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
11/333,400	01/18/2006	Nader Asghari-Kamrani	KAMR001US0

CONFIRMATION NO. 4456

POWER OF ATTORNEY NOTICE

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

OC000000079578588

Date Mailed: 12/29/2015

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 12/17/2015.

- The Power of Attorney to you in this application has been revoked by the applicant.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).

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/dtdinh/

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
11/333,400	01/18/2006	Nader Asghari-Kamrani	PL0831187

CONFIRMATION NO. 4456

105857
NOVICK, KIM & LEE, PLLC
1604 Spring Hill Road, Suite 320
Vienna, VA 22182

POA ACCEPTANCE LETTER

OC000000079578658

Date Mailed: 12/29/2015

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 12/17/2015.

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

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/dtdinh/

PTO/SB/81A (12-08)
Approved for use through 11/30/2011. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

PATENT - POWER OF ATTORNEY OR REVOCATION OF POWER OF ATTORNEY WITH A NEW POWER OF ATTORNEY AND CHANGE OF CORRESPONDENCE ADDRESS

Patent Number	8,281,129
Issue Date	October 2, 2012
First Named Inventor	Nader Asghari-Kamrani
Title	DIRECT AUTHENTICATION...
Attorney Docket Number	PL0831187

I hereby revoke all previous powers of attorney given in the above-identified patent.

☐ 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) with respect to the patent identified above, and to transact all business in the United States Patent and Trademark Office connected therewith: 105867

OR

☐ I hereby appoint Practitioner(s) named below as my/our attorney(s) or agent(s) with respect to the patent 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 patent 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:

☒ Inventor, having ownership of the patent.

OR

☐ Patent owner.

Statement under 37 CFR 3.73(b) (Form PTO/SB/96) submitted herewith or filed on _____

SIGNATURE of Inventor or Patent Owner

Signature		Date	12/15/2015
Name	Nader Asghari-Kamrani	Telephone	703-470-2030
Title and Company			

NOTE: Signatures of all the inventors or patent owners 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.

PTO/SB/81A (12-08)
Approved for use through 11/30/2011. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

PATENT - POWER OF ATTORNEY OR REVOCATION OF POWER OF ATTORNEY WITH A NEW POWER OF ATTORNEY AND CHANGE OF CORRESPONDENCE ADDRESS

Patent Number	8,281,129
Issue Date	October 2, 2012
First Named Inventor	Nader Asghari-Kamrani
Title	DIRECT AUTHENTICATION...
Attorney Docket Number	PL0831187

I hereby revoke all previous powers of attorney given in the above-identified patent.

☐ 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) with respect to the patent identified above, and to transact all business in the United States Patent and Trademark Office connected therewith: 105857

OR

☐ I hereby appoint Practitioner(s) named below as my/our attorney(s) or agent(s) with respect to the patent 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 patent 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:

☒ Inventor, having ownership of the patent.

OR

☐ Patent owner.

Statement under 37 CFR 3.73(b) (Form PTO/SB/96) submitted herewith or filed on _____.

SIGNATURE of Inventor or Patent Owner

Signature		Date	12/15/2015
Name	Kamran Asghari-Kamrani	Telephone	703-233-3363
Title and Company			

NOTE: Signatures of all the inventors or patent owners 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.

Electronic Acknowledgement Receipt	
EFS ID:	24390620
Application Number:	11333400
International Application Number:	
Confirmation Number:	4456
Title of Invention:	DIRECT AUTHENTICATION SYSTEM AND METHOD VIA TRUSTED AUTHENTICATORS
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Customer Number:	58293
Filer:	Jae Youn Kim/Min Gyu Kim
Filer Authorized By:	Jae Youn Kim
Attorney Docket Number:	KAMR001US0
Receipt Date:	17-DEC-2015
Filing Date:	18-JAN-2006
Time Stamp:	10:53:48
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	PL0831187-POA.pdf	3392517 5209c987778a421a11a9414ed8222e291c2b017b	no	2
Warnings:					
Information:					

Total Files Size (in bytes):	3392517

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.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/333,400	10/02/2012	8281129	KAMR001US0	4456

58293 7590 09/12/2012

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 548 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;

Certification Under 37 C.F.R. § 1.8

I hereby certify that on August 13, 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: August 13, 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.: 11/333,400

FILING DATE: January 18, 2006

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: DIRECT AUTHENTICATION SYSTEM AND METHOD VIA TRUSTED AUTHENTICATORS

ATTORNEY DOCKET: KAMR001US0

CONFIRMATION NO.: 4456

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

AMENDMENT UNDER 37 C.F.R. § 1.312

In response to the Notice of Allowance mailed May 17, 2012, the Applicants hereby respectfully submit the following amendments and remarks:

Amendments to the Claims begin on page 2.

Remarks begin on page 3.

OK to enter.
/a.n./ 08/28/2012

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.
11/333,400	01/18/2006	Nader Asghari-Kamrani	KAMR001US0	4456

58293 7590 09/04/2012

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
09/04/2012	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

Response to Rule 312 Communication	Application No.	Applicant(s)
	11/333,400	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 –

1. ☒ The amendment filed on *13 August 2012* under 37 CFR 1.312 has been considered, and has been:

a) ☐ entered.

b) ☒ entered as directed to matters of form not affecting the scope of the invention.

c) ☐ disapproved because the amendment was filed after the payment of the issue fee.
Any amendment filed after the date the issue fee is paid must be accompanied by a petition under 37 CFR 1.313(c)(1) and the required fee to withdraw the application from issue.

d) ☐ disapproved. See explanation below.

e) ☐ entered in part. See explanation below.

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

PRINTER RUSH

(PTO ASSISTANCE)

Application:	11333400	**Examiner:**	Nobahar	**GAU:**	2432
From:	Floyd Brown	**Location:**	RTFM	**Creation Date:**	08/17/2012

Tracking #: Week Date:

DOC CODE	DOC DATE	MISCELLANEOUS
[ ] 1449		[ ] Continuing Data
[ ] IDS		[ ] Foreign Priority
[ ] CLM		[ ] Document Legibility
[ ] IIFW/FWCLM		[ ] Fees
[ ] SRFW		[ ] Petition (TC)
[ ] DRW		[ ] Other
[ ] OATH		
[X] 312	08/13/2012	
[ ] SPEC		

[RUSH] Message:

Please respond to the 8-13-12 A.NA.

Thanks,
FB

[XRUSH] Response:

Amendments to the claims do not affect the scope of the claims. Please enter.
See the attachment.

Initials: a.n.

08/28/2012

Examiner: PUBS contacts - for DESIGNS: Don Fairchild, 703-756-1566; for ALL OTHER files: Bernadette Queen, 703-756-1565.
NOTE: This form will be included as part of the official USPTO record with the response document coded as XRUSH.
REV: Oct 11

Certification Under 37 C.F.R. § 1.8

I hereby certify that on August 13, 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: August 13, 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.: 11/333,400

FILING DATE: January 18, 2006

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: DIRECT AUTHENTICATION SYSTEM AND METHOD VIA TRUSTED AUTHENTICATORS

ATTORNEY DOCKET: KAMR001US0

CONFIRMATION NO.: 4456

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

AMENDMENT UNDER 37 C.F.R. § 1.312

In response to the Notice of Allowance mailed May 17, 2012, the Applicants hereby respectfully submit the following amendments and remarks:

Amendments to the Claims begin on page 2.

Remarks begin on page 3.

In the Claims:

Please amend claim 21 only to correct a typographical error in the last line.

21. (Currently Amended) A computer implemented method to authenticate an individual in communication with an entity over a communication network during a communication between the entity and the individual, the computer implemented method comprising:

receiving electronically a request for a dynamic code for the individual, which request is received from the individual by a trusted-authenticator's computer during an authentication of the individual by the entity;

calculating by the trusted-authenticator's computer the dynamic code for the individual in response to the request during the authentication of the individual by the entity, wherein the dynamic code is valid for a predefined time and becomes invalid after being used;

sending by the trusted-authenticator's computer electronically the dynamic code to the individual during the authentication of the individual by the entity;

receiving by the trusted-authenticator's computer electronically an authentication request from the entity to authenticate the individual based on a user information and the dynamic code included in the authentication request, wherein the entity receives the user information and the dynamic code from the individual; and

authenticating by the trusted-authenticator's computer an identity of the individual based on the user information and the dynamic code included in the authentication request, wherein the result of the authentication is ~~provide~~ provided to the entity.

REMARKS

The Applicants gratefully acknowledge the Examiner's issuance of a notice of allowance. In accordance with 37 C.F.R. § 1.312, the Applicants respectfully request entry of the amendment to claim 21 to correct a typographical error, which could not have been corrected prior to the notice of allowance as the typographical error was noted in the examiner's amendment that accompanied the notice of allowance. While the Applicants understand that such amendments are a matter of grace with the Patent Office and the Examiner, the Applicants respectfully request the exercise of the Examiner's grace and discretion to enter the proposed amendment.

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 13, 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:	13481450
Application Number:	11333400
International Application Number:	
Confirmation Number:	4456
Title of Invention:	DIRECT AUTHENTICATION SYSTEM AND METHOD VIA TRUSTED AUTHENTICATORS
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Customer Number:	58293
Filer:	Michael P. Fortkort
Filer Authorized By:	
Attorney Docket Number:	KAMR001US0
Receipt Date:	13-AUG-2012
Filing Date:	18-JAN-2006
Time Stamp:	14:51:44
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 Notice of Allowance (Rule 312)	rule_312_amendment_filed_0801312_11333400.pdf	22786 df355a3fb0db19736bcaacddd52955b762a6cd1a	no	3
Warnings:					
Information:					

Total Files Size (in bytes):	22786

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.

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.
11/333,400	01/18/2006	Nader Asghari-Kamrani	KAMR001US0	4456

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	$0	$0	$870	08/17/2012

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:	11333400
Filing Date:	18-Jan-2006
Title of Invention:	DIRECT AUTHENTICATION SYSTEM AND METHOD VIA TRUSTED AUTHENTICATORS
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Filer:	Michael P. Fortkort
Attorney Docket Number:	KAMR001US0

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
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**870**

Electronic Acknowledgement Receipt	
EFS ID:	13482165
Application Number:	11333400
International Application Number:	
Confirmation Number:	4456
Title of Invention:	DIRECT AUTHENTICATION SYSTEM AND METHOD VIA TRUSTED AUTHENTICATORS
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Customer Number:	58293
Filer:	Michael P. Fortkort
Filer Authorized By:	
Attorney Docket Number:	KAMR001US0
Receipt Date:	13-AUG-2012
Filing Date:	18-JAN-2006
Time Stamp:	15:21:09
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$870
RAM confirmation Number	1973
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_11333400.pdf	121297 9d881257929a083e4e2246a4ee9bd02cf687b71f	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30319 bc809a1f372e6e08cd46eb43a2ba43ffe7fbecc1	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	151616		

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 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.: 11/333,400

FILING DATE: January 18, 2006

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: DIRECT AUTHENTICATION SYSTEM AND METHOD VIA TRUSTED AUTHENTICATORS

ATTORNEY DOCKET: KAMR001US0

CONFIRMATION NO.: 4456

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

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:	12864240
Application Number:	11333400
International Application Number:	
Confirmation Number:	4456
Title of Invention:	DIRECT AUTHENTICATION SYSTEM AND METHOD VIA TRUSTED AUTHENTICATORS
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Customer Number:	58293
Filer:	Michael P. Fortkort
Filer Authorized By:	
Attorney Docket Number:	KAMR001US0
Receipt Date:	25-MAY-2012
Filing Date:	18-JAN-2006
Time Stamp:	09:59:22
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	Applicant summary of interview with examiner	Interview_Summary_11333400_042612.pdf	21618 2564440ed155cec687d41131da829ff254236840	no	3

Warnings:
Information:

Total Files Size (in bytes):	21618

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 05/17/2012

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: 05/17/2012

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/333,400	01/18/2006	Nader Asghari-Kamrani	KAMR001US0	4456

TITLE OF INVENTION: DIRECT AUTHENTICATION SYSTEM AND METHOD VIA TRUSTED AUTHENTICATORS

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$870	$0	$0	$870	08/17/2012

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: 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)

58293 7590 05/17/2012
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.
11/333,400	01/18/2006	Nader Asghari-Kamrani	KAMR001US0	4456

TITLE OF INVENTION: DIRECT AUTHENTICATION SYSTEM AND METHOD VIA TRUSTED AUTHENTICATORS

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$870	$0	$0	$870	08/17/2012

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.
11/333,400	01/18/2006	Nader Asghari-Kamrani	KAMR001US0	4456

58293 7590 05/17/2012

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: 05/17/2012

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 433 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 433 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.

Notice of Allowability	Application No.	Applicant(s)	
	11/333,400	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 03/05/2012*.
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 *21-31,34-38,41-51,53-58 and 62-80*.
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 05/11/12.

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.

1-20. (Cancelled)

21. (Currently Amended) A computer implemented method to authenticate an individual in communication with an entity over a communication network during a communication between the entity and the individual, the computer implemented method comprising:

receiving electronically a request for a dynamic code for the individual, which request is received from the individual by a trusted-authenticator's computer during an authentication of the individual by the entity;

calculating by the trusted-authenticator's computer the dynamic code for the individual in response to the request during the authentication of the individual by the

entity, wherein the dynamic code is valid for a predefined time and becomes invalid after being used;

sending by the trusted-authenticator's computer electronically the dynamic code to the individual during the authentication of the individual by the entity;

receiving by the trusted-authenticator's computer electronically an authentication request from the entity to authenticate the individual based on a user information and the dynamic code included in the authentication request, wherein the entity receives the user information and the dynamic code from the individual; and

~~verifying~~ authenticating by the trusted-authenticator's computer an identity of the individual based on the user information and the dynamic code included in the authentication request, wherein the result of the authentication is provide to the entity.

22. (Previously Presented) The computer implemented method of claim 21, 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 the first trusted-authenticator.

23. (Previously Presented) The computer implemented method of claim 21, 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.

24. (Currently Amended) The computer implemented method of claim 21, wherein the dynamic code includes a time-dependent ~~SecureCode~~ code.

25. (Previously Presented) The computer implemented method of claim 21, wherein at least the dynamic code is encrypted.

26. (Currently Amended) A computer implemented method for an entity to authenticate an individual over a communication network during a communication with the individual, the method comprising:

requesting electronically by the entity both a user information and a dynamic code from the individual in order to validate the individual's identity during the communication with the individual, which the individual obtains the dynamic code from a computer associated with a trusted-authenticator during the communication between the individual and the entity, wherein the dynamic code is valid for a predefined time and becomes invalid after being used;

receiving electronically by the entity both the user information and the dynamic code from the individual; and

receiving by the entity a message from ~~authenticating the individual based on verification by~~ the computer associated with the trusted-authenticator that ~~of~~ the user information and the dynamic code received by the computer associated with the trusted-authenticator from the entity during the communication between the individual and the entity properly authenticates the ~~user~~ individual in response to an authentication request

from the entity to the trusted-authenticator including the user information and dynamic code.

27. (Previously Presented) The computer implemented method of claim 26, wherein the user information and the dynamic code comprise credentials for verifying the individual's identity.

28. (Currently Amended) The computer implemented method of claim 26, wherein the dynamic code includes a time-dependent ~~SecureCode~~ code.

29. (Previously Presented) The computer implemented method of claim 26, wherein at least the dynamic code is encrypted.

30. (Previously Presented) The computer implemented method of claim 26, wherein the entity corresponds to a business, organization, or another individual.

31. (Previously Presented) The computer implemented method of claim 26, wherein a computer associated with a first trusted-authenticator calculates the dynamic code and provides the dynamic code to the individual during communication between the individual and the entity.

32. (Cancelled)

33. (Cancelled)

34. (Currently Amended) A computer implemented method for a website to authenticate an individual over a communication network during a communication session between the individual and the website, the computer implemented method comprising:

requesting by a computer associated with the website both a user information and a dynamic code from the individual in order to validate the individual's identity, wherein the dynamic code is valid for a predefined time and becomes invalid after being used;

receiving both the user information and the dynamic code from the individual, which individual receives the dynamic code from a computer associated with a trusted-authenticator during the communication session between the individual and the website; and

creating an authentication request message including the user information and the dynamic code and providing the authentication request message to ~~a first~~ the computer associated with [[a]] the trusted-authenticator, wherein the trusted authenticator ~~authenticating~~ authenticates the individual based on the user information and the dynamic code; and

receiving by the computer associated with the website a message from the computer associated with the trusted-authenticator whether the individual is

authenticated or not during the communication session between the individual and the website.

35. (Previously Presented) The computer implemented method of claim 34, wherein the user information and the dynamic code comprise credentials for verifying the individual's identity.

36. (Currently Amended) The computer implemented method of claim 34, wherein the dynamic code includes a non-predictable and time-dependent ~~SecureCode~~ code.

