-Entity generates a SecureCode that becomes invalid by one of a timer event and a validation event.

46. (previously presented) The method as recited in claim 45, wherein the SecureCode becomes invalid when a predefined period of time passes.

47. (original) The method as recited in claim 1, wherein said Central-Entity generates SecureCode with dependence on one or more alphanumeric values.

48. (previously presented) The method as recited in claim 47, wherein said one or more alphanumeric values are one or more of the following: unique key, ID, login name, password, identification phrase, wherein said identification phrase is an account number, phone number, IP address, Hardware key, software key or serial number.

49. (canceled)

50. (original) The method as recited in claim 1, wherein said digital identity is a SecureCode.

51. (original) The method as recited in claim 1, wherein said user communicates with said Central-Entity over a communication network.

52. (original) The system as recited in claim 21, wherein said digital identity is a SecureCode.

53. (original) The method as recited in claim 1, wherein said user communicates with said External-Entity over a communication network.

54. (original) The system as recited in claim 21, wherein said user communicates with said Central-Entity over a communication network.

55. (original) The system as recited in claim 21, wherein said user communicates with said External-Entity over a communication network.

56-57. (canceled)

58. (previously presented) The method as recited in claim 1, wherein said SecureCode is generated based on a request submitted by said user over a communication network.

59. (canceled)

60. (previously presented) The method as recited in claim 58, wherein said request is initiated by said user through a standard interface provided to said user.

61-62. (canceled)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT:	ASGHARI-KAMRANI ET AL.	DOCKET NO:	6583P3445
SERIAL NO:	12/210,926	EXAMINER:	NOBAHAR, A.
FILED:	09/15/2008	ART UNIT:	2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

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

Weiss & Moy, P.C.
4204 N. Brown Ave.
Scottsdale, AZ 85251-3914

February 17, 2010

I hereby certify that on the 17th day of February, 2010, this correspondence is being filed electronically on EFS-Web.

/Veronica-Adele R. Cao/
Veronica-Adele R. Cao
Reg. No. 52,694

AMENDMENT LETTER

Dear Examiner Nobahar:

Applicants thank the Examiner for the telephonic interview that took place on February 16, 2010. In view of the discussion that took place during the interview, Applicants hereby respond to the Office Action dated December 1, 2009 in connection with the above-identified patent application. Please amend the subject patent application as follows:

CLAIM AMENDMENTS

1. (currently amended) A method for authenticating a user in e-commerce for a transaction based on a digital identity issued by a Central-Entity, the method comprising:

a. the user communicates with an External-Entity to perform a secure transaction with the External-Entity;

b. the External-Entity requires the user to authenticate itself by providing a valid digital identity before executing the transaction;

c. the user establishes communication with the Central-Entity and submits a request for a dynamic SecureCode in response to the External-Entity's requirement;

d. the Central-Entity:

i. dynamically generates a dynamic SecureCode for the user in response to the user request, wherein said SecureCode is alphanumeric;

ii. algorithmically combines said generated SecureCode with user-specific information before providing the SecureCode to the user;

iii. maintains a copy of said generated SecureCode; and

iv. provides said generated SecureCode to the user,

e. the External-Entity receives a digital identity from the user, wherein the digital identity comprises a UserName and said

generated SecureCode, and forwards said digital identity to the Central-Entity for authentication of the user;

f. the Central-Entity receives said digital identity, validates said digital identity based on said SecureCode maintained in its system, and if valid, then authenticates the user and sends an affirmation message to the External-Entity; and

g. upon receipt of an affirmation message from the Central-Entity, the External-Entity executes the transaction.

2. (original) A method as recited in claim 1, wherein said user has a pre-existing relationship with the External-Entity.

3. (original) A method as recited in claim 1, wherein said user has no pre-existing relationship with the External-Entity.

4. (previously presented) A method as recited in claim 1, wherein said External-Entity and said Central-Entity use a SecureCode that is algorithmically combined with said user-specific information.

5-11. (canceled)

12. (original) A method as recited in claim 1, wherein said digital identity is based on a logical combination of the SecureCode and the user-specific information.

13. (original) A method as recited in claim 1, wherein said digital identity is based on the SecureCode and the user-specific information.

14. (original) The method of claim 1, wherein the user-specific information comprises UserName.

15. (previously presented) The method of claim 14, wherein the UserName corresponds to a alphanumeric name, ID, login name, an identification phrase, wherein said identification phrase is an account number, phone number, IP address, hardware key, software key, or serial number.

16. (original) The method of claim 1, wherein the transaction corresponds to a financial transaction.

17. (original) The method of claim 1, wherein the transaction corresponds to a non-financial transaction.

18. (original) The method of claim 1, wherein the transaction corresponds to access to restricted web-site.

19. (previously presented) The method of claim 1, wherein said communication is done on a communication network, wherein said communication network is Internet, wireless, mobile network, satellite, or private network.

20. (previously presented) The method of claim 1, wherein said communication is done on a communication network including said user, said Central-Entity, and said External-Entity.

21. (currently amended) A system for authenticating a user in e-commerce for a transaction based on a digital identity issued by a Central-Entity, the system comprising:

a. the user in communication with an External-Entity to perform a secure transaction with the External-Entity;

b. the External-Entity requires the user to authenticate itself by providing a valid digital identity before executing the transaction;

c. the user in communication with the Central-Entity and with a request for a dynamic SecureCode in response to the External-Entity's requirement;

d. the Central-Entity adapted to:

i. dynamically generate a dynamic SecureCode for the user in response to the user request, wherein said SecureCode is alphanumeric;

ii. algorithmically combine said generated SecureCode with user-specific information before providing the SecureCode to the user;

iii. maintain a copy of said generated SecureCode; and

iv. provide said SecureCode to the user,

e. the External-Entity adapted to receive a digital identity from the user, wherein the digital identity comprises a UserName and said generated SecureCode, and to forward said digital identity to the Central-Entity to authenticate the user;

f. the Central-Entity further adapted to validate the received said digital identity based on said SecureCode maintained in its system, and if valid, then to authenticate the user, and send an affirmation message to the External-Entity; and

g. the External-Entity further adapted to execute the transaction upon receipt of an affirmation message from the Central-Entity.

22. (original) A system as recited in claim 21, wherein said user has a pre-existing relationship with the External-Entity.

23. (original) A system as recited in claim 21, wherein said user has no pre-existing relationship with the External-Entity.

24. (previously presented) A system as recited in claim 21, wherein said External-Entity and said Central-Entity use a SecureCode that is algorithmically combined with said user-specific information.

25-31. (canceled)

32. (original) A system as recited in claim 21, wherein said digital identity is based on a logical combination of the SecureCode and the user-specific information.

33. (original) A system as recited in claim 21, wherein said digital identity is based on the SecureCode and the user-specific information.

34. (original) The system of claim 21, wherein the user-specific information comprises UserName.

35. (previously presented) The system of claim 34, wherein the UserName corresponds to a alphanumeric name, ID, login name, identification phrase, wherein said identification phrase is an account number, phone number, IP address, hardware key, software key, or serial number.

36. (original) The system of claim 21, wherein the transaction corresponds to a financial transaction.

37. (original) The system of claim 21, wherein the transaction corresponds to a non-financial transaction.

38. (original) The system of claim 21, wherein the transaction corresponds to access to restricted web-site.

39. (previously presented) The system of claim 21, wherein said communication is done on a communication network and wherein said communication network is Internet, wireless, mobile network, satellite, or private network.

40. (previously presented) The system of claim 21, wherein said communication is done on a communication network including said user, said Central-Entity, and said External-Entity.

41. (previously presented) A method as recited in claim 4, wherein said External-Entity is using said algorithmically combined SecureCode to authenticate a user's identity.

42. (canceled)

43. (previously presented) A method as recited in claim 4, wherein said Central-Entity is using said algorithmically combined SecureCode to authenticate a user's identity.

44. (original) A method as recited in claim 1, wherein said External-Entity and said Central-Entity are the same entity.

45. (previously presented) The method as recited in claim 1, wherein said Central-Entity generates a SecureCode that becomes invalid by one of a timer event and a validation event.

46. (previously presented) The method as recited in claim 45, wherein the SecureCode becomes invalid when a predefined period of time passes.

47. (original) The method as recited in claim 1, wherein said Central-Entity generates SecureCode with dependence on one or more alphanumeric values.

48. (previously presented) The method as recited in claim 47, wherein said one or more alphanumeric values are one or more of the following: unique key, ID, login name, password, identification phrase, wherein said identification phrase is an account number, phone number, IP address, Hardware key, software key or serial number.

49. (canceled)

50. (original) The method as recited in claim 1, wherein said digital identity is a SecureCode.

51. (original) The method as recited in claim 1, wherein said user communicates with said Central-Entity over a communication network.

52. (original) The system as recited in claim 21, wherein said digital identity is a SecureCode.

53. (original) The method as recited in claim 1, wherein said user communicates with said External-Entity over a communication network.

54. (original) The system as recited in claim 21, wherein said user communicates with said Central-Entity over a communication network.

55. (original) The system as recited in claim 21, wherein said user communicates with said External-Entity over a communication network.

56-57. (canceled)

58. (previously presented) The method as recited in claim 1, wherein said SecureCode is generated based on a request submitted by said user over a communication network.

59. (canceled)

60. (previously presented) The method as recited in claim 58, wherein said request is initiated by said user through a standard interface provided to said user.

61-62. (canceled)

REMARKS

I. Claim Rejections Based on 35 U.S.C. §102

The Examiner has rejected Claims 1-4, 12-24, 32-39, 43, 45, 46, 50-55, 58, and 60 under 35 U.S.C. §102(b) as being anticipated by Franklin et al. (US 5,883,810).

In response, Applicants have amended independent Claims 1 and 21 to include the limitation that the SecureCode is alphanumeric. This amendment is supported by the Specification (see definition for SecureCode in the Background of the Invention section).

Claims 1 and 21, as amended are not anticipated by Franklin et al. Claims 1 and 21 are anticipated by Franklin et al. only if each and every element as set forth in the claims are found in the single prior art reference. MPEP 2131.

The Franklin et al. reference discloses that the transaction number resembles a credit card number. Franklin specifically states that, "the transaction number and real customer account number are both 16-digit, mod, numbers identically formatted with four spaced sets of 4-digits. To the customer (and every other participant in the transaction), the transaction number appears to be a valid credit card number. Only the issuing bank differentiates the transaction numbers from the real customer account numbers. The customer uses the proxy transaction number in the transaction with the merchant."

Franklin, column 4, lines 56-65. Franklin's invention is thus limited to the very specific situation of merchant purchases because the transaction number must be in the form of a credit card number.

In Applicants' invention, the SecureCode is alphanumeric, containing letters and numbers. Franklin et al. does not disclose this. In fact, the transaction number of Franklin cannot be alphanumeric because credit card numbers are purely numeric, containing no letters. Because Franklin et al. does not disclose each and every limitation of amended Claims 1 and 21, they cannot be anticipated by Franklin et al. These rejections should now be obviated. And because Claims 2-4, 12-20, 22-24, 32-39, 43, 45, 46, 50-55, 58, and 60 depend upon amended Claims 1 and 21, they cannot be anticipated by Franklin et al. and those rejections should also be obviated.

II. Claim Rejections Based on 35 U.S.C. §103

The Examiner has rejected claims 41, 44, 47, and 48 as being unpatentable over Franklin et al. in view of the examiner Official Notice.

If the proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification. MPEP 2143.01. As detailed above, The

Franklin et al. reference cannot be modified to meet the Applicants' invention. If the transaction number of Franklin et al. is modified to include letters and numbers, then the transaction number will no longer appear as a credit card number and it will not be able to be read by a merchant. This would frustrate the purpose of the transaction number as the transaction will no longer be able to be conducted. Claim 1 is therefore not unpatentable over Franklin et al. And because Claims 41, 44, 47, and 48 depend upon amended independent Claim 1, they too are not unpatentable over Franklin et al. These rejections should therefore be obviated.

III. Conclusion

It is not believed that this Amendment Letter requires any additional fees, but if there are any fees incurred by this communication, please deduct them from our Deposit Account NO. 23-0830.

Respectfully submitted,

/Veronica-Adele R. Cao/
Veronica-Adele R. Cao
Reg. No. 52,694
Tel: (480) 994-8888

Weiss & Moy, P.C.
4204 N. Brown Ave.
Scottsdale, AZ 85251-3914

Electronic Acknowledgement Receipt

EFS ID:	7027046
Application Number:	12210926
International Application Number:	
Confirmation Number:	7516
Title of Invention:	Centralized Identification and Authentication System and Method
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Customer Number:	23504
Filer:	Veronica-Adele Dela Roca Cao/Tiffany Little
Filer Authorized By:	Veronica-Adele Dela Roca Cao
Attorney Docket Number:	Kamrani-00001
Receipt Date:	17-FEB-2010
Filing Date:	15-SEP-2008
Time Stamp:	16:26:13
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	Amendment Copy Claims/Response to Suggested Claims	Kamrani_6583P3445_AMND.pdf	497420 05fcf92d395d2e303d432acf5b1a545762745c08	no	15

Warnings:

Information:

Total Files Size (in bytes):	497420

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 (07-06)
Approved for use through 1/31/2007. 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 12/210,926	Filing Date 09/15/2008	☒ To be Mailed

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	
□ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
□ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			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 $250 ($125 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			TOTAL	

APPLICATION AS AMENDED – PART II

		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
AMENDMENT	**02/17/2010**	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 41	Minus	** 62	= 0	X $26 =	0	OR	X $ =	
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $110 =	0	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	**0**	OR	TOTAL ADD’L FEE	

		(Column 1)		(Column 2)	(Column 3)					
AMENDMENT		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 number found in the appropriate box in column 1.

Legal Instrument Examiner:
/KATRINA HARLING/

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.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. 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 12/210,926	Filing Date 09/15/2008	☒ To be Mailed

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	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			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 $250 ($125 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			TOTAL	

APPLICATION AS AMENDED – PART II

		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
AMENDMENT	**02/17/2010**	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 41	Minus	** 62	= 0	X $26 =	0	OR	X $ =	
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $110 =	0	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	**0**	OR	TOTAL ADD’L FEE	

		(Column 1)		(Column 2)	(Column 3)					
AMENDMENT		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 number found in the appropriate box in column 1.

Legal Instrument Examiner:
/KATRINA HARLING/

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.
12/210,926	09/15/2008	Nader Asghari-Kamrani	Kamrani-00001	7516

23504 7590 12/01/2009
WEISS & MOY PC
4204 NORTH BROWN AVENUE
SCOTTSDALE, AZ 85251

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	PAPER NUMBER
2432	
MAIL DATE	DELIVERY MODE
12/01/2009	PAPER

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

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

Office Action Summary	**Application No.** 12/210,926	**Applicant(s)** ASGHARI-KAMRANI ET AL.	
	Examiner ABDULHAKIM NOBAHAR	**Art Unit** 2432	

-- 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 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, 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 *09/09/2009*.

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

3)□ 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

4)☒ Claim(s) *1-4,12-24,32-41,43-48,50-55,58 and 60* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,12-24,32-41,43-48,50-55,58,60* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ 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).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

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).

a)□ All b)□ Some * c)□ None of:

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) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This office action is in response to applicant's amendment filed on 09/09/2009.

2. Claims 1-4, 12-24, 32-41, 43-48, 50-55, 58 and 60 are pending.

3. The terminal disclaimer filed on 09/08/2009 is acknowledged and the double patenting rejection is withdrawn.

4. Applicant's arguments with respect to the objection to specification and calims and rejections of claims under 35 USC § 112 have been fully considered and are persuasive. Therefore, the rejections have been withdrawn. However, upon further consideration of the amended claims, a new ground(s) of rejection is made.

Claim Rejections - 35 USC § 102

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-4, 12-24, 32-39, 43, 45, 46, 50-55, 58 and 60 are rejected under 35 U.S.C. 102(b) as being anticipated by Franklin et al (US 5,883,810 A); hereinafter Franklin.

Regarding claims 1, 21, 50-55 and 58, Franklin discloses:

A method for authenticating a user in e-commerce for a transaction based on a digital identity issued by a Central-Entity (see, e.g., Fig. 1, where issuing bank corresponds to the recited Central-Entity), the method comprising:

a. the user communicates with an External-Entity to perform a secure transaction with the External-Entity (see abstract, where the merchant corresponds to the recited External-Entity);

b. the External-Entity requires the user to authenticate itself by providing a valid digital identity before executing the transaction (see, e.g., abstract, where the merchant corresponds to the recited External-Entity);

c. the user establishes communication with the Central-Entity and submits a request for a dynamic SecureCode in response to the External-Entity's requirement (see, e.g., Fig. 1, col. 1, line 65-col. 2, line 20 where the card corresponds to the recited SecureCode; col. 4, line 49-col. 5, line 3, where the transaction number for only a single use and with a limited life corresponds to the recited dynamic SecureCode);

d. the Central-Entity:

i. dynamically generates a dynamic SecureCode for the user in response to the user request (see, e.g., Fig. 2; col. 4, line 59-col. 5, line 3, where the transaction number for only a single use and with a limited life corresponds to the recited dynamic SecureCode);

ii. algorithmically combines said generated SecureCode with user-specific information before providing the SecureCode to the user (see, e.g., col. 7, line 40-col. 8, line5);

iii. maintains a copy of said generated SecureCode (see, e.g., col. 7, line 40-col. 8, line5); and

iv. provides said generated SecureCode to the user (see, e.g., col. 7, line 40-col. 8, line5),

e. the External-Entity receives a digital identity from the user, wherein the digital identity comprises a UserName and said generated SecureCode, and forwards said digital identity to the Central-Entity for authentication of the user (see, e.g., col. 7, line 40-col. 8, line5);

f. the Central-Entity receives said digital identity, validates said digital identity based on said SecureCode maintained in its system, and if valid, then authenticates the user and sends an affirmation message to the External-Entity (see, e.g., col. 8, line 15+; col. 10, lines 15-50); and

g. upon receipt of an affirmation message from the Central-Entity, the External-Entity executes the transaction (see, e.g., col. 11, lines 32-44).

Regarding claims 2 and 22, Franklin discloses:

A method as recited in claim 1, wherein said user has a pre-existing relationship with the External-Entity (see, e.g., col. 8, line 15+, where before the transaction phase the customer has opened an account with the bank).

Regarding claims 3 and 23, Franklin discloses:

A method as recited in claim 1, wherein said user has no pre-existing relationship with the External-Entity (see, e.g., col. 5, line 23+, where before the registration phase the customer did not have an account with the bank).

Regarding claims 4 and 24, Franklin discloses:

A method as recited in claim 1, wherein said External-Entity and said Central-Entity use a SecureCode that is algorithmically combined with said user-specific information (see, e.g., col. 7, line 40-col. 8, line5).

Regarding claims 12 and 32, Franklin discloses:

A method as recited in claim 1, wherein said digital identity is based on a logical combination of the SecureCode and the user-specific information (see, e.g., col. 4, line 36+, where a certificate is a logical combination of information; col. 7, line 40-col. 8, line5).

Regarding claims 13 and 33, Franklin discloses:

A method as recited in claim 1, wherein said digital identity is based on the SecureCode and the user-specific information (see, e.g., col. 6, lines 25-32).

