24, 28 and 36. (Previously Presented) 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).

25, 29 and 37. (Previously Presented) 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).

27 and 35. (Previously Presented) The computer implemented method of claim 26, wherein the static and dynamic code comprise credentials for verifying the individual's identity (see, e.g., col. 8, lines 6-14 and col. 8, lines 57-65).

30. (Previously Presented) 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).

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

44, 49 and 54. (Previously Presented)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).

45, 50 and 55. (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 (see, e.g., col. 4, lines 50-55, random temporary transaction number).

52. (Previously Presented) 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:

(New) 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 et al (US 5,883,810 A); hereinafter Franklin in view of the examiner Official Notice.

Regarding claims 42, 47, 58, 53 and 63, Franklin 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

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

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

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

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

Abdulhakim Nobahar
Examiner
Art Unit 2432

/A. N./
Examiner, Art Unit 2432

/Jung Kim/
Primary Examiner, AU 2432

Index of Claims	Application/Control No.	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		
	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		
	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						✓	✓		

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 11/19/2010

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

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
11/19/2010	PAPER

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

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

Interview Summary	Application No.	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 P. Fortkort, Reg. No. 35,141*. (4)*Mr. Kamran Asghari-Kamrani*.

Date of Interview: *10 November 2010*.

Type: a)☐ Telephonic b)☐ Video Conference
c)☒ Personal [copy given to: 1)☐ applicant 2)☐ applicant's representative]

Exhibit shown or demonstration conducted: d)☐ Yes e)☒ No.
If Yes, brief description: _____.

Claim(s) discussed: *21*.

Identification of prior art discussed: *5,883,810*.

Agreement with respect to the claims f)☐ was reached. g)☐ was not reached. h)☒ N/A.

Substance of Interview including description of the general nature of what was agreed to if an agreement was reached, or any other comments: *Mr. Fortkort discussed the elements recited in claim 21 in view of the prior art Franklin et al and stated that the differences of claimed invention and the prior art will be further explained in the applicants' response to the Office Action*.

(A fuller description, if necessary, and a copy of the amendments which the examiner agreed would render the claims allowable, if available, must be attached. Also, where no copy of the amendments that would render the claims allowable is available, a summary thereof must be attached.)

THE FORMAL WRITTEN REPLY TO THE LAST OFFICE ACTION MUST INCLUDE THE SUBSTANCE OF THE INTERVIEW. (See MPEP Section 713.04). If a reply to the last Office action has already been filed, APPLICANT IS GIVEN A NON-EXTENDABLE PERIOD OF THE LONGER OF ONE MONTH OR THIRTY DAYS FROM THIS INTERVIEW DATE, OR THE MAILING DATE OF THIS INTERVIEW SUMMARY FORM, WHICHEVER IS LATER, TO FILE A STATEMENT OF THE SUBSTANCE OF THE INTERVIEW. See Summary of Record of Interview requirements on reverse side or on attached sheet.

/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.

Certification Under 37 C.F.R. § 1.8

I hereby certify that on November 18, 2010 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: November 18, 2010 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 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 meeting with them and their representative on November 10, 2010 as part of an Interview. During the interview, the Applicants described the development of their invention and discussed the applicability of the main reference, Franklin et al., to the claims at issue. The Applicants noted that the Franklin et

al. reference does not relate to authentication of an individual but rather to authorization of a credit card transaction, and thus the claims were not anticipated by Franklin et al. No final agreement was reached regarding the claims and the rejections.

CONCLUSION

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

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

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

Respectfully submitted,

By /Michael P. Fortkort/ Date: November 18, 2010
Michael P. Fortkort (Reg. No. 35,141)

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

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

Electronic Acknowledgement Receipt

EFS ID:	8870672
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:	18-NOV-2010
Filing Date:	18-JAN-2006
Time Stamp:	17:52:16
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_111810.pdf	18092 7c872f25daad8376b9da797d699e44d3eaf21425	no	2

Warnings:	
Information:	

Total Files Size (in bytes):	18092

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 12, 2010 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: November 12, 2010 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 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 OFFICE ACTION

Sir:

In response to the Office Action mailed September 21, 2010, the Applicants hereby respectfully submit the following amendments and remarks:

Amendments to the Claims begin on page 2.

Remarks begin on page 15.

In the Claims:

Please amend the claims as follows:

1-20. (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. (Currently Amended) The computer implemented method of claim 21, wherein the request for the dynamic code is received by a computer associated with ~~the~~ 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. (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~~ trusted-authenticator in response to a request for ~~a~~ the dynamic code from the ~~trusted authenticator~~ trusted-authenticator during authentication of the individual by the entity and was calculated by the ~~trusted authenticator~~ trusted-authenticator during authentication of the

individual by the entity;

sending electronically by the entity an authentication request to a ~~trusted-authenticator~~ 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~~ 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. (Currently Amended) The computer implemented method according to claim 41, wherein the entity and the ~~trusted-authenticator~~ trusted-authenticator are the same.

43. (Currently Amended) The computer implemented method according to claim 41, wherein the entity and the ~~trusted-authenticator~~ 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~~ trusted-authenticator during authentication of the individual by the entity;

receiving electronically the dynamic code from the ~~trusted authenticator~~ trusted-authenticator during authentication of the individual by the entity, which dynamic code was calculated by a computer associated with the ~~trusted authenticator~~ 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 ~~a trusted authenticator~~ the trusted-authenticator for verification by the ~~trusted authenticator~~ 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~~ trusted-authenticator of the user information and dynamic code received from the individual during authentication of the individual by the entity.

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

48. (Currently Amended) The computer implemented method according to claim 46, wherein the entity and the ~~trusted-authenticator~~ 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. (Currently Amended) The computer implemented method according to claim 51, wherein the entity comprises a ~~trusted authenticator~~ trusted-authenticator.

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

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 and received from a ~~trusted authenticator~~ 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~~ 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~~ 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~~ trusted-authenticator and sent by a second computer associated with the ~~trusted~~

~~authenticator~~ 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 ~~a third computer associated with~~ the ~~trusted authenticator~~ trusted-authenticator during said communication between the individual and the entity; and

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

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

Please cancel claims 59-61 without disclaimer of or prejudce to the subject matter contained therein.

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 ~~a~~ 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~~ 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~~ 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~~ 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 and 34-38 and 41-64 were previously pending. Claims 59-62 have been cancelled without disclaimer of or prejudice to the subject matter contained therein. Claims 41, 43, 46, 47, 48, 53, 54, 56, 57 and 63 have been amended to correct certain informalities noted by the Examiner. Claims 21-31, 34-38 and 41-58 and 63-64 remain pending.

DOUBLE PATENTING

The Office Action provisionally rejected claims21-23, 26, 27, 30, 31, 34, 38, 41-44, 46-49, 51-54 and 56-64 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 or the claims in the copending application, the Applicants will timely file a terminal disclaimer, which will obviate this rejection.

SPECIFICATION

The Office Action objected to the specification as failing to provide antecedent basis for the claimed subject matter of claim 57. Specifically, the Office Action contends that a first, second and third computer associated with a trusted-authenticator is not described in the specification. Fig 2b shows two computers associated with the trusted authenticator. Additionally, the Applicants respectfully point the Examiner to the last paragraph of page 23, which states: "Although not shown specifically in Fig. 2a and Fig. 2b it should be understood that one or more additional parties or entities may be introduced along the communication route within the scope of the present invention. Among other things, such additional parties may be useful for calculating and validating dynamic keys or expediting, screening, and correctly routing

electronic communications between the parties." The Applicants respectfully submit that this statement supports the recited subject matter of claim 57. However, to expedite the issuance of a notice of allowance, the Applicants have removed the reference in claim 57 to a third computer. Reconsideration and withdrawal of the objection to the specification is respectfully requested.

CLAIM OBJECTIONS

The Examiner objected to claims 21-31, 34-38 and 41-64 due to certain informalities. First, the Examiner objected to the mixed use of hyphenated and non-hyphenated versions of "trusted-authenticator" (i.e., also "trusted authenticator") throughout the claims. The Applicants have amended the claims to use the hyphenated version of "trusted-authenticator" in all instances.

Second, the Examiner cites claim 21, line 5 "for the individual" and suggests "from the individual" is appropriate. However, the Applicants note that the phrase "for the individual" is correct as the claim intends to recite that the request is for a dynamic code for the individual. In other words, the dynamic code belongs to or is associated with the individual.

Third, the Examiner cites claim 23, line 2 "the first trusted-authenticator" which has been corrected to "a first trusted-authenticator" as suggested by the Examiner.

Third, the Examiner cites claim 41, line 5 "with dynamic code" but the Applicants cannot find the cited language. The Applicants respectfully submit the recited portion of line 5 is correct, as the claim recites that the dynamic code is received by a computer that is associated with the entity. However, the Applicants have amended the term "which dynamic code" to be "which said dynamic code" in case this is the informality to which the Examiner intended to refer.

Fourth, the Examiner cites claim 41, line 6, which has been amended as suggested by the Examiner.

Fifth, the Examiner cites claim 41, line 11 for another instance of "a dynamic code." However, this recitation actually states "a received dynamic code" as opposed to "a dynamic code" and is therefore stated with proper antecedent basis.

Sixth, the Examiner cites claim 46, line 13, which has been amended as suggested by the Examiner.

Seventh, the Examiner cites claim 46, line 16. However, this recitation is correctly stated. The claim intends to recite that the acceptance or denial of authentication is received from the entity.

Eighth, the Examiner cites claim 54, line 3 which has been amended as suggested by the Examiner.

Ninth, the Examiner cites claim 62, line 4 which has been amended as suggested by the Examiner.

The Applicants thank the Examiner for his diligence and attention to detail and respectfully request reconsideration and withdrawal of the claim objections in light of the above remarks and amendments.

CLAIMS REMAIN PATENTABLE OVER *FRANKLIN ET AL.*

The Office Action rejected claims 21-31, 34-38 and 41-64 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.*"]. The Office Action contends that *Franklin et al.* discloses all of the elements of the claims at issue. The Applicants respectfully disagree with the Office Action's characterization of these

references vis-à-vis the claims at issue and respectfully request reconsideration and withdrawal of the rejection in light of the following remarks.

Background on Anticipation

To anticipate a claim, a single prior art reference must expressly or inherently disclose each claim limitation. But disclosure of each claim element is not quite enough … anticipation requires the presence in a single prior art disclosure of all elements of a claimed invention *arranged as in the claims*. *Finisar v. DirecTV*, 523 F.3d 1323, 1334 (Fed. Cir. 2008) (emphasis supplied).

The reference must enable one to make the claimed invention without further research or experimentation. *In re Hall*, 781 F.2d 897, 899 (Fed. Cir. 1986). The disclosure in an assertedly anticipating reference must be adequate to enable possession of the desired subject matter. *It is insufficient to name or describe the desired subject matter*, if it cannot be produced without undue experimentation. *Elan Pharmaceuticals, Inc. v. Mayo Foundation for Medical Educ. and Research*, 346 F.3d 1051, 1055 (Fed. Cir. 2003) (emphasis supplied).

Inherency

With regard to inherency, inherency can only be established if a feature is necessarily present, even though it is not explicitly disclosed by a reference. Inherency may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient. As stated in MPEP § 2112(IV):

> The fact that a certain result or characteristic may occur or be present in the prior art is not sufficient to establish the inherency of that result or characteristic. *In re Rijckaert*, 9 F.3d 1531, 1534, 28 USPQ2d 1955, 1957 (Fed. Cir. 1993) (emphasis supplied)…" To establish inherency, the extrinsic evidence 'must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary

> skill. Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient.'" *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999) (emphasis supplied).

Stated another way, the doctrine of inherency requires that the missing descriptive matter MUST be present, and if there is another way of performing a missing descriptive function, then the missing descriptive function is NOT inherently disclosed.

***Franklin et al.* Does not Expressly or Inherently Disclose Each Element of the Claims Arranged as in the Claims**

Franklin et al. fails to disclose each element of the claims arranged as in the claims for at least three reasons. First, *Franklin et al.* does not disclose the dynamic code that is recited in all of the independent claims, from which the remaining claims ultimately depend. The Office Action cites the temporary transaction number as being the claimed dynamic code (see Office Action, page 5, third to last line). The temporary transaction number of *Franklin et al.* is simply not a "code," but merely a numerical value that looks like a credit card number. Thus, the temporary transaction number of *Franklin et al.* is simply not the recited SecureCode.

Second, claim 21 recites "receiving … an authentication request… based on … a received dynamic code." Simply put, in *Franklin et al.* there is no request for authentication that includes a dynamic code. *Franklin et al.* does not use the temporary transaction number to AUTHENTICATE the user. *See Aff. Kamrani, ¶ 8.* Rather, the system of *Franklin et al.* uses the temporary transaction number to AUTHORIZE a credit card transaction with the bank. *See Aff. Kamrani, ¶ 8.* Authentication is an entirely different process than credit card authorization. *See Aff. Kamrani, ¶ 6-7.* Credit card authorization merely confirms that the temporary transaction

number is a valid account number and there are sufficient funds to pay the desired transaction. *See Aff. Kamrani, ¶ 7.* In contrast, authentication is a process by which the authenticator states that the individual is who the individual says he is. *See Aff. Kamrani, ¶ 6.* Thus, *Franklin et al.* fails to disclose receiving a request for authentication that includes the dynamic code as recited in claim 21 and the remaining independent claims.

Third, claim 21 recites "verifying an identity of the individual based on the … received dynamic code." *Franklin et al.* does not verify the identity of the user at all but merely authorizes a transaction based on the temporary transaction number, hence *Franklin et al.* also fails to disclose this claim element, which also appears in independent claim 21.

Thus, for at least these three reasons the Applicants respectfully submit that the claims at issue are neither anticipated by nor rendered obvious by *Franklin et al*. Reconsideration and withdrawal of the rejection of these claims is respectfully requested.

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

The Office Action rejected claims 42, 47 and 53 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 claims at issue, except for "wherein said Eternal-Entity and said Central-Entity are the same entity," for which the Office Action provides certain Official Notice. The Office Action takes Official Notice for this teaching missing from *Franklin et al.* Even assuming *arguendo* that the Office Action's citation of Official Notice is proper, because these claims ultimately depend from independent claims that have been shown to be patentable over *Franklin et al.*, these claims remains patentable over

Franklin et al. for at least the same reasons discussed above. The Applicants therefore respectfully request reconsideration and withdrawal of the rejection of claims 42, 47 and 53.

CONCLUSION

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

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

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

Respectfully submitted,

By /Michael P. Fortkort/ Date: November 12, 2010
Michael P. Fortkort (Reg. No. 35,141)

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

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

Certification Under 37 C.F.R. § 1.8

I hereby certify that on November 12, 2010 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: November 12, 2010 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 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 September 17, 2010 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.

3. In 2003, I obtained an Accredited ACH Professional certification from NACHA (The Electronic Payment Association). There are only approximately 3500 professionals with this certification in the United States.

4. I am familiar with the specification and claims of the present Application as pending and as amended in accordance with a response filed concurrently herewith.

5. I have reviewed the art cited by the Examiner in the present proceeding and in particular, U.S. Patent No. 5,883,810 (*Franklin et al.*).

6. One of skill in the authentication art would understand that authentication of a user involves determining whether a user is, in fact, who he or she claims to be. This is supported by, for example, Exhibit A to this Affidavit, which is from a recent publication by Hitachi ID Systems that that defines authentication as "Authentication is any process by which a system verifies the identity of a User who wishes to access it."

7. In contrast, one of skill in the art of authentication would understand the difference between authentication of a user and credit card authorization that occurs during a credit card payment transaction, which involves receiving a customer'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 customer's order. This is supported by, for example, Exhibit B to this Affidavit, which describes credit card authorization as "An authorization is an approval on a cardholder account for a sale

amount." This understanding is further supported by, for example, Exhibit C to this Affidavit which states: "The term "authorization" refers to the process of verifying with a prepaid card issuer that an account has sufficient funds available and is in good standing. When a prepaid debit card transaction is 'authorized,' the available balance of the account is reduced by the authorized amount."