37. (Previously Presented) The computer implemented method of claim 34, wherein at least the dynamic code is encrypted.

38. (Previously Presented) The computer implemented method of claim 34, wherein a second computer associated with the trusted-authenticator calculates the dynamic code and provides the dynamic code to the individual during the communication session between the individual and the website.

39. (Cancelled)

40. (Cancelled)

41. (Currently Amended) A computer implemented method for authenticating an individual in communication with an entity over a communication network during communication between the entity and the individual, the method comprising:

receiving by a computer associated with the entity a dynamic code from the individual during authentication of the individual by the entity, which said dynamic code was sent to the individual by a computer associated with a trusted-authenticator in response to a request for the dynamic code from the computer associated with the trusted-authenticator sent by the individual during authentication of the individual by the entity and was calculated by the computer associated with the trusted-authenticator during authentication of the individual by the entity, wherein the dynamic code is valid for a predefined time and becomes invalid after being used;

sending electronically by the computer associated with the entity an authentication request to [[a]] the computer associated with the trusted-authenticator to authenticate the individual based on a user information and a received dynamic code included in the authentication request, wherein said authentication request is sent during authentication of the individual by the entity; and

receiving electronically by the entity a message from the computer associated with the trusted-authenticator either confirming or denying an identity of the individual based on the user information and the received dynamic code included in the authentication request from the entity during the time of authentication of the individual by the entity.

42. (Previously Presented) The computer implemented method according to claim 41, wherein the entity and the trusted-authenticator are the same.

43. (Previously Presented) The computer implemented method according to claim 41, wherein the entity and the trusted-authenticator are different.

44. (Previously Presented) The computer implemented method according to claim 41, wherein said dynamic code is calculated after receiving the request from the individual for the dynamic code.

45. (Previously Presented) The computer implemented method according to claim 41, wherein said dynamic code comprises a different value each time the dynamic code is requested by the individual.

46. (Currently Amended) A computer implemented method for authenticating an individual in communication with an entity during communication between the entity and the individual, the computer implemented method comprising:

sending electronically by the individual a request for a dynamic code to a computer associated with a trusted-authenticator during authentication of the individual by the entity;

receiving electronically by the individual the dynamic code from the computer associated with the trusted-authenticator during authentication of the individual by the

entity, which the dynamic code was calculated by ~~a computer associated with~~ the trusted-authenticator during authentication of the individual by the entity, wherein the dynamic code is valid for a predefined time and becomes invalid after being used;

sending electronically by the entity a user information and the dynamic code ~~and user information~~ received from the individual during authentication of the individual by the entity to the computer associated with the trusted-authenticator for verification by the computer associated with the trusted-authenticator during authentication of the individual by the entity; and

receiving electronically by the individual acceptance or denial of authentication from the entity based on said verification by the computer associated with the trusted-authenticator of the user information and the dynamic code received from the individual during authentication of the individual by the entity.

47. (Previously Presented) The computer implemented method according to claim 46, wherein the entity and the trusted-authenticator are the same.

48. (Previously Presented) The computer implemented method according to claim 46, wherein the entity and the trusted-authenticator are different.

49. (Previously Presented) The computer implemented method according to claim 46, wherein said dynamic code is calculated after receiving the request from the individual for the dynamic code.

50. (Previously Presented) The computer implemented method according to claim 46, wherein said dynamic code comprises a different value each time the dynamic code is requested for an individual.

51. (Currently Amended) A computer implemented method to authenticate an individual during communication between the individual and ~~another~~ an entity, the method comprising:

receiving by a computer associated with a trusted-authenticator electronically a request for a dynamic code for the individual, wherein the request is received directly or indirectly from the individual during authentication of the individual by the entity;

sending by the computer associated with the trusted-authenticator the dynamic code electronically to the individual during authentication of the individual by the entity, wherein the dynamic code is valid for a predefined time and becomes invalid after being used;

receiving electronically by the computer associated with the trusted-authenticator an authentication request from the entity to authenticate the individual based on a user information and the dynamic code received from the individual during authentication of the individual by the entity, wherein said authentication request is received during authentication of the individual by the entity; and

authenticating ~~verifying~~ by [[a]] the computer associated with the trusted-authenticator an identity of the individual based on the user information and the received dynamic code in response to the authentication request from the entity during

the time of authentication of the individual by the entity, wherein said authenticating of the individual occurs during said authentication between the individual and the entity, wherein the result of the authentication is provided to the entity.

52. (Cancelled)

53. (Previously Presented) The computer implemented method according to claim 51, wherein the entity comprises a trusted-authenticator.

54. (Previously Presented) The computer implemented method according to claim 51, wherein said dynamic code is calculated after receiving the request for the dynamic code.

55. (Previously Presented) The computer implemented method according to claim 51, wherein said dynamic code comprises a different value each time the dynamic code is requested for the individual.

56. (Currently Amended) A computer implemented method to perform a two-factor authentication of an individual based on ~~a user information as~~ a first credential and ~~a dynamic code as~~ a second credential during communication over a network between an entity and the individual, the method comprising:

receiving electronically by the entity from a computer associated with a trusted-authenticator a message indicating acceptance or denial of two-factor authentication ~~from the entity~~ based on a user information and a dynamic code ~~two credentials~~ received by the entity from the individual during an authentication of the individual by the entity, wherein:

said user information comprises the first credential and said dynamic code comprises the second credential;

said dynamic code was calculated by [[a]] the computer ~~program~~ associated with [[a]] the trusted-authenticator and provided by the computer associated with the trusted authenticator to the individual during said communication between the entity and the individual, wherein the dynamic code is valid for a predefined time and becomes invalid after being used;

said user information and said dynamic code were electronically received from the entity and verified by the computer associated with the trusted-authenticator during the authentication of the individual by the entity; and

said dynamic code comprises a different value each time the individual receives [[a]] the dynamic code from [[a]] the computer associated with the trusted-authenticator.

57. (Currently Amended) A computer implemented method to perform a two-factor authentication of an individual based on ~~a user information as~~ a first credential and ~~a dynamic code as~~ a second credential during a communication between ~~the~~ an entity and the individual, the method comprising:

accepting or denying ~~electronically~~ by a first computer associated with a trusted-authenticator of [[a]] the two-factor authentication of the individual based on a user information and a dynamic code ~~two credentials received from the individual~~, wherein:

said user information comprises the first credential and said dynamic code comprises the second credential;

said dynamic code was calculated by a ~~first~~ second computer associated with [[a]] the trusted-authenticator and sent by [[a]] the second computer associated with the trusted-authenticator to the individual during the communication between the individual and the entity, wherein the dynamic code is valid for a predefined time and becomes invalid after being used;

said user information and said dynamic code were received electronically by the entity from the individual during the communication between the individual and the entity;

said user information and said dynamic code were received electronically by said first computer associated with the trusted authenticator from the entity during authentication of the individual by the entity and were verified by said first computer associated with the trusted-authenticator during said communication between the individual and the entity;

said accepting or denying of the two-factor authentication of the individual is performed by said first computer associated with the trusted-authenticator and the result of the authentication is provided to the entity during said authentication between the individual and the entity; and

said ~~first~~ second computer associated with said trusted-authenticator calculates a different value for said dynamic code each time the individual requests a dynamic code from the trusted-authenticator.

58. (Previously Presented) The computer implemented method according to claim 57, wherein the first computer and the second computer are the same.

59. (Cancelled).

60. (Cancelled).

61. (Cancelled).

62. (Currently Amended) A computer implemented method to perform a two-factor authentication of an individual based on ~~a user information as~~ a first credential and ~~a dynamic code as~~ a second credential during an authentication ~~communication~~ between ~~the~~ an entity and the individual, the method comprising:

accepting or denying ~~electronically~~ by a first computer associated with a trusted-authenticator of the two-factor authentication of the individual based on a user information and a dynamic code ~~two credentials received from the individual~~, wherein:

said user information comprises the first credential and said dynamic code comprises the second credential;

said dynamic code was calculated by a second computer associated with [[a]] the trusted-authenticator and sent to the individual for said authentication between the individual and the entity, wherein the dynamic code is valid for a predefined time and becomes invalid after being used;

said user information and said dynamic code were received electronically by the entity from the individual during said authentication between the individual and the entity;

said user information and said dynamic code were received electronically by the trusted authenticator from the entity during the authentication of the individual by the entity and the user information was verified by [[a]] said first computer and the dynamic code was verified by [[a]] the second computer associated with the trusted-authenticator during said authentication ~~communication~~ between the individual and the entity;

said verification of the user information and the dynamic code performed by the first computer and the second computer associated with the trusted-authenticator and the result of the verification is provided to the entity during said authentication between the individual and the entity; and

said dynamic code comprises a different value each time the individual receives a dynamic code from [[a]] the trusted-authenticator.

63. (Previously Presented) The computer implemented method according to claim 62, wherein the first computer and the second computer are the same.

64. (Previously Presented) The computer implemented method according to claim 62, wherein said dynamic code is valid for a predefined time and may be used by the individual before becoming invalid.

65. (Previously Presented) The computer implemented method of claim 34, wherein a computer program associated with the trusted-authenticator calculates the dynamic code and provides the dynamic code to the individual during the communication session between the individual and the website.

66. (Currently Amended) The computer implemented method of claim 21, wherein the user information is verified by a first computer and the dynamic code is verified by a second computer.

67. (Previously Presented) The computer implemented method according to claim 34, wherein the website and the trusted-authenticator are the same.

68. (Currently Amended) The computer implemented method of claim 34, wherein the user information is verified by a first computer and the dynamic code is verified by a second computer associated with the trusted-authenticator.

69. (Previously Presented) The computer implemented method according to claim 41, wherein the entity and the trusted-authenticator are the same.

70. (Currently Amended) The computer implemented method of claim 41 wherein the user information is verified by a first computer and the dynamic code is verified by a second computer associated with the trusted-authenticator.

71. (Currently Amended) The computer implemented method of claim 56, wherein the user information is verified by a first computer and the dynamic code is verified by a second computer associated with the trusted-authenticator.

72. (Previously Presented) The computer implemented method according to claim 56, wherein the entity and the trusted-authenticator are the same.

73. (Previously Presented) The computer implemented method according to claim 57, wherein the entity and the trusted-authenticator are the same.

74. (Previously Presented) The computer implemented method according to claim 46, wherein the dynamic code is alphanumeric.

75. (Previously Presented) The computer implemented method according to claim 56, wherein the dynamic code is alphanumeric.

76. (Previously Presented) The computer implemented method according to claim 21, wherein the dynamic code is alphanumeric.

77. (Previously Presented) The computer implemented method according to claim 26, wherein the dynamic code is alphanumeric.

78. (Previously Presented) The computer implemented method according to claim 34, wherein the dynamic code is alphanumeric.

79. (Previously Presented) The computer implemented method according to claim 41, wherein the dynamic code is alphanumeric.

80. (Previously Presented) The computer implemented method according to claim 57, wherein the dynamic code is alphanumeric.

Allowable Subject Matter

1. Claims 21-31, 34-38, 41-51, 53-58 and 62-80 are allowed.

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

The primary reasons for the allowance of the claims 21-31, 34-38, 41-51, 53-58 and 62-80 are the inclusion of the following limitations that are not found in the prior art 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 21-25, 21 and 76: receiving by the trusted-authenticator's computer electronically an authentication request from the entity to authenticate the individual based on a user information and the dynamic code included in the

authentication request, wherein the entity receives the user information and the dynamic code from the individual; and

authenticating by the trusted-authenticator's computer an identity of the individual based on the user information and the dynamic code included in the authentication request, wherein the result of the authentication is provide to the entity.

Claims 26-31 and 77: receiving by the entity a message from the computer associated with the trusted-authenticator that the user information and the dynamic code received by the computer associated with the trusted-authenticator from the entity during the communication between the individual and the entity properly authenticates the individual in response to an authentication request from the entity to the trusted-authenticator including the user information and dynamic code.

Claims 34-38, 65, 67, 68 and 78: creating an authentication request message including the user information and the dynamic code and providing the authentication request message to the computer associated with the trusted-authenticator, wherein the trusted authenticator authenticates the individual based on the user information and the dynamic code; and

receiving by the computer associated with the website a message from the computer associated with the trusted-authenticator whether the individual is authenticated or not during the communication session between the individual and the website.

Claims 41-45, 69, 70, and 79: sending electronically by the computer associated with the entity an authentication request to the computer associated with the trusted-

authenticator to authenticate the individual based on a user information and a received dynamic code included in the authentication request, wherein said authentication request is sent during authentication of the individual by the entity; and

receiving electronically by the entity a message from the computer associated with the trusted-authenticator either confirming or denying an identity of the individual based on the user information and the received dynamic code included in the authentication request from the entity during the time of authentication of the individual by the entity.

Claims 46-50 and 74: sending electronically by the entity a user information and the dynamic code received from the individual during authentication of the individual by the entity to the computer associated with the trusted-authenticator for verification by the computer associated with the trusted-authenticator during authentication of the individual by the entity; and

receiving electronically by the individual acceptance or denial of authentication from the entity based on said verification by the computer associated with the trusted-authenticator of the user information and the dynamic code received from the individual during authentication of the individual by the entity.

Claims 51 and 53-55: receiving electronically by the computer associated with the trusted-authenticator an authentication request from the entity to authenticate the individual based on a user information and the dynamic code received from the individual during authentication of the individual by the entity, wherein said

authentication request is received during authentication of the individual by the entity; and

authenticating by the computer associated with the trusted-authenticator an identity of the individual based on the user information and the received dynamic code in response to the authentication request from the entity during the time of authentication of the individual by the entity, wherein said authenticating of the individual occurs during said authentication between the individual and the entity, wherein the result of the authentication is provided to the entity.

Claims 56, 71, 72 and 75: receiving electronically by the entity from a computer associated with a trusted-authenticator a message indicating acceptance or denial of two-factor authentication based on a user information and a dynamic code received by the entity from the individual during an authentication of the individual by the entity; and

said user information and said dynamic code were electronically received from the entity and verified by the computer associated with the trusted-authenticator during the authentication of the individual by the entity.

Claims 57, 58, 73 and 80: said user information and said dynamic code were received electronically by said first computer associated with the trusted authenticator from the entity during authentication of the individual by the entity and were verified by said first computer associated with the trusted-authenticator during said communication between the individual and the entity;

said accepting or denying of the two-factor authentication of the individual is performed by said first computer associated with the trusted-authenticator and the result

of the authentication is provided to the entity during said authentication between the individual and the entity.

Claims 62, 63 and 64: said user information and said dynamic code were received electronically by the trusted authenticator from the entity during the authentication of the individual by the entity and the user information was verified by said first computer and the dynamic code was verified by the second computer associated with the trusted-authenticator during said authentication between the individual and the entity; and

said verification of the user information and the dynamic code performed by the first computer and the second computer associated with the trusted-authenticator and the result of the verification is provided to the entity during said authentication between the individual and the entity.

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.

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).