Regarding claims 14 and 34, Franklin discloses:

The method of claim 1, wherein the user-specific information comprises UserName (see, e.g., col. 6, lines 25-32).

Regarding claims 15 and 35, Franklin discloses:

The method of claim 14, wherein the UserName corresponds to a alphanumeric name, ID, login name, an identification phrase, wherein said identification phrase is an account number, phone number, IP address, hardware key, software key, or serial number (see, e.g., col. 6, lines 25-32).

Regarding claims 16 and 36, Franklin discloses:

The method of claim 1, wherein the transaction corresponds to a financial transaction (see, e.g., col. 3, lines 34-47).

Regarding claims 17 and 37, Franklin discloses:

The method of claim 1, wherein the transaction corresponds to a non-financial transaction (see, e.g., col. 1, lines 19-25, <u>order goods and/or services,</u> where services may include non-financial transaction such as accessing secured information, application, web sites or other resources).

Regarding claims 18 and 38, Franklin discloses:

The method of claim 1, wherein the transaction corresponds to access to restricted web-site (see, e.g., col. 1, lines 19-25, <u>order goods and/or services,</u> where services may include non-financial transaction such as accessing secured information, application , web sites or other resources).

Regarding claims 19 and 39, Franklin discloses:

The method of claim 1, wherein said communication is done on a communication network, wherein said communication network is Internet, wireless, mobile network, satellite, or private network (see, e.g., Fig. 1).

Regarding claims 20 and 40, Franklin discloses:

The method of claim 1, wherein said communication is done on a communication network including said user, said Central-Entity, and said External-Entity (see, e.g., Fig. 1).

Regarding claim 43, Franklin discloses:

A method as recited in claim 4, wherein said Central-Entity is using said algorithmically combined SecureCode to authenticate a user's identity (see, e.g., col. 11, lines 11-30, where the bank uses the the transaction number corresponding to the recited algorithmically combined SecureCode and other transaction information for authentication of the customer).

Regarding claim 45, Franklin discloses:

The method as recited in claim 1, wherein said Central-Entity generates a SecureCode that becomes invalid by one of a timer event and a validation event (see, e.g., col. 2, lines 12-20, where “for a single transaction” corresponds to the recited validation event and “a short expiration term" corresponds to the recited timer event).

Regarding claim 46, Franklin discloses:

The method as recited in claim 45, wherein the SecureCode becomes invalid when a predefined period of time passes (see, e.g., col. 2, lines 12-20, where “a short expiration term" corresponds to the recited predefined period of time).

Regarding claim 60, Franklin discloses:

The method as recited in claim 58, wherein said request is initiated by a user through a standard interface provided to said user (see, e.g., col. 5, lines 55-60).

Claim Rejections - 35 USC § 103

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

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, 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.

Claims 41, 44, 47 and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Franklin et al (US 5,883,810 A); hereinafter Franklin in view of the examiner Official Notice**.

Regarding claims 41 and 44, Franklin does not expressly disclose:

wherein said External-Entity is using said algorithmically combined SecureCode to authenticate a user's identity; and

wherein said External-Entity and said Central-Entity are the same entity.

Official Notice is taken that it is old and well-known practice in the art that some institutions such as providers of email services to users or some of the department stores providing their own credit cards to the customers directly authenticate, without receiving authentication services from a third party, the users and the customers whenever a user logging on to the provider's website for email service usage or a customer purchasing goods using a department store's credit card. In this case the Central-Entity and the External-Entity are the same institution that having an account for the user or the customer. Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to modify the system of Franklin to have one entity to be as the same Central-Entity and External-Entity. The deployment of one entity to issue a SecurCode to a user and also to authenticate the user when using the SecurCode would make the system of Franklin a versatile and a flexible system, in another word a scalable system.

Regarding claim 47, Franklin does not expressly disclose:

The method as recited in claim 1, wherein said Central-Entity generates SecureCode with dependence on one or more alphanumeric values.

Official Notice is taken that it is old and well-known practice in the art that an institution providing a service to a customer generates a key, passphrase, pass-code or a digital identifier made of a combination of numbers and characters (i.e., alphanumeric) for the customer. Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to implement a scheme in the Franklin system to generate alphanumeric digital identifier in order to make the system of Franklin a versatile and a flexible system.

Regarding claim 48, Franklin discloses:

The method as recited in claim 47, wherein said one or more alphanumeric values are one or more of the following: unique key, ID, login name, password, identification phrase, wherein said identification phrase is an account number, phone number, IP address, Hardware key, software key or serial number (see, e.g., col. 6, lines 25-62).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See attached PTO-892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ABDULHAKIM NOBAHAR whose telephone number is (571)272-3808. The examiner can normally be reached on M-T 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner’s supervisor, Gilberto Barron can be reached on 571-272-3799. 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.

Abdulhakim Nobahar
Examiner
Art Unit 2432

/A. N./
Examiner, Art Unit 2432

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432

Notice of References Cited	Application/Control No. 12/210,926	Applicant(s)/Patent Under Reexamination ASGHARI-KAMRANI ET AL.	
	Examiner ABDULHAKIM NOBAHAR	Art Unit 2432	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2002/0188481 A1	12-2002	Berg et al.	705/4
*	B	US-6,529,885 B1	03-2003	Johnson, Richard C.	705/64
*	C	US-2007/0073621 A1	03-2007	Dulin et al.	705/050
*	D	US-2008/0016003 A1	01-2008	Hutchison et al.	705/067
*	E	US-7,546,274 B2	06-2009	Ingram et al.	705/43
*	F	US-7,353,541 B1	04-2008	Ishibashi et al.	726/26
*	G	US-5,883,810 A	03-1999	Franklin et al.	700/232
	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	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.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S78	20939	(726/2-5,21 713/155,168,170 705/35,39,44,50,64,67).ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 13:21
S79	5	ASGHARI-KAMRANI near (NADER KAMRAN)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 14:10
S80	5998	S78 and (online Internet electronic $4 web website cyber) near3 (shop $4 commerce$3 purchas$3 buy$3 trad$3 business)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 14:20
S81	3554	S78 and (online Internet electronic $4 web website cyber) near3 (vend $3 retail$3 sell$3 procur$5 exchang $3)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 14:21
S82	7155	S80 S81	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 14:21
S83	5507	S82 and ((user client consumer customer subscrib$3 buy$3 purchas $3 shop$4 member person entity party) near3 (authenticat$3 or verif $4 or verification or valid$5 authoriz$5 confirm$3))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 14:23
S84	2779	S82 and ((trad$3 entity party pay $3 spend$3 partner) near3 (authenticat$3 or verif$4 or verification or valid$5 authoriz$5 confirm$3))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 14:25
S85	5630	S83 S84	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 14:25
S86	4627	S85 and ((user or client consumer customer subscrib$3 buy$3 purchas $3 shop$4) near5 (center$3 central $5 centre centralization bank$3 or broker$4 or authority authoritative or authoriz$5 official$3 or trust$3))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 14:26

S87	3074	S85 and ((trad$3 member person entity party pay$3 spend$3 partner) near5 (center$3 central$5 centre centralization or broker$4 or authority authoritative or authoriz$5 official$3 or trust$3))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 14:28
S88	4967	S86 S87	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 14:28
S89	4217	S88 and ((identity or identif$4 or identification or ID or code securecode password secret$3 PIN passphrase key) near5 (authenticat$3 match$4 compar$4 check$3 examin$5 verif$4 verification valid$5))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 14:40
S90	2636	S89 and ((identity or identif$4 or identification or Id or code securecode password secret$3 PIN passphrase) near5 (match$4 compar$4 check$3 examin$5 verif$4 verification valid$5) same (deny$4 den$4 reject$4 approv$4 disapprov$4 accept$4 allow$4 permit$4 permision authoriz$5))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 14:42
S91	1727	S90 and ((register$5 apply$4 application request$4 enlist$4 enroll$4 sign$3 ask$3) near5 (center$3 central$5 centre centralization or bank$3 broker$4 or authority authoritative or authoriz$5 official$3 or trust$3) same (identity or identif$4 or identification or ID or code securecode password secret$3 PIN passphrase key))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 14:44
S92	1616	S91 and ((center$3 central$5 centre centralization or bank$3 broker$4 or authority authoritative or authoriz$5 official$3 or trust$3) near5 (identity or identif$4 or identification or ID or code securecode password secret$3 PIN passphrase key))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 14:45
S93	1429	S92 and ((identity or identif$4 or identification or Id or code securecode password secret$3 PIN passphrase key) near3 (tim$3 or predict$4 unpredict$4 or temp or tempora$4 or one onetime variable varying or dynamic$4 provision$4 intrim transi$4 short single))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 14:46

S94	915	S92 and ((identity or identif$4 or identification or Id or code securecode password secret$3 PIN passphrase key) near3 (time-base $3 timebased time-depend$3 time $3 depend$3))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 14:48
S95	1439	S93 S94	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 14:48
S96	1426	S95 and ((user or client consumer customer subscrib$3 buy$3 purchas $3 shop$4 trad$3 entity member person party pay$3 spend$3 partner commerc$3 commerciality business counterpart) same (center $3 central$5 centre centralization bank$3 or broker$4 or authority authoritative or authoriz$5 or party official$3 or trust$3) same (retail $3 or vend$3 market$3 aftermarket $3 store or provid$3 or merchant or sell$3 or distribut$3 or site or web or recipient or destination sppl $4))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 14:53
S97	1134	S96 and ((user or client consumer customer subscrib$3 buy$3 purchas $3 shop$4 trad$3 entity member person party pay$3 spend$3 partner commerc$3 commerciality business counterpart) same (center $3 central$5 centre centralization bank$3 or broker$4 or authority authoritative or authoriz$5 or party official$3 or trust$3) same (retail $3 or vend$3 market$3 aftermarket $3 store or provid$3 or merchant or sell$3 or distribut$3 or site or web or recipient or destination sppl $4) same (online Internet electronic$4 web website cyber network$3) same (authenticat$4 or verif$5 or verification or ascertain$5 or valid$5 confirm$5))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 14:56
S98	833	S97 and ((user or client consumer customer subscrib$3 buy$3 purchas $3 shop$4 trad$3 entity member person party pay$3 spend$3 partner commerc$3 commerciality business counterpart) same (center $3 central$5 centre centralization bank$3 or broker$4 or authority authoritative or authoriz$5 or party official$3 or trust$3) same (retail $3 or vend$3 market$3 aftermarket $3 store or provid$3 or merchant or sell$3 or distribut$3 or site or web or recipient or destination sppl	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 15:04

		$4) same (online Internet electronic$4 web website cyber network$3) same (authenticat$4 or verif$5 or verification or ascertain$5 or valid$5 confirm$5) same (identity or identif$4 or identification or ID or code securecode password secret$3 PIN passphrase key) same (deny$4 den $4 reject$4 approv$4 disapprov$4 accept$4 allow$4 disallow$3 grant $3 permit$4 permission authoriz$5 refus$3 forbid$4 inhibit$3 prohibit $3))				
S99	634	S98 and ((user or client consumer customer subscrib$3 buy$3 purchas $3 shop$4 trad$3 entity member person party pay$3 spend$3 partner commerc$3 commerciality business counterpart) same (center $3 central$5 centre centralization bank$3 or broker$4 or authority authoritative or authoriz$5 or party official$3 or trust$3) same (retail $3 or vend$3 market$3 aftermarket $3 store or provid$3 or merchant or sell$3 or distribut$3 or site or web or recipient or destination sppl $4) same (online Internet electronic$4 web website cyber network$3) same (authenticat$4 or verif$5 or verification or ascertain$5 or valid$5 confirm$5) same (identity or identif$4 or identification or ID or code securecode password secret$3 PIN passphrase key) same (authenticat $3 match$4 compar$4 check$3 examin$5 verif$4 verification valid $5) same (deny$4 den$4 reject$4 approv$4 disapprov$4 accept$4 allow$4 disallow$3 grant$3 permit $4 permission authoriz$5 refus$3 forbid$4 inhibit$3 prohibit$3) same (goods merchandis$4 servic$3 access$3 supplies commodit$3 product produce))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 15:08
S100	300	S99 and ((user or client consumer customer subscrib$3 buy$3 purchas $3 shop$4 trad$3 entity member person party pay$3 spend$3 partner commerc$3 commerciality business counterpart) near5 (identity or identif$4 or identification or ID or code securecode password secret$3 PIN passphrase key) same (center$3 central$5 centre centralization bank $3 or broker$4 or authority authoritative or authoriz$5 or party official$3 or trust$3) near5 (retail	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 15:13

		$3 or vend$3 market$3 aftermarket $3 store or provid$3 or merchant or sell$3 or distribut$3 or site or web or recipient or destination sppl $4) same (online Internet electronic$4 web website cyber network$3) same (authenticat$4 or verif$5 or verification or ascertain$5 or valid$5 confirm$5) same (authenticat$3 match$4 compar$4 check$3 examin$5 verif $4 verification valid$5) same (deny $4 den$4 reject$4 approv$4 disapprov$4 accept$4 allow$4 disallow$3 grant$3 permit$4 permission authoriz$5 refus$3 forbid$4 inhibit$3 prohibit$3) same (goods merchandis$4 servic$3 access$3 supplies commodit$3 product produce))				
S101	235	S100 and ((user or client consumer customer subscrib$3 buy $3 purchas$3 shop$4 trad$3 entity member person party pay$3 spend $3 partner commerc$3 commerciality business counterpart) near5 (identity or identif$4 or identification or ID or code securecode password secret $3 PIN passphrase key) same (center$3 central$5 centre centralization bank$3 or broker$4 or authority authoritative or authoriz$5 or party official$3 or trust$3) near5 (retail$3 or vend$3 market$3 aftermarket$3 store or provid$3 or merchant or sell$3 or distribut$3 or site or web or recipient or destination sppl$4) same (online Internet electronic$4 web website cyber network$3) same (authenticat$4 or verif$5 or verification or ascertain$5 or valid $5 confirm$5) same (user or client consumer customer subscrib$3 buy $3 purchas$3 shop$4 trad$3 entity member person party pay$3 spend $3 partner commerc$3 commerciality business counterpart) near5 (authenticat$3 match$4 compar$4 check$3 examin$5 verif$4 verification valid $5) same (deny$4 den$4 reject$4 approv$4 disapprov$4 accept$4 allow$4 disallow$3 grant$3 permit $4 permission authoriz$5 refus$3 forbid$4 inhibit$3 prohibit$3) same (goods merchandis$4 servic$3 access$3 supplies commodit$3 product produce))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 15:14

S102	188	S101 and ((user or client consumer customer subscrib$3 buy$3 purchas$3 shop$4 trad$3 entity member person party pay$3 spend$3 partner commerc$3 commerciality business counterpart) near5 (identity or identif$4 or identification or ID or code securecode password secret$3 PIN passphrase key) same (center$3 central$5 centre centralization bank$3 or broker$4 or authority authoritative or authoriz$5 or party official$3 or trust$3) near5 (retail$3 or vend$3 market$3 aftermarket$3 store or provid$3 or merchant or sell$3 or distribut$3 or site or web or recipient or destination sppl$4) same (online Internet electronic$4 web website cyber network$3) same (authenticat$4 or verif$5 or verification or ascertain$5 or valid$5 confirm$5) same (user or client consumer customer subscrib$3 buy$3 purchas$3 shop$4 trad$3 entity member person party pay$3 spend$3 partner commerc$3 commerciality business counterpart) near5 (authenticat$3 match$4 compar$4 check$3 examin$5 verif$4 verification valid$5) same (deny$4 den$4 reject$4 approv$4 disapprov$4 accept$4 allow$4 disallow$3 grant$3 permit$4 permission authoriz$5 refus$3 forbid$4 inhibit$3 prohibit$3) same (retail$3 or vend$3 market$3 aftermarket$3 store or provid$3 or merchant or sell$3 or distribut$3 or site or web or recipient or destination sppl$4) near5 (goods merchandis$4 servic$3 access$5 supplies commodit$3 product produce))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 15:17
S103	166	S102 and ((user or client consumer customer subscrib$3 buy$3 purchas$3 shop$4 trad$3 entity member person party pay$3 spend$3 partner commerc$3 commerciality business counterpart) with (identity or identif$4 or identification or ID or code securecode password secret$3 PIN passphrase key) with (center$3 central$5 centre centralization bank$3 or broker$4 or authority authoritative or authoriz$5 or party official$3 or trust$3) with (generat$3 creat$3 mak$3 form$5 produc$4 calculat	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 15:29

		$3 comput$5 provid$3 supply$3))				
S104	141	S103 and ((user or client consumer customer subscrib$3 buy $3 purchas$3 shop$4 trad$3 entity member person party pay$3 spend $3 partner commerc$3 commerciality business counterpart) with (identity or identif$4 or identification or ID or code securecode password secret $3 PIN passphrase key) with (center$3 central$5 centre centralization bank$3 or broker$4 or authority authoritative or authoriz$5 or party official$3 or trust$3) near5 (generat$3 creat$3 mak$3 form$5 produc$4 calculat $3 comput$5 provid$3 supply$3))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 15:30
S105	136	S104 and ((user or client consumer customer subscrib$3 buy $3 purchas$3 shop$4 trad$3 entity member person party pay$3 spend $3 partner commerc$3 commerciality business counterpart) near5 (identity or identif$4 or identification or ID or code securecode password secret $3 PIN passphrase key) with (center$3 central$5 centre centralization bank$3 or broker$4 or authority authoritative or authoriz$5 or party official$3 or trust$3) near5 (generat$3 creat$3 mak$3 form$5 produc$4 calculat $3 comput$5 provid$3 supply$3))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 15:31
S106	124027	(online Internet electronic$4 web website cyber) near3 (shop$4 commerce$3 purchas$3 buy$3 trad $3 business transaction)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 16:12
S107	111159	(online Internet electronic$4 web website cyber network$3) near3 (vend$3 retail$3 sell$3 procur$5 exchang$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 16:13
S108	206307	S106 S107	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 16:13
S109	58587	S108 and ((user client consumer customer subscrib$3 buy$3 purchas $3 shop$4 member person entity party) near3 (authenticat$3 or verif $4 or verification or valid$5 authoriz$5 confirm$3))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 16:13

S110	16508	S108 and ((trad$3 entity party pay $3 spend$3 partner counterpart) near3 (authenticat$3 or verif$4 or verification or valid$5 authoriz$5 confirm$3))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 16:14
S111	59615	S109 S110	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 16:14
S112	19781	S111 and @pd>="20070701"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 16:15
S113	13267	S112 and ((user or client consumer customer subscrib$3 buy $3 purchas$3 shop$4) near5 (center$3 central$5 centre centralization bank$3 or broker$4 or authority authoritative or authoriz$5 official$3 or trust$3))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 16:16
S114	7236	S112 and ((trad$3 member person entity party pay$3 spend$3 partner) near5 (center$3 central$5 centre centralization or broker$4 or authority authoritative or authoriz$5 official$3 or trust$3))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 16:16
S115	14553	S113 S114	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 16:16
S116	10614	S115 and ((identity or identif$4 or identification or ID or code securecode password secret$3 PIN passphrase key) near5 (authenticat $3 match$4 compar$4 check$3 examin$5 verif$4 verification valid $5))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 16:17
S117	5633	S116 and ((identity or identif$4 or identification or Id or code securecode password secret$3 PIN passphrase) near5 (match$4 compar$4 check$3 examin$5 verif $4 verification valid$5) same (deny $4 den$4 reject$4 approv$4 disapprov$4 accept$4 allow$4 permit$4 permision authoriz$5))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 16:19