8. One of skill in the art of authentication would understand that the temporary transaction number of *Franklin et al.* is not used for authentication of the user but rather for authorization of payment.

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

FURTHER AFFIANT SAYETH NOT.

In witness whereof,

Nader Asghari-Kamrani

11/12/2010

Date

EXHIBIT A

Definition of Authentication

Authentication is any process by which a system verifies the identity of a User who wishes to access it. Since Access Control is normally based on the identity of the User who requests access to a resource, Authentication is essential to effective Security.

Authentication may be implemented using Credentials, each of which is composed of a User ID and Password. Alternately, Authentication may be implemented with Smart Cards, an Authentication Server or even a Public Key Infrastructure.

Users are frequently assigned (with or without their knowledge) Tickets, which are used to track their Authentication state. This helps various systems manage Access Control without frequently asking for new Authentication information.

©Hitachi ID Systems, Inc.

500, 1401 - 1 Street SE, Calgary AB Canada T2G 2J3 Tel: 1.403.233.0740 Fax: 1.403.233.0735 E-Mail: sales@Hitachi-ID.com

www.Hitachi-ID.com

EXHIBIT B

Authorizations

An authorization is an approval on a cardholder account for a sale amount. An authorization hold is a reduction of the cardholder's credit line for the amount of the sale. This hold can remain on the cardholder's account for up to 30 days, depending upon the issuing bank policy.

When you're conducting a transaction and you need an authorization, remember that the authorization must be for the identical sale amount. If you receive an authorization for the wrong amount, delete the incorrect authorization, and re-authorize for the exact dollar amount. However, you can pre-authorize for a different amount than the sale amount if you're in any of these industries: car rental, hotel, mail/telephone order, or restaurant.

Here are some typical authorization methods, followed by some common response codes and what you should do in each case.

Authorization methods

- **Terminal:** Obtained electronically through your terminal by magnetically swipe reading or manually entering the credit card number.
- **Voice:** Obtained when a when contact is made with our authorization center, either through the automated system or when speaking to a representative at the authorization center.
- **Direct solutions/Autobats:** Obtained when you compile your sales at the end of the day and transmit them to Wells Fargo Merchant Services electronically. Wells Fargo Merchant Services will then authorize and process the merchant sales.
- **Tape authorizations:** Obtained through a personal computer or a terminal. Works in the same manner as a terminal authorization.
- **Tape ECR (Electronic Cash Register):** Works in the same manner as a terminal authorization.

Response codes

Approved. Normally followed by a 2 to 6 digit code.

Declined. If you receive this response you should never accept the card. Request another form of payment. If you receive an authorization from an alternate source, such as the issuing bank, after receiving a decline message through the terminal or VRU, you may be subject to chargebacks and cancellation of your sales agreement.

If a foreign card gets a referral message, the authorization center should contact the issuing bank for further information. Due to the time differences to reach these countries, it may take up to two business days to get an authorization response. An authorization representative will contact you with the response when it's received. Wait before processing the transaction — or providing the customer with the merchandise. If the response is a referral response or an authorization by phone, the authorization/transaction must be force entered.

Referral. This response indicates the card issuer is requesting direct contact with the business in order to authorize the sale. Contact the Wells Fargo Merchant Services authorization center for Visa®, MasterCard®, and Discover® Network. For American Express, contact the appropriate authorization center.

Hold card/Call center. Indicates that the card issuer is requesting the card be removed from circulation. Never accept the credit card for payment when this response is received.

Call center. This response indicates the card issuer is requesting direct contact with the business in order to authorize the sale. Contact the Wells Fargo Merchant Services authorization center for Visa®, MasterCard®, and Discover® Network. For American Express, contact the appropriate authorization center.

EXHIBIT C

Authorization

The term "authorization" refers to the process of verifying with a prepaid card issuer that an account has sufficient funds available and is in good standing. When a prepaid debit card transaction is "authorized", the available balance of the account is reduced by the authorized amount.

In some types of prepaid debit card transactions (such as "pay at the pump" gasoline purchases, hotel room transactions, or car rental transactions), an authorization hold may be placed on the account which is larger than the actual transaction amount.

More Filed under: Glossary

Other Prepaid Card Terms & Information You Should Know:

Skimming
Network Branded Prepaid Cards
Settlement bank
Automated Teller Machine (ATM)
Rebate Card

Electronic Acknowledgement Receipt

EFS ID:	8828772
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-NOV-2010
Filing Date:	18-JAN-2006
Time Stamp:	16:24:02
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_OA_mailed_091710_filed_111210.pdf	85782 ddcff48983c534ed3f2a449dc42a380bf542bba0	no	21

Warnings:	
Information:	

2	Rule 130, 131 or 132 Affidavits	11333400_132_Affidavit_filed_111210.pdf	4038559 112f0b3f4510a85d1d79bfcffb0b3de62c3c2472	no	7
Warnings:					
Information:					
			Total Files Size (in bytes):	4124341	

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	11/12/2010	(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))	* 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) 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:
/LINDA WISE/

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

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

Doc Code: M865 or FAI.REQ.INTV

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

Applicant Initiated Interview Request Form

Application No.: 11/333,400 First Named Applicant: NADER ASGHARI-KAMRANI
Examiner: NOBAHAR, ABDULHAKIM Art Unit: 2432 Status of Application: NON-FINAL REJECTION MAILED

Tentative Participants:
(1) MICHAEL P. FORTKORT (2) NADER ASGHARAI-KAMRANI
(3) KAMRAN ASCHARI-KAMRANI (4) _____

Proposed Date of Interview: NOVEMBER 10, 2010 **Proposed Time:** 11:00 A.M. **(AM/PM)**

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

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

Issues To Be Discussed

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

[ ] Continuation Sheet Attached [ ] Proposed Amendment or Arguments Attached
Brief Description of Arguments to be Presented: DIFFERENCES BETWEEN CLAIMS AND CITED ART

An interview was conducted on the above-identified application on NOVEMBER 10, 2010

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

/MICHAEL P. FORTKORT/
Applicant/Applicant's Representative Signature

_____
Examiner/SPE Signature

MICHAEL P. FORTKORT
Typed/Printed Name of Applicant or Representative

35,141
Registration Number, if applicable

Electronic Acknowledgement Receipt

EFS ID:	8756888
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:	03-NOV-2010
Filing Date:	18-JAN-2006
Time Stamp:	08:54:11
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	Letter Requesting Interview with Examiner	Interview_Request_110310_11333400.pdf	299842 7f5b82bdc984ee213e7bdb5f558344379f3251b4	no	1

Warnings:	
Information:	

Total Files Size (in bytes):	299842

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 09/21/2010

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

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
09/21/2010	PAPER

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

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

Office Action Summary	Application No.	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 *16 July 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 and 41-64* 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 and 41-64* 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 07/16/2010.

2. Claims 21-31, 34-38 and 41-64 are pending.

3. Claims 58-64 are newly added claims.

Response to Arguments

Applicant's arguments with respect to the rejections of claims 21-31, 34-38 and 41-64 stated in the Remarks 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 and 56-64** 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 and 56-64 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.

Specification

The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: Claim 57 recites that a first computer, a second computer and a third computer are associated with the trusted authenticator which is not described in the specification. Proper correction is necessary to be applied to the claim in order to avoid that the amended parts considered as new matter.

Claim Objections

Claims 21-31, 34-38 and 41-64 are objected to because of the following informalities: some of these claims recite “trusted-authenticator”, some recite “trusted authenticator” and some recite both. Claims should be amended to recite just one form of this phrase in order to be uniform and consistent.

Claim 21 in line 5 recites “for the individual” rather than “from the individual”.

Claim 23 in line 2 recites the limitation "the first trusted-authenticator”. It should recites "a first trusted-authenticator” similar to claim 22.

Claim 41 in line 5 recites “with dynamic code” rather than “with the dynamic code”.

Claim 41 in line 6 recites “a request for a dynamic code” rather than “a request for the dynamic code”.

Claim 41 in line 11 recites “a dynamic code” rather than “the dynamic code”.

Claim 46 in line 13 recites “the entity to a trusted authenticator” rather than “the entity to the trusted authenticator”.

Claim 46 in line 16 recites “receiving…denial of authentication from the entity” which should be amended to recite “receiving…denial of authentication by the entity”.

Claim 54 in line 3 recites “dynamic key” which should be reciting “dynamic code”.

Claim 62 in line 4 recites “a two-factor” which should be reciting “the two-factor”.

Appropriate correction is required.

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 –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.
>
> (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 and 41-64 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:

(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 (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. (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 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).

24, 28 and 36. (Currently Amended) 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).

25, 29 and 37. (Currently Amended) 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).

27 and 35. (Currently Amended) The computer implemented method of claim 26, wherein the static and dynamic code comprise credentials for verifying the individual's identity (see, e.g., col. 8, lines 6-14 and col. 8, lines 57-65).

30. (Currently Amended) 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).

Claims 42, 47 and 53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Franklin et al (US 5,883,810 A); hereinafter Franklin in view of the examiner Official Notice.

Regarding claim 44, Franklin 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 and customers are authenticated by the respective institution independent from a. 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.

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

44, 49 and 54. (Currently Amended)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).

45, 50 and 55. (Currently Amended) 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).

52. (Currently Amended) 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 claims 58-61 and 63, these claims are rejected as applied to the like elements of claims 42, 47 and 53.

Regarding claim 64, Franklin discloses:

(New) 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).

Conclusion

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

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

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

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Abdulhakim Nobahar
/A. N./
Examiner, Art Unit 2432

/Gilberto Barron Jr./
Supervisory Patent 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			
	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			
	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						✓			

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 : July 16, 2010	This patent is subject to a Terminal Disclaimer	

Approved/Disapproved by:
Henry D. Jefferson

U.S. Patent and Trademark Office

Certification Under 37 C.F.R. § 1.8

I hereby certify that on July 16, 2010 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: July 16, 2010 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 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 OFFICE ACTION

Sir:

In response to the Office Action mailed July 6, 2010, the Applicants hereby respectfully submit the following amendments and remarks:

Amendments to the Claims begin on page 2.

Remarks begin on page 15.

In the Claims:

Please amend the claims as follows:

1-20. (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 ~~by a computer over a communication network~~ electronically a request ~~to generate~~ for a dynamic ~~key~~ code for the individual, which request is received during authentication of the individual by the entity;

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

sending ~~by a computer~~ electronically the dynamic ~~key~~ code ~~over a communication network~~ to the individual during authentication of the individual by the entity;

receiving ~~by a computer~~ electronically an authentication request to authenticate the individual based on a ~~received~~ user information ~~static key~~ and ~~a received~~ the dynamic ~~key~~ code included in the authentication request; and

verifying ~~by a computer~~ an identity of the individual based on the ~~received~~ user information ~~static key~~ and the ~~received~~ dynamic ~~key~~ code included in the authentication request.

22. (Currently Amended) The computer implemented method of claim 21, wherein the

request for the dynamic ~~key~~ code is received by a computer associated with a first trusted-authenticator and the authentication request ~~from the entity~~ is received by ~~a computer associated with~~ the first trusted-authenticator.

23. (Currently Amended) The computer implemented method of claim 21, wherein the request for the dynamic ~~key~~ code is received by a computer associated with the first trusted-authenticator and the authentication request ~~from the entity~~ 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 ~~key~~ code includes a non-predictable and time-dependent SecureCode.

25. (Currently Amended) The computer implemented method of claim 21, wherein at least the dynamic ~~key~~ 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 ~~static key~~ user information and a dynamic ~~key~~ code from the individual in order to validate the individual's identity during communication with the individual, which individual obtains the dynamic ~~key~~ code from a computer associated with a trusted-authenticator during the communication between the individual and the entity;

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

creating an authentication request message including both the ~~received~~ user information and the received dynamic code ~~static and dynamic keys~~ and providing the authentication request message to ~~a computer associated with~~ a trusted-authenticator ~~over the communication network~~, the ~~computer~~ trusted-authenticator authenticating the individual based on a combination of the ~~received~~ user information and the received dynamic code ~~static and dynamic keys~~.

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

29. (Currently Amended) The computer implemented method of claim 26, wherein at least the dynamic ~~key~~ code is encrypted.

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

31. (Currently Amended) The computer implemented method of claim 26, wherein a

computer associated with a first trusted-authenticator calculates the dynamic ~~key~~ code and provides the dynamic ~~key~~ code ~~over a communication network~~ 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 ~~static key and a dynamic key~~ from the individual in order to validate the individual's identity;

receiving ~~by a computer associated with the website~~ both the user information and the dynamic code ~~static and dynamic keys~~ from the individual, which individual receives the dynamic ~~key~~ code during the communication session between the individual and the website; and

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

35. (Currently Amended) The computer implemented method of claim 34, wherein the user information and the dynamic code ~~static and dynamic keys~~ comprise credentials for verifying the individual's identity.

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

37. (Currently Amended) The computer implemented method of claim 34, wherein at least the dynamic ~~key~~ code is encrypted.

38. (Currently Amended) The computer implemented method of claim 34, wherein a second computer associated with the trusted-authenticator calculates the dynamic ~~key~~ code and provides the dynamic ~~key~~ 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 ~~key~~ code during authentication of the individual by the entity, which dynamic ~~key~~ code was sent to the individual ~~over a communication network~~ by a trusted authenticator in response to a request for a dynamic ~~key~~ 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 ~~a computer associated with~~ the entity an authentication request to a trusted authenticator to authenticate the individual based on a ~~received static key~~ user information and a received dynamic ~~key~~ code included in the authentication request, wherein said authentication request is sent during authentication of the individual by the entity; and

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

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

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

44. (Currently Amended) The computer implemented method according to claim 41, wherein said dynamic ~~key~~ code is calculated ~~by a computer~~ after receiving the request from the individual for the dynamic ~~key~~ code.

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

46. (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 computer implemented method comprising:

sending electronically a request ~~by a computer~~ for a dynamic ~~key~~ code ~~over a communication network~~ to a trusted authenticator during authentication of the individual by the entity;

receiving electronically the dynamic ~~key~~ code from the trusted authenticator ~~over a communication network~~ during authentication of the individual by the entity, which dynamic ~~key~~ code was calculated by a computer associated with the trusted authenticator during authentication of the individual by the entity;

sending ~~by a computer~~ electronically the dynamic ~~key~~ code and ~~a static key~~ user information during authentication of the individual by the entity ~~for submission~~ to a trusted authenticator ~~and~~ 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 ~~static key and the dynamic key~~ received from the individual during authentication of the individual by the entity.

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

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

49. (Currently Amended) The computer implemented method according to claim 46, wherein said dynamic ~~key~~ code is calculated ~~by a computer~~ after receiving the request from the individual for the dynamic ~~key~~ code.

50. (Currently Amended) The computer implemented method according to claim 46, wherein said dynamic ~~key~~ code comprises a different value each time the dynamic ~~key~~ 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 ~~over a communication network~~,

the method comprising:

receiving electronically ~~by a computer~~ a request for a dynamic ~~key~~ code ~~over a communication network~~, wherein the request is received during authentication of the individual by the entity;

sending the dynamic ~~key~~ code electronically ~~by a computer over a communication network~~ to the individual during authentication of the individual by the entity;

receiving electronically an authentication request ~~by a computer~~ from the entity to authenticate the individual based on a ~~static key and a dynamic key~~ 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 ~~received~~ user information and the received dynamic code ~~static key and the received dynamic key~~ in response to the authentication request from the entity during the time of authentication of the individual by the entity.

52. (Currently Amended) 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.

53. (Currently Amended) The computer implemented method according to claim 51,

wherein the entity comprises a trusted authenticator.

54. (Currently Amended) The computer implemented method according to claim 51, wherein said dynamic ~~key~~ code is calculated ~~by a computer~~ after receiving the request for the dynamic key.