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

/Abdulhakim Nobahar/
Examiner, Art Unit 2432

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11333400	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	09/02/2008	03/01/2009	06/15/2009	12/01/2009	06/20/2010	09/16/2010	01/11/2011	07/26/2011	05/03/2012
	1	✓	✓	-	-	-	-	-	-	-
	2	✓	-	-	-	-	-	-	-	-
	3	✓	✓	-	-	-	-	-	-	-
	4	✓	✓	-	-	-	-	-	-	-
	5	✓	✓	-	-	-	-	-	-	-
	6	✓	✓	-	-	-	-	-	-	-
	7	✓	✓	-	-	-	-	-	-	-
	8	✓	✓	-	-	-	-	-	-	-
	9	✓	✓	-	-	-	-	-	-	-
	10	✓	✓	-	-	-	-	-	-	-
	11	✓	✓	-	-	-	-	-	-	-
	12	✓	✓	-	-	-	-	-	-	-
	13	✓	-	-	-	-	-	-	-	-
	14	✓	✓	-	-	-	-	-	-	-
	15	✓	✓	-	-	-	-	-	-	-
	16	✓	✓	-	-	-	-	-	-	-
	17	✓	✓	-	-	-	-	-	-	-
	18	✓	✓	-	-	-	-	-	-	-
	19	✓	✓	-	-	-	-	-	-	-
	20	✓	✓	-	-	-	-	-	-	-
1	21			✓	✓	✓	✓	✓	✓	=
2	22			✓	✓	✓	✓	✓	✓	=
3	23			✓	✓	✓	✓	✓	✓	=
4	24			✓	✓	✓	✓	✓	✓	=
5	25			✓	✓	✓	✓	✓	✓	=
8	26			✓	✓	✓	✓	✓	✓	=
9	27			✓	✓	✓	✓	✓	✓	=
10	28			✓	✓	✓	✓	✓	✓	=
11	29			✓	✓	✓	✓	✓	✓	=
12	30			✓	✓	✓	✓	✓	✓	=
13	31			✓	✓	✓	✓	✓	✓	=
	32			✓	-	-	-	-	-	-
	33			✓	-	-	-	-	-	-
15	34			✓	✓	✓	✓	✓	✓	=
16	35			✓	✓	✓	✓	✓	✓	=
17	36			✓	✓	✓	✓	✓	✓	=

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11333400	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	09/02/2008	03/01/2009	06/15/2009	12/01/2009	06/20/2010	09/16/2010	01/11/2011	07/26/2011	05/03/2012
18	37			✓	✓	✓	✓	✓	✓	=
19	38			✓	✓	✓	✓	✓	✓	=
	39			✓	-	-	-	-	-	-
	40			✓	-	-	-	-	-	-
24	41					✓	✓	✓	✓	=
25	42					✓	✓	✓	✓	=
26	43					✓	✓	✓	✓	=
27	44					✓	✓	✓	✓	=
28	45					✓	✓	✓	✓	=
32	46					✓	✓	✓	✓	=
33	47					✓	✓	✓	✓	=
34	48					✓	✓	✓	✓	=
35	49					✓	✓	✓	✓	=
36	50					✓	✓	✓	✓	=
38	51					✓	✓	✓	✓	=
	52					✓	✓	✓	✓	-
39	53					✓	✓	✓	✓	=
40	54					✓	✓	✓	✓	=
41	55					✓	✓	✓	✓	=
42	56					✓	✓	✓	✓	=
46	57						✓	✓	✓	=
	58						✓	✓	✓	=
47	59						✓	-	-	-
	60						✓	-	-	-
	61						✓	-	-	-
50	62						✓	✓	✓	=
51	63						✓	✓	✓	=
52	64								✓	=
20	65									=
6	66									=
21	67									=
22	68									=
29	69									=
30	70									=
43	71									=
44	72									=

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11333400	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	09/02/2008	03/01/2009	06/15/2009	12/01/2009	06/20/2010	09/16/2010	01/11/2011	07/26/2011	05/03/2012
48	73									=
37	74									=
45	75									=
7	76									=
14	77									=
23	78									=
31	79									=
49	80									=

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11333400	ASGHARI-KAMRANI ET AL.
	Examiner	**Art Unit**
	ABDULHAKIM NOBAHAR	2432

ORIGINAL		INTERNATIONAL CLASSIFICATION														
CLASS	SUBCLASS	CLAIMED									NON-CLAIMED					
713	168	H	0	4	L	29 / 06 (2006.0)										
CROSS REFERENCE(S)		G	0	6	Q	20 / 00 (2012.0)										

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

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

/ABDULHAKIM NOBAHAR/ Examiner.Art Unit 2432	05/03/2012	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	52	
/GILBERTO BARRON JR/ Supervisory Patent Examiner.Art Unit 2432	05/14/2012	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	21	1B

U.S. Patent and Trademark Office

Part of Paper No. 20120503

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 2:05:52 PM
H:\EAST\Workspaces\11333400_12210926.wsp

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11333400	ASGHARI-KAMRANI ET AL.
	Examiner	Art Unit
	ABDULHAKIM NOBAHAR	2432

SEARCHED

Class	Subclass	Date	Examiner
713	182-186	6/17/2009	AN
726	2,5,8,18,27,28	6/17/2009	AN
705	64,67,72,76,78	6/17/2009	AN
	See attached report		
713	184 (see attached report)	6/24/2010	AN
	Search updated (see attached report)	12/16/2011 12/29/2011 5/3/2012	AN

SEARCH NOTES

Search Notes	Date	Examiner
PALM inventor name search	12/16/2011	AN
EAST inventor name search	12/16/2011	AN
EAST text only search	12/16/2011	AN
Search updated (see attached report)	12/16/2011 12/29/2011 5/3/2012	AN

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner
713	184,182-186	12/16/2011 5/3/2012	AN
726	2,5,8,18,27,28	12/16/2011 5/3/2012	AN
705	64,67,72,76,78	12/16/2011 5/3/2012	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
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 2:36:41 PM
H:\EAST\Workspaces\11333400_12210926.wsp

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.
11/333,400	01/18/2006	Nader Asghari-Kamrani	KAMR001US0	4456

58293 7590 05/07/2012

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
05/07/2012	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.	Applicant(s)	
	11/333,400	ASGHARI-KAMRANI ET AL.	
	Examiner	Art Unit	
	ABDULHAKIM NOBAHAR	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: *21, 26, 34, 41, 46, 51, 56, 57 and 62*.

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 form 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.: 11/333,400 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

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

Electronic Acknowledgement Receipt	
EFS ID:	12553122
Application Number:	11333400
International Application Number:	
Confirmation Number:	4456
Title of Invention:	Direct authentication system and method via trusted authenticators
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Customer Number:	58293
Filer:	Michael P. Fortkort
Filer Authorized By:	
Attorney Docket Number:	KAMR001US0
Receipt Date:	16-APR-2012
Filing Date:	18-JAN-2006
Time Stamp:	17:51:32
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	Letter Requesting Interview with Examiner	interview_request_for_042612_filed_041612_11333400.pdf	175373 0b657b4412e542c0f6002df29a676b8342a47a73	no	1
Warnings:					
Information:					

Total Files Size (in bytes):	175373

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 5, 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 5, 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.: 11/333,400

FILING DATE: January 18, 2006

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: Direct Authentication System and Method Via Trusted Authenticators

ATTORNEY DOCKET: KAMR001US0

CONFIRMATION NO.: 4456

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 17, 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:

1-20. (Cancelled)

21. (Previously Presented) A computer implemented method to authenticate an individual in communication with an entity over a communication network during communication between the entity and the individual, the computer implemented method comprising:

receiving electronically a request for a dynamic code for the individual, which request is received during authentication of the individual by the entity;

calculating the dynamic code for the individual in response to the request during authentication of the individual by the entity, wherein the dynamic code is valid for a predefined time and becomes invalid after being used;

sending electronically the dynamic code to the individual during authentication of the individual by the entity;

receiving electronically an authentication request to authenticate the individual based on a user information and the dynamic code included in the authentication request; and

verifying an identity of the individual based on the user information and the dynamic code included in the authentication request.

22. (Previously Presented) The computer implemented method of claim 21, 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 the first trusted-authenticator.

23. (Previously Presented) The computer implemented method of claim 21, 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.

24. (Previously Presented) The computer implemented method of claim 21, wherein the dynamic code includes a time-dependent SecureCode.

25. (Previously Presented) The computer implemented method of claim 21, wherein at least the dynamic code is encrypted.

26. (Previously Presented) A computer implemented method for an entity to authenticate an individual over a communication network during communication with the individual, the method comprising:

requesting electronically both a user information and a dynamic code from the individual in order to validate the individual's identity during communication with the individual, which individual obtains the dynamic code from a computer associated with a trusted-authenticator during the communication between the individual and the entity, wherein the dynamic code is valid for a predefined time and becomes invalid after being used;

receiving electronically both the user information and the dynamic code from the individual; and

authenticating the individual based on verification by the trusted-authenticator of the user

information and the dynamic code received during communication between the individual and the entity.

27. (Previously Presented) The computer implemented method of claim 26, wherein the user information and the dynamic code comprise credentials for verifying the individual's identity.

28. (Previously Presented) The computer implemented method of claim 26, wherein the dynamic code includes a time-dependent SecureCode.

29. (Previously Presented) The computer implemented method of claim 26, wherein at least the dynamic code is encrypted.

30. (Previously Presented) The computer implemented method of claim 26, wherein the entity corresponds to a business, organization, or another individual.

31. (Previously Presented) The computer implemented method of claim 26, wherein a computer associated with a first trusted-authenticator calculates the dynamic code and provides the dynamic code to the individual during communication between the individual and the entity.

32. (Cancelled)

33. (Cancelled)

34. (Previously Presented) A computer implemented method for a website to authenticate an individual over a communication network during a communication session between the individual and the website, the computer implemented method comprising:

requesting by a computer associated with the website both a user information and a dynamic code from the individual in order to validate the individual's identity, wherein the dynamic code is valid for a predefined time and becomes invalid after being used;

receiving both the user information and the dynamic code from the individual, which individual receives the dynamic code during the communication session between the individual and the website; and

creating an authentication request message including the user information and the dynamic code and providing the authentication request message to a first computer associated with a trusted-authenticator, the trusted authenticator authenticating the individual based on the user information and the dynamic code.

35. (Previously Presented) The computer implemented method of claim 34, wherein the user information and the dynamic code comprise credentials for verifying the individual's identity.

36. (Previously Presented) The computer implemented method of claim 34, wherein the dynamic code includes a non-predictable and time-dependent SecureCode.

37. (Previously Presented) The computer implemented method of claim 34, wherein at

least the dynamic code is encrypted.

38. (Previously Presented) The computer implemented method of claim 34, wherein a second computer associated with the trusted-authenticator calculates the dynamic code and provides the dynamic code to the individual during the communication session between the individual and the website.

39. (Cancelled)

40. (Cancelled)

41. (Previously Presented) A computer implemented method for authenticating an individual in communication with an entity over a communication network during communication between the entity and the individual, the method comprising:

receiving by a computer associated with the entity a dynamic code during authentication of the individual by the entity, which said dynamic code was sent to the individual by a trusted-authenticator in response to a request for the dynamic code from the trusted-authenticator during authentication of the individual by the entity and was calculated by the trusted-authenticator during authentication of the individual by the entity, wherein the dynamic code is valid for a predefined time and becomes invalid after being used;

sending electronically by the entity an authentication request to a trusted-authenticator to authenticate the individual based on a user information and a received dynamic code included in the authentication request, wherein said authentication request is sent during authentication of the

individual by the entity; and

receiving electronically by the entity a message from the trusted-authenticator either confirming or denying an identity of the individual based on the user information and the received dynamic code included in the authentication request from the entity during the time of authentication of the individual by the entity.

42. (Previously Presented) The computer implemented method according to claim 41, wherein the entity and the trusted-authenticator are the same.

43. (Previously Presented) The computer implemented method according to claim 41, wherein the entity and the trusted-authenticator are different.

44. (Previously Presented) The computer implemented method according to claim 41, wherein said dynamic code is calculated after receiving the request from the individual for the dynamic code.

45. (Previously Presented) The computer implemented method according to claim 41, wherein said dynamic code comprises a different value each time the dynamic code is requested by the individual.

46. (Previously Presented) A computer implemented method for authenticating an individual in communication with an entity during communication between the entity and the individual, the computer implemented method comprising:

sending electronically a request for a dynamic code to a trusted-authenticator during authentication of the individual by the entity;

receiving electronically the dynamic code from the trusted-authenticator during authentication of the individual by the entity, which dynamic code was calculated by a computer associated with the trusted-authenticator during authentication of the individual by the entity, wherein the dynamic code is valid for a predefined time and becomes invalid after being used;

sending electronically the dynamic code and user information during authentication of the individual by the entity to the trusted-authenticator for verification by the trusted-authenticator during authentication of the individual by the entity; and

receiving electronically acceptance or denial of authentication from the entity based on verification by the trusted-authenticator of the user information and dynamic code received from the individual during authentication of the individual by the entity.

47. (Previously Presented) The computer implemented method according to claim 46, wherein the entity and the trusted-authenticator are the same.

48. (Previously Presented) The computer implemented method according to claim 46, wherein the entity and the trusted-authenticator are different.

49. (Previously Presented) The computer implemented method according to claim 46, wherein said dynamic code is calculated after receiving the request from the individual for the dynamic code.

50. (Previously Presented) The computer implemented method according to claim 46, wherein said dynamic code comprises a different value each time the dynamic code is requested for an individual.

51. (Previously Presented) A computer implemented method to authenticate an individual during communication between the individual and another entity, the method comprising:

receiving electronically a request for a dynamic code, wherein the request is received during authentication of the individual by the entity;

sending the dynamic code electronically to the individual during authentication of the individual by the entity, wherein the dynamic code is valid for a predefined time and becomes invalid after being used;

receiving electronically an authentication request from the entity to authenticate the individual based on a user information and dynamic code received from the individual during authentication of the individual by the entity, wherein said authentication request is received during authentication of the individual by the entity; and

verifying by a computer an identity of the individual based on the user information and the received dynamic code in response to the authentication request from the entity during the time of authentication of the individual by the entity.

52. (Previously Presented) The computer implemented method according to claim 51, further comprising:

sending electronically a confirmation or denial authentication message to the entity during

authentication of the individual by the entity.

53. (Previously Presented) The computer implemented method according to claim 51, wherein the entity comprises a trusted-authenticator.

54. (Previously Presented) The computer implemented method according to claim 51, wherein said dynamic code is calculated after receiving the request for the dynamic code.

55. (Previously Presented) The computer implemented method according to claim 51, wherein said dynamic code comprises a different value each time the dynamic code is requested for the individual.

56. (Previously Presented) A computer implemented method to perform a two-factor authentication of an individual based on a user information as a first credential and a dynamic code as a second credential during communication over a network between an entity and the individual, the method comprising:

receiving electronically acceptance or denial of two-factor authentication from the entity based on two credentials received from the individual, wherein:

said user information comprises the first credential and said dynamic code comprises the second credential;

said dynamic code was calculated by a computer program associated with a trusted-authenticator and provided to the individual during said communication between the entity and the individual, wherein the dynamic code is valid for a predefined time and becomes invalid after

being used;

said user information and said dynamic code were electronically received and verified by the trusted-authenticator during authentication of the individual by the entity; and

said dynamic code comprises a different value each time the individual receives a dynamic code from a trusted-authenticator.

57. (Previously Presented) A computer implemented method to perform a two-factor authentication of an individual based on a user information as a first credential and a dynamic code as a second credential during communication between the entity and the individual, the method comprising:

accepting or denying electronically of a two-factor authentication of the individual based on two credentials received from the individual, wherein:

said user information comprises the first credential and said dynamic code comprises the second credential;

said dynamic code was calculated by a first computer associated with a trusted-authenticator and sent by a second computer associated with the trusted-authenticator to the individual during communication between the individual and the entity, wherein the dynamic code is valid for a predefined time and becomes invalid after being used;

said user information and said dynamic code were received electronically during authentication of the individual by the entity and were verified by the trusted-authenticator during said communication between the individual and the entity; and

said first computer associated with said trusted-authenticator calculates a different value for said dynamic code each time the individual requests a dynamic code from the trusted-

authenticator.

58. (Previously Presented) The computer implemented method according to claim 57, wherein the first computer and the second computer are the same.

59. (Cancelled).

60. (Cancelled).

61. (Cancelled).

62. (Previously Presented) A computer implemented method to perform a two-factor authentication of an individual based on a user information as a first credential and a dynamic code as a second credential during communication between the entity and the individual, the method comprising:

accepting or denying electronically of the two-factor authentication of the individual based on two credentials received from the individual, wherein:

said user information comprises the first credential and said dynamic code comprises the second credential;

said dynamic code was calculated by a trusted-authenticator and sent to the individual for authentication between the individual and the entity, wherein the dynamic code is valid for a predefined time and becomes invalid after being used;

said user information and said dynamic code were received electronically during

authentication of the individual by the entity and user information was verified by a first computer and dynamic code was verified by a second computer associated with the trusted-authenticator during said communication between the individual and the entity; and

said dynamic code comprises a different value each time the individual receives a dynamic code from a trusted-authenticator.

63. (Previously Presented) The computer implemented method according to claim 62, wherein the first computer and the second computer are the same.

64. (Previously Presented) The computer implemented method according to claim 62, wherein said dynamic code is valid for a predefined time and may be used by the individual before becoming invalid.

65. (Previously Presented) The computer implemented method of claim 34, wherein a computer program associated with the trusted-authenticator calculates the dynamic code and provides the dynamic code to the individual during the communication session between the individual and the website.

66. (Previously Presented) The computer implemented method of claim 21, wherein the user information is verified by a first computer and dynamic code is verified by a second computer.

67. (Previously Presented) The computer implemented method according to claim 34,

wherein the website and the trusted-authenticator are the same.

68. (Previously Presented) The computer implemented method of claim 34, wherein the user information is verified by a first computer and dynamic code is verified by a second computer associated with the trusted-authenticator.

69. (Previously Presented) The computer implemented method according to claim 41, wherein the entity and the trusted-authenticator are the same.

70. (Previously Presented) The computer implemented method of claim 41 wherein the user information is verified by a first computer and dynamic code is verified by a second computer associated with the trusted-authenticator.

71. (Previously Presented) The computer implemented method of claim 56, wherein the user information is verified by a first computer and dynamic code is verified by a second computer associated with the trusted-authenticator.

72. (Previously Presented) The computer implemented method according to claim 56, wherein the entity and the trusted-authenticator are the same.