S118	2968	S117 and ((register$5 apply$4 application request$4 enlist$4 enroll$4 sign$3 ask$3) near5 (center$3 central$5 centre centralization or bank$3 broker$4 or authority authoritative or authoriz$5 official$3 or trust$3) same (identity or identif$4 or identification or ID or code securecode password secret$3 PIN passphrase key))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 16:20
S119	1078	S118 and ((user or client consumer customer subscrib$3 buy$3 purchas$3 shop$4 trad$3 entity member person party pay$3 spend$3 partner commerc$3 commerciality business counterpart) near5 (identity or identif$4 or identification or ID or code securecode password secret$3 PIN passphrase key) with (center$3 central$5 centre centralization bank$3 or broker$4 or authority authoritative or authoriz$5 or party official$3 or trust$3) near5 (generat$3 creat$3 mak$3 form$5 produc$4 calculat$3 comput$5 provid$3 supply$3))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 16:21
S120	1037	S119 and ((center$3 central$5 centre centralization or bank$3 broker$4 or authority authoritative or authoriz$5 official$3 or trust$3) near5 (identity or identif$4 or identification or ID or code securecode password secret$3 PIN passphrase key))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 16:22
S121	954	S120 and ((identity or identif$4 or identification or Id or code securecode password secret$3 PIN passphrase key) near3 (tim$3 or predict$4 unpredict$4 or temp or tempora$4 or one onetime variable varying or dynamic$4 provision$4 intrim transi$4 short single))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 16:23
S122	611	S120 and ((identity or identif$4 or identification or Id or code securecode password secret$3 PIN passphrase key) near3 (time-base$3 timebased time-depend$3 time$3 depend$3))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 16:24
S123	961	S121 S122	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 16:24

S124	956	S123 and ((user or client consumer customer subscrib$3 buy $3 purchas$3 shop$4 trad$3 entity member person party pay$3 spend $3 partner commerc$3 commerciality business counterpart) same (center$3 central$5 centre centralization bank $3 or broker$4 or authority authoritative or authoriz$5 or party official$3 or trust$3) same (retail $3 or vend$3 market$3 aftermarket $3 store or provid$3 or merchant or sell$3 or distribut$3 or site or web or recipient or destination sppl $4))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 16:24
S125	457	S124 and ((user or client consumer customer subscrib$3 buy $3 purchas$3 shop$4 trad$3 entity member person party pay$3 spend $3 partner commerc$3 commerciality business counterpart) same (center$3 central$5 centre centralization bank $3 or broker$4 or authority authoritative or authoriz$5 or party official$3 or trust$3) same (retail $3 or vend$3 market$3 aftermarket $3 store or provid$3 or merchant or sell$3 or distribut$3 or site or web or recipient or destination sppl $4) same (online Internet electronic$4 web website cyber network$3) same (authenticat$4 or verif$5 or verification or ascertain$5 or valid$5 confirm$5) same (identity or identif$4 or identification or ID or code securecode password secret$3 PIN passphrase key) same (authenticat $3 match$4 compar$4 check$3 examin$5 verif$4 verification valid $5) same (deny$4 den$4 reject$4 approv$4 disapprov$4 accept$4 allow$4 disallow$3 grant$3 permit $4 permission authoriz$5 refus$3 forbid$4 inhibit$3 prohibit$3) same (goods merchandis$4 servic$3 access$3 supplies commodit$3 product produce))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 16:25

S126	457	S125 and ((user or client consumer customer subscrib$3 buy $3 purchas$3 shop$4 trad$3 entity member person party pay$3 spend $3 partner commerc$3 commerciality business counterpart) with (identity or identif$4 or identification or ID or code securecode password secret $3 PIN passphrase key) with (center$3 central$5 centre centralization bank$3 or broker$4 or authority authoritative or authoriz$5 or party official$3 or trust$3) with (generat$3 creat$3 mak$3 form$5 produc$4 calculat $3 comput$5 provid$3 supply$3))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 16:26
S127	124	S126 and ((user or client consumer customer subscrib$3 buy $3 purchas$3 shop$4 trad$3 entity member person party pay$3 spend $3 partner commerc$3 commerciality business counterpart) near5 (identity or identif$4 or identification or ID or code securecode password secret $3 PIN passphrase key) same (center$3 central$5 centre centralization bank$3 or broker$4 or authority authoritative or authoriz$5 or party official$3 or trust$3) near5 (retail$3 or vend$3 market$3 aftermarket$3 store or provid$3 or merchant or sell$3 or distribut$3 or site or web or recipient or destination sppl$4) same (online Internet electronic$4 web website cyber network$3) same (authenticat$4 or verif$5 or verification or ascertain$5 or valid $5 confirm$5) same (user or client consumer customer subscrib$3 buy $3 purchas$3 shop$4 trad$3 entity member person party pay$3 spend $3 partner commerc$3 commerciality business counterpart) near5 (authenticat$3 match$4 compar$4 check$3 examin$5 verif$4 verification valid $5) same (deny$4 den$4 reject$4 approv$4 disapprov$4 accept$4 allow$4 disallow$3 grant$3 permit $4 permission authoriz$5 refus$3 forbid$4 inhibit$3 prohibit$3) same (retail$3 or vend$3 market$3 aftermarket$3 store or provid$3 or merchant or sell$3 or distribut$3 or site or web or recipient or destination sppl$4) near5 (goods merchandis$4 servic$3 access$5 supplies commodit$3 product	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/09/23 16:27

		produce))				
S130	6	Rosko and authenticat$3	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/11/20 15:49
S131	604	Rosko and (user or client consumer customer subscrib$3 buy$3 purchas$3 shop$4 trad$3 entity member person party pay$3 spend$3 partner commerc$3 commerciality business counterpart) and (identity or identif$4 or identification or ID or code securecode password secret$3 PIN passphrase key) and (center$3 central$5 centre centralization bank$3 or broker$4 or authority authoritative or authoriz$5 or party official$3 or trust$3 master$3 manag$5) and (generat$3 creat$3 mak$3 form$5 produc$4 calculat$3 comput$5 provid$3 supply$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/11/20 22:28
S132	40	S131 and (user or client consumer customer subscrib$3 buy$3 purchas$3 shop$4 trad$3 entity member person party pay$3 spend$3 partner commerc$3 commerciality business counterpart) same (identity or identif$4 or identification or ID or code securecode password secret$3 PIN passphrase key) same (center$3 central$5 centre centralization bank$3 or broker$4 or authority authoritative or authoriz$5 or party official$3 or trust$3 master$3 manag$5) same (generat$3 creat$3 mak$3 form$5 produc$4 calculat$3 comput$5 provid$3 supply$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/11/20 22:29
S133	158	Rosko.in.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/11/20 22:30
S134	6	S132 and S133	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/11/20 22:31
S135	2	"5557516".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/11/20 22:43

S136	2	"5826241".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/11/20 22:43
S137	2	"5883810".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/11/20 22:43
S138	2	"5890137".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/11/20 22:43
S139	8	S135 S136 S137 S138	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/11/20 22:44

11/22/2009 10:39:46 PM
H:\ EAST\ Workspaces\ 09940635_12210926.wsp

Index of Claims	**Application/Control No.** 12210926	**Applicant(s)/Patent Under Reexamination** ASGHARI-KAMRANI ET AL.
	Examiner ABDULHAKIM NOBAHAR	**Art Unit** 2432

✓	**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	07/06/2009	11/20/2009							
	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. 12210926	**Applicant(s)/Patent Under Reexamination** ASGHARI-KAMRANI ET AL.
	Examiner ABDULHAKIM NOBAHAR	**Art Unit** 2432

✓	**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	07/06/2009	11/20/2009							
	37	✓	✓							
	38	✓	✓							
	39	✓	✓							
	40	✓	✓							
	41	✓	✓							
	42	✓	-							
	43	✓	✓							
	44	✓	✓							
	45	✓	✓							
	46	✓	✓							
	47	✓	✓							
	48	✓	✓							
	49	✓	-							
	50	✓	✓							
	51	✓	✓							
	52	✓	✓							
	53	✓	✓							
	54	✓	✓							
	55	✓	✓							
	56	✓	-							
	57	✓	-							
	58	✓	✓							
	59	✓	-							
	60	✓	✓							
	61	✓	-							
	62	✓	-							

Search Notes	**Application/Control No.** 12210926	**Applicant(s)/Patent Under Reexamination** ASGHARI-KAMRANI ET AL.
	Examiner ABDULHAKIM NOBAHAR	**Art Unit** 2432

SEARCHED

Class	Subclass	Date	Examiner
726	2-5,21	7/6/2009 9/23/2009	AN
713	155,168,170	9/23/2009	AN
705	35,39,44,50,64,67	9/23/2009	AN
	See attached report		

SEARCH NOTES

Search Notes	Date	Examiner
East Inventors names search (see attached report)	7/6/2009 9/23/2009	AN
EAST text search only (see attached report)	7/6/2009 9/23/2009 11/22/2009	AN
PALM inventors names search	9/23/2009	AN

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner
726	2-5,21	9/23/2021	AN
713	155,168,170	9/23/2009	AN
705	35,39,44,50,64,67	9/23/2009	AN
	See attached report		

/A. N./ Examiner.Art Unit 2432	

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
12/210,926	09/15/2008	Nader Asghari-Kamrani	Kamrani-00001

CONFIRMATION NO. 7516

23504
WEISS & MOY PC
4204 NORTH BROWN AVENUE
SCOTTSDALE, AZ 85251

POA ACCEPTANCE LETTER

OC000000037863116

Date Mailed: 10/16/2009

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 09/08/2009.

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

/mdjones/

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

page 1 of 1

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
12/210,926	09/15/2008	Nader Asghari-Kamrani	Kamrani-00001

CONFIRMATION NO. 7516

63670
MAXVALUEIP CONSULTING
11204 ALBERMYRTLE ROAD
POTOMAC, MD 20854

POWER OF ATTORNEY NOTICE

OC000000037863087

Date Mailed: 10/16/2009

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 09/08/2009.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

/mdjones/

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

Application Number	Application/Control No. 12/210,926	Applicant(s)/Patent under Reexamination ASGHARI-KAMRANI ET AL.	

Document Code - DISQ	**Internal Document – DO NOT MAIL**

TERMINAL DISCLAIMER	☒ APPROVED	□ DISAPPROVED
Date Filed : 09/08/09	**This patent is subject to a Terminal Disclaimer**	**REASONS:**

Approved/Disapproved by:

Jan Hurley
Paralegal Specialist
Patent Legal Research Center

09/25/09

U.S. Patent and Trademark Office

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT:	ASGHARI-KAMRANI ET AL.	DOCKET NO:	6583P3445
SERIAL NO:	12/210,926	EXAMINER:	NOBAHAR, A.
FILED:	09/15/2008	ART UNIT:	2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

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

Weiss & Moy, P.C.
4204 N. Brown Ave.
Scottsdale, AZ 85251-3914

September 9, 2009

I hereby certify that on the 9th day of September, 2009, this correspondence is being filed electronically on EFS-Web.

/Veronica-Adele R. Cao/
Veronica-Adele R. Cao
Reg. No. 52,694

SUPPLEMENTAL AMENDMENT

Dear Examiner Nobahar:

This is a Supplemental Amendment that should take the place of the Amendment Letter filed yesterday. This is a response to the Office Action dated July 14, 2009 in connection with the above-identified patent application Please amend the subject patent application as follows:

CLAIM AMENDMENTS

1. (currently amended) A method for authenticating a user in e-commerce for a transaction based on a digital identity issued by a Central-Entity, the method comprising:

a. the user communicates with an External-Entity [[and performs]] to perform a secure transaction with the External-Entity;

b. the External-Entity requires the user to authenticate itself by providing a valid digital identity before executing the transaction;

c. the user establishes communication with the Central-Entity and submits a request for a dynamic SecureCode in response to the External-Entity's requirement;

d. the Central-Entity:

i. dynamically generates a dynamic SecureCode for the user in response to the user request;

ii. algorithmically combines said generated SecureCode with user-specific information before providing the SecureCode to the user;

iii. maintains a copy of said generated SecureCode; and

iv. provides said generated SecureCode to the user,

e. the External-Entity receives a digital identity from the user, wherein the digital identity comprises a UserName and said

generated SecureCode, and forwards said digital identity to the Central-Entity for authentication of the user;

f. the Central-Entity receives said digital identity, validates said digital identity based on said SecureCode maintained in its system, and if valid, then authenticates the user and sends an affirmation message to the External-Entity; and

g. upon receipt of an affirmation message from the Central-Entity, the External-Entity executes the transaction.

2. (original) A method as recited in claim 1, wherein said user has a pre-existing relationship with the External-Entity.

3. (original) A method as recited in claim 1, wherein said user has no pre-existing relationship with the External-Entity.

4. (currently amended) A method as recited in claim 1, wherein said External-Entity and said Central-Entity ~~share~~ use a SecureCode that is algorithmically combined with said user-specific information ~~cryptographic algorithm~~.

5-11. (canceled)

12. (original) A method as recited in claim 1, wherein said digital identity is based on a logical combination of the SecureCode and the user-specific information.

13. (original) A method as recited in claim 1, wherein said digital identity is based on the SecureCode and the user-specific information.

14. (original) The method of claim 1, wherein the user-specific information comprises UserName.

15. (currently amended) The method of claim 14, wherein the UserName corresponds to a alphanumeric name, ID, login name, an identification phrase, wherein said identification phrase is an account number, phone number, IP address, hardware key, software key, or serial number.

16. (original) The method of claim 1, wherein the transaction corresponds to a financial transaction.

17. (original) The method of claim 1, wherein the transaction corresponds to a non-financial transaction.

18. (original) The method of claim 1, wherein the transaction corresponds to access to restricted web-site.

19. (currently amended) The method of claim 1, wherein said communication is done on a communication network, wherein said communication network is ~~including~~ Internet, wireless, mobile network, satellite, or private network.

20. (currently amended) The method of claim 1, wherein said communication is done on a communication network including said user, said Central-Entity, and said External-Entity ~~at least a server and a client device~~.

21. (currently amended) A system for authenticating a user in e-commerce for a transaction based on a digital identity issued by a Central-Entity, the system comprising:

a. the user in communication with an External-Entity [[and performs]] to perform a secure transaction with the External-Entity;

b. the External-Entity requires the user to authenticate itself by providing a valid digital identity before executing the transaction;

c. the user in communication with the Central-Entity and with a request for a dynamic SecureCode in response to the External-Entity's requirement;

d. the Central-Entity adapted to:

i. dynamically generate a dynamic SecureCode for the user in response to the user request;

ii. algorithmically combine said generated SecureCode with user-specific information before providing the SecureCode to the user;

iii. maintain a copy of said generated SecureCode; and

iv. provide said SecureCode to the user,

e. the External-Entity adapted to receive a digital identity from the user, wherein the digital identity comprises a UserName and said generated SecureCode, and to forward said digital identity to the Central-Entity to authenticate the user;

f. the Central-Entity further adapted to validate the received said digital identity based on said SecureCode maintained in its system, and if valid, then to authenticate the user, and send an affirmation message to the External-Entity; and

g. the External-Entity further adapted to execute the transaction upon receipt of an affirmation message from the Central-Entity.

22. (original) A system as recited in claim 21, wherein said user has a pre-existing relationship with the External-Entity.

23. (original) A system as recited in claim 21, wherein said user has no pre-existing relationship with the External-Entity.

24. (currently amended) A system as recited in claim 21, wherein said External-Entity and said Central-Entity ~~share~~ use a SecureCode that is algorithmically combined with said user-specific information ~~cryptographic algorithm~~.

25-31. (canceled)

32. (original) A system as recited in claim 21, wherein said digital identity is based on a logical combination of the SecureCode and the user-specific information.

33. (original) A system as recited in claim 21, wherein said digital identity is based on the SecureCode and the user-specific information.

34. (original) The system of claim 21, wherein the user-specific information comprises UserName.

35. (currently amended) The system of claim 34, wherein the UserName corresponds to a alphanumeric name, ID, login name, identification phrase, wherein said identification phrase is an account number, phone number, IP address, hardware key, software key, or serial number.

36. (original) The system of claim 21, wherein the transaction corresponds to a financial transaction.

37. (original) The system of claim 21, wherein the transaction corresponds to a non-financial transaction.

38. (original) The system of claim 21, wherein the transaction corresponds to access to restricted web-site.

39. (currently amended) The system of claim 21, wherein said communication is done on a communication network and wherein said communication network is ~~including~~ Internet, wireless, mobile network, satellite, or private network.

40. (currently amended) The system of claim 21, wherein said communication is done on a communication network including said user, said Central-Entity, and said External-Entity ~~at least a server and a client device~~.

41. (currently amended) A method as recited in claim 4, wherein said External-Entity is using said ~~shared cryptographic algorithm~~ algorithmically combined SecureCode to authenticate a user's identity ~~based on said SecureCode~~.

42. (canceled)

43. (currently amended) A method as recited in claim 4, wherein said Central-Entity is using said ~~shared cryptographic algorithm~~ algorithmically combined SecureCode to authenticate a user's identity ~~based on said SecureCode~~.

44. (original) A method as recited in claim 1, wherein said External-Entity and said Central-Entity are the same entity.

45. (currently amended) The method as recited in claim 1, wherein said Central -Entity generates a SecureCode ~~with dependence~~ that becomes invalid by one of a timer event and a validation event ~~on at least a dynamic variable~~.

46. (currently amended) The method as recited in claim 45, wherein the SecureCode becomes invalid when a predefined period of time passes ~~said dynamic variable is time~~.

47. (original) The method as recited in claim 1, wherein said Central-Entity generates SecureCode with dependence on one or more alphanumeric values.

48. (currently amended) The method as recited in claim 47, wherein said one or more alphanumeric values are one or more of the following: unique key, ID, login name, password, identification phrase, wherein said identification phrase is an account number, phone number, IP address, Hardware key, software key or serial number.

49. (canceled)

50. (original) The method as recited in claim 1, wherein said digital identity is a SecureCode.

51. (original) The method as recited in claim 1, wherein said user communicates with said Central-Entity over a communication network.

52. (original) The system as recited in claim 21, wherein said digital identity is a SecureCode.

53. (original) The method as recited in claim 1, wherein said user communicates with said External-Entity over a communication network.

54. (original) The system as recited in claim 21, wherein said user communicates with said Central-Entity over a communication network.

55. (original) The system as recited in claim 21, wherein said user communicates with said External-Entity over a communication network.

56-57. (canceled)

58. (currently amended) The method as recited in claim 1, wherein said ~~request~~ SecureCode is generated based on a request submitted by said user over a communication network ~~event~~.