55. (Currently Amended) The computer implemented method according to claim 51, wherein said dynamic ~~key~~ code comprises a different value each time the dynamic ~~key~~ 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 ~~static key~~ user information as a first credential and a dynamic ~~key~~ code as a second credential during communication over a network between an entity and the individual, the method comprising receiving electronically ~~by a computer~~ acceptance or denial of two-factor authentication from the entity based on two credentials received from the individual, wherein:

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

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

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

during authentication of the individual by the entity; and

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

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

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

said dynamic ~~key~~ 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 ~~static key and said dynamic key~~ user information and said dynamic code were received ~~via computer~~ electronically during authentication of the individual by the entity and were verified by a third computer associated with 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 ~~key~~ code each time the individual requests a dynamic ~~key~~ code from the trusted authenticator.

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

59. (New) The computer implemented method according to claim 57, wherein the first computer and the third computer are the same.

60. (New) The computer implemented method according to claim 57, wherein the second computer and the third computer are the same.

61. (New) The computer implemented method according to claim 57, wherein the first computer, the second computer and the third are the same.

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

64. (New) 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 and 34-38 and 41-57 were previously pending. Claims 21-31 and 34-38 and 41-57 have been amended to more particularly recite the invention claimed therein. Claims 58-64 have been added to further define the claimed invention. Claims 21-31, 34-38 and 41-64 remain pending.

CLAIM OBJECTIONS

The Examiner objected to the claim listing as failing to indicate the status of claims 1-20. The Applicant apologize for this oversight and have indicated in the listing herein that these claims were cancelled. The Applicants respectfully request reconsideration and withdrawal of the claim objections.

CLAIMS REJECTED UNDER 35 U.S.C. § 112, ¶ 2

The Examiner rejected claims 21-31, 34-38, and 41-57 under 35 U.S.C. § 112, ¶ 2 as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicants regard as the invention. The Applicants have amended the claims at issue in accordance with the Examiner's remarks. Reconsideration and withdrawal of the rejection of these claims is respectfully requested.

APPLICANT'S EARLIER REMARKS

The Examiner's finding that the Applicants' earlier filed Remarks and Affidavit Under Rule 132 have overcome the prior art rejections is gratefully acknowledged.

DOUBLE PATENTING

The Examiner rejected claims 21-31, 34-38 and 41-57 under the judicially created doctrine of obviousness-type double patenting based on U.S. Patent No. 7,356,837 by the same inventors. The Applicants have attached a terminal disclaimer disclaiming the period of any patent issuing from this application beyond the term of U.S. Patent No. 7,356,837. As such, reconsideration and withdrawal of this rejection is respectfully requested.

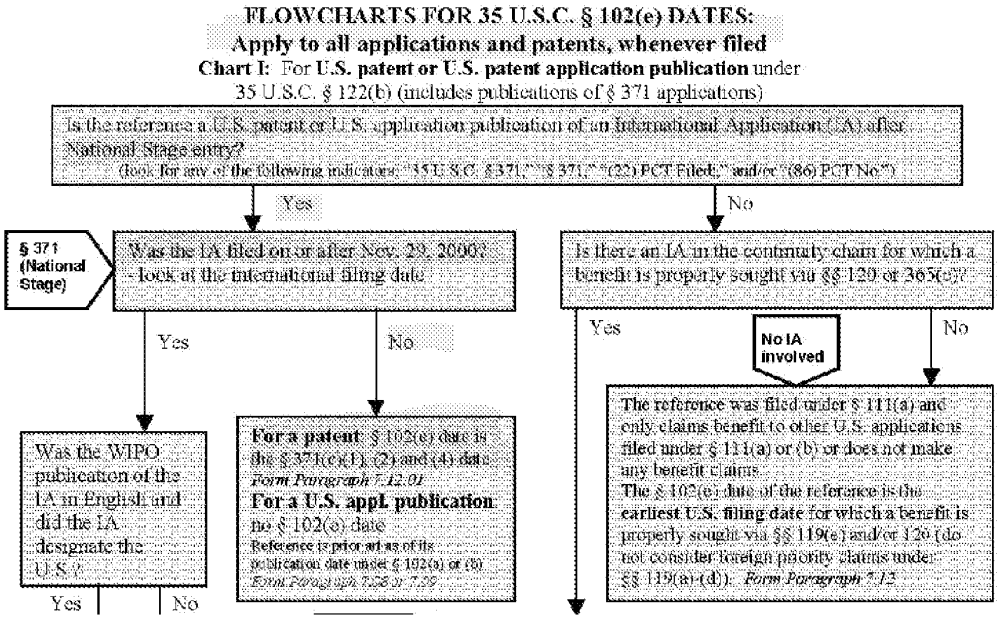
CLAIMS ARE PATENTABLE OVER CHEN

The Examiner rejected claims 21-31, 34-38 and 41-57 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 7,096,204 to Chen et al. [hereinafter "Chen et al."]. The Applicant respectfully submits that Chen et al. is not prior art under 102(e) to the claims of the present application, which claims priority to U.S. Patent No. 7,356,837 filed on August 29, 2001 by the same inventors.

As indicated by the Examiner, because Chen et al. has an international filing date prior to November 29, 2000 Chen et al. is applied under provisions of 35 U.S.C. 102 and 374, prior to the AIPA amendments. *See* M.P.E.P. 706.02(f)(1)I(C)(3). Thus, according to the M.P.E.P. because Chen et al. is a U.S. patent, one should "apply the reference under 35 U.S.C. 102(e) as of the earlier of the date of completion of the requirements of 35 U.S.C. 371(c)(1), (2) and (4) or the filing date of the later-filed U.S. application that claimed the benefit of the international application." As there is no later-filed U.S. application claiming the benefit of the international application, the correct date of Chen et al. is the date of completion of the requirements of 35

U.S.C. 371(c)(1), (2) and (4), which as listed on the face of Chen et al. is August 23, 2002. Thus, the earliest date that Chen et al. can be applied as prior art under 35 U.S.C. §102(e) is August 23, 2002. But, the present application claims priority to the earlier filed patent application bearing a filing date of August 29, 2001 which predates the 102(e) date of Chen et al. Consequently, Chen et al. is not valid prior art under 102(e) to the claims of the present application.

A copy of the flow chart from the M.P.E.P. is reproduced below for the convenience of the Examiner, which indicates the proper 102(e) date is the 371(c)(1)(2) and (4) date or August 23, 2002.



The Applicants respectfully request reconsideration and withdrawal of the rejection of these claims.

CONCLUSION

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

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

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

Respectfully submitted,

By /Michael P. Fortkort/ Date: July 16, 2010
Michael P. Fortkort (Reg. No. 35,141)

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

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

PTO/SB/26 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT	Docket Number (Optional) 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*, NADER ASGHARI-KAMRANI and KAMRAN ASGH, of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term **prior patent** No. 7,356,837 as the term of said prior patent is defined in 35 U.S.C. 154 and 173, and as the term of said **prior patent** is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the **prior patent** are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term as defined in 35 U.S.C. 154 and 173 of the **prior patent**, "as the term of said **prior patent** is presently shortened by any terminal disclaimer," in the event that said **prior patent** later:

expires for failure to pay a maintenance fee;
is held unenforceable;
is found invalid by a court of competent jurisdiction;
is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
has all claims canceled by a reexamination certificate;
is reissued; or
is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

Check either box 1 or 2 below, if appropriate.

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

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

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

/Michael P. Fortkort/ — July 16, 2010
Signature — Date

MICHAEL P. FORTKORT
Typed or printed name

703-435-9390
Telephone Number

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

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

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

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	7	26	182
Independent claims in excess of 3	2201	1	110	110
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
Statutory disclaimer	2814	1	70	70
		Total in USD ($)		**362**

Electronic Acknowledgement Receipt	
EFS ID:	8029532
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-JUL-2010
Filing Date:	18-JAN-2006
Time Stamp:	11:09:59
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$362
RAM confirmation Number	7890
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	Response_to_OA_mailed_070610_in11333400_filed_071610.pdf	437636 f66608f663030009d2af5cf8191d158650c94338	no	18
Warnings:					
Information:					
2	Terminal Disclaimer Filed	Terminal_Disclaimer_071610_re_11333400.pdf	517537 7b36b4e27528458dca843350af0a8538ea605a61	no	1
Warnings:					
Information:					
3	Fee Worksheet (PTO-875)	fee-info.pdf	33096 ec9911bce4d108d1cffe52f211cf3eec34c6eba0	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	988269		

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

		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
AMENDMENT	07/16/2010	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 44	Minus	** 37	= 7	X $26 =	182	OR	X $ =	
	Independent (37 CFR 1.16(h))	* 9	Minus	***8	= 1	X $110 =	110	OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE	292	OR	TOTAL ADD'L FEE	

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

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

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

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

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

Legal Instrument Examiner:
/C. DESSAU/

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 07/06/2010

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

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
07/06/2010	PAPER

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

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

Office Action Summary	Application No.	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 *08 June 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 and 41-57* 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 and 41-57* 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 06/08/2010.

2. Claims 21-31, 34-38 and 41-57 are pending.

3. Claims 41-57 are new.

Claim Objections

The amendment to the claims filed on 06/08/2010 does not comply with the requirements of 37 CFR 1.121(c) because the status of claims 1-20 is not provided in the listing of claims. Amendments to the claims filed on or after July 30, 2003 must comply with 37 CFR 1.121(c) which states:

(c) *Claims*. Amendments to a claim must be made by rewriting the entire claim with all changes (*e.g.*, additions and deletions) as indicated in this subsection, except when the claim is being canceled. Each amendment document that includes a change to an existing claim, cancellation of an existing claim or addition of a new claim, must include a complete listing of all claims ever presented, including the text of all pending and withdrawn claims, in the application. The claim listing, including the text of the claims, in the amendment document will serve to replace all prior versions of the claims, in the application. In the claim listing, the status of every claim must be indicated after its claim number by using one of the following identifiers in a parenthetical expression: (Original), (Currently amended), (Canceled), (Withdrawn), (Previously presented), (New), and (Not entered).

(1) *Claim listing.* All of the claims presented in a claim listing shall be presented in ascending numerical order. Consecutive claims having the same status of "canceled" or "not entered" may be aggregated into one statement (*e.g.*, Claims 1–5 (canceled)). The claim listing shall commence on a separate sheet of the amendment document and the sheet(s) that contain the text of any part of the claims shall not contain any other part of the amendment.

(2) *When claim text with markings is required.* All claims being currently amended in an amendment paper shall be presented in the claim listing, indicate a status of "currently amended," and be submitted with markings to indicate the changes that have been made relative to the immediate prior version of the claims. The text of any added subject matter must be shown by underlining the added text. The text of any deleted matter must be shown by strike-through except that double brackets placed

before and after the deleted characters may be used to show deletion of five or fewer consecutive characters. The text of any deleted subject matter must be shown by being placed within double brackets if strike-through cannot be easily perceived. Only claims having the status of "currently amended," or "withdrawn" if also being amended, shall include markings. If a withdrawn claim is currently amended, its status in the claim listing may be identified as "withdrawn—currently amended."

(3) *When claim text in clean version is required.* The text of all pending claims not being currently amended shall be presented in the claim listing in clean version, *i.e.*, without any markings in the presentation of text. The presentation of a clean version of any claim having the status of "original," "withdrawn" or "previously presented" will constitute an assertion that it has not been changed relative to the immediate prior version, except to omit markings that may have been present in the immediate prior version of the claims of the status of "withdrawn" or "previously presented." Any claim added by amendment must be indicated with the status of "new" and presented in clean version, *i.e.*, without any underlining.

(4) *When claim text shall not be presented; canceling a claim.*

(i) No claim text shall be presented for any claim in the claim listing with the status of "canceled" or "not entered."

(ii) Cancellation of a claim shall be effected by an instruction to cancel a particular claim number. Identifying the status of a claim in the claim listing as "canceled" will constitute an instruction to cancel the claim.

(5) *Reinstatement of previously canceled claim.* A claim which was previously canceled may be reinstated only by adding the claim as a "new" claim with a new claim number.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

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

Claims 21-31, 34-38 and 41-57 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Normally an entity, a device, an item, an element or an individual is preceded by article "a" when recited in a claim for the first time. Thereafter, that entity, device, item, element or individual is preceded by article "the" if recited in that claim or any

independent claims for any subsequent number of times. This practice has not been followed in numerous places throughout the amended and new claims. Therefore, the claims are indefinite because it is not clear whether the same computer, entity and individual are involved and performing the recited functions or different ones. The applicant should make appropriate corrections to the claims to rectify the indefiniteness of the claims caused by this issue.

Claim 22 recites the limitation "the authentication request from the entity" in lines 2 and 3. There is insufficient antecedent basis for this limitation in the claim.

Claim 23 recites the limitation "the first trusted-authenticator" in lines 2 and the limitation "the authentication request from the entity" in lines 2 and 3. There is insufficient antecedent basis for this limitation in the claim.

Response to Arguments

Applicant's arguments with respect to the rejections of claims stated in the Remarks and in the Affidavit filed under 132 rule on 06/08/2010 have been fully considered and are persuasive. Therefore, the rejections have been withdrawn. However, upon further consideration of the amended claims, a new ground(s) of rejection is made.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 21-31, 34-38 and 41-57 of the instant application are anticipated by claims 1-14 of the U.S. Patent No. **7,356,837**. The patented claims teach the same invention as claimed by the pending claims. Claims 21-31, 34-38 and 41-57 of the instant application are included in the limitations of the patented claims, but lack some of the minor detailed features of the patented claims and therefore are broader. Claims 21-31, 34-38 and 41-57 of the instant application therefore are not patently distinct from the earlier patented claims 1-14 and as such are unpatentable for obvious-type double patenting.

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 –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claims 21-31, 34-38 and 41-57 are rejected under 35 U.S.C. 102(e) as being anticipated by Chen et al. (US 7,096,204 B1), hereinafter Chen.

Regarding claims 21, 26, 34, 41, 46 and 51, Chen discloses:

(Currently Amended) A 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. 9), the method comprising:

receiving by a computer over a communication network a request to generate a dynamic key for the individual, which request is received during authentication of the

individual by the entity (see, e.g., BRIEF SUMMARY, ¶ (6), temporary identity corresponds to the recited dynamic key; DETAILED DESCRIPTION, ¶ (80), gets a temporary identity; ¶ (85));

calculating by a computer a dynamic key for the individual in response to the request during authentication of the individual by the entity (see, e.g., DETAILED DESCRIPTION, ¶ (80), (89) and Fig. 9, where the ISP which is the client of the bank issues a temporary identity and a session key to the consumer);

sending by a computer the dynamic key over a communication network to the individual during authentication of the individual by the entity (see, e.g., Fig. 9, via 1211);

receiving by a computer an authentication request to authenticate the individual based on a received static key and a received dynamic key included in the authentication request (see, e.g., DETAILED DESCRIPTION, ¶ (80) and Fig. 9, where the vendor 1203 receives the temporary identity and the session key from the consumer via 1218; the session key or one of other consumer's information such as name, address, phone number or email address which normally is used in a transaction between a vendor or a consumer can be considered as a static key); and

verifying by a computer an identity of the individual based on the received static key and the received dynamic key included in the authentication request (see, e.g., DETAILED DESCRIPTION, ¶ (80), where the vendor is able to verify whether the the temporary identity and the session key are issued by the ISP).

Chen discloses:

22, 31 and 38. (Currently Amended) The method of claim 21, wherein the request for the dynamic key is received by a computer associated with a first trusted-authenticator and the authentication request from the entity is received by a computer associated with the first trusted-authenticator (see, e.g., Fig. 9, computer 1202).

23. (Currently Amended) The method of claim 21, wherein the request for the dynamic key is received by a computer associated with the first trusted-authenticator (see, e.g., Fig. 9, computer 1202) and the authentication request from the entity is received by a computer associated with a second trusted-authenticator that is different than the first trusted-authenticator (see, e.g., Fig. 9, BANK 1 or Bank 2).