73. (Previously Presented) The computer implemented method according to claim 57, wherein the entity and the trusted-authenticator are the same.

74. (Previously Presented) The computer implemented method according to claim 46, wherein the dynamic code is alphanumeric.

75. (Previously Presented) The computer implemented method according to claim 56, wherein the dynamic code is alphanumeric.

76. (Previously Presented) The computer implemented method according to claim 21, wherein the dynamic code is alphanumeric.

77. (Previously Presented) The computer implemented method according to claim 26, wherein the dynamic code is alphanumeric.

78. (Previously Presented) The computer implemented method according to claim 34, wherein the dynamic code is alphanumeric.

79. (Previously Presented) The computer implemented method according to claim 41, wherein the dynamic code is alphanumeric.

80. (Previously Presented) The computer implemented method according to claim 57, wherein the dynamic code is alphanumeric.

REMARKS

Claims 21-31, 34-38, 41-58 and 62-80 were previously pending. Claims 1-20, 32-33, 39-40, 59-61 have been previously cancelled without disclaimer of or prejudice to the subject matter contained therein. Claims 21-31, 34-38, 41-58 and 62-80 remain pending.

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

The Office Action rejected claims 21-31, 34-38, 41, 43-46, 48-52, 54-57, 62 and 64 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 21, 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 030512, ¶¶13-15; Aff. K. Kamrani filed 030512, ¶¶14-16; Aff. Hewitt filed 030512, ¶¶17-19;* and *Aff. Hosseinzadeh filed 030512, ¶¶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 030512, ¶¶16-19; Aff. K. Kamrani filed 030512, ¶¶17-20; Aff. Hewitt filed 030512, ¶¶21-23;* and *Aff. Hosseinzadeh filed 030512, ¶¶16-19.*

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

The Claims at issue include the limitations that the dynamic code is generated during the transaction between the user and the External-Entity and that the so generated dynamic code 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 030512, ¶¶13-15; Aff. K. Kamrani filed 030512, ¶¶14-16; Aff. Hewitt filed 030512, ¶¶17-19;* and *Aff. Hosseinzadeh filed 030512, ¶¶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 030512, ¶¶16-19; Aff. K. Kamrani filed 030512, ¶¶17-20; Aff. Hewitt filed 030512, ¶¶21-23;* and *Aff.*

Hosseinzadeh filed 030512, ¶¶16-19. Hill is merely cited for the claim element that the dynamic code becomes invalid after use.

Nonce Is Not Recited Dynamic Code

The Examiner equates the nonce of *Kaliski, Jr.* to the dynamic code of the present application ("wherein the nonce corresponds to the recited dynamic code." Office Action, p. 4). But the Applicants respectfully submit that the nonce is not equivalent to the recited dynamic code. *Aff. N. Kamrani filed 030512, ¶¶5-8; Aff. K. Kamrani filed 030512, ¶¶6-9; Aff. Hewitt filed 030512, ¶¶9-12;* and *Aff. Hosseinzadeh filed 030512, ¶¶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 030512, ¶¶13-15; Aff. K. Kamrani filed 030512, ¶¶14-16; Aff. Hewitt filed 030512, ¶¶17-19;* and *Aff. Hosseinzadeh filed 030512, ¶¶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 030512, ¶¶5-8; Aff. K. Kamrani filed 030512, ¶¶6-9; Aff. Hewitt filed 030512, ¶¶9-12;* and *Aff. Hosseinzadeh filed 030512, ¶¶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 030512, ¶¶10-12; Aff. K. Kamrani filed 030512, ¶¶11-13; Aff. Hewitt filed 030512, ¶¶14-16;* and *Aff. Hosseinzadeh filed 030512, ¶¶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 dynamic code." 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 030512, ¶9; Aff. K. Kamrani filed 030512, ¶10; Aff. Hewitt filed 030512, ¶13;* and *Aff. Hosseinzadeh filed 030512, ¶9.* Thus, neither reference includes the recited claim elements of: (1) authenticating the user based on a dynamic code; (2) receiving an authentication request message by a Central Entity, which message includes a dynamic code generated by the Central Entity; (3) authenticating the user by the Central Entity that generated the dynamic code. 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 5, 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 5, 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 5, 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.: 11/333,400

FILING DATE: January 18, 2006

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: Direct Authentication System and Method Via Trusted Authenticators

ATTORNEY DOCKET: KAMR001US0

CONFIRMATION NO.: 4456

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 17, 2012 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 11/333,400 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 dynamic code

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 dynamic code 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 dynamic code 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 code" 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 dynamic code, 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 dynamic code. 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 dynamic code 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

3-2-12
Date

Certification Under 37 C.F.R. § 1.8

I hereby certify that on March 5, 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 5, 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.: 11/333,400

FILING DATE: January 18, 2006

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: Direct Authentication System and Method Via Trusted Authenticators

ATTORNEY DOCKET: KAMR001US0

CONFIRMATION NO.: 4456

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 17, 2012 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 11/333,400 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 dynamic code

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 dynamic code 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 dynamic code 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 code" 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 dynamic code, 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 dynamic code. 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 dynamic code 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.*, 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,

James Hewitt — Date: March 2, 2012

Certification Under 37 C.F.R. § 1.8

I hereby certify that on March 5, 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 5, 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.: 11/333,400

FILING DATE: January 18, 2006

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: Direct Authentication System and Method Via Trusted Authenticators

ATTORNEY DOCKET: KAMR001US0

CONFIRMATION NO.: 4456

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 17, 2012 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 11/333,400 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. 11/333,400, 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 dynamic code

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 dynamic code 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 dynamic code 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 code" 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 *Kamvar*. 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 dynamic code, 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 dynamic code. 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 dynamic code 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.*

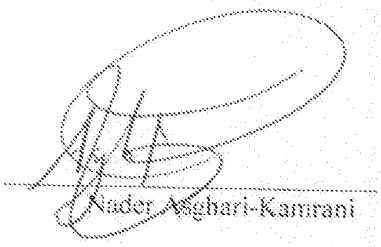
> The merchant module includes administration functions. These maintain a count of how many unused authentication tokens remain, and send a request for further tokens to the payment service when that number falls below a predetermined threshold.

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.

In witness whereof,



Nader Asghari-Kamrani

03/02/2012
Date

Certification Under 37 C.F.R. § 1.8

I hereby certify that on March 5, 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 5, 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.: 11/333,400

FILING DATE: January 18, 2006

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: Direct Authentication System and Method Via Trusted Authenticators

ATTORNEY DOCKET: KAMR001US0

CONFIRMATION NO.: 4456

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 17, 2012 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 11/333,400 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. 11/333,400, 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 dynamic code

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 dynamic code 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 dynamic code 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 dynamic code" 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 dynamic code, 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 dynamic code. 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 dynamic code 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 $(0 \leq s \leq n-1)$ 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

3/2/2012
Date

Electronic Acknowledgement Receipt	
EFS ID:	12221275
Application Number:	11333400
International Application Number:	
Confirmation Number:	4456
Title of Invention:	Direct authentication system and method via trusted authenticators
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Customer Number:	58293
Filer:	Michael P. Fortkort
Filer Authorized By:	
Attorney Docket Number:	KAMR001US0
Receipt Date:	05-MAR-2012
Filing Date:	18-JAN-2006
Time Stamp:	12:11:48
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	11333400_Response_to_Office_Action_mailed_011712.pdf	89310 81a0398086b6eff77667d13f7f396a9f64be934d	no	23

Warnings:
Information:

2	Rule 130, 131 or 132 Affidavits	11333400_132_Affidavit_Hossienzadeh_filed_030512.pdf	316563 ec3c1b3d2f17decb51e33f5408d37dae3050ff2a	no	8
Warnings:					
Information:					
3	Rule 130, 131 or 132 Affidavits	11333400_132_Affidavit_Hewitt_filed_030512.pdf	5806166 911dc8e1f494b71d2cdbdaf182281f229373ccc6	no	8
Warnings:					
Information:					
4	Rule 130, 131 or 132 Affidavits	11333400_132_Affidavit_nKamrani_filed_030512.pdf	8604186 baa1c6907d95cb5044b97b55a71338066f4282af	no	8
Warnings:					
Information:					
5	Rule 130, 131 or 132 Affidavits	11333400_132_Affidavit_KKamrani_filed_030512.pdf	7631482 49ee35612345b03ed06b4447afec01e76326f1b6	no	8
Warnings:					
Information:					
		Total Files Size (in bytes):	22447707		

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.

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 11/333,400	Filing Date 01/18/2006	☐ 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

AMENDMENT	03/05/2012	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 53	Minus	** 53	= 0	X $30 =	0	OR	X $ =	
	Independent (37 CFR 1.16(h))	* 9	Minus	***9	= 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	0	OR	TOTAL ADD'L FEE	

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)	OR	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:
/NICOLE LAWRENCE/

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.
11/333,400	01/18/2006	Nader Asghari-Kamrani	KAMR001US0	4456

58293 7590 01/17/2012

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
01/17/2012	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.	Applicant(s)	
	11/333,400	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 --

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) *21-31,34-38,41-58 and 62-80* is/are pending in the application.

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

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *21-31,34-38,41-58 and 62-80* 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 communication is in response to applicants Amendment after Non-final rejection received on 11/17/2011.

2. A terminal disclaimer for this application was filed on 12/12/2011. Thus, the double patenting rejections are withdrawn.

3. Claims 21-31, 34-38, 41-58 and 62-80 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) 21-31, 34-38, 41-58 and 62-80 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 of rejection as follows.

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.

> (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.

The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 21-31, 34-38, 41, 43-46, 48-52, 54-57, 62 and 64 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 21, 26, 34, 41, 46 and 51, Kaliski discloses:

(Claim 21 as representative) A computer implemented method to authenticate an individual in communication with an entity over a communication network during communication between the entity and the individual (see, e.g., abstract and Fig. 7), the computer implemented method comprising:

receiving electronically a request for a dynamic code for the individual, which request is received during authentication of the individual by the entity (see, e.g., [0110] and Fig. 7, where providing client information 772 to an authentication server 730 corresponds to the recited request for a dynamic code);

calculating the dynamic code for the individual in response to the request during authentication of the individual by the entity, 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, step 773, where the blinded R plus the nonce corresponds to the recited dynamic code);

sending by a computer the dynamic code over a communication network to the individual during authentication of the individual by the entity (see, e.g., [0111] and Fig. 7, step 773);

receiving electronically an authentication request to authenticate the individual based on a user information and the dynamic code included in the authentication request (see, e.g., [0111], where the blinded result R and nonce or other session identifier corresponds to the recited user information and the dynamic code, Fig. 7, steps 774 and 776 and [0112], where the message includes the nonce); and

verifying an identity of the individual based on the user information and the dynamic code included in the authentication request (see, e.g., [0111], where the blinded result R and nonce or other session identifier corresponds to the recited user information and the dynamic code, [109] and [0112], where authenticating the client corresponds to verifying the identity of the individual).

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).

Kaliski discloses:

(Claims 22, 31, 38 and 65) The computer implemented method of claim 21, 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 the first trusted-authenticator (see, e.g., Fig. 7, where the authentication server receives the request for the dynamic code at step 772, provide the dynamic code to the user at step 773 and receives the request for authentication at step 776).

(Claims 24, 28 and 36) The computer implemented method of claim 21, wherein the dynamic code includes a time-dependent SecureCode (see, e.g.,

[0044]: “time-based code”, [0057]: “The authentication 65 thus can take place in various ways, including without limitation by transmission… time-based code”, [0111], where the nonce corresponds to the recited SecureCode which is generated by the authentication server each time upon the client request).

(Claims 25, 29 and 37) The computer implemented method of claim 21, wherein at least the dynamic code is encrypted (see, e.g., [0007], [0044]: “encrypted secret” and [0062]).

(Claims 27 and 35) The computer implemented method of claim 26, wherein the user information and dynamic code comprise credentials for verifying the individual's identity (see, e.g., Fig. 7, step 774, where PW and nonce are used to verify the individual's identity).

Kaliski-Hill discloses:

(Claim 30) The computer implemented method of claim 26, wherein the entity corresponds to a business, organization, or another individual (see, e.g., Kaliski: Fig. 7, web server 710 and Hill: Fig. 1, merchant 500).

Regarding claims 42, 47, 58, 53, 63, 67, 69, 72 and 73, Kaliski disclose:
The computer implemented method according to claim 41, wherein the entity and the trusted authenticator are the same (see, e.g., [0101]-[0103], where the user only interacts with the web server 610).

Kaliski discloses:

(Claims 43 and 48) The computer implemented method according to claim 41, wherein the entity and the trusted-authenticator are different (see, e.g., Fig. 7, where the web server is the entity and the authentication server is the trusted authenticator).

Kaliski discloses:

(Claims 44, 49 and 54) The computer implemented method according to claim 41, wherein said dynamic code is calculated by a computer after receiving the request from the individual for the dynamic code (see, e.g., [0110], Fig. 7, steps 772 and 773).

Kaliski-Hill discloses:

(Claims 45, 50 and 55) The computer implemented method according to claim 41, wherein said dynamic code comprises a different value each time the dynamic code is requested by the individual (see, e.g., Kaliski: [0044]: “time-based code”, [0057]: “The authentication 65 thus can take place in various ways, including without limitation by transmission… time-based code”, where the time- means a dynamic code which is not permanent and Hill: col. 6, lines 25-30, where a one-time password means that the dynamic code is calculated for only one time to be used).

Kaliski-Hill discloses:

(Claim 52) The computer implemented method according to claim 51, further comprising:

sending electronically a confirmation or denial authentication message by a computer to the entity during authentication of the individual by the entity (see, e.g., Kaliski: [0112] and Hill: col. 6, lines 45-50).

Regarding claims 56, 57 and 62, these claims are rejected as applied to the like elements of claims 21, 26, 27, 34, 35, 41, 45, 46, 50, 51 and 55.

Regarding claim 64, Kaliski discloses:

The computer implemented method according to claim 62, wherein said dynamic code is valid for a predefined time and may be used by the individual before becoming invalid (see, e.g., [0044]: “time-based code”, [0057]: “The authentication 65 thus can take place in various ways, including without limitation by transmission… time-based code”).

Regarding claims 74-80, Kaliski discloses:

The computer implemented method according to claim 46, wherein the dynamic code is alphanumeric (see [0033]).

Claims 23, 66, 68, 70 and 71 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 23, 68, 70 and 71, Kaliski-Hill does not expressly disclose: The computer implemented method of claim 21, 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.

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 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 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.

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. 11/333,400	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-2010/0100724 A1	04-2010	Kaliski, JR., Burton S.	713/155
*	B	US-6,236,981 B1	05-2001	Hill, Jake	705/67
*	C	US-2002/0040346 A1	04-2002	Kwan, Khai Hee	705/51
*	D	US-2002/0046189 A1	04-2002	Morita et al.	705/67
*	E	US-2002/0133412 A1	09-2002	OLIVER et al.	705/26
*	F	US-2002/0184143 A1	12-2002	Khater, Ali Mohamed	705/39
*	G	US-2004/0030752 A1	02-2004	Selgas et al.	709/206
*	H	US-7,150,038 B1	12-2006	Samar, Vipin	726/8
*	I	US-6,067,621 A	05-2000	Yu et al.	713/172
	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.	Applicant(s)/Patent Under Reexamination
	11333400	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	09/02/2008	03/01/2009	06/15/2009	12/01/2009	06/20/2010	09/16/2010	01/11/2011	07/26/2011	01/03/2012
	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.	Applicant(s)/Patent Under Reexamination
	11333400	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	09/02/2008	03/01/2009	06/15/2009	12/01/2009	06/20/2010	09/16/2010	01/11/2011	07/26/2011	01/03/2012
	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.	Applicant(s)/Patent Under Reexamination
	11333400	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	09/02/2008	03/01/2009	06/15/2009	12/01/2009	06/20/2010	09/16/2010	01/11/2011	07/26/2011	01/03/2012
	73									✓
	74									✓
	75									✓
	76									✓
	77									✓
	78									✓
	79									✓
	80									✓

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

1/3/2012 5:00:01 PM
H:\EAST\Workspaces\11333400_12210926.wsp

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11333400	ASGHARI-KAMRANI ET AL.
	Examiner	**Art Unit**
	ABDULHAKIM NOBAHAR	2432

SEARCHED			
Class	**Subclass**	**Date**	**Examiner**
713	182-186	6/17/2009	AN
726	2,5,8,18,27,28	6/17/2009	AN
705	64,67,72,76,78	6/17/2009	AN
	See attached report		
713	184 (see attached report)	6/24/2010	AN
	Search updated (see attached report)	12/16/2011 12/29/2011	AN

SEARCH NOTES		
Search Notes	**Date**	**Examiner**
PALM inventor name search	12/16/2011	AN
EAST inventor name search	12/16/2011	AN
EAST text only search	12/16/2011	AN
See attached report	12/16/2011 12/29/2011	AN

INTERFERENCE SEARCH			
Class	**Subclass**	**Date**	**Examiner**
713	184,182-186	12/16/2011	AN
726	2,5,8,18,27,28	12/16/2011	AN
705	64,67,72,76,78	12/16/2011	AN
	See attached report		

/ABDULHAKIM NOBAHAR/ Examiner.Art Unit 2432	

Application Number	Application/Control No.	Applicant(s)/Patent under Reexamination	
	11/333,400	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

PTO/SB/25 (08-11)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

TERMINAL DISCLAIMER TO OBVIATE A PROVISIONAL DOUBLE PATENTING REJECTION OVER A PENDING "REFERENCE" APPLICATION	Docket Number (Optional) KAMR001US0

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

Application No.: 11/333,400

Filed: JANUARY 18, 2006

For: Direct authentication system and method via trusted authenticators

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 12/210,926, filed September 15, 2008, 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/	December 12, 2011
Signature	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.