59. (canceled)

60. (currently amended) The method as recited in claim 58, wherein said request ~~event~~ is [[a]] initiated by said user ~~user's~~ through a standard interface provided to said user ~~authentication request at said External-Entity~~.

61-62. (canceled)

REMARKS

I. Objections to the Specification

a. Claims 4-11, 20, 24-31, 40-46, 49, and 56-62

Claims 4, 24, 41, and 43 have been amended to more closely resemble the language in the Specification. Support for this amendment may be found at p.6:14-17 and p.11:16-18.

Claims 5, 6, 7, 8, 9, 10, 11, 25, 26, 27, 28, 29, 30, 31, 42, 49, 56, 57, 59, 61, and 62 have been canceled.

Claim 20 and 40 have been amended to more closely resemble the language in the Specification. Support for these amendments may be found at p.9:7-9.

Claim 44 remains in its original form because it is supported by the Specification. The Specification, at p.3:20-21 and p.4:3-4, explains that the Central-Entity could be a bank or a credit card-issuing company. Similarly, the External-Entity could be a bank or credit card issuing company as well. This rejection should therefore be obviated.

Claims 45 and 46 have been amended to more closely resemble the language in the Specification. Support for these amendments may be found at p.12:6-13.

Claims 58 and 60 have been amended to more closely resemble the language in the Specification. Support for these amendments may be found at p.9:7-9 and p. 10:6-16.

b. Claims 15, 35, and 48

Claims 15, 35, and 48 have been amended to clarify that account number, phone number, IP address, hardware key, software key, and serial number are types of "other identification phrases" that may be used. Support for this amendment is found at p. 4:5-7.

c. Claims 19 and 39

Claims 19 and 39 have been amended to clarify that wireless, mobile network, satellite, or private network are types of "communication networks," like the Internet, that may be used. Support for this amendment is found at p.1:19-21.

Applicants feel that these amendments overcome the objections to the Specification.

II. Claim Objections

The Examiner has objected to Claim 1 and 21 based on informalities in line 3 of each of Claims 1 and 21. Claim 1 and Claim 21, as amended, now overcome the objection.

III. Claim Rejections Based on 35 U.S.C. §112

The Examiner has rejected Claims 4-11, 15, 19, 20, 24-31, 35, 39-46, 48, 49, and 56-62 under 35 U.S.C. §112, first paragraph. The Claims have been amended as indicated above. Applicants feel that these amendments overcome the rejections.

IV. Double Patenting

The Examiner has rejected Claims 1-3, 12-19, 21-23, 32-38, 47, and 50-55 s being anticipated by claims 1, 4-7 and 10-12 of U.S. Patent No. 7,356,837. A terminal disclaimer and the related fee are being filed and paid herewith.

V. Allowable Subject Matter

Applicants thank the Examiner for the indication of the allowability of Claims 1-62 if rewritten to overcome the rejections under 35 U.S.C. §112, 1st paragraph and the claim objections. As mentioned above a terminal disclaimer is also being filed herewith.

VI. Conclusion

A $70 payment for a terminal disclaimer was paid with the Amendment Letter submitted yesterday and therefore is not being paid again here. It is not believed that this Supplemental Amendment requires any additional fees, but if there are any fees incurred by this communication, please deduct them from our Deposit Account NO. 23-0830.

Respectfully submitted,

/Veronica-Adele R. Cao/
Veronica-Adele R. Cao
Reg. No. 52,694
Tel: (480) 994-8888

Weiss & Moy, P.C.
4204 N. Brown Ave.
Scottsdale, AZ 85251-3914

Electronic Acknowledgement Receipt

EFS ID:	6035778
Application Number:	12210926
International Application Number:	
Confirmation Number:	7516
Title of Invention:	Centralized Identification and Authentication System and Method
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Customer Number:	63670
Filer:	Veronica-Adele Dela Roca Cao/Marianna Hann
Filer Authorized By:	Veronica-Adele Dela Roca Cao
Attorney Docket Number:	Kamrani-00001
Receipt Date:	09-SEP-2009
Filing Date:	15-SEP-2008
Time Stamp:	12:50:17
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	Supplemental Response or Supplemental Amendment	Karmani_6583P3445_SUPP_AMD.pdf	48482 6b0598e5e396e64a2a9a40c3629c880d8f87ea2f	no	16

Warnings:

Information:

Total Files Size (in bytes):	48482

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 (07-06)
Approved for use through 1/31/2007. 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 12/210,926	Filing Date 09/15/2008	□ To be Mailed

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	
□ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
□ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			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 $250 ($125 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			TOTAL	

APPLICATION AS AMENDED – PART II

		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
AMENDMENT	**09/09/2009**	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 41	Minus	** 62	= 0	X $26 =	0	OR	X $ =	
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $110 =	0	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	**0**	OR	TOTAL ADD’L FEE	

		(Column 1)		(Column 2)	(Column 3)					
AMENDMENT		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 number found in the appropriate box in column 1.

Legal Instrument Examiner:
/MARQUITA D. JONES/

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.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT:	ASGHARI-KAMRANI ET AL.	DOCKET NO:	6583P3445
SERIAL NO:	12/210,926	EXAMINER:	NOBAHAR, A.
FILED:	09/15/2008	ART UNIT:	2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

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

Weiss & Moy, P.C.
4204 N. Brown Ave.
Scottsdale, AZ 85251-3914

September 8, 2009

I hereby certify that on the 8th day of September, 2009, this correspondence is being filed electronically on EFS-Web.

/Veronica-Adele R. Cao/
Veronica-Adele R. Cao
Reg. No. 52,694

AMENDMENT LETTER

Dear Examiner Nobahar:

This is a response to the Office Action dated July 14, 2009 in connection with the above-identified patent application

Please amend the subject patent application as follows:

CLAIM AMENDMENTS

1. (currently amended) A method for authenticating a user in e-commerce for a transaction based on a digital identity issued by a Central-Entity, the method comprising:

a. the user communicates with an External-Entity [[and performs]] to perform a secure transaction with the External-Entity;

b. the External-Entity requires the user to authenticate itself by providing a valid digital identity before executing the transaction;

c. the user establishes communication with the Central-Entity and submits a request for a dynamic SecureCode in response to the External-Entity's requirement;

d. the Central-Entity:

i. dynamically generates a dynamic SecureCode for the user in response to the user request;

ii. algorithmically combines said generated SecureCode with user-specific information before providing the SecureCode to the user;

iii. maintains a copy of said generated SecureCode; and

iv. provides said generated SecureCode to the user,

e. the External-Entity receives a digital identity from the user, wherein the digital identity comprises a UserName and said

generated SecureCode, and forwards said digital identity to the Central-Entity for authentication of the user;

f. the Central-Entity receives said digital identity, validates said digital identity based on said SecureCode maintained in its system, and if valid, then authenticates the user and sends an affirmation message to the External-Entity; and

g. upon receipt of an affirmation message from the Central-Entity, the External-Entity executes the transaction.

2. (original) A method as recited in claim 1, wherein said user has a pre-existing relationship with the External-Entity.

3. (original) A method as recited in claim 1, wherein said user has no pre-existing relationship with the External-Entity.

4. (currently amended) A method as recited in claim 1, wherein said External-Entity and said Central-Entity ~~share~~ use a SecureCode that is algorithmically combined with said user-specific information without revealing said user-specific information ~~cryptographic algorithm~~.

5-11. (canceled)

12. (original) A method as recited in claim 1, wherein said digital identity is based on a logical combination of the SecureCode and the user-specific information.

13. (original) A method as recited in claim 1, wherein said digital identity is based on the SecureCode and the user-specific information.

14. (original) The method of claim 1, wherein the user-specific information comprises UserName.

15. (currently amended) The method of claim 14, wherein the UserName corresponds to a alphanumeric name, ID, login name, an identification phrase, wherein said identification phrase is an account number, phone number, IP address, hardware key, software key, or serial number.

16. (original) The method of claim 1, wherein the transaction corresponds to a financial transaction.

17. (original) The method of claim 1, wherein the transaction corresponds to a non-financial transaction.

18. (original) The method of claim 1, wherein the transaction corresponds to access to restricted web-site.

19. (currently amended) The method of claim 1, wherein said communication is done on a communication network, wherein said communication network is ~~including~~ Internet, wireless, mobile network, satellite, or private network.

20. (currently amended) The method of claim 1, wherein said communication is done on a communication network including said user, said Central-Entity, and said External-Entity ~~at least a server and a client device~~.

21. (currently amended) A system for authenticating a user in e-commerce for a transaction based on a digital identity issued by a Central-Entity, the system comprising:

a. the user in communication with an External-Entity [[and performs]] to perform a secure transaction with the External-Entity;

b. the External-Entity requires the user to authenticate itself by providing a valid digital identity before executing the transaction;

c. the user in communication with the Central-Entity and with a request for a dynamic SecureCode in response to the External-Entity's requirement;

d. the Central-Entity adapted to:

i. dynamically generate a dynamic SecureCode for the user in response to the user request;

ii. algorithmically combine said generated SecureCode with user-specific information before providing the SecureCode to the user;

iii. maintain a copy of said generated SecureCode; and

iv. provide said SecureCode to the user,

e. the External-Entity adapted to receive a digital identity from the user, wherein the digital identity comprises a UserName and said generated SecureCode, and to forward said digital identity to the Central-Entity to authenticate the user;

f. the Central-Entity further adapted to validate the received said digital identity based on said SecureCode maintained in its system, and if valid, then to authenticate the user, and send an affirmation message to the External-Entity; and

g. the External-Entity further adapted to execute the transaction upon receipt of an affirmation message from the Central-Entity.

22. (original) A system as recited in claim 21, wherein said user has a pre-existing relationship with the External-Entity.

23. (original) A system as recited in claim 21, wherein said user has no pre-existing relationship with the External-Entity.

24. (currently amended) A system as recited in claim 21, wherein said External-Entity and said Central-Entity ~~share~~ use a SecureCode that is algorithmically combined with said user-specific information without revealing said user-specific information ~~cryptographic algorithm~~.

25-31. (canceled)

32. (original) A system as recited in claim 21, wherein said digital identity is based on a logical combination of the SecureCode and the user-specific information.

33. (original) A system as recited in claim 21, wherein said digital identity is based on the SecureCode and the user-specific information.

34. (original) The system of claim 21, wherein the user-specific information comprises UserName.

35. (currently amended) The system of claim 34, wherein the UserName corresponds to a alphanumeric name, ID, login name, identification phrase, wherein said identification phrase is an account number, phone number, IP address, hardware key, software key, or serial number.

36. (original) The system of claim 21, wherein the transaction corresponds to a financial transaction.

37. (original) The system of claim 21, wherein the transaction corresponds to a non-financial transaction.

38. (original) The system of claim 21, wherein the transaction corresponds to access to restricted web-site.

39. (currently amended) The system of claim 21, wherein said communication is done on a communication network and wherein said communication network is ~~including~~ Internet, wireless, mobile network, satellite, or private network.

40. (currently amended) The system of claim 21, wherein said communication is done on a communication network including said user, said Central-Entity, and said External-Entity ~~at least a server and a client device~~.

41. (currently amended) A method as recited in claim 4, wherein said External-Entity is using said ~~shared cryptographic algorithm~~ algorithmically combined SecureCode to authenticate a user's identity ~~based on said SecureCode~~.

42. (canceled)

43. (currently amended) A method as recited in claim 4, wherein said Central-Entity is using said ~~shared cryptographic algorithm~~ algorithmically combined SecureCode to authenticate a user's identity ~~based on said SecureCode~~.

44. (original) A method as recited in claim 1, wherein said External-Entity and said Central-Entity are the same entity.

45. (currently amended) The method as recited in claim 1, wherein said Central -Entity generates a SecureCode ~~with dependence~~ that becomes invalid by one of a timer event and a validation event ~~on at least a dynamic variable~~.

46. (currently amended) The method as recited in claim 45, wherein the SecureCode becomes invalid when a predefined period of time passes ~~said dynamic variable is time~~.

47. (original) The method as recited in claim 1, wherein said Central-Entity generates SecureCode with dependence on one or more alphanumeric values.

48. (currently amended) The method as recited in claim 47, wherein said one or more alphanumeric values are one or more of the following: unique key, ID, login name, password, identification phrase, wherein said identification phrase is an account number, phone number, IP address, Hardware key, software key or serial number.

49. (canceled)

50. (original) The method as recited in claim 1, wherein said digital identity is a SecureCode.

51. (original) The method as recited in claim 1, wherein said user communicates with said Central-Entity over a communication network.

52. (original) The system as recited in claim 21, wherein said digital identity is a SecureCode.

53. (original) The method as recited in claim 1, wherein said user communicates with said External-Entity over a communication network.

54. (original) The system as recited in claim 21, wherein said user communicates with said Central-Entity over a communication network.

55. (original) The system as recited in claim 21, wherein said user communicates with said External-Entity over a communication network.

56-57. (canceled)

58. (currently amended) The method as recited in claim 1, wherein said ~~request~~ SecureCode is generated based on a request submitted by said user over a communication network ~~event~~.

59. (canceled)

60. (currently amended) The method as recited in claim 58, wherein said request ~~event~~ is [[a]] initiated by said user ~~user's~~ through a standard interface provided to said user ~~authentication request at said External-Entity~~.

61-62. (canceled)

REMARKS

I. Objections to the Specification

a. Claims 4-11, 20, 24-31, 40-46, 49, and 56-62

Claims 4, 24, 41, and 43 have been amended to more closely resemble the language in the Specification. Support for this amendment may be found at p.6:14-17 and p.11:16-18.

Claims 5, 6, 7, 8, 9, 10, 11, 25, 26, 27, 28, 29, 30, 31, 42, 49, 56, 57, 59, 61, and 62 have been canceled.

Claim 20 and 40 have been amended to more closely resemble the language in the Specification. Support for these amendments may be found at p.9:7-9.

Claim 44 remains in its original form because it is supported by the Specification. The Specification, at p.3:20-21 and p.4:3-4, explains that the Central-Entity could be a bank or a credit card-issuing company. Similarly, the External-Entity could be a bank or credit card issuing company as well. This rejection should therefore be obviated.

Claims 45 and 46 have been amended to more closely resemble the language in the Specification. Support for these amendments may be found at p.12:6-13.

Claims 58 and 60 have been amended to more closely resemble the language in the Specification. Support for these amendments may be found at p.9:7-9 and p. 10:6-16.

b. Claims 15, 35, and 48

Claims 15, 35, and 48 have been amended to clarify that account number, phone number, IP address, hardware key, software key, and serial number are types of "other identification phrases" that may be used. Support for this amendment is found at p. 4:5-7.

c. Claims 19 and 39

Claims 19 and 39 have been amended to clarify that wireless, mobile network, satellite, or private network are types of "communication networks," like the Internet, that may be used. Support for this amendment is found at p.1:19-21.

Applicants feel that these amendments overcome the objections to the Specification.

II. Claim Objections

The Examiner has objected to Claim 1 and 21 based on informalities in line 3 of each of Claims 1 and 21. Claim 1 and Claim 21, as amended, now overcome the objection.

III. Claim Rejections Based on 35 U.S.C. §112

The Examiner has rejected Claims 4-11, 15, 19, 20, 24-31, 35, 39-46, 48, 49, and 56-62 under 35 U.S.C. §112, first paragraph. The Claims have been amended as indicated above. Applicants feel that these amendments overcome the rejections.

IV. Double Patenting

The Examiner has rejected Claims 1-3, 12-19, 21-23, 32-38, 47, and 50-55's being anticipated by claims 1, 4-7 and 10-12 of U.S. Patent No. 7,356,837. A terminal disclaimer and the related fee are being filed and paid herewith.

V. Allowable Subject Matter

Applicants thank the Examiner for the indication of the allowability of Claims 1-62 if rewritten to overcome the rejections under 35 U.S.C. §112, 1st paragraph and the claim objections. As mentioned above a terminal disclaimer is also being filed herewith.

VI. Conclusion

A $70 payment for a terminal disclaimer is being paid herewith. It is not believed that this Amendment Letter requires any additional fees, but if there are any fees incurred by this communication, please deduct them from our Deposit Account NO. 23-0830.

Respectfully submitted,

/Veronica-Adele R. Cao/
Veronica-Adele R. Cao
Reg. No. 52,694
Tel: (480) 994-8888

Weiss & Moy, P.C.
4204 N. Brown Ave.
Scottsdale, AZ 85251-3914

PTO/SB/26 (07-09)
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 displays a valid OMB control number.

TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT	Docket Number (Optional) 6583P3445

In re Application of: Nader Asghari-Kamrani et al.

Application No.: 12/210,926

Filed: September 15, 2008

For: Centralized Identification and Authentication System and Method

The owner*, Nader Asghari-Kamrani &Kamran Asghari-Kamran, of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term **prior patent** No. 7,356,837 as the term of said prior patent is defined in 35 U.S.C. 154 and 173, and as the term of said **prior patent** is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the **prior patent** are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term as defined in 35 U.S.C. 154 and 173 of the **prior patent**, "as the term of said **prior patent** is presently shortened by any terminal disclaimer," in the event that said **prior patent** later:

expires for failure to pay a maintenance fee;
is held unenforceable;
is found invalid by a court of competent jurisdiction;
is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
has all claims canceled by a reexamination certificate;
is reissued; or
is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

Check either box 1 or 2 below, if appropriate.

1. □ For submissions on behalf of a business/organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the business/organization.

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 willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2. ☑ The undersigned is an attorney or agent of record. Reg. No. 52,694

/Veronica-Adele R. Cao/ September 8, 2009
Signature Date

Veronica-Adele R. Cao
Typed or printed name

(480) 994-8888
Telephone Number

☑ Terminal disclaimer fee under 37 CFR 1.20(d) included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

This collection of information is required by 37 CFR 1.321. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 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.

Privacy Act Statement

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

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

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

Electronic Patent Application Fee Transmittal

Application Number:	12210926
Filing Date:	15-Sep-2008
Title of Invention:	Centralized Identification and Authentication System and Method
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Filer:	Veronica-Adele Dela Roca Cao/Marianna Hann
Attorney Docket Number:	Kamrani-00001

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:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Statutory disclaimer	2814	1	70	70
		Total in USD ($)		**70**

Electronic Acknowledgement Receipt

EFS ID:	6027132
Application Number:	12210926
International Application Number:	
Confirmation Number:	7516
Title of Invention:	Centralized Identification and Authentication System and Method
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Customer Number:	63670
Filer:	Veronica-Adele Dela Roca Cao/Marianna Hann
Filer Authorized By:	Veronica-Adele Dela Roca Cao
Attorney Docket Number:	Kamrani-00001
Receipt Date:	08-SEP-2009
Filing Date:	15-SEP-2008
Time Stamp:	14:07:17
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$70
RAM confirmation Number	346
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1	Power of Attorney	Karmani_6583P3445_POA2.pdf	149482 fcae89a24ed365741d692bb2f7cedb463242cb13	no	2
Warnings:					
Information:					
2	Amendment/Req. Reconsideration-After Non-Final Reject	Karmani_6583P3445_AMD.pdf	492523 7ceb98724dfbdba9e38e11bbd4681e8674b2a3b6	no	15
Warnings:					
Information:					
3	Terminal Disclaimer Filed	Karmani_6583P3445_TERM.pdf	210773 e9d7889c7810d8f221705e3304dd5a69f12b6f11	no	2
Warnings:					
Information:					
4	Fee Worksheet (PTO-875)	fee-info.pdf	29832 c02ac4c1ea615aec543bfb918532f7cda0f43982	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	882610		

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/81 (01-09)
Approved for use through 11/30/2011. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

POWER OF ATTORNEY OR REVOCATION OF POWER OF ATTORNEY WITH A NEW POWER OF ATTORNEY AND CHANGE OF CORRESPONDENCE ADDRESS

Application Number	12/210,928
Filing Date	September 15, 2008
First Named Inventor	Nader Asghari-Kamrani
Title	Centralized Identification and...
Art Unit	2131
Examiner Name	Nobahar, Abdulhakim
Attorney Docket Number	6583P3445

I hereby revoke all previous powers of attorney given in the above-identified application.