24, 28 and 36. (Previously Presented) The method of claim 21, wherein the dynamic key includes a non-predictable and time-dependent SecureCode (see, e.g., DETAILED DESCRIPTION, ¶ (68), (80) and (89), where the temporary identity is used for one purchasing session).

25, 29 and 37. (Previously Presented) The method of claim 21, wherein at least the dynamic key is encrypted (see, e.g., DETAILED DESCRIPTION, ¶ (48), (58) and (89)).

27 and 35. (Currently Amended) The method of claim 26, wherein the static and dynamic keys comprise credentials for verifying the individual's identity (see, e.g., DETAILED DESCRIPTION, ¶ (70), (80) and (88), where it is inherent in the system that user credentials are either part of the static and temporary keys or being used and transmitted along with these keys).

30. (Previously Presented) The method of claim 26, wherein the entity corresponds to a business, organization, or another individual (see, e.g., Fig. 9, vendor).

42, 47 and 53. (New) The method according to claim 41, wherein the entity and the trusted authenticator are the same (see, e.g., DETAILED DESCRIPTION, ¶ (79) and Fig. 8, vendor 1103).

43 and 48. (New) The method according to claim 41, wherein the entity and the trusted authenticator are different (see, e.g., DETAILED DESCRIPTION, ¶ (80) and Fig. 9, vendor 1203 and ISP 1202).

44, 49 and 54. (New) The method according to claim 41, wherein said dynamic key is calculated by a computer after receiving the request from the individual for the dynamic key (see, e.g., DETAILED DESCRIPTION, ¶ (80) and Fig. 9, ISP 1202 calculates the temporary key after receiving a request from the consumer).

45, 50 and 55. (New) The method according to claim 41, wherein said dynamic key comprises a different value each time the dynamic key is requested by the individual (see, e.g., DETAILED DESCRIPTION, ¶ (89), where the temporary identity is used for one purchasing session which means the temporary identity is unique and it is different for different purchasing session).

52. (New) The method according to claim 51, further comprising:

sending a confirmation or denial authentication message by a computer to the entity during authentication of the individual by the entity (see, e.g., DETAILED DESCRIPTION, ¶ (80) and Fig. 9, 1221, where verifying the temporary identity means confirmation or denial).

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

Conclusion

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

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

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

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

Abdulhakim Nobahar
/A. N./
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-7,334,735 B1	02-2008	Antebi et al.	235/492
*	B	US-7,237,117 B2	06-2007	Weiss, Kenneth P.	713/182
*	C	US-6,845,453 B2	01-2005	Scheidt et al.	726/5
*	D	US-7,111,173 B1	09-2006	Scheidt, Edward M.	713/186
*	E	US-6,539,092 B1	03-2003	Kocher, Paul C.	380/252
*	F	US-4,885,778 A	12-1989	Weiss, Kenneth P.	713/184
	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				
	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				
	37			✓	✓	✓				
	38			✓	✓	✓				
	39			✓	-	-				
	40			✓	-	-				
	41					✓				
	42					✓				
	43					✓				
	44					✓				
	45					✓				
	46					✓				
	47					✓				
	48					✓				
	49					✓				
	50					✓				
	51					✓				
	52					✓				
	53					✓				
	54					✓				
	55					✓				
	56					✓				
	57					✓				

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 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
S20	946	713/184	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/24 12:03
S21	582	S20 and (dynamic $4 tempora$4 time transi$5 temp onetime interim timewise provision$4 variable varying chang$5 timebased unpredict$4 short) near2 (key password code seed passcode passphrase phrase ID identification identify$3 identity PIN secret securecode pincode secret passname credential)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/24 12:38
S22	482	S21 and (dynamic $4 tempora$4 time transi$5 temp onetime interim timewise provision$4 variable varying chang$5 timebased unpredict$4 short) adj2 (key password code seed passcode passphrase phrase ID identification identify$3 identity PIN secret	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/24 12:39

		securecode pincode secret passname credential)				
S23	331	S21 and (dynamic $4 tempora$4 time transi$5 temp onetime interim timewise provision$4 variable varying chang$5 timebased unpredict$4 short) adj (key password code seed passcode passphrase phrase ID identification identify$3 identity PIN secret securecode pincode secret passname credential)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/24 12:39
S24	116	S23 and (dynamic $4 tempora$4 time transi$5 temp onetime interim timewise provision$4 variable varying chang$5 timebased unpredict$4 short) adj (key password code seed passcode passphrase phrase ID identification identify$3 identity PIN secret securecode pincode secret passname credential) with (authenticat$3 verification verif$4 valid$5)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/24 12:41

S25	5	S24 and fob	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/24 12:42
S26	22	S20 and fob	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/24 13:11
S27	17	"6845453" and (dynamic$4 tempora$4 time transi$5 temp onetime interim timewise provision $4 variable varying chang$5 timebased unpredict$4 short period duration during interval single predict$4) same (key password code seed passcode passphrase phrase ID identification identify$3 identity PIN secret securecode pincode secret passname credential)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/24 13:35
S28	2	"6845453".pn. and (dynamic$4 tempora$4 time transi$5 temp onetime interim timewise provision $4 variable varying chang$5 timebased unpredict$4 short period duration during interval single predict$4) same (key password code seed passcode passphrase phrase	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/24 13:36

		ID identification identify$3 identity PIN secret securecode pincode secret passname credential)				
S30	3	("4885778".pn. "6539092".pn.) and (dynamic$4 tempora$4 time transi$5 temp onetime interim timewise provision $4 variable varying chang$5 timebased unpredict$4 short period duration during interval single predict$4) same (key password code seed passcode passphrase phrase ID identification identify$3 identity PIN secret securecode pincode secret passname credential)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/24 13:55
S31	690	S20 and (authoriz $5 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	2010/06/24 16:11

S35	469	S31 and (dynamic $4 tempora$4 time transi$5 temp onetime interim timewise provision$4 variable varying chang$5 timebased unpredict$4 predict $4 short) near2 (key password code seed passcode passphrase phrase ID identification identify$3 identity PIN secret securecode pincode secret passname credential)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/24 16:16

6/30/2010 10:33:43 PM
H:\EAST\Workspaces\11333400.wsp

Doc code: RCEX
Doc description: Request for Continued Examination (RCE)

PTO/SB/30EFS (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	11/333,400	Filing Date	2006-01-18	Docket Number (if applicable)	KAMR001US0	Art Unit	2432
First Named Inventor	ASGHARI-KAMRANI , NADER			Examiner Name	Mr. Abdulhakim Nobahar		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____

☐ Other _____

☒ Enclosed

☒ Amendment/Reply

☐ Information Disclosure Statement (IDS)

☒ Affidavit(s)/ Declaration(s)

☒ Other REQUEST FOR THREE MONTH EXTENSION OF TIME TO RESPOND TO OFFICE ACTION MAILED 12/08/2009.

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____
(Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other _____

FEES

The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.

☒ The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No 503776

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature

☐ Applicant Signature

PTO/SB/30EFS (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Signature of Registered U.S. Patent Practitioner			
Signature	/Michael P. Fortkort/	Date (YYYY-MM-DD)	2010-06-08
Name	MICHAEL P. FORTKORT	Registration Number	35141

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

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

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

Certification Under 37 C.F.R. § 1.8

I hereby certify that on June 8, 2010 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: June 8, 2010 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 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

PETITION TO EXTEND TIME TO RESPOND AND
RESPONSE TO OFFICE ACTION

Sir:

The Applicant hereby petitions the Assistant Commissioner to grant a three (3) month extension of time, up to and including June 8, 2010, in which to respond to the Office Action mailed December 8, 2009 in the above-identified application ("Office Action"). The small entity

extension fee in the amount of $555.00 will be paid when filing electronically via credit card. Any additional fees may be charged to the deposit account of MICHAEL P FORTKORT PC, Deposit Account No. 50-3776. In response to the Office Action, the Applicant hereby respectfully submits the following amendments and remarks:

Amendments to the Claims begin on page 3.

Remarks begin on page 15.

In the Claims:

Please amend the claims as follows:

21. (Currently Amended) A method ~~for a non-fiduciary business, organization, or another individual~~ to ~~directly~~ authenticate an individual in communication with an entity over a communication network during communication between the entity and the individual ~~without redirecting the individual to another site and without having previous information about the individual~~, the method comprising:

~~The individual communicating with the business, organization, or another individual;~~

~~The business, organization, or another individual communicating a request for both a static key and a dynamic key from the individual;~~

receiving by a computer over a communication network a request to generate a dynamic key for the individual, which request is received during authentication of the individual by the entity;

calculating by a computer a dynamic key for the individual in response to the request during authentication of the individual by the entity;

sending by a computer the dynamic key over a communication network to the individual during authentication of the individual by the entity;

~~In response to the business, organization, or another individual's request, the individual communicating a request for a dynamic key from a first trusted-authenticator;~~

~~In response to the individual's request, the first trusted-authenticator calculating a dynamic key and providing it to the individual;~~

~~The individual providing a combination of the calculated dynamic key and an existing~~

~~static key to the business, organization, or another individual;~~

receiving by a computer an authentication request to authenticate the individual based on a received static key and a received dynamic key included in the authentication request;

~~The business, organization, or another individual constructing an authentication request message containing the static and dynamic keys and communicating the authentication request message to a computer associated with a second trusted-authenticator over the communication network;~~ and

~~The second trusted-authenticator computer~~ verifying by a computer an identity of the individual ~~the individual's identity~~ based on the received static key and the received dynamic key~~s~~ included in the authentication request; ~~and~~

~~sending a confirmation or denial authentication message to the business, organization, or another individual~~.

22. (Currently Amended) The method of claim 21, wherein the request for the dynamic key is received by a computer associated with a first trusted-authenticator and the authentication request from the entity is received by a computer associated with the first ~~and second~~ trusted-authenticator ~~are the same~~.

23. (Currently Amended) The method of claim 21, wherein the request for the dynamic key is received by a computer associated with the first trusted-authenticator and the authentication request from the entity is received by a computer associated with a second trusted-authenticator that is different than the first ~~and second~~ trusted-authenticator ~~are different~~.

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

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

26. (Currently Amended) A method for an non-fiduciary entity to directly authenticate an individual over a communication network during communication with the individual without redirecting the individual to another site and without having previous information about the individual, the method comprising:

Rrequesting both a static key and a dynamic key from the individual in order to validate the individual's identity during communication with the individual, which individual obtains the dynamic key from a computer associated with a trusted-authenticator during the communication between the individual and the entity;

Rreceiving both the static and dynamic keys from the individual; and

Ccreating an authentication request message containing including both the received static and dynamic keys and providing the authentication request message to a computer associated with a trusted-authenticator over the communication network, the computer authenticating the individual based on a combination of the received static and dynamic keys.

27. (Currently Amended) The method of claim 26, wherein the static and dynamic keys contain comprise credentials for verifying the individual's identity.

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

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

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

31. (Currently Amended) The method of claim 26, wherein a computer associated with a first trusted-authenticator calculates the dynamic key and provides ~~it~~ the dynamic key over a communication network to the individual during communication between the individual and the entity ~~for each authentication session~~.

32. (Cancelled) The method of claim 31, the entity creating an authentication request message containing the received static and dynamic keys and providing the authentication request message to the first trusted-authenticator for authentication of the individual.

33. (Cancelled) The method of claim 31, the entity creating an authentication request message containing the received static and dynamic keys and providing the authentication request message to a second trusted-authenticator for authentication of the individual.

34. (Currently Amended) A method for a ~~non-fiduciary~~ website to ~~directly~~ authenticate

an individual over a communication network during a communication session between the individual and the website ~~such that the individual is not redirected to another site and without having previous information about the individual~~, the method comprising:

~~R~~requesting by a computer associated with the website both a static key and a dynamic key from the individual in order to validate the individual's identity; ~~and~~

~~R~~receiving by a computer associated with the website both the static and dynamic keys from the individual, which individual receives the dynamic key during the communication session between the individual and the website; and

~~C~~creating an authentication request message ~~containing~~ including the received static and dynamic keys and providing the authentication request message to a computer associated with a trusted-authenticator over the communication network, the computer authenticating the individual based on the static and dynamic keys.

35. (Currently Amended) The method of claim 34, wherein the static and dynamic keys ~~contain~~ comprise credentials for verifying the individual's identity.

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

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

38. (Currently Amended) The method of claim 34, wherein a computer associated with a

first trusted-authenticator calculates the dynamic key and provides ~~it~~ the dynamic key to the individual during the communication session between the individual and the website ~~for each authentication session~~.

39. (Cancelled) The method of claim 38, the website creating an authentication request message containing the received static and dynamic keys and providing the authentication request message to the first trusted-authenticator for authentication of the individual.

40. (Cancelled) The method of claim 38, the website creating an authentication request message containing the received static and dynamic keys and providing the authentication request message to a second trusted-authenticator for authentication of the individual.

41. (New) A 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 key during authentication of the individual by the entity, which dynamic key was sent to the individual over a communication network by a trusted authenticator in response to a request for a dynamic key 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 by a computer associated with the entity an authentication request to a trusted authenticator to authenticate the individual based on a received static key and a received dynamic key included in the authentication request, wherein said authentication request is sent during

authentication of the individual by the entity; and

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

42. (New) The method according to claim 41, wherein the entity and the trusted authenticator are the same.

43. (New) The method according to claim 41, wherein the entity and the trusted authenticator are different.

44. (New) The method according to claim 41, wherein said dynamic key is calculated by a computer after receiving the request from the individual for the dynamic key.

45. (New) The method according to claim 41, wherein said dynamic key comprises a different value each time the dynamic key is requested by the individual.

46. (New) A 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:

sending a request by a computer for a dynamic key over a communication network to a trusted authenticator during authentication of the individual by the entity;

receiving the dynamic key from the trusted authenticator over a communication network during authentication of the individual by the entity, which dynamic key was calculated by a computer associated with the trusted authenticator during authentication of the individual by the entity;

sending by a computer the dynamic key and a static key during authentication of the individual by the entity for submission to a trusted authenticator and for verification by the trusted authenticator during authentication of the individual by the entity; and

receiving acceptance or denial of authentication from the entity based on verification by the trusted authenticator of the static key and the dynamic key received from the individual during authentication of the individual by the entity.

47. (New) The method according to claim 46, wherein the entity and the trusted authenticator are the same.

48. (New) The method according to claim 46, wherein the entity and the trusted authenticator are different.

49. (New) The method according to claim 46, wherein said dynamic key is calculated by a computer after receiving the request from the individual for the dynamic key.

50. (New) The method according to claim 46, wherein said dynamic key comprises a different value each time the dynamic key is requested for an individual.

51. (New) A method to authenticate an individual during communication between the individual and another entity over a communication network, the method comprising:

receiving by a computer a request for a dynamic key over a communication network, wherein the request is received during authentication of the individual by the entity;

sending the dynamic key by a computer over a communication network to the individual during authentication of the individual by the entity;

receiving an authentication request by a computer from the entity to authenticate the individual based on a static key and a dynamic key 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 received static key and the received dynamic key in response to the authentication request from the entity during the time of authentication of the individual by the entity.

52. (New) The method according to claim 51, further comprising:

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

53. (New) The method according to claim 51, wherein the entity comprises a trusted authenticator.

54. (New) The method according to claim 51, wherein said dynamic key is calculated by a computer after receiving the request for the dynamic key.

55. (New) The method according to claim 51, wherein said dynamic key comprises a different value each time the dynamic key is requested for the individual.