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:	11333400
Filing Date:	18-Jan-2006
Title of Invention:	Direct authentication system and method via trusted authenticators
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Filer:	Michael P. Fortkort
Attorney Docket Number:	KAMR001US0
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:	11589978
Application Number:	11333400
International Application Number:	
Confirmation Number:	4456
Title of Invention:	Direct authentication system and method via trusted authenticators
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Customer Number:	58293
Filer:	Michael P. Fortkort
Filer Authorized By:	
Attorney Docket Number:	KAMR001US0
Receipt Date:	12-DEC-2011
Filing Date:	18-JAN-2006
Time Stamp:	09:58:07
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	8370
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_11333400_filed_121211.pdf	342817 78a7539457a600eb5a12688412edd18f89078ff2	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	29683 c62997079e4e7f6076ca508a257810fb7de366e4	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	372500		

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.: 11/333,400

FILING DATE: January 18, 2006

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: DIRECT AUTHENTICATION SYSTEM AND METHOD VIA TRUSTED AUTHENTICATORS

ATTORNEY DOCKET: KAMR001US0

CONFIRMATION NO.: 4456

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

RESPONSE TO NON-FINAL OFFICE ACTION

Sir:

The Applicant hereby petitions the Assistant Commissioner to grant a one (1) month extension of time, up to and including December 5, 2011, in which to file a response to the outstanding Office Action mailed August 5, 2011 ("Office Action") in the above-identified application. The small entity one-month extension fee in the amount of $75.00 may be charged

to the credit card on the attached credit card authorization form. Any additional fees may be charged to the deposit account of MICHAEL P FORTKORT PC, Deposit Account No. 50-3776.

In response to the non-final Office Action mailed August 5, 2011, the Applicants hereby respectfully submit the following amendments and remarks:

Amendments to the Claims begin on page 3.

Remarks begin on page 17.

In the Claims:

Please amend the claims as follows:

1-20. (Cancelled)

21. (Currently Amended) A computer implemented method to authenticate an individual in communication with an entity over a communication network during communication between the entity and the individual, the computer implemented method comprising:

receiving electronically a request for a dynamic code for the individual, which request is received during authentication of the individual by the entity;

calculating the dynamic code for the individual in response to the request during authentication of the individual by the entity, wherein the dynamic code is valid for a predefined time and becomes invalid after being used;

sending electronically the dynamic code to the individual during authentication of the individual by the entity;

receiving electronically an authentication request to authenticate the individual based on a user information and the dynamic code included in the authentication request; and

verifying an identity of the individual based on the user information and the dynamic code included in the authentication request.

22. (Previously Presented) The computer implemented method of claim 21, 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 the first trusted-authenticator.

23. (Previously Presented) The computer implemented method of claim 21, 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.

24. (Currently Amended) The computer implemented method of claim 21, wherein the dynamic code includes a ~~non-predictable and~~ time-dependent SecureCode.

25. (Previously Presented) The computer implemented method of claim 21, wherein at least the dynamic code is encrypted.

26. (Currently Amended) A computer implemented method for an entity to authenticate an individual over a communication network during communication with the individual, the method comprising:

requesting electronically both a user information and a dynamic code from the individual in order to validate the individual's identity during communication with the individual, which individual obtains the dynamic code from a computer associated with a trusted-authenticator during the communication between the individual and the entity, wherein the dynamic code is valid for a predefined time and becomes invalid after being used;

receiving electronically both the user information and the dynamic code from the individual; and

authenticating the individual based on verification by the trusted-authenticator of the user

information and the dynamic code received during communication between the individual and the entity

~~creating an authentication request message including both the user information and the received dynamic code and providing the authentication request message to a trusted-authenticator, the trusted-authenticator authenticating the individual based on a combination of the user information and the received dynamic code~~.

27. (Previously Presented) The computer implemented method of claim 26, wherein the user information and the dynamic code comprise credentials for verifying the individual's identity.

28. (Currently Amended) The computer implemented method of claim 26, wherein the dynamic code includes a ~~non-predictable and~~ time-dependent SecureCode.

29. (Previously Presented) The computer implemented method of claim 26, wherein at least the dynamic code is encrypted.

30. (Previously Presented) The computer implemented method of claim 26, wherein the entity corresponds to a business, organization, or another individual.

31. (Previously Presented) The computer implemented method of claim 26, wherein a computer associated with a first trusted-authenticator calculates the dynamic code and provides the dynamic code to the individual during communication between the individual and the entity.

32. (Cancelled)

33. (Cancelled)

34. (Currently Amended) A computer implemented method for a website to authenticate an individual over a communication network during a communication session between the individual and the website, the computer implemented method comprising:

requesting by a computer associated with the website both a user information and a dynamic code from the individual in order to validate the individual's identity, wherein the dynamic code is valid for a predefined time and becomes invalid after being used;

receiving both the user information and the dynamic code from the individual, which individual receives the dynamic code during the communication session between the individual and the website; and

creating an authentication request message including the user information and the dynamic code and providing the authentication request message to a first computer associated with a trusted-authenticator, the trusted authenticator authenticating the individual based on the user information and the dynamic code.

35. (Previously Presented) The computer implemented method of claim 34, wherein the user information and the dynamic code comprise credentials for verifying the individual's identity.

36. (Previously Presented) The computer implemented method of claim 34, wherein the dynamic code includes a non-predictable and time-dependent SecureCode.

37. (Previously Presented) The computer implemented method of claim 34, wherein at least the dynamic code is encrypted.

38. (Previously Presented) The computer implemented method of claim 34, wherein a second computer associated with the trusted-authenticator calculates the dynamic code and provides the dynamic code to the individual during the communication session between the individual and the website.

39. (Cancelled)

40. (Cancelled)

41. (Currently Amended) A computer implemented method for authenticating an individual in communication with an entity over a communication network during communication between the entity and the individual, the method comprising:

receiving by a computer associated with the entity a dynamic code during authentication of the individual by the entity, which said dynamic code was sent to the individual by a trusted-authenticator in response to a request for the dynamic code from the trusted-authenticator during authentication of the individual by the entity and was calculated by the trusted-authenticator during authentication of the individual by the entity, wherein the dynamic code is valid for a

predefined time and becomes invalid after being used;

sending electronically by the entity an authentication request to a trusted-authenticator to authenticate the individual based on a user information and a received dynamic code included in the authentication request, wherein said authentication request is sent during authentication of the individual by the entity; and

receiving electronically by the entity a message from the trusted-authenticator either confirming or denying an identity of the individual based on the user information and the received dynamic code included in the authentication request from the entity during the time of authentication of the individual by the entity.

42. (Previously Presented) The computer implemented method according to claim 41, wherein the entity and the trusted-authenticator are the same.

43. (Previously Presented) The computer implemented method according to claim 41, wherein the entity and the trusted-authenticator are different.

44. (Previously Presented) The computer implemented method according to claim 41, wherein said dynamic code is calculated after receiving the request from the individual for the dynamic code.

45. (Previously Presented) The computer implemented method according to claim 41, wherein said dynamic code comprises a different value each time the dynamic code is requested by the individual.

46. (Currently Amended) A computer implemented method for authenticating an individual in communication with an entity during communication between the entity and the individual, the computer implemented method comprising:

sending electronically a request for a dynamic code to a trusted-authenticator during authentication of the individual by the entity;

receiving electronically the dynamic code from the trusted-authenticator during authentication of the individual by the entity, which dynamic code was calculated by a computer associated with the trusted-authenticator during authentication of the individual by the entity, wherein the dynamic code is valid for a predefined time and becomes invalid after being used;

sending electronically the dynamic code and user information during authentication of the individual by the entity to the trusted-authenticator for verification by the trusted-authenticator during authentication of the individual by the entity; and

receiving electronically acceptance or denial of authentication from the entity based on verification by the trusted-authenticator of the user information and dynamic code received from the individual during authentication of the individual by the entity.

47. (Previously Presented) The computer implemented method according to claim 46, wherein the entity and the trusted-authenticator are the same.

48. (Previously Presented) The computer implemented method according to claim 46, wherein the entity and the trusted-authenticator are different.

49. (Previously Presented) The computer implemented method according to claim 46, wherein said dynamic code is calculated after receiving the request from the individual for the dynamic code.

50. (Previously Presented) The computer implemented method according to claim 46, wherein said dynamic code comprises a different value each time the dynamic code is requested for an individual.

51. (Currently Amended) A computer implemented method to authenticate an individual during communication between the individual and another entity, the method comprising:

receiving electronically a request for a dynamic code, wherein the request is received during authentication of the individual by the entity;

sending the dynamic code electronically to the individual during authentication of the individual by the entity, wherein the dynamic code is valid for a predefined time and becomes invalid after being used;

receiving electronically an authentication request from the entity to authenticate the individual based on a user information and dynamic code received from the individual during authentication of the individual by the entity, wherein said authentication request is received during authentication of the individual by the entity; and

verifying by a computer an identity of the individual based on the user information and the received dynamic code in response to the authentication request from the entity during the time of authentication of the individual by the entity.

52. (Previously Presented) The computer implemented method according to claim 51, further comprising:

sending electronically a confirmation or denial authentication message to the entity during authentication of the individual by the entity.

53. (Previously Presented) The computer implemented method according to claim 51, wherein the entity comprises a trusted-authenticator.

54. (Previously Presented) The computer implemented method according to claim 51, wherein said dynamic code is calculated after receiving the request for the dynamic code.

55. (Previously Presented) The computer implemented method according to claim 51, wherein said dynamic code comprises a different value each time the dynamic code is requested for the individual.

56. (Currently Amended) A computer implemented method to perform a two-factor authentication of an individual based on a user information as a first credential and a dynamic code as a second credential during communication over a network between an entity and the individual, the method comprising:

receiving electronically acceptance or denial of two-factor authentication from the entity based on two credentials received from the individual, wherein:

said user information comprises the first credential and said dynamic code comprises the second credential;

said dynamic code was calculated by a computer program associated with ~~and received from~~ a trusted-authenticator and provided to the individual during said communication between the entity and the individual, wherein the dynamic code is valid for a predefined time and becomes invalid after being used;

said user information and said dynamic code were electronically received and verified by the trusted-authenticator during authentication of the individual by the entity; and

said dynamic code comprises a different value each time the individual receives a dynamic code from a trusted-authenticator.

57. (Currently Amended) A computer implemented method to perform a two-factor authentication of an individual based on a user information as a first credential and a dynamic code as a second credential during communication between the entity and the individual, the method comprising:

accepting or denying electronically of a two-factor authentication of the individual based on two credentials received from the individual, wherein:

said user information comprises the first credential and said dynamic code comprises the second credential;

said dynamic code was calculated by a first computer associated with a trusted-authenticator and sent by a second computer associated with the trusted-authenticator to the individual during communication between the individual and the entity, wherein the dynamic code is valid for a predefined time and becomes invalid after being used;

said user information and said dynamic code were received electronically during authentication of the individual by the entity and were verified by the trusted-authenticator during

said communication between the individual and the entity; and

said first computer associated with said trusted-authenticator calculates a different value for said dynamic code each time the individual requests a dynamic code from the trusted-authenticator.

58. (Previously Presented) The computer implemented method according to claim 57, wherein the first computer and the second computer are the same.

59. (Cancelled).

60. (Cancelled).

61. (Cancelled).

62. (Currently Amended) A computer implemented method to perform a two-factor authentication of an individual based on a user information as a first credential and a dynamic code as a second credential during communication between the entity and the individual, the method comprising:

accepting or denying electronically of the two-factor authentication of the individual based on two credentials received from the individual, wherein:

said user information comprises the first credential and said dynamic code comprises the second credential;

said dynamic code was calculated by a trusted-authenticator and sent to the individual for

authentication between the individual and the entity, wherein the dynamic code is valid for a predefined time and becomes invalid after being used;

said user information and said dynamic code were received electronically during authentication of the individual by the entity and user information was verified by a first computer and dynamic code was verified by a second computer associated with the trusted-authenticator during said communication between the individual and the entity; and

said dynamic code comprises a different value each time the individual receives a dynamic code from a trusted-authenticator.

63. (Previously Presented) The computer implemented method according to claim 62, wherein the first computer and the second computer are the same.

64. (Previously Presented) The computer implemented method according to claim 62, wherein said dynamic code is valid for a predefined time and may be used by the individual before becoming invalid.

65. (New) The computer implemented method of claim 34, wherein a computer program associated with the trusted-authenticator calculates the dynamic code and provides the dynamic code to the individual during the communication session between the individual and the website.

66. (New) The computer implemented method of claim 21, wherein the user information is verified by a first computer and dynamic code is verified by a second computer.

67. (New) The computer implemented method according to claim 34, wherein the website and the trusted-authenticator are the same.

68. (New) The computer implemented method of claim 34, wherein the user information is verified by a first computer and dynamic code is verified by a second computer associated with the trusted-authenticator.

69. (New) The computer implemented method according to claim 41, wherein the entity and the trusted-authenticator are the same.

70. (New) The computer implemented method of claim 41 wherein the user information is verified by a first computer and dynamic code is verified by a second computer associated with the trusted-authenticator.

71. (New) The computer implemented method of claim 56, wherein the user information is verified by a first computer and dynamic code is verified by a second computer associated with the trusted-authenticator.

72. (New) The computer implemented method according to claim 56, wherein the entity and the trusted-authenticator are the same.

73. (New) The computer implemented method according to claim 57, wherein the entity and the trusted-authenticator are the same.

74. (New) The computer implemented method according to claim 46, wherein the dynamic code is alphanumeric.

75. (New) The computer implemented method according to claim 56, wherein the dynamic code is alphanumeric.

76. (New) The computer implemented method according to claim 21, wherein the dynamic code is alphanumeric.

77. (New) The computer implemented method according to claim 26, wherein the dynamic code is alphanumeric.

78. (New) The computer implemented method according to claim 34, wherein the dynamic code is alphanumeric.

79. (New) The computer implemented method according to claim 41, wherein the dynamic code is alphanumeric.

80. (New) The computer implemented method according to claim 57, wherein the dynamic code is alphanumeric.

REMARKS

Claims 21-31, 34-38, 41-58 and 62-64 were previously pending. Claims 1-20, 32-33, 39-40, 59-61 have been previously cancelled without disclaimer of or prejudice to the subject matter contained therein. Claims 21, 24, 26, 28, 34, 41, 46, 51, 56, 57 and 62 have been amended to more particularly describe the claimed invention. Claims 65-80 have been added to more particularly describe the claimed invention. Claims 21-31, 34-38, 41-58 and 62-80 remain pending.

DOUBLE PATENTING

The Office Action provisionally rejected claims 21-23, 26, 27, 30, 31, 34, 38, 41-44, 46-49, 51-54, 56-58 and 62-64 under the judicially created doctrine of obviousness-type double patenting as being unpatentable over co-pending claims 1, 12, 14, 21, 33, 34, 36, 37, 40, 41, 43, 44, 51, 53-55, 58, 60-66, 69, 70, 73, 74, and 80 of co-pending application No. 12/210,926. Upon allowance of these claims in either application, the Applicants will timely file a terminal disclaimer, which will obviate this rejection.

CLAIMS REMAIN PATENTABLE OVER *FRANKLIN ET AL.* AND *FOX ET AL.* TAKEN ALONE OR IN COMBINATION

The Office Action rejected claims 21-31, 34-38, 41, 43-46, 48-52, 54-57, 62 and 64 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 21, the Office Action asserts that Franklin discloses all of the elements of the claim at issue, except for "receiving electronically an authentication request to authenticate the individual based on a user information and the dynamic code included in the authentication request" and "verifying an identity of the individual based on the user information and the dynamic code included in the authentication request." 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 code is calculated during the transaction between the user and the External-Entity and that the so calculated dynamic code is included in an authentication request and then used to verify the identity of 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 calculated 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 code during the transaction that is then used to validate the identity of 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 code 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 code 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 code and for other claim steps the Office Action uses the GRC as the

recited dynamic code. 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 code 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 code requested during authentication of the individual is then calculated and sent to the user. The same dynamic code is then received as part of an authentication request and the user identity is validated based on the same dynamic code.