☐ A Power of Attorney is submitted herewith.

OR

☒ I hereby appoint Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith: 23504

OR

☐ I hereby appoint Practitioner(s) named below as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith:

Practitioner(s) Name	Registration Number

Please recognize or change the correspondence address for the above-identified application to:

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

OR

☐ The address associated with Customer Number:

OR

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

I am the:

☒ Applicant/Inventor.

OR

☐ Assignee of record of the entire interest. See 37 CFR 3.71.
Statement under 37 CFR 3.73(b) (Form PTO/SB/96) submitted herewith or filed on ______________________.

SIGNATURE of Applicant or Assignee of Record

Signature	Kamran	Date	9/4/09
Name	Kamran Asghari-Kamrani	Telephone	
Title and Company			

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☒ *Total of 2 forms are submitted.

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

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

PTO/SB/81 (01-09)
Approved for use through 11/30/2011. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

POWER OF ATTORNEY OR REVOCATION OF POWER OF ATTORNEY WITH A NEW POWER OF ATTORNEY AND CHANGE OF CORRESPONDENCE ADDRESS

Application Number	12/210,926
Filing Date	09/15/2008
First Named Inventor	Nader Asghari-Kamrani
Title	Centralized Identification..
Art Unit	2432
Examiner Name	Nobahar, Abdulhakim
Attorney Docket Number	6583P3445

I hereby revoke all previous powers of attorney given in the above-identified application.

□ A Power of Attorney is submitted herewith.

OR

☒ I hereby appoint Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith: **23504**

OR

□ I hereby appoint Practitioner(s) named below as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith:

Practitioner(s) Name	Registration Number

Please recognize or change the correspondence address for the above-identified application to:

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

OR

□ The address associated with Customer Number:

OR

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

I am the:

☒ Applicant/Inventor.

OR

□ Assignee of record of the entire interest. See 37 CFR 3.71.
Statement under 37 CFR 3.73(b) (Form PTO/SB/96) submitted herewith or filed on ____________.

SIGNATURE of Applicant or Assignee of Record

Signature		Date	08/13/09
Name	Nader Asghari-Kamrani	Telephone	703-470-8030
Title and Company			

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☒ *Total of 1 forms are submitted.

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

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

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
12/210,926	09/15/2008	Nader Asghari-Kamrani	Kamrani-00001

CONFIRMATION NO. 7516

63670
MAXVALUEIP CONSULTING
11204 ALBERMYRTLE ROAD
POTOMAC, MD 20854

MISCELLANEOUS NOTICE

OC000000037494063

Date Mailed: 08/26/2009

A communication which cannot be delivered in electronic form has been mailed to the applicant.

Doc Code: N572

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 DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
12/210,926	09/15/2008	Nader Asghari-Kamrani	Kamrani-00001

CONFIRMATION NO. 7516

OC000000037494063

63670
MAXVALUEIP CONSULTING
11204 ALBERMYRTLE ROAD
POTOMAC, MD 20854

Cc: WEISS & MOY PC
4204 NORTH BROWN AVENUE
SCOTTSDALE, AZ 85251

Date Mailed: 08/24/2009

DENIAL OF REQUEST FOR POWER OF ATTORNEY

The request for Power of Attorney filed 08/18/09 is acknowledged. However, the request cannot be granted at this time for the reason stated below.

□ The revocation is not signed by the applicant, the assignee of the entire interest, or one particular principal attorney having the authority to revoke.

□ The Power of Attorney is from an assignee and the Certificate required by 37 CFR 3.73(b) has not been received.

□ The person signing for the assignee has omitted their empowerment to sign on behalf of the assignee.

□ The inventor(s) is without authority to appoint attorneys since the assignee has intervened as provided by 37 CFR 3.71.

☑ The signature(s) of Kamran Asghari-Kamrani , a co-inventor in this application, has been omitted. The Power of Attorney will be entered upon receipt of confirmation signed by said co-inventor(s).

□ The person(s) appointed in the Power of Attorney is not registered to practice before the U.S. Patent and Trademark Office.

Questions relating to this Notice should be directed to the Application Assistance Unit.

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

PTO/SB/81 (01-09)
Approved for use through 11/30/2011. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

POWER OF ATTORNEY OR REVOCATION OF POWER OF ATTORNEY WITH A NEW POWER OF ATTORNEY AND CHANGE OF CORRESPONDENCE ADDRESS

Application Number	12/210,926
Filing Date	09/15/2008
First Named Inventor	Nader Asghari-Kamrani
Title	Centralized Identification..
Art Unit	2432
Examiner Name	Nobahar, Abdulhakim
Attorney Docket Number	6583P3445

I hereby revoke all previous powers of attorney given in the above-identified application.

□ A Power of Attorney is submitted herewith.

OR

☒ I hereby appoint Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith: 23504

OR

□ I hereby appoint Practitioner(s) named below as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith:

Practitioner(s) Name	Registration Number

Please recognize or change the correspondence address for the above-identified application to:

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

OR

□ The address associated with Customer Number:

OR

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

I am the:

☒ Applicant/Inventor.

OR

□ Assignee of record of the entire interest. See 37 CFR 3.71.
Statement under 37 CFR 3.73(b) (Form PTO/SB/96) submitted herewith or filed on ________________.

SIGNATURE of Applicant or Assignee of Record

Signature		Date	08/13/09
Name	Nader Asghari-Kamrani	Telephone	703-470-8030
Title and Company			

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☒ *Total of 1 forms are submitted.

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

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

Electronic Acknowledgement Receipt

EFS ID:	5911038
Application Number:	12210926
International Application Number:	
Confirmation Number:	7516
Title of Invention:	Centralized Identification and Authentication System and Method
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Customer Number:	63670
Filer:	Veronica-Adele Dela Roca Cao/Marianna Hann
Filer Authorized By:	Veronica-Adele Dela Roca Cao
Attorney Docket Number:	Kamrani-00001
Receipt Date:	18-AUG-2009
Filing Date:	15-SEP-2008
Time Stamp:	16:48:35
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Power of Attorney	Karmani_6583P3445_POA.pdf	72944 6f5fc350838b3134cb5766d0ff4b044b10b39647	no	1

Warnings:

Information:

Total Files Size (in bytes):	72944

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.
12/210,926	09/15/2008	Nader Asghari-Kamrani	Kamrani-00001	7516

63670 7590 07/14/2009

MAXVALUEIP CONSULTING
11204 ALBERMYRTLE ROAD
POTOMAC, MD 20854

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	PAPER NUMBER
2432	
MAIL DATE	DELIVERY MODE
07/14/2009	PAPER

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

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

Office Action Summary	**Application No.** 12/210,926	**Applicant(s)** ASGHARI-KAMRANI ET AL.	
	Examiner ABDULHAKIM NOBAHAR	**Art Unit** 2432	

-- 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* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, 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 _____.

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

3)□ 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

4)☒ Claim(s) *1-62* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-62* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 September 2008* 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).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

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).

a)□ All b)□ Some * c)□ None of:

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) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *09/15/2008*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Specification

The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required:

The specification does not provide descriptions for the limitations of claims 4-11, 20, 24-31, 40-46, 49 and 56-62.

The specification does not provide descriptions for the limitation "account number, phone number, IP address, hardware key, software key, or serial number" in the claims 15, 35 and 48.

The specification does not provide descriptions for the limitation "wireless, mobile network, satellite, or private network" in the claims 19 and 39.

Claim Objections

Claims 1 and 21 are objected to because of the following informalities: These claims in line 3 recite "the user communicates…and performs" which should be changed to "the user communicates…~~and~~ to performs" because the user has not been authenticated yet and intends to perform a transaction with an External-Entity. Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 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.

Claims 4-11, 15, 19, 20, 24-31, 35, 39-46, 48, 49 and 56-62 are rejected under 35 U.S.C. 112, 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(s), at the time the application was filed, had possession of the claimed invention. These claims include limitations as described above that are not described in the specification.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1-3, 12-19, 21-23, 32-38, 47 and 50-55 of the instant application is anticipated by claims 1, 4-7 and 10-12 of the U.S. Patent No. 7,356,837 B2. The claims 1, 4-7 and 10-12 of the patent contain all the limitations of claims 1-3, 16-19, 21-23, 36-38, 51 and 53-55 of the instant application. Claims 1-3, 16-19, 21-23, 36-38, 51 and 53-55 of the instant application therefore are not patently distinct from the earlier patented claims 1, 4-7 and 10-12 and as such are unpatentable for obvious-type double patenting.

Allowable Subject Matter

Claims 1-62 would be allowable if rewritten or amended to overcome the rejections under 35 U.S.C. 112, 1st paragraph and claim objections, set forth in this Office action. These claims are also rejected under nonstatutory double patenting rejection, which requires the applicants to formally file a timely terminal disclaimer.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ABDULHAKIM NOBAHAR whose telephone number is (571)272-3808. The examiner can normally be reached on M-T 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. 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.

July 6, 2009

/A. N./
Examiner, Art Unit 2432

/Benjamin E Lanier/
Primary Examiner, Art Unit 2432

Page 1 of 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

BIB DATA SHEET

CONFIRMATION NO. 7516

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
12/210,926	09/15/2008 RULE	713	2432	Kamrani-00001

APPLICANTS

Nader Asghari-Kamrani, Centreville, VA;
Kamran Asghari-Kamrani, Centreville, VA;

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

This application is a CON of 11/239,046 09/30/2005 PAT 7,444,676
which claims benefit of 60/615,603 10/05/2004
This application 12/210,926 09/15/2008
is a CON of 09/940,635 08/29/2001 PAT 7,356,837

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

** **IF REQUIRED, FOREIGN FILING LICENSE GRANTED** ** ** SMALL ENTITY **
09/29/2008

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☐ No Verified and Acknowledged /ABDULHAKIM NOBAHAR/ Examiner's Signature	☐ Met after Allowance Initials	**STATE OR COUNTRY**	**SHEETS DRAWINGS**	**TOTAL CLAIMS**	**INDEPENDENT CLAIMS**
		VA	5	62	2

ADDRESS

MAXVALUEIP CONSULTING
11204 ALBERMYRTLE ROAD
POTOMAC, MD 20854
UNITED STATES

TITLE

Centralized Identification and Authentication System and Method

FILING FEE RECEIVED 1485	FEES: Authority has been given in Paper No.____________ to charge/credit DEPOSIT ACCOUNT No.____________ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other ________________ ☐ Credit

Index of Claims	**Application/Control No.** 12210926	**Applicant(s)/Patent Under Reexamination** ASGHARI-KAMRANI ET AL.
	Examiner ABDULHAKIM NOBAHAR	**Art Unit** 2432

✓	**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	07/06/2009								
	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.** 12210926	**Applicant(s)/Patent Under Reexamination** ASGHARI-KAMRANI ET AL.
	Examiner ABDULHAKIM NOBAHAR	**Art Unit** 2432

✓	**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	07/06/2009								
	37	✓								
	38	✓								
	39	✓								
	40	✓								
	41	✓								
	42	✓								
	43	✓								
	44	✓								
	45	✓								
	46	✓								
	47	✓								
	48	✓								
	49	✓								
	50	✓								
	51	✓								
	52	✓								
	53	✓								
	54	✓								
	55	✓								
	56	✓								
	57	✓								
	58	✓								
	59	✓								
	60	✓								
	61	✓								
	62	✓								

Search Notes	**Application/Control No.** 12210926	**Applicant(s)/Patent Under Reexamination** ASGHARI-KAMRANI ET AL.
	Examiner ABDULHAKIM NOBAHAR	**Art Unit** 2432

SEARCHED

Class	Subclass	Date	Examiner
726	2,4,5,21	7/6/2009	AN

SEARCH NOTES

Search Notes	Date	Examiner
East Inventors names search (see attached report)	7/6/2009	AN
Overal EAST - BRS search (see attached report)	7/6/2009	AN

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

/A. N./ Examiner.Art Unit 2432	

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L2	5	ASGHARI-KAMRANI near (NADER KAMRAN)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/06 09:06
L3	106192	(online Internet electronic$4 web cyber) near3 (shop$4 commerc$3 purchas$3 buy $3 trad$3 business retail$3 sell$3 procur$5)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/06 09:10
L4	106189	3 and @pd>="2001121"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/06 09:12
L5	34078	4 and ((user client consumer customer subscrib$3 buy$3 purchas$3 shop$4) near3 (authenticat$3 or verif$4 or verification or valid$5 authoriz$5 confirm$3))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/06 09:12
L6	11103	4 and ((trad$3 entity party pay$3 spend$3 partner) near3 (authenticat$3 or verif $4 or verification or valid$5 authoriz$5 confirm$3))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/06 09:13
L7	36263	5 6	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/06 09:13
L9	23661	7 and ((user or client consumer customer subscrib $3 buy$3 purchas$3 shop $4) near5 (center$3 central $5 centre centralization or broker$4 or authority authoritative or authoriz$5 official$3 or trust$3))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/06 09:14
L10	11508	7 and ((trad$3 entity party pay$3 spend$3 partner) near5 (center$3 central$5 centre centralization or broker$4 or authority authoritative or authoriz$5 official$3 or trust$3))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/06 09:15

L11	25376	9 10	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/06 09:17
L12	16733	11 and ((identity or identif$4 or identification or Id or code securecode password secret$3 PIN passphrase) near5 (match$4 compar$4 check$3 examin$5 verif$4 verification valid$5))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/06 09:17
L13	5159	12 and ((identity or identif$4 or identification or Id or code securecode password secret$3 PIN passphrase) near5 (match$4 compar$4 check$3 examin$5 verif$4 verification valid$5) near5 (deny$4 den$4 reject$4 approv$4 disapprov$4 accept $4 allow$4 permit$4 permision authoriz$5))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/06 09:17
L14	4429	13 and (user or client consumer customer subscribing subscriber buying buyer purchaser purchasing shopper shopping trader trading entity party paying payer spender spend partner person outfit verture counterpart) adj2 (register $5 apply$4 application request$4 enlist$4 enroll$4 sign$3 ask$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/06 09:18
L16	3644	14 and ((register$5 apply$4 application request$4 enlist $4 enroll$4 sign$3 ask$3) near5 (center$3 central$5 centre centralization or broker$4 or authority authoritative or authoriz$5 official$3 or trust$3))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/06 09:23
L18	3381	16 and ((center$3 central$5 centre centralization or broker$4 or authority authoritative or authoriz$5 or party official$3 or trust$3) near5 (identity or identif$4 or identification or Id or code securecode password secret$3 PIN passphrase))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/06 09:24

L19	3018	18 and ((identity or identif$4 or identification or Id or code securecode password secret$3 PIN passphrase) near3 (tim$3 or predict$4 unpredict$4 or temp or tempora$4 or one onetime variable varying or dynamic $4 provision$4 intrim transi $4 short singl))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/06 09:26
L20	2181	19 and ((identity or identif$4 or identification or Id or code securecode password secret$3 PIN passphrase) near3 (time-base$3 timebased time-depend$3 time$3 depend$3))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/06 09:27
L21	3018	19 20	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/06 09:27
L22	2965	21 and ((user or client consumer customer subscrib $3 buy$3 purchas$3 shop$4 trad$3 entity party pay$3 spend$3 partner commerc$3 commerciality business counterpart) same (center$3 central$5 centre centralization or broker$4 or authority authoritative or authoriz$5 or party oficial$3 or trust$3) same (retail$3 or market$3 aftermarket$3 store or provid$3 or merchant or sell$3 or distribut$3 or site or web or recipient or destination sppl $4))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/06 09:28
L23	1749	22 and ((user or client consumer customer subscrib $3 buy$3 purchas$3 shop$4 trad$3 entity party pay$3 spend$3 partner commerc$3 commerciality business counterpart) same (center$3 central$5 centre centralization or broker$4 or authority authoritative or authoriz$5 or party official$3 or trust$3) same (retail$3 or market$3 aftermarket$3 store or provid$3 or merchant or sell$3 or distribut$3 or site or web or	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/06 09:29

		recipient or destination sppl $4) same (online Internet electronic$4 web network$3) same (authenticat$4 or verif $5 or verification or ascertain $5 or valid$5))				
L24	505	23 and ((user or client consumer customer subscrib $3 buy$3 purchas$3 shop$4 trad$3 entity party pay$3 spend$3 partner commerc$3 commerciality business counterpart) near5 (center $3 central$5 centre centralization or broker$4 or authority authoritative or authoriz$5 or party official$3 or trust$3) same (retail$3 or market$3 aftermarket$3 store or provid$3 or merchant or sell$3 or distribut$3 or site or web or recipient or destination sppl $4) near5 (online Internet electronic$4 web network$3) same (authenticat$4 or verif $5 or verification or ascertain $5 or valid$5) same (identity or identif$4 or identification or Id or code securecode password secret$3 PIN passphrase) same (deny$4 den$4 reject$4 approv$4 disapprov$4 accept$4 allow $4 permit$4 permision authoriz$5))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/06 09:34
L25	157	24 and ((user or client consumer customer subscrib $3 buy$3 purchas$3 shop$4 trad$3 entity party pay$3 spend$3 partner commerc$3 commerciality business counterpart) near5 (center $3 central$5 centre centralization or broker$4 or authority authoritative or authoriz$5 or party official$3 or trust$3) same (retail$3 or market$3 aftermarket$3 store or provid$3 or merchant or sell$3 or distribut$3 or site or web or recipient or destination sppl $4) same (online Internet electronic$4 web network$3) same (authenticat$4 or verif $5 or verification or ascertain	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/06 09:37

		$5 or valid$5) same (identity or identif$4 or identification or Id or code securecode password secret$3 PIN passphrase) near5 (tim$3 or predict$4 unpredict$4 or temp or tempora$4 or one onetime variable varying or dynamic$4 provision$4 intrim transi$4 short) same (deny$4 den$4 reject$4 approv$4 disapprov$4 accept$4 allow$4 permit$4 permision authoriz$5) same (match$3 compar$4 check$3 examin$5 verif$4 verification valid$5) same (goods merchandis$4 servic$3 access$3 supplies commodit$3 product produce))				
L26	124	25 and ((identity or identif$4 or identification or Id or code securecode password secret$3 PIN passphrase) near3 (tempora$4 onetime variable varying or dynamic$4 single dynamic))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/06 09:39
L27	3613	726/2 726/4 726/5 726/21	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/06 09:40
L28	683	27 and ((identity or identif$4 or identification or Id or code securecode password secret$3 PIN passphrase) near3 (tempora$4 onetime variable varying or dynamic$4 single dynamic))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/06 09:41
L29	26	28 and ((user or client consumer customer subscrib$3 buy$3 purchas$3 shop$4 trad$3 entity party pay$3 spend$3 partner commerc$3 commerciality business counterpart) near5 (center$3 central$5 centre centralization or broker$4 or authority authoritative or authoriz$5 or party official$3 or trust$3) same (retail$3 or market$3 aftermarket$3 store or provid$3 or merchant or sell$3 or distribut$3 or site or web or recipient or destination sppl	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/06 09:42