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

said static key comprises the first credential and said dynamic key comprises the second credential;

said dynamic key was calculated and received from a trusted authenticator during said communication between the entity and the individual;

said static key and said dynamic key were received during authentication of the individual by the entity and verified by the trusted authenticator during authentication of the individual by the entity; and

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

57. (New) A method to perform a two-factor authentication of an individual based on a static key as a first credential and a dynamic key as a second credential during communication between the entity and the individual, the method comprising accepting or denying via a computer of a two-factor authentication of the individual based on two credentials received from

the individual, wherein:

said static key comprises the first credential and said dynamic key comprises the second credential;

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

said static key and said dynamic key were received via computer during authentication of the individual by the entity and were verified by a computer associated with the trusted authenticator during said communication between the individual and the entity; and

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

REMARKS

Claims 21-31 and 34-38 were previously pending. Claims 1-20, 32-33 and 39-40 have been previously cancelled without disclaimer of or prejudice to the subject matter contained therein. Claims 21-23, 26-27, 31, 34-35, 38 have been amended to more particularly recite the claimed invention. Claims 24-25, 28-30, 36-37 remain unchanged from previously submitted versions. Claims 41-57 have been added to further define the claimed invention. Claims 21-31 and 34-38 and 41-57 are now pending.

Claims Are Patentable Over Johnson

The Examiner rejected claims 21-31 and 34-38 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,529,885 to Johnson [hereinafter "*Johnson*"]. The Examiner contends that this single reference discloses all of the elements recited in the claims at issue. The Applicant respectfully disagrees with the Examiner's characterization of this reference vis-à-vis the claims at issue and requests reconsideration and withdrawal of the rejection of these claims based on this reference in light of the following remarks.

In support of the Examiner's rejection, he cites the following passages and drawings from *Johnson*, which are reproduced herein for convenience of the reader.

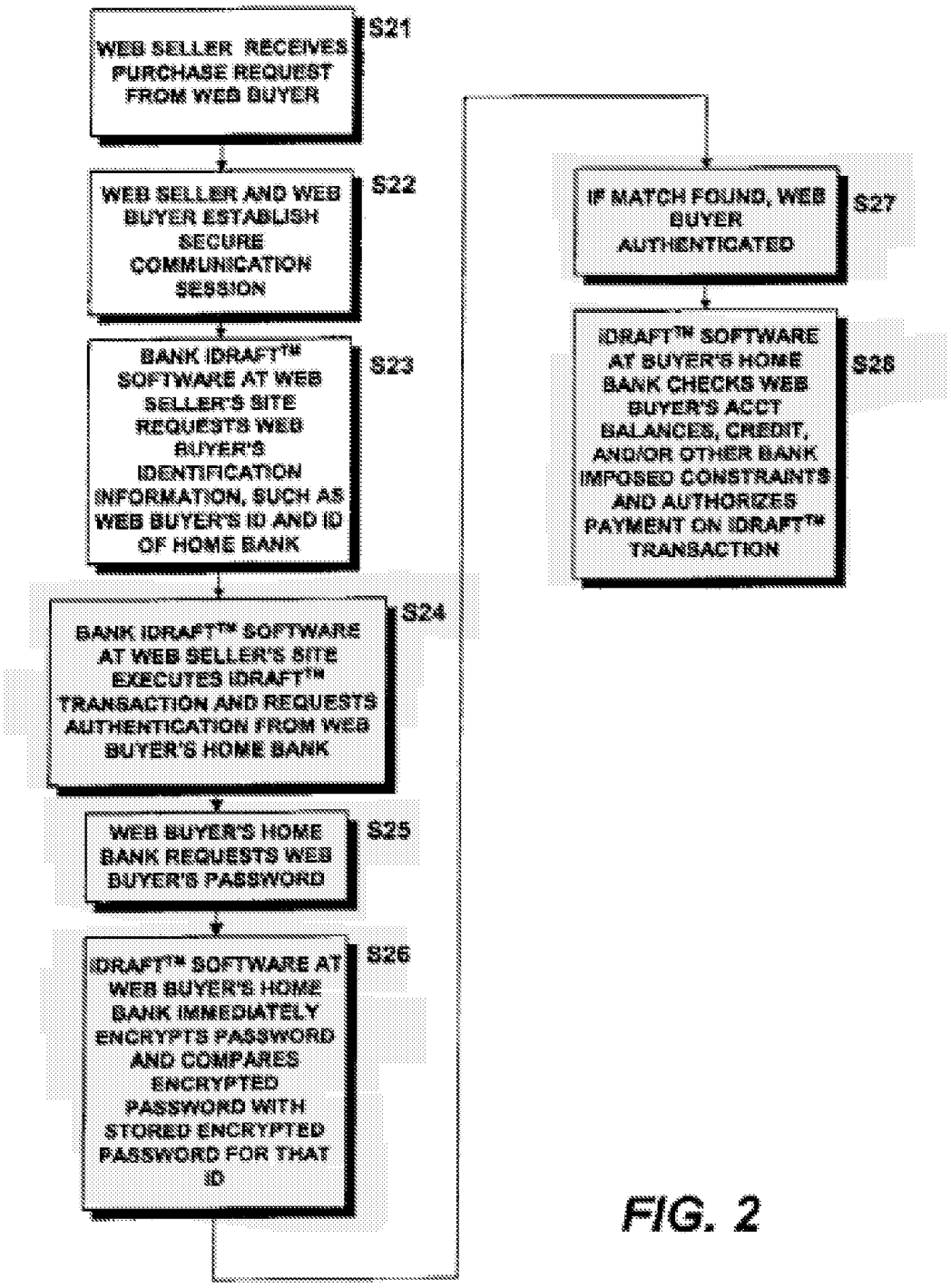
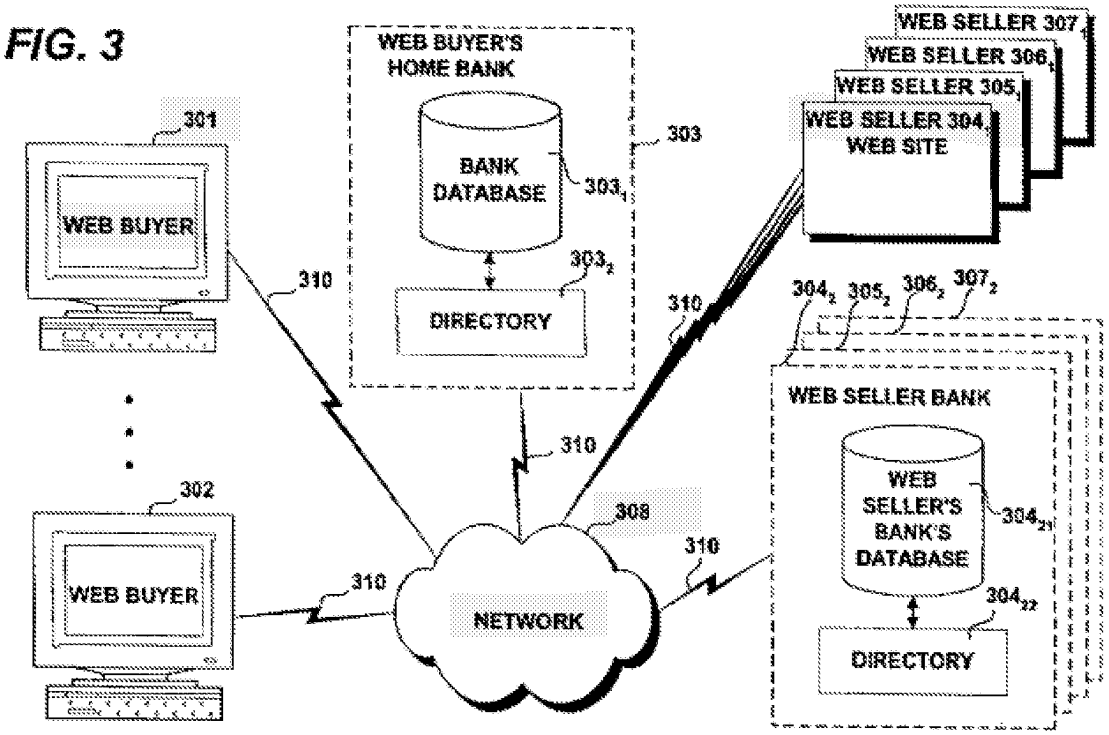

WEB SELLER RECEIVES PURCHASE REQUEST FROM WEB BUYER
S21
WEB SELLER AND WEB BUYER ESTABLISH SECURE COMMUNICATION SESSION
S22
BANK IDRAFT™ SOFTWARE AT WEB SELLER'S SITE REQUESTS WEB BUYER'S IDENTIFICATION INFORMATION, SUCH AS WEB BUYER'S ID AND ID OF HOME BANK
S23
BANK IDRAFT™ SOFTWARE AT WEB SELLER'S SITE EXECUTES IDRAFT™ TRANSACTION AND REQUESTS AUTHENTICATION FROM WEB BUYER'S HOME BANK
S24
WEB BUYER'S HOME BANK REQUESTS WEB BUYER'S PASSWORD
S25
IDRAFT™ SOFTWARE AT WEB BUYER'S HOME BANK IMMEDIATELY ENCRYPTS PASSWORD AND COMPARES ENCRYPTED PASSWORD WITH STORED ENCRYPTED PASSWORD FOR THAT ID
S26
IF MATCH FOUND, WEB BUYER AUTHENTICATED
S27
IDRAFT™ SOFTWARE AT BUYER'S HOME BANK CHECKS WEB BUYER'S ACCT BALANCES, CREDIT, AND/OR OTHER BANK IMPOSED CONSTRAINTS AND AUTHORIZES PAYMENT ON IDRAFT™ TRANSACTION
S28

FIG. 2

FIG. 3



Col. 4, lines 61-67

being a precondition to the bank releasing payment on the draft to a payee of the draft. Each party to the draft requesting access to the computer site is authenticated by encrypting at least a portion of an identification information provided by the requesting party over a secure channel and successfully matching the encrypted identification information with a stored encrypted identifier that is unique to the requesting party. Payment on the draft is released to the

Col. 8, lines 45-57

retinal scans and/or voiceprints, for example. An illustrative embodiment of the present invention is disclosed below wherein the identification information includes the identification string and password pair, it being understood that other identification information (such as biometric data, for example) may be substituted therefor or used in conjunction therewith without departing from the scope of the present invention.

The identification string (hereafter "ID") preferably includes both alphabetical and numerical (alphanumerical) characters and uniquely identifies the draft drawer (such as a Web buyer) from other drawers. The bank may conduct tests to ensure the uniqueness of the ID. Likewise, the password also preferably includes alphanumeric characters.

Col. 8, lines 64-67

including the drawee (such as the bank) and the payees (such as the Web sellers). To insure that the selected passwords remains known only to the Web buyer, the selected password is preferably immediately encrypted upon receipt thereof and stored by the bank only in its encrypted form. This may

Col. 9, lines 9-16

invention, as shown at step S11A. Alternatively, the Web buyer may log onto his or her home bank Web site (or other equivalent bank presence on a public or private network), although some banks may prefer or require the Web buyer to physically visit the bank or branch to fill out the necessary paperwork and obtain an in-person holographic signature. A Web buyer's home bank may be the Web buyer's broker or savings institution, or may be that bank at which he or she maintains a checking account, for example. Preferably, the

Col 9, lines 29-37

Wide Web server of the Web buyer's home bank. Once the Web buyer has reached his or her home bank's Web site (or physically visited the bank and authorized participation in the iDraft™ system according to the present invention), the Web buyer may be assigned an ID and prompted to select a password after filling out any appropriate paperwork or entering the requisite identification information in the fields supplied at the Web buyer's home bank Web site, as outlined at step S12A. Alternatively, the Web buyer may select both

Col. 11, lines 37-41

Preferably, the home bank stores the Web Buyer's ID, encrypted password and other relevant financial and personal information in a data structure managed by Directory software, as shown in the previously-discussed step S13A of FIG. 1A. Directory software typically includes a repository

Col. 12, lines 44-67

for authenticated Web buyers, for example. The Web buyer and the Web seller may then establish a secure communication channel conforming, for example, to the SSL protocol (or some other secure and standardized protocol), as shown in step **S22**. According to step **S23**, the bank iDraft™ software at Web seller's site (maintained and controlled—or caused to be maintained and controlled—by a participating iDraft™ bank, such as the Web seller's home bank, for example) may then request the Web buyer's identification information. Such identification information includes the Web buyer's ID, may include the identification of the Web buyer's home bank (if this is the first time the Web buyer has made a purchase from this Web seller), selected biometric data and/or other security information requested by the Web buyer's home bank. The identification information, however, does not include the Web buyer's password, as such is communicated only to the Web buyer's home bank. The identification information may be sent over the secure communication channel established in step **S22** between the Web buyer's Web-enabled device (such as a personal computer, for example) and the Web Seller's server. As shown in step **S24**, the bank iDraft™ software at Web seller's site receives the Web buyer's identification information and executes an iDraft™ transaction. Before, the iDraft™ transaction is honored by the Web buyer's home bank, however, the Web buyer must be authenticated. For

Col. 13, lines 42-60

Returning now to FIG. **2**, if it is determined that the two encrypted passwords match (and correspond to the proper ID), the Web buyer may be authenticated, as shown at Step **S27**. The Web buyer's home bank may wish to check the now-authenticated Web buyer's current account balances or credit limits before authorizing or releasing payment on the iDraft™ transaction presented to it by the Web seller, as shown in step **S28**. Once payment is released, the Web buyer's account is debited for the amount of purchase (plus any applicable iDraft™ fees from the Web buyer's home bank and/or the Web seller's bank) and the Web seller's account is correspondingly credited for the amount of purchase. Alternatively, a selected payment instrument may be charged with the purchase, as arranged between the Web buyer's home bank and the Web buyer. The Web seller, in this manner, is assured that the Web buyer's home bank will not repudiate the draft (as it has been authorized by an authenticated Web buyer) and that payment on the draft presented to the Web buyer's home bank will be made. If,

Col. 14, lines 5-20

The Web buyer is authenticated by his or her home bank for one session only: the Web buyer will need to be authenticated again the next time he or she logs on to the Web seller's Web site. However, the Web buyer need not necessarily re-enter the identification of his or her home bank the next time he or she purchases an item from that Web Seller. Indeed, the Web seller may store the Web buyer's ID and the identification of the Web buyer's home bank in a master file maintained locally, such as within the Web seller's server. In this manner, the next time the Web buyer visits the Web seller's Web site, the Web seller will know which bank is the Web buyer's home bank and may contact that bank automatically for authentication of a further iDraft™ transaction for the Web buyer's next purchase, assuming the Web buyer has not changed his or her home bank.

The security of the Web buyer's personal and/or financial information, as well as the security of the transaction between the Web buyer and Web seller itself, is assured at several levels. Indeed, all communications involving the

Col. 15, lines 57-60

Directory software. For simplicity of illustration, only the database **304**$_{21}$, and the Directory software **304**$_{22}$ of the Web seller **304**, is shown in FIG. **3**. In the case wherein Web buyer **301** and a Web seller **304**$_1$, for example, share the same home bank **304**$_2$, the Web buyer's home bank **303** may be omitted, all transactions occurring within the bank **304**$_2$.

Col. 15, lines 61-63

be omitted, all transactions occurring within the bank **304**$_2$. That is, the Directory software at Web seller **304**$_1$ causes an LDAP-formatted (for example) query to be sent to the Web seller's (and Web buyer's) home bank **304**$_2$, which query contains the ID of the Web buyer **101** and an identification of the Web buyer **301**'s home bank (in this case, the Web

Col. 16, lines 1-17

301, encrypt it and consult its database **304**$_{21}$ to match the Web buyer **301**'s ID and encrypted password with the stored and encrypted password corresponding to that ID. If a match is found, the Web buyer **301** is authenticated for this transaction only. The Web seller **304**$_1$ and the Web buyer **301**'s home bank **304**$_2$ may, thereafter, check the Web buyer **301**'s accounts to determine whether Web buyer **301** has sufficient funds on deposit to cover the amount of purchase of the iDraft™ transaction and any iDraft™ transaction fees associated therewith. If so, the electronic draft presented by the Web Seller **304**$_1$ to the Web seller's home bank **304**$_2$ for the Web buyer **301**'s purchases will be honored by the parties' common home bank **304**$_2$. That is, a notification may be dispatched to the Web seller **304**$_1$ and/or to the Web buyer **301**, the notification indicating that the bank **304**$_2$ will in fact honor the draft. The Web seller **304**$_1$, thereafter may release the goods or perform the services in question with complete assurance that it will be paid therefor.