The temporary transaction number of *Franklin et al.* cannot be used to verify the identity of the user 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 calculated 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 calculated 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 code" 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 claims 42, 47, 53, 58 and 63 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 entity and the trusted authenticator 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 these claims ultimately depend from independent claims 41, 46, 51, 57 and 62 respectively, which have been shown to be patentable over the combination of *Franklin et al.* and *Fox et al.*, claims 42, 47, 53, 58 and 63 remain 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 claims 42, 47, 53, 58 and 63.

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.: 11/333,400

FILING DATE: January 18, 2006

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: DIRECT AUTHENTICATION SYSTEM AND METHOD VIA TRUSTED AUTHENTICATORS

ATTORNEY DOCKET: KAMR001US0

CONFIRMATION NO.: 4456

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 5, 2011 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 11/333,400 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. 11/333,400, 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 code disclosed in U.S. Patent Application No. 11/333,400 and one of skill in the art upon reading both *Franklin et al.* and U.S. Patent Application No. 11/333,400 would NOT consider the dynamic code 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 code (*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. 11/333,400 which dynamic code is calculated during authentication of the individual by the entity, which dynamic code is included in an authentication request and which dynamic code is used to verify the identity of 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 code of U.S. Patent Application No. 11/333,400 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 code.

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 code 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 code because GRC is public information and OTS is not a secret number from the time the user receives GRC from a financial institutions.

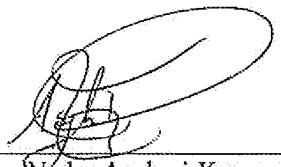
21. Also the statement "the GRC corresponds to the recited dynamic code" is inaccurate. In *Fox et al.* a financial institution verifies the identity of the user by verifying user's digital signature using user's public key. If a user does not digitally sign the GRC or any other document, the financial 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 digital signature and public key protocol to verify a user. In *Kamrani*, a dynamic code 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.: 11/333,400

FILING DATE: January 18, 2006

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: DIRECT AUTHENTICATION SYSTEM AND METHOD VIA TRUSTED AUTHENTICATORS

ATTORNEY DOCKET: KAMR001US0

CONFIRMATION NO.: 4456

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 5, 2011 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 11/333,400 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. 11/333,400, 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 code disclosed in U.S. Patent Application No. 11/333,400 and one of skill in the art upon reading both *Franklin et al.* and U.S. Patent Application No. 11/333,400 would NOT consider the dynamic code 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 code (*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. 11/333,400 which dynamic code is calculated during authentication of the individual by the entity, which dynamic code is included in an authentication request and which dynamic code is used to verify the identity of 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 code of U.S. Patent Application No. 11/333,400 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 code.

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 code 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 code 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 digital signature and public key protocol to verify a user. In *Kamrani*, a dynamic code 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.: 11/333,400

FILING DATE: January 18, 2006

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: DIRECT AUTHENTICATION SYSTEM AND METHOD VIA TRUSTED AUTHENTICATORS

ATTORNEY DOCKET: KAMR001US0

CONFIRMATION NO.: 4456

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 5, 2011 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 11/333,400 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. 11/333/,400 ("*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 code disclosed in U.S. Patent Application No. 11/333,400 and one of skill in the art upon reading both *Franklin et al.* and U.S. Patent Application No. 11/333,400 would NOT consider the dynamic code 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 code (*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. 11/333,400 which dynamic code is calculated during authentication of the individual by the entity, which dynamic code is included in an authentication request and which dynamic code is used to verify the identity of 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 code of U.S. Patent Application No. 11/333,400 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 code.

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 code 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 code 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 digital signature and public key protocol to verify a user. In *Kamrani*, a dynamic code 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.: 11/333,400

FILING DATE: January 18, 2006

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: DIRECT AUTHENTICATION SYSTEM AND METHOD VIA TRUSTED AUTHENTICATORS

ATTORNEY DOCKET: KAMR001US0

CONFIRMATION NO.: 4456

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 5, 2011 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 11/333,400 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. 11/333/,400 ("*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 code disclosed in U.S. Patent Application No. 11/333,400 and one of skill in the art upon reading both *Franklin et al.* and U.S. Patent Application No. 11/333,400 would NOT consider the dynamic code 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 code (*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. 11/333,400 which dynamic code is calculated during authentication of the individual by the entity, which dynamic code is included in an authentication request and which dynamic code is used to verify the identity of 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 code of U.S. Patent Application No. 11/333,400 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 code.

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 code 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 code 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 digital signature and public key protocol to verify a user. In *Kamrani*, a dynamic code 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
James Hewitt

Nov. 12, 2011
Date

Electronic Patent Application Fee Transmittal

Application Number:	11333400
Filing Date:	18-Jan-2006
Title of Invention:	Direct authentication system and method via trusted authenticators
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Filer:	Michael P. Fortkort
Attorney Docket Number:	KAMR001US0

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	16	30	480
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 $0 paid	2251	1	75	75
Miscellaneous:				
			Total in USD ($)	**555**

Electronic Acknowledgement Receipt	
EFS ID:	11429041
Application Number:	11333400
International Application Number:	
Confirmation Number:	4456
Title of Invention:	Direct authentication system and method via trusted authenticators
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Customer Number:	58293
Filer:	Michael P. Fortkort
Filer Authorized By:	
Attorney Docket Number:	KAMR001US0
Receipt Date:	17-NOV-2011
Filing Date:	18-JAN-2006
Time Stamp:	13:13:06
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$555
RAM confirmation Number	10729
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	11333400_Response_to_Office_Action_Mailed_080511_filed_111711.pdf	99537 56a901934c715b0dc046778573a19fa21566bfad	no	25
Warnings:					
Information:					
2	Rule 130, 131 or 132 Affidavits	Affidavit_Nader_Kamrani_11333400_filed_111711.pdf	1685313 317c81db310fd17cd374391e1305608efc2ee17e	no	7
Warnings:					
Information:					
3	Rule 130, 131 or 132 Affidavits	Affidavit_Kamran_Kamrani_11333400_filed_111711.pdf	1681964 c9e61eb928b109cbcb32ac036a3202f7f06f8f23	no	7
Warnings:					
Information:					
4	Rule 130, 131 or 132 Affidavits	Affidavit_Hosseinzadeh_11333400_filed_111711.pdf	222557 244eb5fe824b27a01da5b483fd83cf0687dfe4b5	no	7
Warnings:					
Information:					
5	Rule 130, 131 or 132 Affidavits	Affidavit_Hewitt_11333400_filed_111711.pdf	4871078 d2409c241664e9ac5bc0e41101ae9f276c908e89	no	7
Warnings:					
Information:					
6	Fee Worksheet (SB06)	fee-info.pdf	31808 84974e1b33a4088db07cd69e438a6c806281441f	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	8592257		

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.: 11/333,400

FILING DATE: January 18, 2006

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: DIRECT AUTHENTICATION SYSTEM AND METHOD VIA TRUSTED AUTHENTICATORS

ATTORNEY DOCKET: KAMR001US0

CONFIRMATION NO.: 4456

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

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:	11431388
Application Number:	11333400
International Application Number:	
Confirmation Number:	4456
Title of Invention:	Direct authentication system and method via trusted authenticators
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Customer Number:	58293
Filer:	Michael P. Fortkort
Filer Authorized By:	
Attorney Docket Number:	KAMR001US0
Receipt Date:	17-NOV-2011
Filing Date:	18-JAN-2006
Time Stamp:	15:22:11
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Applicant summary of interview with examiner	Interview_Summary_11333400_111711.pdf	20521 74ebad3f5a98afad7aad1a834e503ad67fb5efee	no	2
Warnings:					
Information:					

Total Files Size (in bytes):	20521

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 11/333,400	Filing Date 01/18/2006	☐ 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

AMENDMENT	11/17/2011	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 53	Minus	** 44	= 9	X $30 =	270	OR	X $ =	
	Independent (37 CFR 1.16(h))	* 9	Minus	***9	= 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	270	OR	TOTAL ADD'L FEE	

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)	OR	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:
/CHERYL CLARK/

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.
11/333,400	01/18/2006	Nader Asghari-Kamrani	KAMR001US0	4456

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.	Applicant(s)	
	11/333,400	ASGHARI-KAMRANI ET AL.	
	Examiner	Art Unit	
	ABDULHAKIM NOBAHAR	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: *21*.

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.: 11/333,400 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 _____

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

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:	11227172
Application Number:	11333400
International Application Number:	
Confirmation Number:	4456
Title of Invention:	Direct authentication system and method via trusted authenticators
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Customer Number:	58293
Filer:	Michael P. Fortkort
Filer Authorized By:	
Attorney Docket Number:	KAMR001US0
Receipt Date:	20-OCT-2011
Filing Date:	18-JAN-2006
Time Stamp:	12:21:36
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_11333400.pdf	421585 e0e428df6afec001aab0b8918d2e3231914eff7b	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 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.
11/333,400	01/18/2006	Nader Asghari-Kamrani	KAMR001US0	4456

58293 7590 08/05/2011

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
08/05/2011	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.	Applicant(s)	
	11/333,400	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 --

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 *14 April 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) *21-31,34-38,41-58 and 62-64* 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) *21-31,34-38,41-58 and 62-64* 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

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.

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. See *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) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

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).

The pending **Claims 21-23, 26, 27, 30, 31, 34, 38, 41-44, 46-49, 51-54, 56-58 and 62-64** are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over the copending **claims 1, 12, 14, 21, 33, 34, 36, 37, 40, 41, 43, 44, 51, 53-55, 58, 60-66, 69, 70, 73, 74 and 80** of copending Application No. 12/210,926.

Although the conflicting claims are not identical, they are not patentably distinct from each other. The pending claims claim substantially the same invention that the

copending claim do, but the corresponding limitations in the pending claims lack some features. For example, the independent copending claims 1 and 21 includes a feature as Central-Entity which is not included in the independent claims 21, 26, 34, 41, 46 and 51 of the instant application. Thus, the pending claims are broader than the copending claims.

Therefore, the instant claims 21, 22, 26, 27, 30, 31, 34, 38, 41-44, 46-49, 51-54, 56-58 and 62-64 are anticipated by claims 1, 12, 14, 21, 33, 34, 36, 37, 40, 41, 43, 44, 51, 53-55, 58, 60-66, 69, 70, 73, 74 and 80 of the copending Application No. 12/210,926.

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.

The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 21-31, 34-38, 41, 43-46, 48-52, 54-57, 62 and 64 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 21, 26, 34, 41, 46 and 51, Franklin discloses:

(Claim 21 as representative) A computer implemented method to authenticate an individual in communication with an entity over a communication network during communication between the entity and the individual (see, e.g., abstract and Fig. 1), the computer implemented method comprising:

receiving electronically a request for a dynamic code for the individual, which request is received during authentication of the individual by the 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 code);

calculating the dynamic code for the individual in response to the request during authentication of the individual by the entity (see, e.g., col. 8, lines 57-67);

sending by a computer the dynamic code over a communication network to the individual during authentication of the individual by the entity (see, e.g., col. 10, line 6-10);

Franklin, however, does not expressly disclose:

receiving electronically an authentication request to authenticate the individual based on a user information and the dynamic code included in the authentication request; and

verifying an identity of the individual based on the user information and the dynamic code included in the authentication request.

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]).

Franklin discloses:

(Claims 22, 31 and 38) The computer implemented method of claim 21, 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 the first trusted-authenticator (see, e.g., Fig. 5 and col. 10, lines 61-67).

(Claim 23) The computer implemented method of claim 21, wherein the request for the dynamic code is received by a computer associated with a first trusted-authenticator (see, e.g., Fig. 3, computer 32) and the authentication request is received by a computer associated with a second trusted-authenticator that is different than the first trusted-authenticator (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).

(Claims 24, 28 and 36) The computer implemented method of claim 21, wherein the dynamic code includes a non-predictable and time-dependent SecureCode (see, e.g., col. 2, lines 12-20, where “a short expiration term" means that the transaction code is time-dependent).

(Claims 25, 29 and 37) The computer implemented method of claim 21, wherein at least the dynamic code is encrypted (see, e.g., col. 6, line 66+, where the cryptographic module for secure communication between the customer and issuing bank indicates that the transaction code is encrypted when it is transmitted).

Regarding claims 27 and 35, Franklin does not expressly disclose:

The computer implemented method of claim 26, wherein the user information and dynamic code comprise credentials for verifying the individual's identity.

Fox, however discloses:

The computer implemented method of claim 26, wherein the user information and dynamic code comprise credentials for verifying the individual's identity (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]).

Franklin discloses:

(Claim 30) The computer implemented method of claim 26, wherein the entity corresponds to a business, organization, or another individual (see, e.g., Column 3, lines 39-41).

Franklin discloses:

(Claims 43 and 48) The computer implemented method according to claim 41, wherein the entity and the trusted-authenticator are different (see, e.g., Fig. 3, where tha merchant is the entity and the bank is the trusted authenticator).

Franklin discloses:

(Claims 44, 49 and 54) The computer implemented method according to claim 41, wherein said dynamic code is calculated by a computer after receiving the request from the individual for the dynamic code (see, e.g., col. 8, lines 57-67).

(Claims 45, 50 and 55) The computer implemented method according to claim 41, wherein said dynamic code comprises a different value each time the dynamic code is requested by the individual (see, e.g., col. 4, lines 50-55, random temporary transaction number).

(Claim 52) The computer implemented method according to claim 51, further comprising:

sending electronically a confirmation or denial authentication message by a computer to the entity during authentication of the individual by the entity (see, e.g., col. 11, lines 14-30).

Regarding claims 56, 57 and 62, these claims are rejected as applied to the like elements of claims 21, 26, 27, 34, 35, 41, 45, 46, 50, 51 and 55.

Regarding claim 64, Franklin discloses:

The computer implemented method according to claim 62, wherein said dynamic code is valid for a predefined time and may be used by the individual before becoming invalid (see, e.g., col. 9, lines 43-47).

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.

The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 42, 47, 58, 53 and 63 are rejected under 35 U.S.C. 103(a) as being unpatentable over Franklin in view of FOX as applied to claims 21-31, 34-38, 41, 43-46, 48-52, 54-57, 62 and 64 above and further in view of the examiner Official Notice.

Regarding claims 42, 47, 58, 53 and 63, Franklin-Fox does not expressly disclose:

wherein the entity and the trusted authenticator are the same.

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 of 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 or customers are authenticated directly by the respective institution. In this case the entity and the trusted authenticator 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 institution to be as the same trusted authenticator and entity. The deployment of one institution to issue a dynamic code to and authenticate the user when using the dynamic code 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. 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

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

Notice of References Cited	Application/Control No. 11/333,400	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-6,067,621 A	05-2000	Yu et al.	713/172
*	D	US-5,732,137 A	03-1998	Aziz, Ashar	713/155
*	E	US-6,715,082 B1	03-2004	Chang et al.	726/8
*	F	US-5,535,276 A	07-1996	Ganesan, Ravi	713/155
	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.	Applicant(s)/Patent Under Reexamination
	11333400	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	09/02/2008	03/01/2009	06/15/2009	12/01/2009	06/20/2010	09/16/2010	01/11/2011	07/26/2011	
	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
	11333400	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	09/02/2008	03/01/2009	06/15/2009	12/01/2009	06/20/2010	09/16/2010	01/11/2011	07/26/2011	
	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						✓	✓	✓	

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11333400	ASGHARI-KAMRANI ET AL.
	Examiner	Art Unit
	ABDULHAKIM NOBAHAR	2432

SEARCHED			
Class	Subclass	Date	Examiner
713	182-186	6/17/2009	AN
726	2,5,8,18,27,28	6/17/2009	AN
705	64,67,72,76,78	6/17/2009	AN
	See attached report		
713	184 (see attached report)	6/24/2010	AN
	Search updated (see attached report)	7/26/2011	AN

SEARCH NOTES		
Search Notes	Date	Examiner

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

/A. N./ Examiner.Art Unit 2132	

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S38	14	("20020188481" "6529885" "5757917" "5557516" "5826241" "5883810" "5890137").pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/26 09:12
S40	0	S38 and fob	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/07/26 09:13
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

7/26/2011 10:28:41 PM
H:\EAST\Workspaces\11333400.wsp

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
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

7/28/2011 11:42:45 AM
H:\EAST\Workspaces\11333400.wsp

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.: 11/333,400

FILING DATE: January 18, 2006

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: DIRECT AUTHENTICATION SYSTEM AND METHOD VIA TRUSTED AUTHENTICATORS

ATTORNEY DOCKET: KAMR001US0

CONFIRMATION NO.: 4456

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

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:	10459398
Application Number:	11333400
International Application Number:	
Confirmation Number:	4456
Title of Invention:	Direct authentication system and method via trusted authenticators
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Customer Number:	58293
Filer:	Michael P. Fortkort
Filer Authorized By:	
Attorney Docket Number:	KAMR001US0
Receipt Date:	06-JUL-2011
Filing Date:	18-JAN-2006
Time Stamp:	13:16:36
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_11333400_070611.pdf	17703 229135d6ab1b8c3ff4b543f34d2c099781a20979	no	2

Warnings:	
Information:	

Total Files Size (in bytes):	17703

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.
11/333,400	01/18/2006	Nader Asghari-Kamrani	KAMR001US0	4456

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.	Applicant(s)	
	11/333,400	ASGHARI-KAMRANI ET AL.	
	Examiner	Art Unit	
	ABDULHAKIM NOBAHAR	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: *24 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: *21*.