		$4) same (online Internet electronic$4 web network$3) same (authenticat$4 or verif $5 or verification or ascertain $5 or valid$5) same (identity or identif$4 or identification or Id or code securecode password secret$3 PIN passphrase) near5 (tim$3 or predict$4 unpredict$4 or temp or tempora$4 or one onetime variable varying or dynamic$4 provision$4 intrim transi$4 short) same (deny$4 den$4 reject$4 approv$4 disapprov$4 accept $4 allow$4 permit$4 permision authoriz$5) same (match$3 compar$4 check$3 examin$5 verif$4 verification valid$5) same (goods merchandis$4 servic$3 access$3 supplies commodit $3 product produce))				
L32	16	29 and @pd>="20071121"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/06 09:51
L33	24383	3 and @pd>="20071121"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/06 09:52
L35	45	25 and @pd>="20071121"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/06 09:54

7/6/2009 9:57:21 AM
C:\ Documents and Settings\ hnobahar\ My Documents\ EAST\ Workspaces\ 09940635_12210926.wsp

PTO/SB/08A (09-06)
Approved for use through 03/31/2007. 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.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	
Filing Date	
First Named Inventor	
Art Unit	
Examiner Name	
Attorney Docket Number	Kamrani-00001

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
/H.N./		US- 4747050	05/24/1988	Brachtl et al.	
/H.N./		US- 4965568	10/23/1990	Atalla et al.	
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]
						□
						□
						□
						□
						□
						□

Examiner Signature	/Abdulhakim Nobahar/	Date Considered	07/06/2009

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

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 2 hours 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, 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 (1-800-786-9199) 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
12/210,926	09/15/2008	Nader Asghari-Kamrani	Kamrani-00001

CONFIRMATION NO. 7516

PUBLICATION NOTICE

OC000000033964136

63670
MAXVALUEIP CONSULTING
11204 ALBERMYRTLE ROAD
POTOMAC, MD 20854

Title: Centralized Identification and Authentication System and Method

Publication No.US-2009-0013182-A1
Publication Date:01/08/2009

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

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
12/210,926	09/15/2008	2131	1485	Kamrani-00001	62	2

CONFIRMATION NO. 7516

63670
MAXVALUEIP CONSULTING
11204 ALBERMYRTLE ROAD
POTOMAC, MD 20854

FILING RECEIPT

OC000000032335586

Date Mailed: 10/01/2008

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**

Applicant(s)

Nader Asghari-Kamrani, Centreville, VA;
Kamran Asghari-Kamrani, Centreville, VA;

Power of Attorney: The patent practitioners associated with Customer Number 63670

Domestic Priority data as claimed by applicant

This application is a CON of 11/239,046 09/30/2005
which claims benefit of 60/615,603 10/05/2004
This application 12/210,926
is a CON of 09/940,635 08/29/2001 PAT 7,356,837

Foreign Applications

If Required, Foreign Filing License Granted: 09/29/2008

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 12/210,926**

Projected Publication Date: 01/08/2009

Non-Publication Request: No

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

Title

Centralized Identification and Authentication System and Method

Preliminary Class

713

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 (1-866-999-4158).

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).

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
12/210,926	09/15/2008	Nader Asghari-Kamrani	Kamrani-00001

CONFIRMATION NO. 7516

63670
MAXVALUEIP CONSULTING
11204 ALBERMYRTLE ROAD
POTOMAC, MD 20854

POA ACCEPTANCE LETTER

OC000000032335599

Date Mailed: 10/01/2008

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 09/15/2008.

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

/ntrinh/

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

page 1 of 1

PTO/SB/05 (04-05)
Approved for use through 07/31/2006. 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.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	Kamrani-00001
First Inventor	
Title	
Express Mail Label No.	

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO: **Commissioner for Patents**
P.O. Box 1450
Alexandria VA 22313-1450

1. □ **Fee Transmittal Form** (e.g., PTO/SB/17)
(Submit an original and a duplicate for fee processing)
2. ☑ **Applicant claims small entity status**.
See 37 CFR 1.27.
3. ☑ **Specification** [*Total Pages*___________]
Both the claims and abstract must start on a new page
(For information on the preferred arrangement, see MPEP 608.01(a))
4. ☑ **Drawing(s)** (*35 U.S.C. 113*) [*Total Sheets* __________]
5. **Oath or Declaration** [*Total Sheets* __________]
a. ☑ Newly executed (original or copy)
b. □ A copy from a prior application (37 CFR 1.63(d))
(for continuation/divisional with Box 18 completed)
i. □ DELETION OF INVENTOR(S)
Signed statement attached deleting inventor(s) name in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
6. □ **Application Data Sheet.** See 37 CFR 1.76
7. □ **CD-ROM or CD-R** in duplicate, large table or Computer Program *(Appendix)*
□ Landscape Table on CD
8. **Nucleotide and/or Amino Acid Sequence Submission**
(if applicable, items a. – c. are required)
a. □ Computer Readable Form (CRF)
b. Specification Sequence Listing on:
i. □ CD-ROM or CD-R (2 copies); or
ii. □ Paper
c. □ Statements verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

9. □ **Assignment Papers** (cover sheet & document(s))
Name of Assignee_______________________________
____
10. □ **37 CFR 3.73(b) Statement** *(when there is an assignee)* ☑ **Power of Attorney**
11. □ **English Translation Document** *(if applicable)*
12. ☑ **Information Disclosure Statement** (PTO/SB/08 or PTO-1449)
□ Copies of citations attached
13. □ **Preliminary Amendment**
14. □ **Return Receipt Postcard** (MPEP 503)
(*Should be specifically itemized)*
15. □ **Certified Copy of Priority Document(s)**
(if foreign priority is claimed)
16. □ **Nonpublication Request** under 35 U.S.C. 122(b)(2)(B)(i). Applicant must attach form PTO/SB/35 or equivalent.
17. ☑ Other: Examiner Nobahar examined and allowed the parent case (PN 7356837).

18. If a CONTINUING APPLICATION, *check appropriate box, and supply the requisite information below and in the first sentence of the specification following the title, or in an Application Data Sheet under 37 CFR 1.76:*

☑ Continuation □ Divisional □ Continuation-in-part (CIP) of prior application No.: 11/239,046................

Prior application information: *Examiner* A. Nobahar (PN 7356837) *Art Unit:* Examiner Nobahar

19. CORRESPONDENCE ADDRESS

☑ The address associated with Customer Number: 63670 ***OR*** □ Correspondence address below

Name					
Address					
City		State		Zip Code	
Country		Telephone		Email	

Signature	/Bijan Tadayon, Reg.# 47349/	Date	Sept-3-2008
Name (Print/Type)	Bijan Tadayon	Registration No. (Attorney/Agent)	47349

This collection of information is required by 37 CFR 1.53(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 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.

Privacy Act Statement

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

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

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

Centralized Identification and Authentication System and Method

Related Applications

This application is a Continuation of Application Number 11/239,046, filed 9-30-2005, with a priority of a US provisional application 60/615,603, filed Oct-5-2004, with the same inventors and assignee. This application is also a Continuation of another US application 09/940,635, filed Aug 29, 2001, and patented as PN 7,356,837, on Apr-8-2008, titled "Centralized identification and authentication system and method", with the same inventors and assignee. Please note that the current application has the same exact specification and Figures as those submitted with the original application 09/940,635, filed Aug 29, 2001.

BACKGROUND OF THE INVENTION

1. FIELD OF THE INVENTION

The present invention relates to a centralized identification and authentication system and method for identifying an individual over a communication network such as Internet, to increase security in e-commerce. More particularly a method and system for generation of a dynamic, non-predictable and time dependent SecureCode for the purpose of positively identifying an individual.

2. DESCRIPTION OF THE RELATED ART

The increasing use of the Internet and the increase of businesses utilizing e-commerce have lead to a dramatic increase in customers releasing confidential personal and financial information, in the form of social security numbers, names, addresses, credit card numbers and bank account numbers, to identify themselves. This will allow them to get access to the restricted web sites or electronically purchase desired goods or services. Unfortunately this type of identification is not only unsafe but also it is not a foot proof that the user is really the person he says he is. The effect of these increases is reflected in the related art.

U.S. Pat. No. 5,732,137 issued to Aziz outlines a system and method for providing remote user authentication in a public computer network such as the Internet. More specifically, the system and method provides for remote authentication using a one-time password scheme having a secure out-of-band channel for initial password delivery.

U.S. Pat. No. 5,815,665 issued to Teper et al. outlines the use of a system and method for enabling consumers to anonymously, securely and conveniently purchase on-line services from multiple service providers over a distributed network, such as the Internet. Specifically, a trusted third-party broker provides billing and security services for registered service providers via an online brokering service, eliminating the need for the service providers to provide these services.

U.S. Pat. No 5,991,408 issued to Pearson , et al. outlines a system and method for using a biometric element to create a secure identification and verification system, and more specifically to an apparatus and a method for creating a hard problem which has a representation of a biometric element as its solution.

Although each of the previous patents outline a valuable system and method, what is really needed is a system and method that offers digital identity to the users and allows them to participate in e-commerce without worrying about the privacy and security. In addition to offering security and privacy to the users, the new system has to be simple for businesses to adopt and also doesn’t require the financial institutions to change their existing systems. Such a secure, flexible and scalable system and method would be of great value to the businesses that would like to participate in today’s electronic commerce.

None of the above inventions and patents, taken either singularly or in combination, is seen to describe the instant inven¬tion as claimed. Thus a centralized identification and authentication system and method solving the aforementioned problems is desired.

For convenience, the term "user" is used throughout to represent both a typical person consuming goods and services as well as a business consuming goods and services.

As used herein, a "Central-Entity" is any party that has user's personal and/or financial information, UserName, Password and generates dynamic, non-predictable and time dependable SecureCode for the user. Examples of Central-Entity are: banks, credit card issuing companies or any intermediary service companies.

As also used herein, an "External-Entity" is any party offering goods or services that users utilize by directly providing their UserName and SecureCode as digital identity. Such entity could be a merchant, service provider or an online site. An "External-Entity" could also be an entity that receives the user's digital identity indirectly from the user through another External-Entity, in order to authenticate the user, such entity could be a bank or a credit card issuing company.

The term “UserName” is used herein to denote any alphanumeric name, id, login name or other identification phrase, which may be used by the “Central-Entity” to identify the user.

The term “Password” is used herein to denote any alphanumeric password, secret code, PIN, prose phrase or other code, which may be stored in the system to authenticate the user by the “Central-Entity”.

The term “SecureCode” is used herein to denote any dynamic, non-predictable and time dependent alphanumeric code, secret code, PIN or other code, which may be broadcast to the user over a communication network, and may be used as part of a digital identity to identify a user as an authorized user.

The term "digital identity" is used herein to denote a combination of user's "SecureCode" and user's information such as "UserName", which may result in a dynamic, non-predictable and time dependable digital identity that could be used to identify a user as an authorized user.

The term “financial information” is used herein to denote any credit card and banking account information such as debit cards, savings accounts and checking accounts.

SUMMARY OF THE INVENTION

The invention relates to a system and method provided by a Central-Entity for centralized identification and authentication of users and their transactions to increase security in e-commerce. The system includes:

˜ A Central-Entity: This entity centralizes users personal and financial information in a secure environment in order to prevent the distribution of user's information in e-commerce. This information is then used to create digital identity for the users. The users may use their digital identity to identify themselves instead of providing their personal and financial information to the External-Entities;

˜ A plurality of users: A user represents both a typical person consuming goods and services as well as a business consuming goods and services, who needs to be identified in order to make online purchases or to get access to the restricted web sites. The user registers at the Central-Entity to receive his digital identity, which is then provided to the External-Entity for identification;

˜ A plurality of External-Entities: An External-Entity is any party offering goods or services in e-commerce and needs to authenticate the users based on digital identity.

The user signs-up at the Central-Entity by providing his personal or financial information. The Central-Entity creates a new account with user's personal or financial information and issues a unique UserName and Password to the user. The user provides his Username and Password to the Central-Entity for identification and authentication purposes when accessing the services provided by the Central-Entity. The Central-Entity also generates dynamic, non-predictable and time dependent SecureCode for the user per user's request and issues the SecureCode to the user. The Central-Entity maintains a copy of the SecureCode for identification and authentication of the user's digital identity. The user presents his UserName and SecureCode as digital identity to the External-Entity for identification. When an External-Entity receives the user's digital identity (UserName and SecureCode), the External-Entity will forward this information to the Central-Entity to identify and authenticate the user. The Central-Entity will validate the information and sends an approval or denial response back to the External-Entity.

There are also communications networks for the user, the Central-Entity and the External-Entity to give and receive information between each other.

This invention also relates to a system and method provided by a Central-Entity for centralized identification and authentication of users to allow them access to restricted web sites using their digital identity, preferably without revealing confidential personal or financial information.

This invention further relates to a system and method provided by a Central-Entity for centralized identification and authentication of users to allow them to purchase goods and services from an External-Entity using their digital identity, preferably without revealing confidential personal or financial information.

Accordingly, it is a principal object of the invention to offer digital identity to the users for identification in e-commerce.

It is another object of the invention to centralize user's personal and financial information in a secure environment.

It is another object of the invention to prevent the user from distributing their personal and financial information.

It is a further object of the invention to keep merchants, service providers, Internet sites and financial institutions satisfied by positively identifying and authenticating the users.

It is another object of the invention to reduce fraud and increase security for e-commerce.

It is another object of the invention to allow businesses to control visitor's access to their web sites.

It is another object of the invention to protect the customer from getting bills for goods and services that were not ordered.

It is another object of the invention to increase customers' trust and reduce customers' fear for e-commerce.

It is another object to decrease damages to the customers, merchants and financial institutions.

It is an object of the invention to provide improved elements and arrangements thereof for the purposes described which are inexpensive, dependable and fully effective in accomplishing its intended purposes.

These and other objects of the present invention will become readily apparent upon further review of the following specification and drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a high-level overview of a centralized identification and authentication system and method according to the present invention.

Fig. 2 is a detailed overview of a centralized identification and authentication system and method according to the present invention.

Fig. 3 is a block diagram of the registration of a customer utilizing a centralized identification and authentication system and method according to the present invention.

Fig. 4 is a block diagram of the transaction of a customer utilizing a centralized identification and authentication system and method according to the present invention.

Fig. 5 is a block diagram of a Central-Entity authorizing a user utilizing a centralized identification and authentication system and method according to the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Detailed descriptions of the preferred embodiment are provided herein. It is to be understood, however, that the present invention may be embodied in various forms. Therefore, specific details disclosed herein are not to be interpreted as limiting, but rather as a basis for the claims and as a representative basis for teaching one skilled in the art to employ the present invention in virtually any appropriately detailed system, structure or manner.

The invention relates to a system 1 and method 2 to identify and authenticate the users and their transactions to increase security in e-commerce. Fig. 1 illustrates a system to positively identify the users 10 in e-commerce based on digital identity.

The system 1 comprises a plurality of users 10, a plurality of External-Entities 20 with goods and services that are desired by the users 10 and a Central-Entity 30 providing a unique UserName and Password to the users 10 and generating dynamic, non-predictable and time dependent SecureCode for the users 10 per user's request. There are also communication networks 50 for the user 10, the Central-Entity 30 and the External-Entity 20 to give and receive information between each other.

It would be desirable to develop a new system 1 and method 2 to centralize user's personal and financial information in a secure environment and to offer digital identity to the users 10 in order to provide privacy, increase security and reduce fraud in e-commerce. Ideally, a secure identification and authentication system 1 would identify legitimate users 10 and unauthorized users 10. This would increase the user's trust, which leads to more sales and cash flow for the merchants/service providers.

The present invention relates to a system 1 and method 2 to support this ideal identification and authentication system. For identification purpose, a digital identity (a unique UserName and a dynamic, non-predictable and time dependent SecureCode) is used by the user 10 at the time of ordering or at the time of accessing a restricted Internet site. A series of steps describing the overall method are conducted between the users 10, the Central-Entity 30 and the External-Entity 20 and are outlined in Fig. 3,4,5.

There are three distinct phases involved in using the centralized identification and authentication system Fig. 2, the first of which being the registration phase, which is depicted in Fig. 3. During the registration phase, the user 10 provides his personal or financial information to the Central-Entity 30. The user 10 registers at the Central-Entity 30, 100, 104 and receives his account and login information such as UserName and Password 108. User 10 can access his account at any time by accessing the Central-Entity's system using a communication network 50 and logging into the system.

Next is the transaction phase, where the user 10 attempts to access a restricted web site or attempts to buy services or products 110, as illustrated in Fig. 4, through a standard interface provided by the External-Entity 20, similar to what exists today and selects digital identity as his identification and authorization or payment option. The External-Entity 20 displays the access or purchase authorization form requesting the user 10 to authenticate himself using his UserName and SecureCode as digital identity. The user 10 requests SecureCode from the Central-Entity 30 by accessing his account over the communication network 50, 114. The Central-Entity 30 generates dynamic, non-predictable and time dependable SecureCode 118 for the user 10. The Central-Entity 30 maintains a copy of the SecureCode for identification and authentication of the user 10 and issues the SecureCode to the user 10. When the user 10 receives the SecureCode 120, the user 10 provides his UserName and SecureCode as digital identity to the External-Entity 20, 124, Fig. 4.

The third phase is identification and authorization phase. Once the user 10 provides his digital identity to the External-Entity 20, the External-Entity 20 forwards user's digital identity along with the identification and authentication request to the Central-Entity 30, 130, as illustrated in Fig. 5. When the Central-Entity 30 receives the request containing the user's digital identity, the Central-Entity 30 locates the user's digital identity (UserName and SecureCode) in the system 134 and compares it to the digital identity received from the External-Entity 20 to identify and validate the user 10, 138. The Central-Entity 30 generates a reply back to the External-Entity 20 via a communication network 50 as a result of the comparison. If both digital identities match, the Central-Entity 30 will identify the user 10 and will send an approval of the identification and authorization request to the External-Entity 20, 140, otherwise will send a denial of the identification and authorization request to the External-Entity 20, 150. The External-Entity 20 receives the approval or denial response in a matter of seconds. The External-Entity 20 might also display the identification and authentication response to the user 10.

To use the digital identity feature, the Central-Entity 30 provides the authorized user 10 the capability to obtain a dynamic, non-predictable and time dependable SecureCode. The user 10 will provide his UserName and SecureCode as digital identity to the External-Entity 20 when this information is required by the External-Entity 20 to identify the user 10.