Col. 19, line 58-col. 20, line 10

According to the present invention, the trusted party (most often the party's home bank) determines the levels of documented identification necessary to support authentication of the notified party to the iTX transaction **500**. The visit to the trusted party may be carried out physically (in person) or may be carried out by visiting the trusted party's Web site and providing evidence of identity, to the satisfaction of the trusted party. Each of the notified parties to the iTX transaction **500**, therefore, may receive a unique ID and may select or be assigned a password, in the manner described above. Alternatively, biometric data or bank-controlled certificates may supplant or supplement the ID-password combination. Indeed, additional advanced security measure

(such as the use of certificates, for example) may be required in the buyer-seller-bank relationship when, for example, large sums of money are transferred via iDraft™ or iDraft-C™ transactions or any other instance wherein the bank requires added measures of security. Such certificates may then be one-time, transaction-specific certificates authorizing the transaction or may be multiple time certificates applied in special circumstances to determine the limits of the transactions. External certificates may unduly burden the free flow of normal e-commerce and their use, preferably, should be relegated to special circumstances. The external certificate (and/or other security measures agreed upon between the iDraft™ bank—or other trusted party as defined above—and the customer), when used, should be provided by the iDraft™ bank to the customer and must be implemented in addition to the authentication of the customer according to the present invention, and not as a substitution therefor.

According to an embodiment of the present invention, should any of the constituent iDraft™ or iDraft-C™ transactions of the iTX transaction **500** (such as the iDraft™ transactions **410**, **420**, **430** or any of the iDraft-C™ transactions **440**, **450** of FIG. **5**) fail, the iTX **500** itself fails with notice to all parties to the transaction. The iDraft™ trans-

A thorough review of these citations fails to find each and every element arranged as in the claims as required by the case law on anticipation.

Background on Anticipation

To anticipate a claim, a single prior art reference must expressly or inherently disclose each claim limitation. But disclosure of each claim element is not quite enough … anticipation requires the presence in a single prior art disclosure of all elements of a claimed invention *arranged as in the claims*. *Finisar v. DirecTV*, 523 F.3d 1323, 1334 (Fed. Cir. 2008) [emphasis supplied].

The reference must enable one to make the claimed invention without further research or experimentation. *In re Hall*, 781 F.2d 897, 899 (Fed. Cir. 1986). The disclosure in an assertedly anticipating reference must be adequate to enable possession of the desired subject matter. *It is insufficient to name or describe the desired subject matter*, if it cannot be produced without undue experimentation. *Elan Pharmaceuticals, Inc. v. Mayo Foundation for Medical Educ. and Research*, 346 F.3d 1051, 1055 (Fed. Cir. 2003) [emphasis supplied].

***Johnson* Fails to Teach Each Element Arranged as in the Claims**

For example, with regard to the independent claim 21, this claim recites "receiving … a request to generate a dynamic key for the individual … during authentication of the individual by the entity." The claims and the specification make clear that the inventive and claimed method comprises a real-time authentication process that operates during a communication session between an individual and an entity, such as an online business transaction. Each of the claims include recitations with this subject matter.

But *Johnson* fails to disclose *inter alia* this element arranged as in the claims. In *Johnson* no dynamic key is sent to the individual while the individual remains in communications with an entity attempting authenticate the individual. Moreover, in *Johnson* no static and dynamic key

are then used by the entity during this authentication attempt. Rather, in *Johnson*, the user merely sends static information to the Web seller, such as:

> the web buyer's identification information. Such identification information includes the Web buyer's ID, may include the identification of the Web buyer's home bank (if this is the first time the Web buyer has made a purchase from the Web seller), selected biometric data and/or other security information requested by the Web buyer's home bank. The identification information, however, does not include the Web buyer's password, as such is communicated only to the Web buyer's home bank.

Col. 12, lines 51-58.

In contrast, in the present invention two pieces of information are used by the entity requesting authentication, such as a Web seller, *i.e.,* the static key and the dynamic key, which dynamic key is provided during the communication session with the entity. The specification of the present invention defines the static key at page 18 as follows:

> The use of "static key" refers to pre-shared information between both the individual **10** and the individual's trusted-authenticator **30**. The static key of an individual **10** is fixed information that does not change automatically and is used for authentication purposes. A static key might be any identification phrases such as password, name, Username, SSN, alias, account number, customer number, etc. or the combination of this information.

Subsequently, the same specification defines the dynamic key as follows:

> The use of "dynamic key" refers to SecureCode which is a key or information that is variable and is provided to the individual **10** by the individual's trusted-authenticator **30** at the time it is needed for authentication. The dynamic key is an alphanumeric code and will have a different value each time the individual receives it from his/her trusted-authenticator **30** for authentication purposes. To increase security a dynamic key may have a non-repeating value, may be time dependent (valid for some period of time) and may be in an encrypted format.

Spec., page 18.

Simply put, *Johnson* fails to disclose the dynamic key as arranged in the claims because *Johnson* fails to disclose a dynamic key that is provided *at the time the dynamic key is needed for authentication*.

Examiner's Comments in Advisory Action Dated April 13, 2010

The Examiner contends that a certificate established by the bank in the Web buyer's computer constitutes a dynamic key as described in the present application. With all due respect, a certificate as taught by *Johnson* is not a dynamic key. *See Aff., ¶6-10.* A certificate as described in *Johnson* cannot be issued in real time, as there are manual steps involved in creating such a certificate, which prevents the issuance of such certificates in real-time or while a user is in communication with another entity. *See Aff., ¶8.* A certificate as described in *Johnson* must be installed in a user's computer, whereas a dynamic key need not be installed. *See Aff., ¶9.* In short, a certificate as described in *Johnson* is not equivalent to the dynamic key disclosed and claimed in the present application. In fact, *Johnson* recognizes that a certificate is not generated in real-time because *Johnson* states that "External certificates may unduly burden the free flow of normal e-commerce and their use, preferably, should be relegated to special circumstances." *Col. 20, lines 9-11.* This statement from *Johnson* recognizes that obtaining a certificate requires a time delay and therefore would unduly burden the free flow of normal e-commerce, which occurs rapidly or in real-time. *See Aff., ¶10.*

But as anticipation requires that each element be found in the prior art reference as arranged in the claims, *Johnson* fails to anticipate the claims because *Johnson* never teaches the concept of the use of a dynamic key obtained during a communication session between the

individual and the entity as arranged in the claims. Thus, *Johnson* fails to anticipate or render obvious the claims at issue.

All pending claims are patentable over *Johnson* for at least this reason. Therefore, the Applicants respectfully request reconsideration and withdrawal of the rejection of the claims at issue based on *Johnson.*

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: June 8, 2010
Michael P. Fortkort (Reg. No. 35,141)

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

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

Electronic 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:	

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	13	26	338
Independent claims in excess of 3	2201	5	110	550
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Extension - 3 months with $0 paid	2253	1	555	555
Miscellaneous:				
Request for continued examination	2801	1	405	405
		Total in USD ($)		**1848**

Electronic Acknowledgement Receipt	
EFS ID:	7770559
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:	
Receipt Date:	08-JUN-2010
Filing Date:	18-JAN-2006
Time Stamp:	16:47:52
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$1848
RAM confirmation Number	3564
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	Rule 130, 131 or 132 Affidavits	Affidavit_060810.pdf	1893156 896f625744e925304a181e9508c426d8ad29f6aa	no	3
Warnings:					
Information:					
2	Request for Continued Examination (RCE)	rce_060810.pdf	798117 831ae03dbdeed9a7560a2d864e0450ffb652a991	no	3
Warnings:					
Information:					
3	Amendment Submitted/Entered with Filing of CPA/RCE	Response_to_OA_mailed_120809_in_11333400_filed_060810.pdf	709119 759b8702b1eaa7fd267353ff47f4bfc01e56aad3	no	28
Warnings:					
Information:					
4	Fee Worksheet (PTO-875)	fee-info.pdf	34848 0e2e432616c8cb491f5f1ba06b0021f6dec91e17	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	3435240		

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 June 8, 2010 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: June 8, 2010 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 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 December 8, 2009 which finally rejected the pending claims, and the Advisory Action mailed April 13, 2010, which affirmed the continued rejection of those 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 this Application, which is the subject of the present proceeding.

2. I have a degree in computer science from Technical University of Vienna in 1993. I have been working in the field of authentication over communication networks since 2000.

3. I am familiar with the specification and claims of the present Application as pending and as amended in accordance with a response filed concurrently herewith.

4. I have reviewed the art cited by the Examiner in the present proceeding and in particular, U.S. Patent No. 6,529,885 (*Johnson*).

5. I am one of skill in the art of authentication, and as such, I am familiar with obtaining and using a certificate as described in *Johnson*.

6. With respect to the Examiner's rejection of the pending claims under 35 U.S.C. § 102(e) as being anticipated by *Johnson*, I disagree that the invention is disclosed in this reference for a variety of reasons, but at a minimum *Johnson* does not teach or suggest the use of a dynamic key as disclosed and claimed in the present Application.

7. One of skill in the art would not consider a certificate as described in *Johnson* to be the same or equivalent to a dynamic key as described in the present Application, as they are quite different.

8. One of skill in the art would understand that a certificate as described in *Johnson* cannot be issued in real time, as there are manual steps involved in validating the request and creating a certificate (Certificate Authority needs to verify and validate individual's identity before issuing a certificate), which prevents the issuance of such in real-time or while a user is in communication with another entity.

9. One of skill in the art would understand that a certificate as described in *Johnson* must be installed in a user's computer, whereas a dynamic key as described in the present invention need not be installed.

10. One of skill in the art upon reading *Johnson* would understand that a certificate as described in *Johnson* is not generated in real-time because *Johnson* states that "External certificates may unduly burden the free flow of normal e-commerce and their use, preferably, should be relegated to special circumstances." *Col. 20, lines 9-11*. One of skill in the art would understand that this statement means that obtaining a certificate requires a time delay and therefore would unduly burden the free flow of normal e-commerce, which occurs rapidly or in real-time.

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.

In witness whereof,

Nader Asghari-Kamrani

06/08/2010
Date

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 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

		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
AMENDMENT	**06/08/2010**	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	** 26	= 11	X $26 =	286	OR	X $ =	
	Independent (37 CFR 1.16(h))	* 8	Minus	***3	= 5	X $110 =	550	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	836	OR	TOTAL ADD'L FEE	

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

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

Legal Instrument Examiner:
/CATHERINE d. SMITH/

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/333,400	01/18/2006	Nader Asghari-Kamrani	

CONFIRMATION NO. 4456

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

POA ACCEPTANCE LETTER

OC000000041731527

Date Mailed: 05/24/2010

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 05/14/2010.

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

/llam/

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

PTO/SB/81 (01-09)
Approved for use through 11/30/2011. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

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

Application Number	11/333,400
Filing Date	January 18, 2006
First Named Inventor	ASGHARI-KAMRANI, NADER
Title	DIRECT AUTHENTICATION SYSTEM AND
Art Unit	2132
Examiner Name	NOBAHAR, A.
Attorney Docket Number	

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

☐ A Power of Attorney is submitted herewith.

OR

☒ I hereby appoint Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith: **58,293**

OR

☒ I hereby appoint Practitioner(s) named below as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith:

Practitioner(s) Name	Registration Number
Michael P. Fortkort	35,141
John A. Fortkort	38,454

Please recognize or change the correspondence address for the above-identified application to:

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

OR

☐ The address associated with Customer Number:

OR

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

I am the:

☒ Applicant/Inventor.

OR

☐ Assignee of record of the entire interest. See 37 CFR 3.71.
Statement under 37 CFR 3.73(b) (Form PTO/SB/96) submitted herewith or filed on _____

SIGNATURE of Applicant or Assignee of Record

Signature		Date	MAY 14, 2010
Name	NADER ASGHARI-KAMRANI	Telephone	703-410-8030
Title and Company	INVENTOR		

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☒ *Total of 2 forms are submitted.

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

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

PTO/SB/81 (01-09)
Approved for use through 11/30/2011. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

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

Application Number	11/333,400
Filing Date	January 18, 2006
First Named Inventor	ASGHARI-KAMRANI, NADER
Title	DIRECT AUTHENTICATION SYSTEM AND
Art Unit	2132
Examiner Name	NOBAHAR, A.
Attorney Docket Number	

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

☐ A Power of Attorney is submitted herewith.

OR

☒ I hereby appoint Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith:

58,293

OR

☒ I hereby appoint Practitioner(s) named below as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith:

Practitioner(s) Name	Registration Number
Michael P. Fortkort	35,141
John A. Fortkort	38,454

Please recognize or change the correspondence address for the above-identified application to:

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

OR

☐ The address associated with Customer Number:

OR

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

I am the:

☒ Applicant/Inventor.

OR

☐ Assignee of record of the entire interest. See 37 CFR 3.71.
Statement under 37 CFR 3.73(b) (Form PTO/SB/96) submitted herewith or filed on _____

SIGNATURE of Applicant or Assignee of Record

Signature		Date	MAY 14, 2010
Name	KAMRAN ASGHARI-KAMRANI	Telephone	703-220-3863
Title and Company	INVENTOR		

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☒ *Total of 2 forms are submitted.

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

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

Electronic Acknowledgement Receipt	
EFS ID:	7617314
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
Correspondence Address:	Nader Asghari-Kamrani - 6558 Palisades Drive - Centreville VA 20121 US 7032225104 kamrani@delphinustechnology.com
Filer:	Michael P. Fortkort
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	14-MAY-2010
Filing Date:	18-JAN-2006
Time Stamp:	16:51:25
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Power of Attorney	POA-for-11333400.pdf	116971 035f61c8cd0ee9f1e0eb6d6e2f63aad3db29b0ef	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	116971		

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		4456

7590 04/13/2010

Nader Asghari-Kamrani
6558 Palisades Drive
Centreville, VA 20121

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
04/13/2010	PAPER

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

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

Advisory Action Before the Filing of an Appeal Brief	**Application No.** 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 08 March 2010 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:
   a) ☒ The period for reply expires *3* months from the mailing date of the final rejection.
   b) ☐ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

   Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   (a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
   (b) ☐ They raise the issue of new matter (see NOTE below);
   (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: _____. (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 and 34-38*.
   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

/A. N./
Examiner, Art Unit 2432

Continuation of 11. does NOT place the application in condition for allowance because: The applicats arguments filed on 03/08/2010 are not pursvasive because Johnson teaches foundamentally and substantially the same as the instant invention. Johnson teaches a method that allows a buyer to carry out online financial transaction via, for example, Internet. The buyer which maintains an account with his bank (see Summary, para 23) in one embodiment receives a certificate from his bank (see Detailed Description, para 8, bank establishes a certificate in the buyer's computerer) based on a web seller requirement (see col. 12 , lines 44-67 col. 14 , lines 5-20). The certificate is dynamic and the buyer ID is static (see Summary, para 19, col. 12, lines 46-62 and col. 19, line 65-col. 20, line 9). Johnson also teaches that the web buyer provides his information including ID and one-time certificate to the web seller (see, e.g., col. 12, lines 42-56, col. 19, line 58-col. 20, line 18 and Fig. 2, step S23). Johnson further teaches that after the web buyer is authenticated and his account is checked by the home bank for enough funds the web seller provides goods or services to the web buyer (see Figs. 2, steps 24-28 and 3 and col. 16, lines 1-17). Therefore, the teachings of Johnson meet the limitations of the instant invention..

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Nader Ashgari-Kamrani et al.