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 instant claims and their allowability over the prior art of record especially authenticating a user based on a dynamic code associated with the user. Examiner stated that a new search must be conducted at this stage to see if 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.: 11/333,400 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

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.

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.
11/333,400	01/18/2006	Nader Asghari-Kamrani	KAMR001US0	4456

58293 7590 05/20/2011

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
05/20/2011	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.	Applicant(s)/Patent under Reexamination	
	11/333,400	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, AU 2432*.

(4) *Benjamin Lanier, Primary Examiner, AU 2432*.

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

Doc Code: AP.PRE.REQ

PTO/SB/33 (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.

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional): KAMR001US0

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	Filed
11/333,400	JANUARY 18, 2006

First Named Inventor: NADER ASGHARI-KAMRANI

Art Unit	Examiner
2432	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.

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.: 11/333,400
FILING DATE: January 18, 2006
EXAMINER: Mr. Abdulhakim Nobahar
ART UNIT: 2432
TITLE: DIRECT AUTHENTICATION SYSTEM AND METHOD VIA TRUSTED AUTHENTICATORS
ATTORNEY DOCKET: KAMR001US0

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 dynamic code; and (2) authentication based on a dynamic code. The Office Action includes at least three major points of legal error and flawed logic in its rejection, as is detailed below.

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, ¶5; Aff. Hewitt, ¶5; Aff. N.Kamrani, ¶6; Aff. K.Kamrani, ¶5; Aff. Shahbazi, ¶5; and Aff. Laing, ¶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). 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 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,¶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 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. Failing to weigh the evidence on this point constitutes reversible error.

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 verifies the identity and authenticity of the customer." (emphasis by Examiner) in an attempt to establish that this reference teaches a request for authentication that includes a dynamic code 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 dynamic code! 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 dynamic code, 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. *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.* 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).

Federal Circuit case law 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) (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 dynamic code and no teaching of authentication based on a dynamic code 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.* 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)
MICHAEL P FORTKORT PC
The International Law Center
13164 Lazy Glen Lane
Oak Hill, Virginia 20171
703-435-9390 (please direct all telephone calls to this number)
703-435-8857 (facsimile)

Electronic Patent Application Fee Transmittal

Application Number:	11333400
Filing Date:	18-Jan-2006
Title of Invention:	Direct authentication system and method via trusted authenticators
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Filer:	Michael P. Fortkort
Attorney Docket Number:	KAMR001US0

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:	9881177
Application Number:	11333400
International Application Number:	
Confirmation Number:	4456
Title of Invention:	Direct authentication system and method via trusted authenticators
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Customer Number:	58293
Filer:	Michael P. Fortkort
Filer Authorized By:	
Attorney Docket Number:	KAMR001US0
Receipt Date:	14-APR-2011
Filing Date:	18-JAN-2006
Time Stamp:	15:03:25
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	1349
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	Notice_of_Appeal_041411.pdf	246418 be942ee8e1eb6c0346b573a7446ecf1f176da707	no	2
Warnings:					
Information:					
2	Pre-Brief Conference request	Pre-Appeal_Request_041411.pdf	233612 066c0b396880677340b2e5700be933a8836c1bdf	no	2
Warnings:					
Information:					
3	Pre-Brief Conference request	11333400_Brief_in_Support_of_Pre-Appeal_Request_041411.pdf	48364 92172e004968140efdb58096f4337200defed324	no	5
Warnings:					
Information:					
4	Fee Worksheet (PTO-875)	fee-info.pdf	29840 2b2137970d74a0b208f2be8e6b793f1a71579c73	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	558234		

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/31 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

NOTICE OF APPEAL FROM THE EXAMINER TO THE BOARD OF PATENT APPEALS AND INTERFERENCES

Docket Number (Optional): KAMR001US0

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	Filed
11/333,400	JANUARY 18, 2006

For: DIRECT AUTHENTICATION SYSTEM...

Art Unit	Examiner
2432	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.

Certification Under 37 C.F.R. § 1.8

I hereby certify that on March 21, 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 21, 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.: 11/333,400

FILING DATE: January 18, 2006

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: DIRECT AUTHENTICATION SYSTEM AND METHOD VIA TRUSTED AUTHENTICATORS

ATTORNEY DOCKET: KAMR001US0

CONFIRMATION NO.: 4456

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 14, 2011 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 11/333,400 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 21, 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 21, 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.: 11/333,400

FILING DATE: January 18, 2006

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: DIRECT AUTHENTICATION SYSTEM AND METHOD VIA TRUSTED AUTHENTICATORS

ATTORNEY DOCKET: KAMR001US0

CONFIRMATION NO.: 4456

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 14, 2011 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 11/333,400 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 21, 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 21, 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.: 11/333,400

FILING DATE: January 18, 2006

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: DIRECT AUTHENTICATION SYSTEM AND METHOD VIA TRUSTED AUTHENTICATORS

ATTORNEY DOCKET: KAMR001US0

CONFIRMATION NO.: 4456

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 14, 2011 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 11/333,400 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 21, 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 21, 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.: 11/333,400

FILING DATE: January 18, 2006

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: DIRECT AUTHENTICATION SYSTEM AND METHOD VIA TRUSTED AUTHENTICATORS

ATTORNEY DOCKET: KAMR001US0

CONFIRMATION NO.: 4456

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 14, 2011 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 11/333,400 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 21, 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 21, 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.: 11/333,400

FILING DATE: January 18, 2006

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: DIRECT AUTHENTICATION SYSTEM AND METHOD VIA TRUSTED AUTHENTICATORS

ATTORNEY DOCKET: KAMR001US0

CONFIRMATION NO.: 4456

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 14, 2011 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 11/333,400 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 21, 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 21, 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.: 11/333,400

FILING DATE: January 18, 2006

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

ATTORNEY DOCKET: KAMR001US0

CONFIRMATION NO.: 4456

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 14, 2011 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 11/333,400, 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

MJ

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.
11/333,400	01/18/2006	Nader Asghari-Kamrani	KAMR001US0	4456

58293 7590 04/06/2011

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
04/06/2011	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.** 11/333,400	**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 21 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: *21-31,34-38,41-58 and 62-64*.
   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 21 March 2011 are not pursuasive. 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 21, 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 21, 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.: 11/333,400

FILING DATE: January 18, 2006

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: DIRECT AUTHENTICATION SYSTEM AND METHOD VIA TRUSTED AUTHENTICATORS

ATTORNEY DOCKET: KAMR001US0

CONFIRMATION NO.: 4456

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 14, 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./ 03/30/2011

Certification Under 37 C.F.R. § 1.8

I hereby certify that on March 21, 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 21, 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.: 11/333,400

FILING DATE: January 18, 2006

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: DIRECT AUTHENTICATION SYSTEM AND METHOD VIA TRUSTED AUTHENTICATORS

ATTORNEY DOCKET: KAMR001US0

CONFIRMATION NO.: 4456

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 14, 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:

1-20. (Cancelled)

21. (Previously Presented) A computer implemented method to authenticate an individual in communication with an entity over a communication network during communication between the entity and the individual, the computer implemented method comprising:

receiving electronically a request for a dynamic code for the individual, which request is received during authentication of the individual by the entity;

calculating the dynamic code for the individual in response to the request during authentication of the individual by the entity;

sending electronically the dynamic code to the individual during authentication of the individual by the entity;

receiving electronically an authentication request to authenticate the individual based on a user information and the dynamic code included in the authentication request; and

verifying an identity of the individual based on the user information and the dynamic code included in the authentication request.

22. (Previously Presented) The computer implemented method of claim 21, 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 the first trusted-authenticator.

23. (Previously Presented) The computer implemented method of claim 21, 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.

24. (Previously Presented) The computer implemented method of claim 21, wherein the dynamic code includes a non-predictable and time-dependent SecureCode.

25. (Previously Presented) The computer implemented method of claim 21, wherein at least the dynamic code is encrypted.

26. (Previously Presented) A computer implemented method for an entity to authenticate an individual over a communication network during communication with the individual, the method comprising:

requesting electronically both a user information and a dynamic code from the individual in order to validate the individual's identity during communication with the individual, which individual obtains the dynamic code from a computer associated with a trusted-authenticator during the communication between the individual and the entity;

receiving electronically both the user information and the dynamic code from the individual; and

creating an authentication request message including both the user information and the received dynamic code and providing the authentication request message to a trusted-

authenticator, the trusted-authenticator authenticating the individual based on a combination of the user information and the received dynamic code.

27. (Previously Presented) The computer implemented method of claim 26, wherein the user information and the dynamic code comprise credentials for verifying the individual's identity.

28. (Previously Presented) The computer implemented method of claim 26, wherein the dynamic code includes a non-predictable and time-dependent SecureCode.

29. (Previously Presented) The computer implemented method of claim 26, wherein at least the dynamic code is encrypted.

30. (Previously Presented) The computer implemented method of claim 26, wherein the entity corresponds to a business, organization, or another individual.

31. (Previously Presented) The computer implemented method of claim 26, wherein a computer associated with a first trusted-authenticator calculates the dynamic code and provides the dynamic code to the individual during communication between the individual and the entity.

32. (Cancelled)

33. (Cancelled)

34. (Previously Presented) A computer implemented method for a website to authenticate an individual over a communication network during a communication session between the individual and the website, the computer implemented method comprising:

requesting by a computer associated with the website both a user information and a dynamic code from the individual in order to validate the individual's identity;

receiving both the user information and the dynamic code from the individual, which individual receives the dynamic code during the communication session between the individual and the website; and

creating an authentication request message including the user information and the dynamic code and providing the authentication request message to a first computer associated with a trusted-authenticator, the trusted authenticator authenticating the individual based on the user information and the dynamic code.

35. (Previously Presented) The computer implemented method of claim 34, wherein the user information and the dynamic code comprise credentials for verifying the individual's identity.

36. (Previously Presented) The computer implemented method of claim 34, wherein the dynamic code includes a non-predictable and time-dependent SecureCode.

37. (Previously Presented) The computer implemented method of claim 34, wherein at least the dynamic code is encrypted.

38. (Previously Presented) The computer implemented method of claim 34, wherein a second computer associated with the trusted-authenticator calculates the dynamic code and provides the dynamic code to the individual during the communication session between the individual and the website.

39. (Cancelled)

40. (Cancelled)

41. (Previously Presented) A computer implemented method for authenticating an individual in communication with an entity over a communication network during communication between the entity and the individual, the method comprising:

receiving by a computer associated with the entity a dynamic code during authentication of the individual by the entity, which said dynamic code was sent to the individual by a trusted-authenticator in response to a request for the dynamic code from the trusted-authenticator during authentication of the individual by the entity and was calculated by the trusted-authenticator during authentication of the individual by the entity;

sending electronically by the entity an authentication request to a trusted-authenticator to authenticate the individual based on a user information and a received dynamic code included in the authentication request, wherein said authentication request is sent during authentication of the individual by the entity; and

receiving electronically by the entity a message from the trusted-authenticator either

confirming or denying an identity of the individual based on the user information and the received dynamic code included in the authentication request from the entity during the time of authentication of the individual by the entity.

42. (Previously Presented) The computer implemented method according to claim 41, wherein the entity and the trusted-authenticator are the same.

43. (Previously Presented) The computer implemented method according to claim 41, wherein the entity and the trusted-authenticator are different.

44. (Previously Presented) The computer implemented method according to claim 41, wherein said dynamic code is calculated after receiving the request from the individual for the dynamic code.

45. (Previously Presented) The computer implemented method according to claim 41, wherein said dynamic code comprises a different value each time the dynamic code is requested by the individual.

46. (Previously Presented) A computer implemented method for authenticating an individual in communication with an entity during communication between the entity and the individual, the computer implemented method comprising:

sending electronically a request for a dynamic code to a trusted-authenticator during authentication of the individual by the entity;

receiving electronically the dynamic code from the trusted-authenticator during authentication of the individual by the entity, which dynamic code was calculated by a computer associated with the trusted-authenticator during authentication of the individual by the entity;

sending electronically the dynamic code and user information during authentication of the individual by the entity to the trusted-authenticator for verification by the trusted-authenticator during authentication of the individual by the entity; and

receiving electronically acceptance or denial of authentication from the entity based on verification by the trusted-authenticator of the user information and dynamic code received from the individual during authentication of the individual by the entity.

47. (Previously Presented) The computer implemented method according to claim 46, wherein the entity and the trusted-authenticator are the same.

48. (Previously Presented) The computer implemented method according to claim 46, wherein the entity and the trusted-authenticator are different.

49. (Previously Presented) The computer implemented method according to claim 46, wherein said dynamic code is calculated after receiving the request from the individual for the dynamic code.

50. (Previously Presented) The computer implemented method according to claim 46, wherein said dynamic code comprises a different value each time the dynamic code is requested for an individual.

51. (Previously Presented) A computer implemented method to authenticate an individual during communication between the individual and another entity, the method comprising:

receiving electronically a request for a dynamic code, wherein the request is received during authentication of the individual by the entity;

sending the dynamic code electronically to the individual during authentication of the individual by the entity;

receiving electronically an authentication request from the entity to authenticate the individual based on a user information and dynamic code received from the individual during authentication of the individual by the entity, wherein said authentication request is received during authentication of the individual by the entity; and

verifying by a computer an identity of the individual based on the user information and the received dynamic code in response to the authentication request from the entity during the time of authentication of the individual by the entity.

52. (Previously Presented) The computer implemented method according to claim 51, further comprising:

sending electronically a confirmation or denial authentication message to the entity during authentication of the individual by the entity.

53. (Previously Presented) The computer implemented method according to claim 51, wherein the entity comprises a trusted-authenticator.

54. (Previously Presented) The computer implemented method according to claim 51, wherein said dynamic code is calculated after receiving the request for the dynamic code.

55. (Previously Presented) The computer implemented method according to claim 51, wherein said dynamic code comprises a different value each time the dynamic code is requested for the individual.

56. (Previously Presented) A computer implemented method to perform a two-factor authentication of an individual based on a user information as a first credential and a dynamic code as a second credential during communication over a network between an entity and the individual, the method comprising receiving electronically acceptance or denial of two-factor authentication from the entity based on two credentials received from the individual, wherein:

said user information comprises the first credential and said dynamic code comprises the second credential;

said dynamic code was calculated by a computer and received from a trusted-authenticator during said communication between the entity and the individual;

said user information and said dynamic code were electronically received and verified by the trusted-authenticator during authentication of the individual by the entity; and

said dynamic code comprises a different value each time the individual receives a dynamic code from a trusted-authenticator.

57. (Previously Presented) A computer implemented method to perform a two-factor

authentication of an individual based on a user information as a first credential and a dynamic code as a second credential during communication between the entity and the individual, the method comprising accepting or denying electronically of a two-factor authentication of the individual based on two credentials received from the individual, wherein:

said user information comprises the first credential and said dynamic code comprises the second credential;

said dynamic code was calculated by a first computer associated with a trusted-authenticator and sent by a second computer associated with the trusted-authenticator to the individual during communication between the individual and the entity;

said user information and said dynamic code were received electronically during authentication of the individual by the entity and were verified by the trusted-authenticator during said communication between the individual and the entity; and

said first computer associated with said trusted-authenticator calculates a different value for said dynamic code each time the individual requests a dynamic code from the trusted-authenticator.

58. (Previously Presented) The computer implemented method according to claim 57, wherein the first computer and the second computer are the same.

59. (Cancelled).

60. (Cancelled).

61. (Cancelled).

62. (Previously Presented) A computer implemented method to perform a two-factor authentication of an individual based on a user information as a first credential and a dynamic code as a second credential during communication between the entity and the individual, the method comprising accepting or denying electronically of the two-factor authentication of the individual based on two credentials received from the individual, wherein:

said user information comprises the first credential and said dynamic code comprises the second credential;

said dynamic code was calculated by a trusted-authenticator and sent to the individual for authentication between the individual and the entity;

said user information and said dynamic code were received electronically during authentication of the individual by the entity and user information was verified by a first computer and dynamic code was verified by a second computer associated with the trusted-authenticator during said communication between the individual and the entity; and

said dynamic code comprises a different value each time the individual receives a dynamic code from a trusted-authenticator.