The Central-Entity 30 may add other information to the SecureCode before sending it to the user 10, by algorithmically combining SecureCode with user's information such as UserName. The generated SecureCode will have all the information needed by the Central-Entity 30 to identify the user 10. In this case the user will only need to provide his SecureCode as digital identity to the External-Entity 20 for identification.

In the preferred embodiment, the user 10 uses the communication network 50 to receive the SecureCode from the Central-Entity 30. The user 10 submits the SecureCode in response to External-Entity's request 124. The SecureCode is preferably implemented through the use of an indicator. This indicator has two states: "on" for valid and "off" for invalid. When the user 10 receives the SecureCode, the SecureCode is in "on" or "valid" state. The Central-Entity 30 may improve the level of security by invalidating the SecureCode after it's use. This may increase the level of difficulty for unauthorized user. Two events may cause a valid SecureCode to become invalid:

1. Timer event: This event occurs when the predefined time passes. As mentioned above the SecureCode is time dependent.

2. Validation event: This event occurs when the SecureCode forwarded to the Central-Entity 30 (as part of digital identity) corresponds to the user's SecureCode held in the system. When this happens the Central-Entity 30 will invalidate the SecureCode to prevent future use and sends an approval identification and authorization message to the External-Entity 20,140.

A valid digital identity corresponds to a valid SecureCode. When the SecureCode becomes invalid, the digital identity will also become invalid.

While the invention has been described in connection with a preferred embodiment, it is not intended to limit the scope of the invention to the particular form set forth, but on the contrary, it is intended to cover such alternatives, modifications, and equivalents as may be included within the spirit and scope of the invention as defined by the appended claims.

Claims

1. A method for authenticating a user in e-commerce for a transaction based on a digital identity issued by a Central-Entity, the method comprising:

a. the user communicates with an External-Entity and performs a secure transaction with the External-Entity;

b. the External-Entity requires the user to authenticate itself by providing a valid digital identity before executing the transaction;

c. the user establishes communication with the Central-Entity and submits a request for a dynamic SecureCode in response to the Extemal-Entity's requirement;

d. the Central-Entity:

i. dynamically generates a dynamic SecureCode for the user in response to the user request;

ii. algorithmically combines said generated SecureCode with user-specific information before providing the SecureCode to the user;

iii. maintains a copy of said generated SecureCode; and

iv. provides said generated SecureCode to the user,

e. the Extemal-Entity receives a digital identity from the user, wherein the digital identity comprises a UserName and said generated SecureCode, and forwards said digital identity to the Central-Entity for authentication of the user;

f. the Central-Entity receives said digital identity, validates said digital identity based on said SecureCode maintained in its system, and if valid, then authenticates the user and sends an affirmation message to the Extemal-Entity; and

g. upon receipt of an affirmation message from the Central-Entity, the Extemal-Entity executes the transaction.

2. A method as recited in claim 1, wherein said user has a pre-existing relationship with the External-Entity.

3. A method as recited in claim 1, wherein said user has no pre-existing relationship with the External-Entity.

4. A method as recited in claim 1, wherein said External-Entity and said Central-Entity share a cryptographic algorithm.

5. A method as recited in claim 1, wherein said External-Entity and said Central-Entity do not share any cryptographic algorithm.

6. A method as recited in claim 1, wherein said External-Entity and said Central-Entity are within the same organization.

7. A method as recited in claim 1, wherein said External-Entity and said Central-Entity are the same organization.

8. A method as recited in claim 7, wherein all the communications and transactions between said External-Entity and said Central-Entity are within said same organization.

9. A method as recited in claim 8, wherein said all the communications and transactions between said External-Entity and said Central-Entity are transparent to said user and an outside observer.

10. A method as recited in claim 8, wherein said all the communications and transactions between said External-Entity and said Central-Entity are done within a same server.

11. A method as recited in claim 8, wherein said all the communications and transactions between said External-Entity and said Central-Entity are done between two or more different servers.

12. A method as recited in claim 1, wherein said digital identity is based on a logical combination of the SecureCode and the user-specific information.

13. A method as recited in claim 1, wherein said digital identity is based on the SecureCode and the user-specific information.

14. The method of claim 1, wherein the user-specific information comprises UserName.

15. The method of claim 14, wherein the UserName corresponds to a alphanumeric name, ID, login name, an identification phrase, account number, phone number, IP address, hardware key, software key, or serial number.

16. The method of claim 1, wherein the transaction corresponds to a financial transaction.

17. The method of claim 1, wherein the transaction corresponds to a non-financial transaction.

18. The method of claim 1, wherein the transaction corresponds to access to restricted web-site.

19. The method of claim 1, wherein said communication is done on a communication network including Internet, wireless, mobile network, satellite, or private network.

20. The method of claim 1, wherein said communication is done on a communication network including at least a server and a client device.

21. A system for authenticating a user in e-commerce for a transaction based on a digital identity issued by a Central-Entity, the system comprising:

a. the user in communication with an External-Entity and performs a secure transaction with the External-Entity;

b. the External-Entity requires the user to authenticate itself by providing a valid digital identity before executing the transaction;

c. the user in communication with the Central-Entity and with a request for a dynamic SecureCode in response to the External-Entity's requirement;

d. the Central-Entity adapted to:

i. dynamically generate a dynamic SecureCode for the user in response to the user request;

ii. algorithmically combine said generated SecureCode with user-specific information before providing the SecureCode to the user;

iii. maintain a copy of said generated SecureCode; and

iv. provide said SecureCode to the user,

e. the Extemal-Entity adapted to receive a digital identity from the user, wherein the digital identity comprises a UserName and said generated SecureCode, and to forward said digital identity to the Central-Entity to authenticate the user;

f. the Central-Entity further adapted to validate the received said digital identity based on said SecureCode maintained in its system, and if valid, then to authenticate the user, and send an affirmation message to the Extemal-Entity; and

g. the Extemal-Entity further adapted to execute the transaction upon receipt of an affirmation message from the Central-Entity.

22. A system as recited in claim 21, wherein said user has a pre-existing relationship with the External-Entity.

23. A system as recited in claim 21, wherein said user has no pre-existing relationship with the External-Entity.

24. A system as recited in claim 21, wherein said External-Entity and said Central-Entity share a cryptographic algorithm.

25. A system as recited in claim 21, wherein said External-Entity and said Central-Entity do not share any cryptographic algorithm.

26. A system as recited in claim 21, wherein said External-Entity and said Central-Entity are within the same organization.

27. A system as recited in claim 21, wherein said External-Entity and said Central-Entity are the same organization.

28. A system as recited in claim 26, wherein all the communications and transactions between said External-Entity and said Central-Entity are within said same organization.

29. A system as recited in claim 28, wherein said all the communications and transactions between said External-Entity and said Central-Entity are transparent to an outside observer and said user.

30. A system as recited in claim 28, wherein said all the communications and transactions between said External-Entity and said Central-Entity are done within a same server.

31. A system as recited in claim 28, wherein said all the communications and transactions between said External-Entity and said Central-Entity are done between two or more different servers.

32. A system as recited in claim 21, wherein said digital identity is based on a logical combination of the SecureCode and the user-specific information.

33. A system as recited in claim 21, wherein said digital identity is based on the SecureCode and the user-specific information.

34. The system of claim 21, wherein the user-specific information comprises UserName.

35. The system of claim 34, wherein the UserName corresponds to a alphanumeric name, ID, login name, identification phrase, account number, phone number, IP address, hardware key, software key, or serial number.

36. The system of claim 21, wherein the transaction corresponds to a financial transaction.

37. The system of claim 21, wherein the transaction corresponds to a non-financial transaction.

38. The system of claim 21, wherein the transaction corresponds to access to restricted web-site.

39. The system of claim 21, wherein said communication is done on a communication network including Internet, wireless, mobile network, satellite, or private network.

40. The system of claim 21, wherein said communication is done on a communication network including at least a server and a client device.

41. A method as recited in claim 4, wherein said External-Entity is using said shared cryptographic algorithm to authenticate a user's identity based on said SecureCode.

42. A method as recited in claim 4, wherein said Central-Entity is using said shared cryptographic algorithm to generate said SecureCode.

43. A method as recited in claim 4, wherein said Central-Entity is using said shared cryptographic algorithm to authenticate a user's identity based on said SecureCode.

44. A method as recited in claim 1, wherein said External-Entity and said Central-Entity are the same entity.

45. The method as recited in claim 1, wherein said Central –Entity generates SecureCode with dependence on at least a dynamic variable.

46. The method as recited in claim 45, wherein said dynamic variable is time.

47. The method as recited in claim 1, wherein said Central-Entity generates SecureCode with dependence on one or more alphanumeric values.

48. The method as recited in claim 47, wherein said one or more alphanumeric values are one or more of the following: unique key, ID, login name, password, identification phrase, account number, phone number, IP address, Hardware key, software key or serial number.

49. The method as recited in claim 47, wherein said one or more alphanumeric values are seed values.

50. The method as recited in claim 1, wherein said digital identity is a SecureCode.

51. The method as recited in claim 1, wherein said user communicates with said Central-Entity over a communication network.

52. The system as recited in claim 21, wherein said digital identity is a SecureCode.

53. The method as recited in claim 1, wherein said user communicates with said External-Entity over a communication network.

54. The system as recited in claim 21, wherein said user communicates with said Central-Entity over a communication network.

55. The system as recited in claim 21, wherein said user communicates with said External-Entity over a communication network.

56. The method as recited in claim 1, wherein said request is generated based on a request event which is automatically generated from a computer, server, or central entity.

57. The method as recited in claim 1, wherein said request is generated based on a request event which is manually generated by an entity or person.

58. The method as recited in claim 1, wherein said request is generated based on a request event.

59. The method as recited in claim 58, wherein said request event is pressing a button.

60. The method as recited in claim 58, wherein said request event is a user's authentication request at said External-Entity.

61. The method as recited in claim 58, wherein said request event is sending a message to said Central-Entity.

62. The method as recited in claim 61, wherein said message is a text message.

ABSTRACT OF THE DISCLOSURE

A method and system is provided by a Central-Entity, for identification and authorization of users over a communication network such as Internet. Central-Entity centralizes users personal and financial information in a secure environment in order to prevent the distribution of user's information in e-commerce. This information is then used to create digital identity for the users. The digital identity of each user is dynamic, non predictable and time dependable, because it is a combination of user name and a dynamic, non predictable and time dependable secure code that will be provided to the user for his identification. The user will provide his digital identity to an External-Entity such as merchant or service provider. The External-Entity is dependent on Central-Entity to identify the user based on the digital identity given by the user. The External-Entity forwards user's digital identity to the Central-Entity for identification and authentication of the user and the transaction. The identification and authentication system provided by the Central-Entity, determines whether the user is an authorized user by checking whether the digital identity provided by the user to the External-Entity, corresponds to the digital identity being held for the user by the authentication system. If they correspond, then the authentication system identifies the user as an authorized user, and sends an approval identification and authorization message to the External-Entity, otherwise the authentication system will not identify the user as an authorized user and sends a denial identification and authorization message to the External-Entity.

DECLARATION FOR UTILITY OR DESIGN PATENT APPLICATION (37 CFR 1.63)

☑ Declaration Submitted With Initial Filing *OR* □ Declaration Submitted after Initial Filing (surcharge (37 CFR 1.16 (e)) required)

Attorney Docket Number	Kamrani1
First Named Inventor	Nader Asghari-Kamrani
COMPLETE IF KNOWN	
Application Number	
Filing Date	
Art Unit	
Examiner Name	

I hereby declare that:

Each inventor's residence, mailing address, and citizenship are as stated below next to their name.

I believe the inventor(s) named below to be the original and first inventor(s) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

Centralized Identification and Authentication System and Method

(Title of the Invention)

the specification of which

☑ is attached hereto

OR

□ was filed on (MM/DD/YYYY) ______ as United States Application Number or PCT International Application Number ______ and was amended on (MM/DD/YYYY) ______ (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or (f), or 365(b) of any foreign application(s) for patent, inventor's or plant breeder's rights certificate(s), or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent, inventor's or plant breeder's rights certificate(s), or any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached? YES	NO
			□	□	□
			□	□	□
			□	□	□
			□	□	□

□ Additional foreign application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto.

PTO/SB/01 (10-05)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

DECLARATION — Utility or Design Patent Application

Direct all correspondence to:	☑ The address associated with Customer Number: 63670	OR	□ Correspondence address below

Name		
Address		
City	State	ZIP
Country	Telephone	Email

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

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 willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

NAME OF SOLE OR FIRST INVENTOR: □ A petition has been filed for this unsigned inventor

Given Name (first and middle [if any]) Nader		Family Name or Surname Asghari-Kamrani	
Inventor's Signature			Date 09-12-2008
Residence: City Centreville	State VA	Country USA	Citizenship USA
Mailing Address 6558 Palisades Dr.			
City Centreville	State VA	Zip 20121	Country USA

☑ Additional inventors or a legal representative are being named on the supplemental sheet(s) PTO/SB/02A or 02LR attached hereto.

[Page 2 of 2]

PTO/SB/02A (07-06)
Approved for use through 01/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

DECLARATION

ADDITIONAL INVENTOR(S)
Supplemental Sheet

Page ______ of ______

Name of Additional Joint Inventor, if any:	☑ A petition has been filed for this unsigned inventor		
Given Name (first and middle (if any))	Family Name or Surname		
Kamran	Asghari-Kamrani		
Inventor's Signature Kam			August-8-08 Date
Centreville Residence: City	VA State	USA Country	Holland (Netherland) Citizenship
6547 Palisades Dr. Mailing Address			
Centreville City	VA State	20121 Zip	USA Country

Name of Additional Joint Inventor, if any:	□ A petition has been filed for this unsigned inventor		
Given Name (first and middle (if any))	Family Name or Surname		
Andrew	Torrance		
Inventor's Signature			Date
Residence: City	State	Country	Citizenship
Mailing Address			
City	State	Zip	Country

Name of Additional Joint Inventor, if any:	□ A petition has been filed for this unsigned inventor		
Given Name (first and middle (if any))	Family Name or Surname		
Inventor's Signature			Date
Residence: City	State	Country	Citizenship
Mailing Address			
City	State	Zip	Country

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 21 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 (1-800-786-9199) and select option 2.

PTO/SB/08A (09-06)
Approved for use through 03/31/2007. 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.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	
Filing Date	
First Named Inventor	
Art Unit	
Examiner Name	
Attorney Docket Number	Kamrani-00001

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US- 4747050			
		US- 4965568			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] -Number [4] -Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]
						□
						□
						□
						□
						□
						□

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

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 2 hours 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, 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 (1-800-786-9199) and select option 2.

1/5

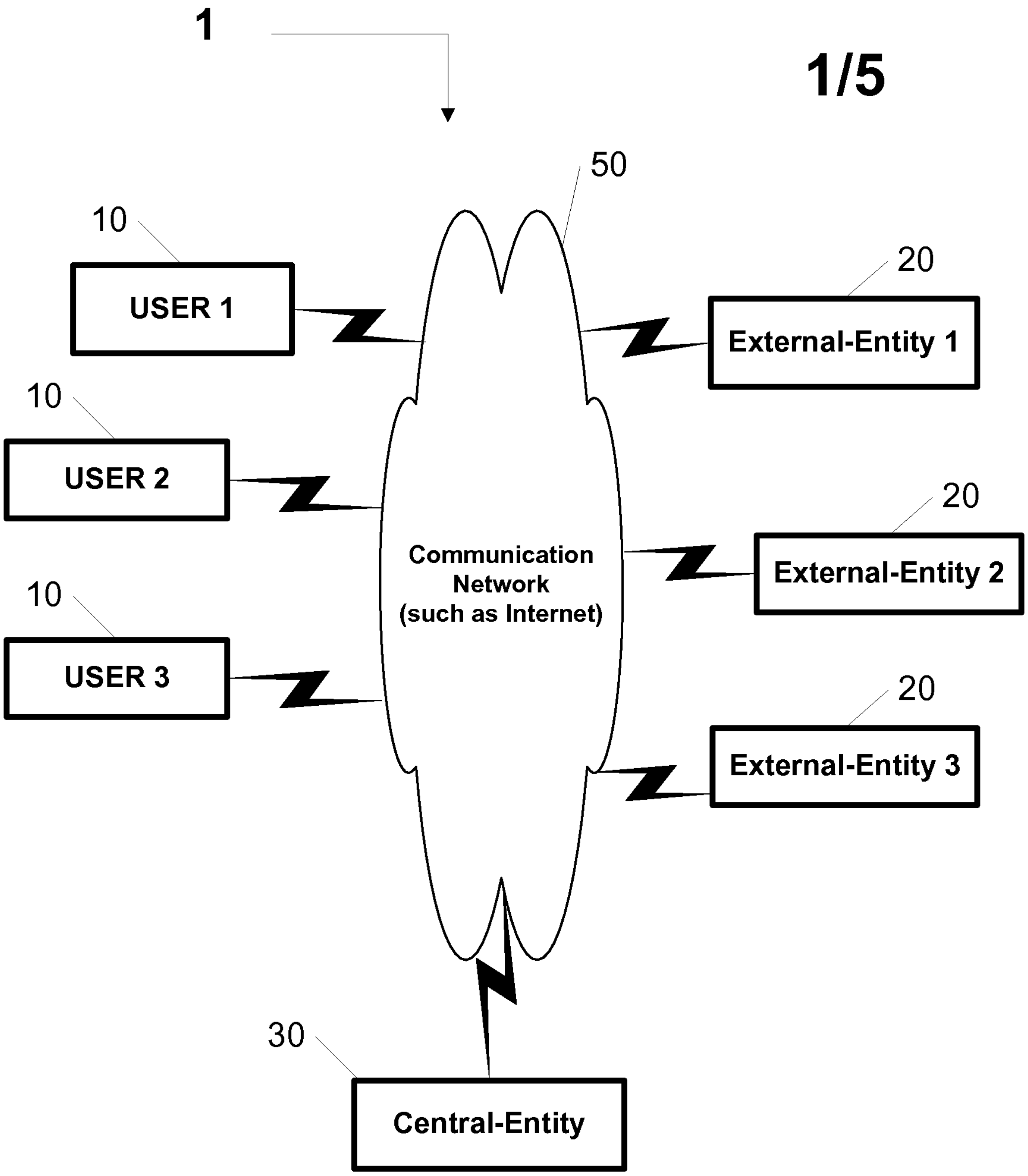

1
50
10
USER 1
20
External-Entity 1
10
USER 2
20
External-Entity 2
Communication
Network
(such as Internet)
10
USER 3
20
External-Entity 3
30
Central-Entity