Application No.: 11/333,400 Confirmation No.: 4456

Filed: 01/18/2006 Art Unit: 2132

For: Direct Authentication System and Method via Trusted Authenticators Examiner: A. Nobahar

OK to enter
/a.n./ 04/10/2010

REMARKS

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

INTRODUCTORY COMMENTS

In response to the Final Office Action mailed 12/08/2009, the Applicants respectfully request reconsideration based on the remarks which follow.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Nader Ashgari-Kamrani et al.

Application No.: 11/333,400 Confirmation No.: 4456

Filed: 01/18/2006 Art Unit: 2132

For: Direct Authentication System and Method via Trusted Authenticators Examiner: A. Nobahar

REMARKS

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

INTRODUCTORY COMMENTS

In response to the Final Office Action mailed 12/08/2009, the Applicants respectfully request reconsideration based on the remarks which follow.

In the claims:

21. (Previously Presented) A method for a non-fiduciary business, organization, or another individual to directly authenticate an individual over a communication network without redirecting the individual to another site and without having previous information about the individual, the method comprising:

The individual communicating with the business, organization, or another individual;

The business, organization, or another individual communicating a request for both a static key and a dynamic key from the individual;

In response to the business, organization, or another individual's request, the individual communicating a request for a dynamic key from a first trusted-authenticator;

In response to the individual's request, the first trusted-authenticator calculating a dynamic key and providing it to the individual;

The individual providing a combination of the calculated dynamic key and an existing static key to the business, organization, or another individual;

The business, organization, or another individual constructing an authentication request message containing the static and dynamic keys and communicating the authentication request message to a computer associated with a second trusted-authenticator over the communication network; and

The second trusted-authenticator computer verifying the individual's identity based on the static and dynamic keys and sending a confirmation or denial authentication message to the business, organization, or another individual.

22. (Previously Presented) The method of claim 21, wherein the first and second trusted-authenticator are the same.

23. (Previously Presented) The method of claim 21, wherein the first and second trusted-authenticator are different.

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

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

26. (Previously Presented) A method for a non-fiduciary entity to directly authenticate an individual over a communication network without redirecting the individual to another site and without having previous information about the individual, the method comprising:

Requesting both a static key and a dynamic key from the individual in order to validate the individual's identity;

Receiving both the static and dynamic keys from the individual; and

Creating an authentication request message containing the received static and dynamic keys and providing the authentication request message to a computer associated with a trusted-authenticator over the communication network, the computer authenticating the individual based on a combination of the received static and dynamic keys.

27. (Previously Presented) The method of claim 26, wherein the static and dynamic keys contain credentials for verifying the individual's identity.

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

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

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

31. (Previously Presented) The method of claim 26, wherein a first trusted-authenticator calculates the dynamic key and provides it to the individual for each authentication session.

32. (Cancelled) The method of claim 31, the entity creating an authentication request message containing the received static and dynamic keys and providing the authentication request message to the first trusted-authenticator for authentication of the individual.

33. (Cancelled) The method of claim 31, the entity creating an authentication request message containing the received static and dynamic keys and providing the authentication request message to a second trusted-authenticator for authentication of the individual.

34. (Previously Presented) A method for a non-fiduciary website to directly authenticate an individual over a communication network such that the individual is not redirected to another site and without having previous information about the individual, the method comprising:

Requesting both a static key and a dynamic key from the individual in order to validate the individual's identity; and

Receiving both the static and dynamic keys from the individual; and

Creating an authentication request message containing the received static and dynamic keys and providing the authentication request message to a computer associated with a trusted-authenticator over the communication network, the computer authenticating the individual based on the static and dynamic keys.

35. (Previously Presented) The method of claim 34, wherein the static and dynamic keys contain credentials for verifying the individual's identity.

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

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

38. (Previously Presented) The method of claim 34, wherein a first-trusted authenticator calculates the dynamic key and provides it to the individual for each authentication session.

39. (Cancelled) The method of claim 38, the website creating an authentication request message containing the received static and dynamic keys and providing the authentication request message to the first trusted-authenticator for authentication of the individual.

40. (Cancelled) The method of claim 38, the website creating an authentication request message containing the received static and dynamic keys and providing the authentication request message to a second trusted-authenticator for authentication of the individual.

REMARKS

Claims 21-31 and 34-38 are currently pending. Claims 21-31 and 34-38 stand rejected. Applicant respectfully requests reconsideration based on the remarks which follow.

I. The Applicant thanks the Office for the careful examination of the present application. However, the Applicant believes that there remains slight – yet significant - confusion on the part of the Office as to what elements are communicated between particular entities in Johnson (US Patent No. 6,529,885) (herein "Johnson") and the invention as claimed. Based on this confusion, a Final Office Action was issued and the previous rejection maintained for the following reasons:

1. Concerning the Applicant's argument that **Johnson submits the cited password or certificate to the bank – not to the seller**, the Office disagreed and incorrectly asserted, without basis, that: "Johnson discloses that in one alternative the bank may provide to the buyer a certificate to submit to the seller." (Final Office Action, page 2).

2. Concerning the Applicant's argument that **Johnson makes it clear that the buyer's personal information (required for authentication) is never communicated to the seller**, the Office disagreed and incorrectly asserted, without basis, that: "Johnson … describes the use of a password for authenticating the buyer by the bank. The authentication of the buyer is

performed *in addition to the aforementioned certificate and ID submitted to the seller by the buyer*" (emphasis added). (Final Office Action, page 3).

3. Concerning the Applicant's argument that **the seller of Johnson must *redirect* the buyer to the bank for authentication**, the Office disagreed and instead incorrectly asserted, without basis, that: "authentication of the buyer is performed through the buyer-seller-bank communication channel not redirected through a separate communication channel." (Final Office Action, page 3).

II. The "Johnson" reference

Johnson is generally directed to a system and method for carrying out Directory-Authenticated electronic transactions. It is firstly noted Johnson operates such that certain elements (User ID, password) are communicated during different communication sessions. For example, Figure 2 of Johnson shows where the user ID is submitted during a communication session between the buyer and seller, and the password is submitted during another communication session between the home bank and buyer. It is secondly noted that in addition to the above types of transactions, Johnson addresses another embodiment involving "iTX" transactions. See generally, Figures 4-6. According to the iTX embodiment, each party to a transaction (buyer, seller, other interested parties) is authenticated to a "central trusted party" via a password (and in some cases, a supplemental certificate).

A. Different Communication Sessions

Figure 2 of Johnson (as annotated by the Applicant below) indicates three different communication sessions[1]: 1) between the buyer and seller (S21-23); 2) between the seller and home bank (S24); and 3) between the home bank and buyer (S25-28).

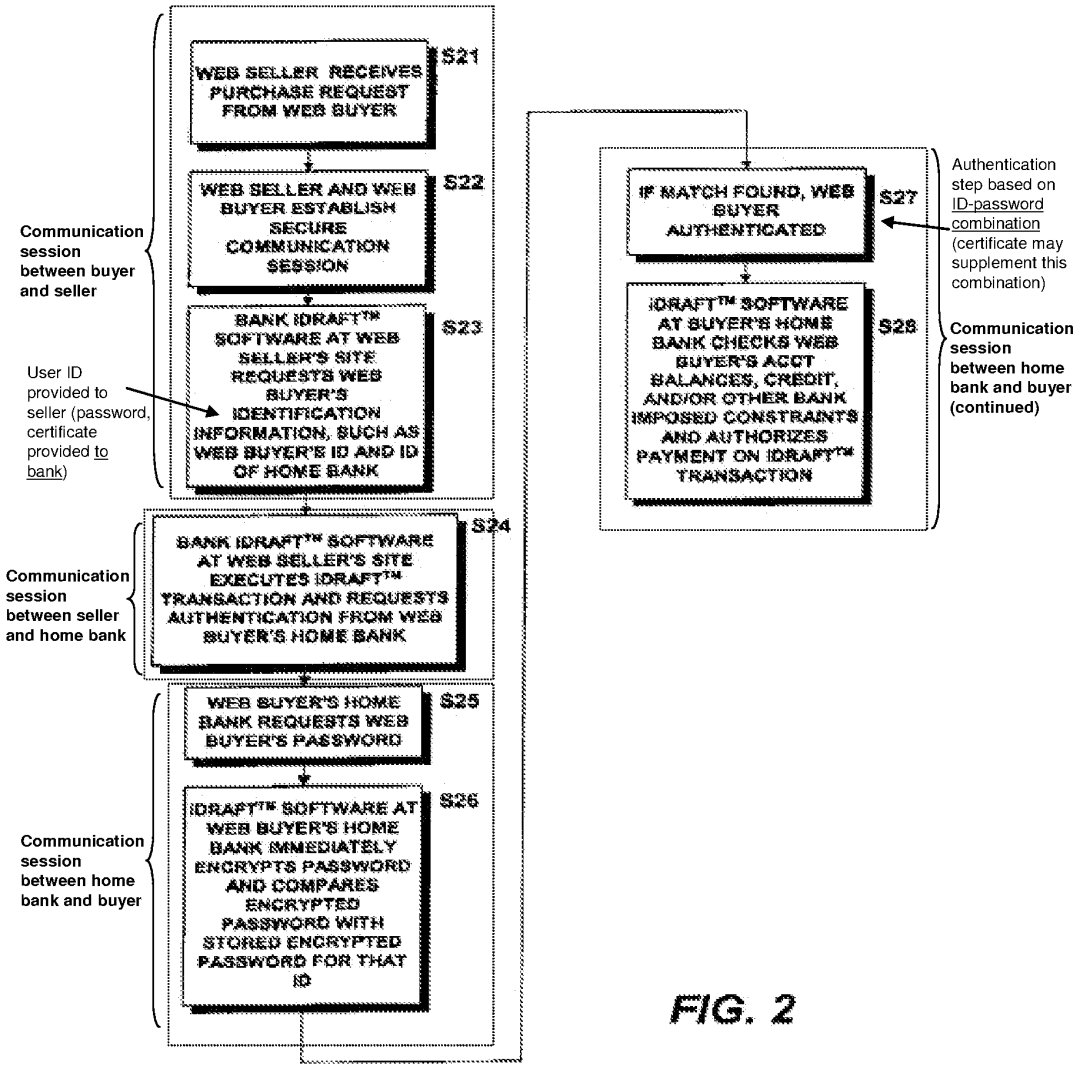


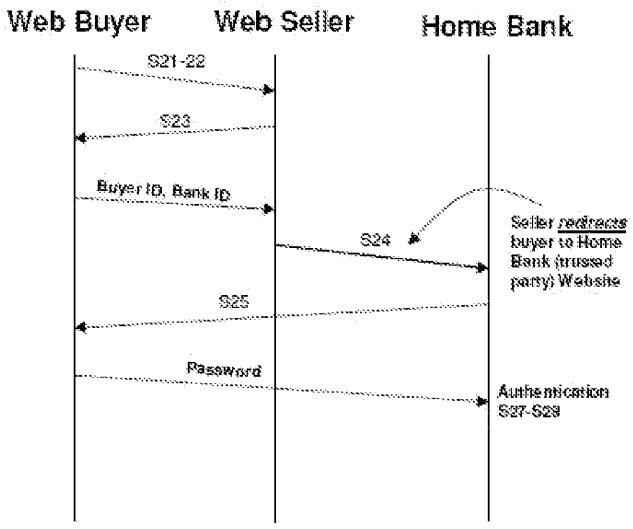
FIG. 2

[1] It is commonly appreciated in the art that an Internet communication session involves a source IP address, destination IP address, source port, and destination port.

In particular, a first communication session is established between the buyer and seller in blocks S21-S23 (see, col. 12 lines 60-62, where a communication channel is established between the Web buyer's computer and the Web seller's server). Step S23 shows where static identification information is provided to the seller, such as web buyer's ID and home bank ID. *Nowhere in steps S21-S23 does Johnson teach or even suggest that a one-time certificate (or a dynamic key for that matter) is provided to the seller.*

Step S24 indicates another communication session between the seller and home bank. According to this step, the Web seller's server submits an authentication request to the home bank and subsequently must redirect the buyer to the home bank server – forming yet another communication session involving the home bank's IP address (see, e.g., col. 15 lines 42-45, where the home bank server 303 is connected to the network 308; and col. 13 lines 1-3, where the Web seller connects the Web buyer with his or her home bank). Thus, it is not until a communication session is established between the home bank's server and the buyer's computer in steps S25-S28, that the buyer submits a password to the home bank for authentication (See, col. 13 lines 6-8, where the Web buyer's home bank requests the Web buyer's password from the buyer).

Below is another illustration provided by the Applicant to better explain the above communication sessions of Johnson:



This figure better illustrates how the Web seller must redirect the web buyer to the destination IP address of the home bank server in step S24. In response to the home bank's request in step S25, the buyer provides his password to the home bank. Thus, authentication is based on information that the buyer provides to the bank (a fiduciary entity) as a result of having been redirected by the seller.

B. "iTX" embodiment

In addition to basic transactions, Johnson addresses an embodiment involving complex transactions where each party to a transaction (buyer, seller, etc.) is authenticated to a "central trusted party" (e.g., a fiduciary entity such as the web buyer's home bank 303, see e.g., col. 4 lines 54-57 and col. 19 lines 55-56). (See also, col. 18 lines 2-6, where each party to the iTX must be authenticated). Figures 4-6 of Johnson show an iTX embodiment that may

include a number of iDraft transactions. Each party to the transaction - whether it be a buyer, seller, or other interested parties - are notified of their requested participation (e.g., via email). Upon notification, each party must preferably take steps to be authenticated to the central trusted party by the iDraft system (col. 19 lines 41-44).

In column 19 lines 55-58, Johnson states that the central trusted party determines the levels of documented identification necessary to support authentication of the notified party to the iTX transaction. *It is in this paragraph and this context only* (i.e., of authentication of each party to the trusted party), that Johnson states in addition to an ID and password, certificates may be used. See col. 19 line 41 – col. 20 line 18. Therefore, the only use of certificates disclosed or even contemplated by Johnson are within the context of authentication in the iTX system. Thus, according to the iTX framework, all parties (buyers, sellers, etc.) are authenticated by, and communicate through, a central trusted party – not directly with one another.

III. Response to Final Rejection

In response to the Office's first incorrect assertion set forth in paragraph I. above, the Applicant maintains nowhere does Johnson teach or even suggest that the buyer submits a certificate to the seller. As explained above, the buyer submits a password (or supplemental certificate) only to the trusted party (i.e., bank) within the context of an iTX transaction. If the Office continues to maintain its assertion, the Applicant respectfully requests that the Office specifically and

particularly point out where Johnson teaches that the buyer submits a certificate to the seller. If the Office is not able to provide this evidence, or is relying on teachings other than Johnson, the Applicant points out that both the 102(e) rejection and Final Office Action are improper and respectfully request that they be withdrawn.

In response to the Office's second incorrect assertion above, nowhere does Johnson teach or suggest that "authentication of the buyer is performed in addition to the aforementioned certificate and ID submitted to the seller by the buyer." As explained in the previous paragraphs, the buyer does not submit a certificate to the seller. Rather, the certificate is only used within the context of authenticating oneself to a central trusted party in an iTX transaction. In particular, Johnson clearly teaches that a certificate may be used to supplant or supplement an ID-password combination. See col. 19 lines 65-67. However, the Applicant points out that the only entity with access to the ID-password combination is the home bank (see col. 5 lines 14-17, where each encrypted identifier may include an ID and encrypted password pair, the pair being stored in a data structure controlled by the *bank* and managed by Directory software). Thus, according to Johnson's own disclosure, it would not make sense to submit a certificate to the seller, since this information would only "supplement" the buyer's ID – not the ID-password combination. Since the password is not provided to the bank until steps S26-S27, a certificate - used to supplant or supplement the ID-password combination - would thus have to be communicated to the home bank.