63. (Previously Presented) The computer implemented method according to claim 62, wherein the first computer and the second computer are the same.

64. (Previously Presented) The computer implemented method according to claim 62, wherein said dynamic code is valid for a predefined time and may be used by the individual

before becoming invalid.

REMARKS

Claims 21-31, 34-38, 41-58 and 62-64 were previously pending. Claims 1-20, 32-33, 39-40, 59-61 have been previously cancelled without disclaimer of or prejudice to the subject matter contained therein. Claims 21-31, 34-38, 41-58 and 62-64 remain pending.

DOUBLE PATENTING

The Office Action provisionally rejected claims 21-23, 26, 27, 30, 31, 34, 38, 41-44, 46-49, 51-54, 56-58 and 62-64 under the judicially created doctrine of obviousness-type double patenting as being unpatentable over copending claims 1, 12, 14, 21, 33, 34, 36, 37, 40, 41, 43, 44, 51, 53-55, 58, 60-66, 69, 70, 73, 74, and 80 of copending application No. 12/210,926. Upon allowance of these claims in either application, the Applicants will timely file a terminal disclaimer, which will obviate this rejection.

CLAIMS REMAIN PATENTABLE OVER *FRANKLIN ET AL.*

The Office Action rejected claims 21-31, 34-38, 41, 43-46, 48-52, 54-57, 62 and 64 under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,883,810 A to *Franklin et al.* [hereinafter "*Franklin et al.*"]. 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 dynamic code; and (2) authentication

based on a dynamic code. 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 three 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.

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 verifies the identity and authenticity of the customer." (emphasis supplied by the Examiner) in an attempt to establish that this reference teaches a request for authentication that includes a dynamic as recited in the claims. However, this request in *Franklin et al.* does not contain the temporary transaction number, which the Examiner had equated to the recited dynamic code! 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 dynamic code. This authentication request of *Franklin et al.* does not teach the claimed

authentication request that includes a dynamic code 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 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 dynamic code and no teaching of authentication based on a dynamic code 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.*

The present invention is directed to the problem of reducing fraud in non face-to-face transactions, such as online transactions, by forming a circle of trust between the trusted-authenticator, the business and the user. *Aff. N.Kamrani, ¶18.* The dynamic code and the process of handling the dynamic code are used to build this trusted relationship. *Id.* After the trusted authenticator receives the user's dynamic code, the trusted authenticator validates the dynamic code and authenticates the user based on the valid dynamic code and informs the business that the user is authentic. *Id.* No such authentication of the user based on validation of the dynamic code occurs in *Franklin et al.*

One of skill in the art of authentication and credit card authorization would understand that *Franklin et al.* does not form a circle of trust between the issuing bank, a merchant and a user. *Id. at ¶19.* The transaction number of *Franklin et al.* and the process of handling the transaction number cannot form a trusted relationship. *Id.* The trusted relationship between the user and the issuing bank of *Franklin et al.* is formed using the user's digital certificate; however, no trusted relationship exists between the user and the merchant in the entire transaction of *Franklin et al. Id.* For the merchant of *Franklin et al.* there is no difference between a user giving an actual credit card number and a user giving a temporary transaction number. *Id.* For the merchant of *Franklin et al.*, processing a temporary transaction number is the same as processing an actual credit card number. *Id.* The issuing bank of *Franklin et al.* also processes a temporary transaction number the same as processing an actual credit card number. *Id.* The issuing bank of

Franklin et al. also processes a temporary transaction number the same as processing an actual credit card number. *Id.* The issuing bank of *Franklin et al.* never authenticates the cardholder to merchant based on the transaction number and the merchant of *Franklin et al.* never receives any information from the issuing bank that the user is authentic. *Id.*

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.

ALL CLAIMS REMAIN PATENTABLE OVER *FRANKLIN ET AL.* AND CERTAIN OFFICIAL NOTICE

The Office Action rejected claims 42, 47, 53, 58 and 63 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 the entity and the trusted authenticator 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.* Even assuming *arguendo* that the Office Action's application of Official Notice in combination with *Franklin et al.* is proper, because these claims ultimately depend from independent claims 41, 46, 51, 57 and 62 respectively, which have been shown to be patentable over *Franklin et al.*, claims 42, 47, 53, 58 and 63 remain 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 claims 42, 47, 53, 58 and 63.

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 21, 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 21, 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 21, 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.: 11/333,400

FILING DATE: January 18, 2006

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: DIRECT AUTHENTICATION SYSTEM AND METHOD VIA TRUSTED AUTHENTICATORS

ATTORNEY DOCKET: KAMR001US0

CONFIRMATION NO.: 4456

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 14, 2011 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 11/333,400 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 et al.* 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.

13. 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

16. 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 driver's license.

17. 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 customer either has the money in their account for debit, or has not hit the 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.

18. To reduce fraud credit card issuing companies such as Visa and Master card 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.

19. 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.

20. 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,

Fred Laing, II

March 18, 2011
Date

Certification Under 37 C.F.R. § 1.8

I hereby certify that on March 21, 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 21, 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.: 11/333,400

FILING DATE: January 18, 2006

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: DIRECT AUTHENTICATION SYSTEM AND METHOD VIA TRUSTED AUTHENTICATORS

ATTORNEY DOCKET: KAMR001US0

CONFIRMATION NO.: 4456

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 14, 2011 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 11/333,400 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, 6457 Palisades Drive, Centreville, Virginia 20121 – one of the inventors in the present application.

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 time to studying, and devising solutions for these multifaceted problems; Knowledgeable in the Computer Architecture Software and Information Security area.

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 et al.* has not been developed for verification of a user's identity since the merchants treat the transaction number in 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.

13. In *Franklin et al.* the merchant cannot distinguish between a recently obtained temporary transaction number and a normal credit card number.

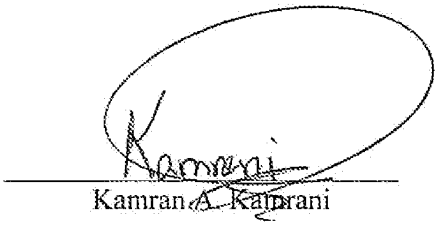
14. *Franklin et al.* does not provide any assurance to the merchant that the payer is authenticated. No assurance is provided because the merchant never receives any message from issuing bank that the user is authentic.

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 A. Kamrani

3/16/2011

Date

Certification Under 37 C.F.R. § 1.8

I hereby certify that on March 21, 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 21, 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.: 11/333,400

FILING DATE: January 18, 2006

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: DIRECT AUTHENTICATION SYSTEM AND METHOD VIA TRUSTED AUTHENTICATORS

ATTORNEY DOCKET: KAMR001US0

CONFIRMATION NO.: 4456

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 14, 2011 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 11/333,400 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. 11/333,400, 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 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 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 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.

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.

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.

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 et al.* has not been developed for verification of a user's identity since the merchants treat the transaction number in 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 dynamic code 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 dynamic code 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 et al.* 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 dynamic code nor authentication of the customer based on the dynamic code. 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.

18. The goal of our invention is to reduce fraud in a non face to face transaction by forming a **circle of trust** between the trusted-authenticator, the business and the user. The dynamic code and the process of handling the dynamic code are used to build this trusted relationship. After trusted authenticator receives the user's dynamic code, the trusted

authenticator validates the dynamic code and authenticates the user based on the valid dynamic code and informs the business that the user is authentic.

19 One of skill in the art of authentication and credit card authorization would understand that *Franklin et al.* does not form a circle of trust between issuing bank, merchant and the user. The transaction number of *Franklin et al.* and the process of handling the transaction number could not create a trusted relationship. The trusted relationship between the user and issuing bank of *Franklin et al.* is formed using user's digital certificate; however no trusted relationships exist between the user and the merchant in the entire transaction process of *Franklin et al.* For the merchant of *Franklin et al.* there is no difference between a user giving an actual credit card number and a user giving a temporary transaction number. For the merchant of *Franklin et al.* processing a temporary transaction number is the same as processing an actual credit card number. The issuing bank of *Franklin et al* .also processes a temporary transaction number the same as processing an actual credit card number. The issuing bank of *Franklin et al.* never authenticates the cardholder based on transaction number and the merchant of *Franklin et al* .never receives any information from the issuing bank that the user is authentic.

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

03/21/2011
Date

Certification Under 37 C.F.R. § 1.8

I hereby certify that on March 21, 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 21, 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.: 11/333,400

FILING DATE: January 18, 2006

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: DIRECT AUTHENTICATION SYSTEM AND METHOD VIA TRUSTED AUTHENTICATORS

ATTORNEY DOCKET: KAMR001US0

CONFIRMATION NO.: 4456

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 14, 2011 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 11/333,400 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 1 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 et al.* has not been developed for verification of a user's identity since the merchants treat the transaction number in 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.

13. In *Franklin et al.* the merchant cannot distinguish between a recently obtained temporary transaction number and a normal credit card number.

14. *Franklin et al.* 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

James Hewitt

3-16-2011

Date

Certification Under 37 C.F.R. § 1.8

I hereby certify that on March 21, 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 21, 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.: 11/333,400

FILING DATE: January 18, 2006

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: DIRECT AUTHENTICATION SYSTEM AND METHOD VIA TRUSTED AUTHENTICATORS

ATTORNEY DOCKET: KAMR001US0

CONFIRMATION NO.: 4456

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 14, 2011 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 11/333,400 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 et al.* has not been developed for verification of a user's identity since the merchants treat the transaction number in 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.

13. In *Franklin et al.* the merchant cannot distinguish between a recently obtained temporary transaction number and a normal credit card number.

14. *Franklin et al.* 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,

Abolfazl Hosseinzadeh

3-16-11
Date

Certification Under 37 C.F.R. § 1.8

I hereby certify that on March 21, 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 21, 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.: 11/333,400

FILING DATE: January 18, 2006

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

ATTORNEY DOCKET: KAMR001US0

CONFIRMATION NO.: 4456

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 14, 2011 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 11/333,400, and pursuant to the provisions of 37 C.F.R. § 1.132. The witness hereby avers and testifies as follows:

MJ

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 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 credit card 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.

MS

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 credit card payment transaction.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 et al.* has not been developed for verification of a user's identity since the merchants treat the transaction number in 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.

13. In *Franklin et al.* the merchant cannot distinguish between a recently obtained temporary transaction number and a normal credit card number.

14. *Franklin et al.* 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.

MS

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,

Majid (Mike) Shahbazi

3/21/2011
Date

Electronic Acknowledgement Receipt

EFS ID:	9700705
Application Number:	11333400
International Application Number:	
Confirmation Number:	4456
Title of Invention:	Direct authentication system and method via trusted authenticators
First Named Inventor/Applicant Name:	Nader Asghari-Kamrani
Customer Number:	58293
Filer:	Michael P. Fortkort
Filer Authorized By:	
Attorney Docket Number:	KAMR001US0
Receipt Date:	21-MAR-2011
Filing Date:	18-JAN-2006
Time Stamp:	15:31:55
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	11333400_Response_to_Final_Office_Action_Mailed_011411_filed_032111.pdf	101617 7008791ce3f2895d972214eec0e058962b29304b	no	24
Warnings:					
Information:					

2	Rule 130, 131 or 132 Affidavits	11333400_132_Affidavit_Laing_032111.pdf	147730 957a21c4c1a0fac0efa598962b29d45c0e292772	no	6
Warnings:					
Information:					
3	Rule 130, 131 or 132 Affidavits	11333400_132_Affidavit_K_Kamrani_032111.pdf	1447669 ae95b09731631e241491f54c8703d10fdd661d7f	no	4
Warnings:					
Information:					
4	Rule 130, 131 or 132 Affidavits	11333400_132_Affidavit_N_Kamrani_032111.pdf	6528313 0b115a0702728d876596914cebc89a808ace6552	no	5
Warnings:					
Information:					
5	Rule 130, 131 or 132 Affidavits	11333400_132_Affidavit_Hewitt_032111.pdf	1458978 8a85f2c34e63a92a7eb5a9e7581586e4a8c0f286	no	4
Warnings:					
Information:					
6	Rule 130, 131 or 132 Affidavits	11333400_132_Affidavit_Hosseinzadeh_032111.pdf	97828 d8652855a2df0ab7329d9ac67a174c081d4ef460	no	4
Warnings:					
Information:					
7	Rule 130, 131 or 132 Affidavits	11333400_132_Affidavit_Shahbazi_032111.pdf	107665 8c014b3db2be1ff52ac05d002ed3bdaad02415c4	no	4
Warnings:					
Information:					
		Total Files Size (in bytes):	9889800		

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	Filing Date	☐ To be Mailed
11/333,400	01/18/2006	

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

AMENDMENT 03/21/2011

	(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 ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 37	Minus	** 44	= 0	X $26 =	0	OR	X $ =	
Independent (37 CFR 1.16(h))	* 9	Minus	***9	= 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	

AMENDMENT

	(Column 1)		(Column 2)	(Column 3)					
	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:
/EVELYN G. NIMMONS/

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.
11/333,400	01/18/2006	Nader Asghari-Kamrani	KAMR001US0	4456

58293 7590 01/14/2011

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
01/14/2011	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.	Applicant(s)	
	11/333,400	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 --

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) *21-31,34-38,41-58 and 62-64* 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) *21-31,34-38,41-58,62-64* 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 21-31, 34-38, 41-58 and 62-64 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 page 19 of the remark applicants argue that the Franklin's temporary transaction number is not a code and therefore cannot be a dynamic 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. The transaction number that is used for a single transaction or has a short finite life is the same as a dynamic code. Thus, the temporary transaction number of Franklin is equivalent to the dynamic code recited in the instant claims.

Applicants also on page 19 of the remark argue that in Franklin there is no request for authentication that includes a dynamic code and on page 20 applicants argue that Franklin does not verify the identity of the user at all but merely authorizes a transaction 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 taken for a single transaction and in a short duration. A temporary transaction number is issued to a user after the user is authentication 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:

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. See *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) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

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).

The pending **Claims 21-23, 26, 27, 30, 31, 34, 38, 41-44, 46-49, 51-54, 56-58 and 62-64** are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over the copending **claims 1, 12, 14, 21, 33, 34, 36, 37, 40, 41, 43, 44, 51, 53-55, 58, 60-66, 69, 70, 73, 74 and 80** of copending Application No. 12/210,926.

Although the conflicting claims are not identical, they are not patentably distinct from each other. The pending claims claim substantially the same invention that the copending claim do, but the corresponding limitations in the pending claims lack some features. For example, the independent copending claims 1 and 21 includes a feature as Central-Entity which is not included in the independent claims 21, 26, 34, 41, 46 and 51 of the instant application. Thus, the pending claims are broader than the copending claims.

Therefore, the instant claims 21, 22, 26, 27, 30, 31, 34, 38, 41-44, 46-49, 51-54, 56-58 and 62-64 are anticipated by claims 1, 12, 14, 21, 33, 34, 36, 37, 40, 41, 43, 44, 51, 53-55, 58, 60-66, 69, 70, 73, 74 and 80 of the copending Application No. 12/210,926.

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 21-31, 34-38, 41, 43-46, 48-52, 54-57, 62 and 64 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 21, 26, 34, 41, 46 and 51, Franklin discloses:

(Previously Presented) A computer implemented method to authenticate an individual in communication with an entity over a communication network during communication between the entity and the individual (see, e.g., abstract and Fig. 1), the computer implemented method comprising:

receiving electronically a request for a dynamic code for the individual, which request is received during authentication of the individual by the 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 code);

calculating the dynamic code for the individual in response to the request during authentication of the individual by the entity (see, e.g., col. 8, lines 57-67);

sending by a computer the dynamic code over a communication network to the individual during authentication of the individual by the entity (see, e.g., col. 10, line 6-10);

receiving electronically an authentication request to authenticate the individual based on a user information and the dynamic code included in the authentication

request (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 user information and the dynamic code); and

verifying an identity of the individual based on the user information and the dynamic code included in the authentication request (see, e.g., col. 10, lines 61-63 and col. 11, lines 31-40).

Franklin discloses:

22, 31 and 38. (Previously Presented) The computer implemented method of claim 21, 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 the first trusted-authenticator (see, e.g., Fig. 5 and col. 10, lines 61-67).

23. (Currently Amended) The computer implemented method of claim 21, wherein the request for the dynamic code is received by a computer associated with a first trusted-authenticator (see, e.g., Fig. 3, computer 32) and the authentication request is received by a computer associated with a second trusted-authenticator that is different than the first trusted-authenticator (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).