Figure 1

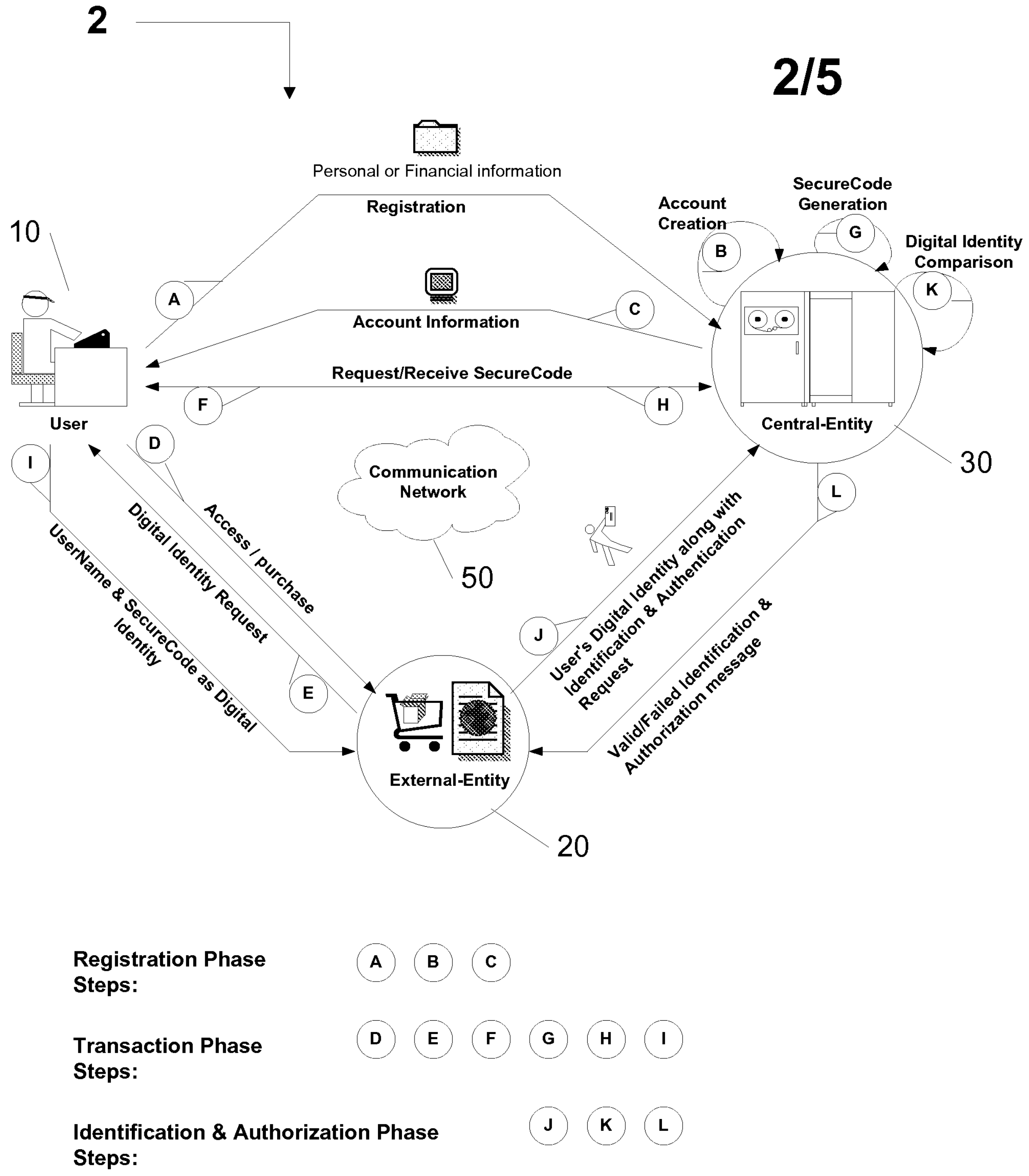

2
Personal or Financial information
Registration
Account Creation
SecureCode Generation
Digital Identity Comparison
10
A
B
C
G
K
Account Information
Request/Receive SecureCode
F
H
User
Central-Entity
30
D
I
Communication Network
50
L
Access / purchase
Digital Identity Request
UserName & SecureCode as Digital Identity
E
J
User's Digital Identity along with Identification & Authentication Request
Valid/Failed Identification & Authorization message
External-Entity
20
Registration Phase Steps:
A B C
Transaction Phase Steps:
D E F G H I
Identification & Authorization Phase Steps:
J K L

Figure 2

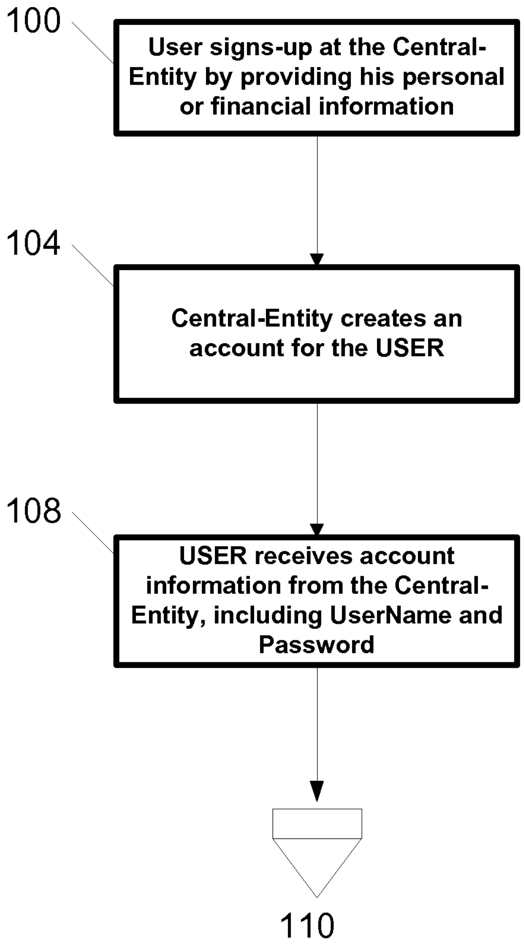

100
User signs-up at the Central-Entity by providing his personal or financial information
104
Central-Entity creates an account for the USER
108
USER receives account information from the Central-Entity, including UserName and Password
110

Figure 3

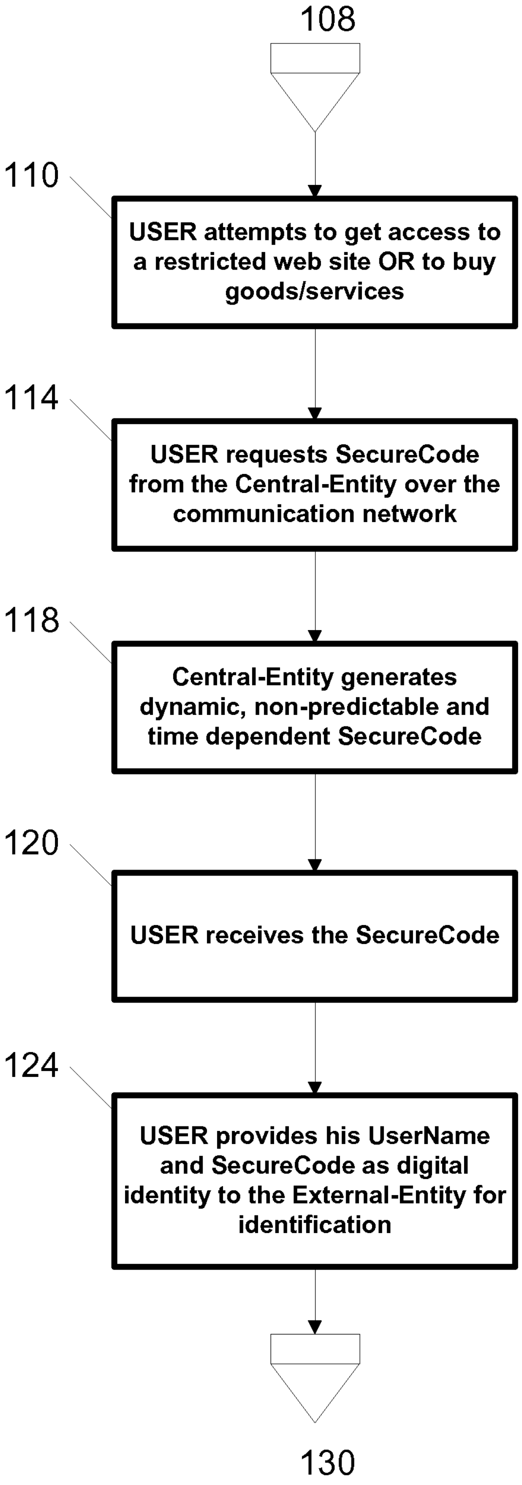

108
110
USER attempts to get access to a restricted web site OR to buy goods/services
114
USER requests SecureCode from the Central-Entity over the communication network
118
Central-Entity generates dynamic, non-predictable and time dependent SecureCode
120
USER receives the SecureCode
124
USER provides his UserName and SecureCode as digital identity to the External-Entity for identification
130

Figure 4

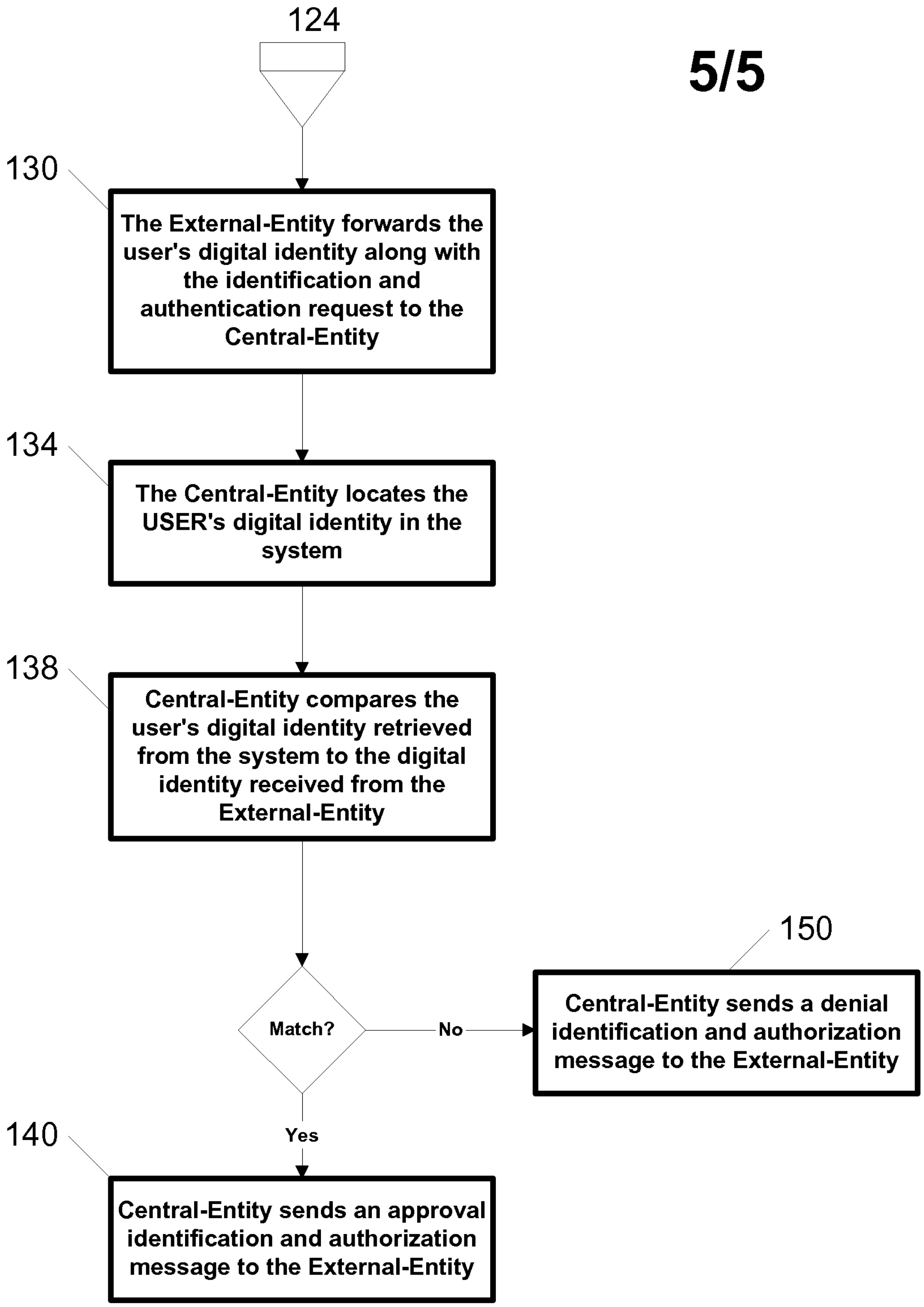

124
130
The External-Entity forwards the user's digital identity along with the identification and authentication request to the Central-Entity
134
The Central-Entity locates the USER's digital identity in the system
138
Central-Entity compares the user's digital identity retrieved from the system to the digital identity received from the External-Entity
Match?
No
150
Central-Entity sends a denial identification and authorization message to the External-Entity
Yes
140
Central-Entity sends an approval identification and authorization message to the External-Entity

Figure 5

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	Centralized Identification and Authentication System and Method
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Filer:	Bijan Tadayon
Attorney Docket Number:	Kamrani-00001

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	75	75
Utility Search Fee	2111	1	255	255
Utility Examination Fee	2311	1	105	105
Pages:				
Claims:				
Claims in excess of 20	2202	42	25	1050
Miscellaneous-Filing:				
Petition:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**1485**

Electronic Acknowledgement Receipt

EFS ID:	3946100
Application Number:	12210926
International Application Number:	
Confirmation Number:	7516
Title of Invention:	Centralized Identification and Authentication System and Method
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Customer Number:	63670
Filer:	Bijan Tadayon
Filer Authorized By:	
Attorney Docket Number:	Kamrani-00001
Receipt Date:	15-SEP-2008
Filing Date:	
Time Stamp:	19:00:30
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$1485
RAM confirmation Number	4230
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1	Transmittal of New Application	utilitytransmitKamrani1.pdf	392575 0217a78dbdb1071acd90f17fe081e07ce2844dd3	no	2
Warnings:					
Information:					
2		Kamrani1Spec.pdf	106519 1b2e499d89aa000563829ab31c53127ef69dc2c4	yes	22
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Specification		1	12	
	Claims		13	21	
	Abstract		22	22	
Warnings:					
Information:					
3	Oath or Declaration filed	declkamrani1.pdf	1837600 0d6b7f029a9920a6eea0b00f1e7a2457af28c43b	no	3
Warnings:					
Information:					
4	Power of Attorney	POAKAMRANI1.pdf	2148169 53a2fbad81517dc1cab87edbf27c54f5800cf4b1	no	2
Warnings:					
Information:					
5	Information Disclosure Statement (IDS) Filed (SB/08)	IDSKamarani1.pdf	95124 12f8702286c9c755af1c1b59005b3e8ba54defe0	no	1
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
6	Drawings-only black and white line drawings	Kamrani1Fig.pdf	64108 5c4e21b3696a5013d4411431caf60bbf77a529ad	no	5
Warnings:					
Information:					
7	Fee Worksheet (PTO-06)	fee-info.pdf	35906 98d97df1f84b2a55a38d45cc42d9af17f8a91e8b	no	2
Warnings:					
Information:					

Total Files Size (in bytes):	4680001

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/81 (01-06)
Approved for use through 12/31/2008. OMB 0851-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

POWER OF ATTORNEY and CORRESPONDENCE ADDRESS INDICATION FORM

Application Number	
Filing Date	
First Named Inventor	Nader Asghari-Kamrani
Title	Centralized Identification and
Art Unit	
Examiner Name	
Attorney Docket Number	Kamrani1

I hereby revoke all previous powers of attorney given in the above-identified application.

I hereby appoint:

☑ Practitioners associated with the Customer Number: 63670

OR

□ Practitioner(s) named below:

Name	Registration Number

as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith.

Please recognize or change the correspondence address for the above-identified application to:

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

OR

□ The address associated with Customer Number:

OR

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

I am the:

☑ Applicant/Inventor.

□ Assignee of record of the entire interest. See 37 CFR 3.71.
Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)

SIGNATURE of Applicant or Assignee of Record

Signature		Date	09-12-2008
Name	Nader Asghari-Kamrani	Telephone	
Title and Company	Inventor and assignee		

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☑ *Total of 1 forms are submitted.

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

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

PTO/SB/81 (01-06)
Approved for use through 12/31/2008. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

POWER OF ATTORNEY and CORRESPONDENCE ADDRESS INDICATION FORM	**Application Number**	
	Filing Date	
	First Named Inventor	Nader Asghari-Kamrani
	Title	Centralized Identification and
	Art Unit	
	Examiner Name	
	Attorney Docket Number	Kamrani1

I hereby revoke all previous powers of attorney given in the above-identified application.

I hereby appoint:

☑ Practitioners associated with the Customer Number: 63670

OR

□ Practitioner(s) named below:

Name	Registration Number

as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith.

Please recognize or change the correspondence address for the above-identified application to:

☑ The address associated with the above-mentioned Customer Number:

OR

□ The address associated with Customer Number:

OR

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

I am the:

☑ Applicant/Inventor.

□ Assignee of record of the entire interest. See 37 CFR 3.71.
Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)

SIGNATURE of Applicant or Assignee of Record

Signature	Kamrani	Date	09-12-2008
Name	Kamran Asghari-Kamrani	Telephone	
Title and Company	Inventor and assignee		

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☑ *Total of 1 forms are submitted.

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

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

DocCode - SCORE

SCORE Placeholder Sheet for IFW Content

Application Number: 12210926 Document Date: 9/15/2008

The presence of this form in the IFW record indicates that the following document type was received in paper and is scanned and stored in the SCORE database.

- Design Drawings

The original paper documents are in the physical artifact folder. The original documents are scanned using a higher quality capture process and stored in SCORE. A copy of these documents are scanned in IFW using the standard quality scanning process. Defects visible in both IFW and SCORE are indicative of defects in the original paper documents.

To access the documents in the SCORE database, refer to instructions developed by SIRA.

At the time of document entry (noted above):

- Examiners may access SCORE content via the eDAN interface.
- Other USPTO employees can bookmark the current SCORE URL (http://es/ScoreAccessWeb/).
- External customers may access SCORE content via the Public and Private PAIR interfaces.

Form Revision Date: October 12, 2006

PTO/SB/06 (12-04)

Filing Date: **09/15/08**

Approved for use through 7/31/2006. 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 12/210,926

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	**310**
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	**510**
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	**210**
TOTAL CLAIMS (37 CFR 1.16(i))	**62** minus 20 =	**42**	X$ 25		OR	X$50	**2100**
INDEPENDENT CLAIMS (37 CFR 1.16(h))	**2** minus 3 =	*	X$105			X$210	
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $260 ($130 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR						
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))			185			370	
			TOTAL			TOTAL	**3130**

* If the difference in column 1 is less than zero, enter "0" in column 2.

APPLICATION AS AMENDED – PART II

AMENDMENT A

	(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDI-TIONAL FEE ($)		RATE ($)	ADDI-TIONAL FEE ($)
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))					N/A		OR	N/A	
					TOTAL ADD'T FEE		OR	TOTAL ADD'T FEE	

AMENDMENT B

	(Column 1)		(Column 2)	(Column 3)			OR		
	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDI-TIONAL FEE ($)		RATE ($)	ADDI-TIONAL FEE ($)
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))					N/A		OR	N/A	
					TOTAL ADD'T FEE		OR	TOTAL ADD'T 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.

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. Paten 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.