In response to the Office's third incorrect assertion above, the Applicant points out that a buyer-seller-bank *relationship* is not the same as a buyer-seller-bank *communication channel*. While Johnson mentions a buyer-seller-bank relationship, nowhere does Johnson teach or even suggest that the buyer, seller and home bank share some sort of common communication channel. Rather what Johnson indicates is quite the opposite. Johnson clearly states that the buyer's password is only communicated to the home bank – not to the seller (see, e.g., col. 12 lines 57-59). However, this statement of Johnson could not hold true if the buyer, seller and bank shared a common buyer-seller-bank communication channel as asserted by the Office.

Because the Office has issued a Final rejection based upon the above incorrect premises, the Applicant respectfully requests that the Final rejection be withdrawn. In addition to the above remarks, the Applicant maintains the previous arguments:

I*V. Rejections Under 35 U.S.C. § 102(e)*

As previously established, the business, organization, or another individual is a non-fiduciary entity. Thus, the business, organization, or another individual disclosed in the present specification is *different* from the trusted-authenticator.

Accordingly, claim 21 recites *inter alia*, "[a] method for a non-fiduciary business, organization or another individual to directly authenticate an individual," "[t]he individual providing a combination of the calculated dynamic key and an existing static key to the business, organization, or another individual," and "[t]he business, organization, or another individual constructing an authentication request message containing the static and dynamic keys and communicating the authentication request message to a computer associated with a second trusted authenticator."

Claims 26 and 34 recite similar limitations - the business, organization, or another individual - or website, respectively "[c]reating an authentication request message containing the received static and dynamic keys and providing the authentication request message to a computer associated with a trusted-authenticator."

Applicant respectfully submits that the above limitations are not taught or even remotely suggested by Johnson as required by 35 USC § 102(e) or § 103(a).

In contrast to the claimed invention, Johnson discloses that a fiduciary, or trusted, entity (bank or government institution) is required to receive the buyer's password, certificate, etc. **Johnson is completely silent regarding the buyer submitting a dynamic key to the seller**. This is because the entire password-based authentication framework of Johnson *necessitates* authentication to take

place on the "front-end" (i.e., via a trusted party). Johnson does not envision a "back-end" authentication framework - where a non-fiduciary business, organization, or another individual receives and *then* submits an individual's static and dynamic keys to a trusted-authority for authentication – as disclosed by the present invention. In fact, Johnson makes it clear that the buyer's personal information (required for authentication) is never communicated to the seller (col. 12 lines 56-58). Thus, Johnson cannot teach or suggest a non-fiduciary entity generating an authentication request message containing both static and dynamic keys as claimed.

Moreover, the "front-end" authentication framework of Johnson precludes the *seller* from directly authenticating the buyer. This is because **the seller of Johnson is required to redirect the buyer to the bank for authentication** (see, col. 12 line 65 – col. 13 line 3, where the web seller causes the web buyer to be connected to their home bank for authentication). However, such redirection undesirably increases security risks because redirecting the customer to another site increases the likelihood of phishing and pharming attacks.

In contrast to Johnson, present claims 21, 26 and 34 state that the business, organization, or another individual directly authenticates the individual. In other words, the present invention provides a "back-end" authentication framework which allows the combined static and dynamic keys to be directly communicated to the business, organization, or another individual. In turn, the business, organization, or another individual then submits an authentication request message containing the keys to a trusted-authority for authentication. As

a result, an individual shopping online can conveniently and securely submit their static and dynamic keys directly to the online merchant without being redirected to another website for authentication, or having to first enter a secure portal. Consequently, the possibility of phishing and pharming attacks are avoided and security is further improved.

For at least the above reasons, Applicant submits that Johnson fails to anticipate independent claims 21, 26, and 34 as well as their dependent claims under 35 USC 102(e) and respectfully request that the rejection of claims 21-31, and 34-38 be withdrawn and the claims allowed.

V. Conclusion

Since it is believed that all aspects of the rejections set forth in the Final Office Action mailed 12/08/2009 have been addressed and overcome, Applicants' submit that the present application is now in condition for allowance. If the examiner believes that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at (571) 228-2938.

Dated: 03/08/2010

Respectfully submitted,

/Shawna J. Shaw/

Shawna J. Shaw

Agent for Applicants
Registration No. 57,091

Electronic Acknowledgement Receipt	
EFS ID:	7157803
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
Correspondence Address:	Nader Asghari-Kamrani - 6558 Palisades Drive - Centreville VA 20121 US 7032225104 kamrani@delphinustechnology.com
Filer:	Shawna Jeannine Shaw
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	08-MAR-2010
Filing Date:	18-JAN-2006
Time Stamp:	11:19:58
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	Claims	11333400_claims.pdf	24245 d1523186a77442b15f02262f2da7aed25b601e47	no	5
Warnings:					
Information:					
2	Applicant Arguments/Remarks Made in an Amendment	11333400_Remarks.pdf	440552 ac04719206a00380adf485e9ea03063384b8f2dd	no	12
Warnings:					
Information:					
		Total Files Size (in bytes):	464797		

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

		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
AMENDMENT	**03/08/2010**	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 20	Minus	** 20	= 0	X $26 =	0	OR	X $ =	
	Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $110 =	0	OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

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

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

Legal Instrument Examiner:
/TONGELINA TUBBS/

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		4456

7590 12/08/2009

Nader Asghari-Kamrani
6558 Palisades Drive
Centreville, VA 20121

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	PAPER NUMBER
2432	
MAIL DATE	DELIVERY MODE
12/08/2009	PAPER

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

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

Office Action Summary	Application No.	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 *22 September 2009*.

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

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

Disposition of Claims

4)☒ Claim(s) *21-31 and 34-38* 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* 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 09/22/2009.

2. Claims 21-31 and 34-38 are pending.

Response to Arguments

Applicant's arguments have been fully considered but they are not persuasive.

Applicants on page 8 of the remark argue that Johnson is completely silent regarding the buyer submitting a dynamic key to the seller.

Examiner respectfully disagrees and asserts that Johnson discloses that in one alternative the bank may provide to the buyer a certificate to submit to the seller. The certificate may be a one-time, transaction-specific certificate authorizing a transaction and is used in the buyer-seller-bank relationship (see col. 19, line 65-col. 20, line 9). This indicates that the certificate is of a dynamic nature and thus the certificate-related information such as an ID or a serial number is dynamic and corresponds to the recited dynamic key. Since the certificate is issued for the buyer, it must bear buyer-specific information such as buyer's name to relate the certificate to the buyer. The buyer specific information corresponds to the recited static key (see also col. 12, lines 46-62, where buyer's information are transmitted to the seller via a secure communication channel).

Applicants also on page 8 of the remark argue that Johnson makes it clear that the buyer's personal informal (required for authentication) is never communicated to me seller (col. 12 lines 56-58).

Examiner respectfully disagrees and asserts that Johnson in col. 12 lines 56-58 describes the use of a password for authenticating the buyer by the bank. The authentication of the buyer is performed in addition to the aforementioned certificate and ID submitted to the seller by the buyer.

Applicants also on page 8 of the remark argue that the "front-end" authentication framework of Johnson precludes the seller from directly authenticating the buyer. This is because the seller of Johnson is required to redirect the buyer to the bank for authentication (see, col. 12, line 65 - col. 13, line 3, where the web seller causes the web buyer to be connected to their home bank for authentication).

Examiner respectfully disagrees and asserts that the authentication of the buyer is performed through the buyer-seller-bank communication channel not redirected through a separate communication channel. As mentioned above the authentication is performed to verify the identity of the buyer which is in addition to the verification of the buyer's certificate information for authorizing a transaction between the buyer and the seller. For the purpose of execution of a transaction a buyer submit information (i.e., ID and certificate) to the seller that has received from his/her bank and the seller submit these information to the bank for verification. Therefore, Johnson teaches the limitations recited in claims 21-31 and 34-38.

Examiner, however, in light of the above submission maintains the previous rejections as follows:

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

Claims 21-31 and 34-38 are rejected under 35 U.S.C. 102(e) as being anticipated by Johnson (6,529,885).

Regarding claims 21, 26 and 34, Johnson discloses:

A method for a non-fiduciary business, organization, or another individual to directly authenticate an individual over a communication network without redirecting the individual to another site and without requiring previous information about the individual, the method comprising:

The individual communicating with the business, organization, or another individual (see, e.g., Fig. 3, where the web buyer 301 communicates with the web seller 304_1 over the network 308);

The business, organization, or another individual communicating a request for both a static key and a dynamic key from the individual (see, e.g., col. 4 , lines 61-65 and col. 12 , lines 44-67, where the identification information corresponds to the recited static key and a dynamic key; col. 14, lines 5-8);

In response to the business, organization, or another individual's request, the individual communicating a request for a dynamic key from a first trusted-authenticator

(see, e.g., col. 9, lines 9-16 and lines 29-37, col. 20, lines 5-10, where the one-time, specific-transaction certificate authorization corresponds to the recited a dynamic key);

In response to the individual's request, the first trusted-authenticator calculating a dynamic key and providing it to the individual (see, e.g., col. 9, lines 9-16 and lines 29-37, col. 20, lines 5-10, where the one-time, specific-transaction certificate authorization corresponds to the recited a dynamic key);

The individual providing a combination of the calculated dynamic key and an existing static key to the business, organization, or another individual (see, e.g., col. 12 , lines 44-67 and col. 13, lines 42-60 and col. 20, lines 5-10, where the iDraft includes static key and dynamic key);

The business, organization, or another individual constructing an authentication request message containing the static and dynamic keys and communicating the authentication request message to a computer associated with a second trusted-authenticator over the communication network (see, e.g., col. 15, lines 61-63, where the Web seller 304_2 causes an LDAP-formatted query to be sent to the Web seller's home bank corresponds to the recited constructing an authentication request message containing the static and dynamic keys and communicating the authentication request message to a second trusted-authenticator); and

The second trusted-authenticator computer verifying the individual's identity based on the static and dynamic keys and sending a confirmation or denial authentication message to the business, organization, or another individual (see the above response to the applicants arguments and also, e.g., col. 16, lines 1-17, where

the Web buyer's home bank and the Web seller's home bank correspond to the recited first and second trusted-authenticators; see also Fig. 2, steps 24-28).

Regarding claim 22, Johnson discloses:

The method of claim 21, wherein the first and second trusted-authenticator are the same entity (see, e.g., col. 15, lines 57-60).

Regarding claim 23, Johnson discloses:

The method of claim 21, wherein the first and second trusted-authenticator are different entities (see, e.g., Fig. 3, where Web buyer's and Web seller's banks are different entities).

Regarding claims 24, 28 and 36, Johnson discloses:

The method of claim 21, wherein the dynamic key includes a non-predictable and time-dependent SecureCode (see, e.g., col. 9, lines 9-13, col. 20, lines 5-10).

Regarding claims 25, 29 and 37, Johnson discloses:

The method of claim 21, wherein at least the dynamic key is encrypted (see, e.g., col. 4, lines 61-67; col. 8, lines 64-67).

Regarding claims 27 and 35, Johnson discloses:

The method of claim 26, wherein the static and dynamic keys contain credentials for verifying the individual's identity (see, e.g., col. 8, lines 45-57; col. 11, lines 37-41).

Regarding claim 30, Johnson discloses:

The method of claim 26, wherein the entity corresponds to a business, organization, or another individual (see, e.g., Fig. 3, where the home banks or the web seller correspond to the recited entity).

Regarding claims 31 and 38, Johnson discloses:

The method of claim 26, wherein a first trusted-authenticator calculates the dynamic key and provides it to the individual for each authentication session (see, e.g., col. 12 , lines 44-67 and col. 13, lines 42-60 and col. 20, lines 5-10, where the iDraft includes static key and dynamic key).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

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

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

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system.

/A. N./
Abdulhakim Nobahar
Examiner, Art Unit 2432

/Gilberto Barron Jr./
Supervisory Patent 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					
	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					
	37			✓	✓					
	38			✓	✓					
	39			✓	-					
	40			✓	-					

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Nader Ashgari-Kamrani et al.

Application No.: 11/333,400 Confirmation No.: 4456

Filed: 01/18/2006 Art Unit: 2132

For: Direct Authentication System and Method via Trusted Authenticators Examiner: A. Nobahar

AMENDMENT AND REMARKS

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

INTRODUCTORY COMMENTS

In response to the Non-Final Office Action mailed 06/23/2009, the Applicants respectfully request reconsideration based on the amendments and remarks which follow.

In the claims:

21. (Amended) A method for a non-fiduciary business, organization, or another individual to directly authenticate an individual over a communication network without redirecting the individual to another site and without having previous information about the individual, the method comprising:

The individual communicating with [[a]] the business, organization, or another individual~~, over a communication network~~;

The business, organization, or another individual communicating a request for both a static key and a dynamic key from the individual;

In response to the business, organization, or another individual's request, the individual communicating a request for a dynamic key from a first trusted-authenticator;

In response to the individual's request, the first trusted-authenticator calculating a dynamic key and providing it to the individual;

The individual providing a combination of the calculated dynamic key and an existing static key to the business, organization, or another individual;

The business, organization, or another individual constructing an authentication request message containing the static and dynamic keys and communicating the authentication request message to a computer associated with a second trusted-authenticator over the communication network; and

The second trusted-authenticator computer verifying the individual's identity based on the static and dynamic keys and sending a confirmation or denial authentication message to the business, organization, or another individual.

22. (Previously Presented) The method of claim 21, wherein the first and second trusted-authenticator are the same.

23. (Previously Presented) The method of claim 21, wherein the first and second trusted-authenticator are different.

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

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

26. (Currently Amended) A method for [[an]] a non-fiduciary entity to directly authenticate an individual over a communication network without redirecting the individual to another site and without having previous information about the individual, the method comprising:

Requesting both a static key and a dynamic key from the individual ~~over the communication network~~ in order to validate the individual's identity;

Receiving both the static and dynamic keys from the individual ~~over the communication network~~; and

Creating an authentication request message containing the received static and dynamic keys and providing the authentication request message to a computer associated with a trusted-authenticator over the communication network, the computer authenticating ~~Authenticating~~ the individual based on a combination of the received static and dynamic keys.

27. (Previously Presented) The method of claim 26, wherein the static and dynamic keys contain credentials for verifying the individual's identity.

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

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

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

31. (Previously Presented) The method of claim 26, wherein a first trusted-authenticator calculates the dynamic key and provides it to the individual for each authentication session.

32. (Cancelled) The method of claim 31, the entity creating an authentication request message containing the received static and dynamic keys and providing the authentication request message to the first trusted-authenticator for authentication of the individual.

33. (Cancelled) The method of claim 31, the entity creating an authentication request message containing the received static and dynamic keys and providing the authentication request message to a second trusted-authenticator for authentication of the individual.

34. (Currently Amended) A method for a non-fiduciary website to directly authenticate an individual over a communication network such that the individual is not redirected to another site and without having previous information about the individual, the method comprising:

Requesting both a static key and a dynamic key from the individual in order to validate the individual's identity; and

Receiving both the static and dynamic keys from the individual ~~over the communication network~~; and

Creatingan authentication request message containing the received static and dynamic keys and providing the authentication request message to a computer associated with a trusted-authenticator over the communication

network, the computer authenticating ~~Authenticating~~ the individual based on the static and dynamic keys.

35. (Previously Presented) The method of claim 34, wherein the static and dynamic keys contain credentials for verifying the individual's identity.

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

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

38. (Previously Presented) The method of claim 34, wherein a first-trusted authenticator calculates the dynamic key and provides it to the individual for each authentication session.

39. (Cancelled) The method of claim 38, the website creating an authentication request message containing the received static and dynamic keys and providing the authentication request message to the first trusted-authenticator for authentication of the individual.

40. (Cancelled) The method of claim 38, the website creating an authentication request message containing the received static and dynamic keys and providing the authentication request message to a second trusted-authenticator for authentication of the individual.

REMARKS

Claims 21, 26 and 34 have been amended. Claims 32, 33, 39 and 40 are cancelled (the subject matter having been incorporated into the independent claims). No new matter has been included. Claims 21-31 and 34-38 remain in the application.

I. Rejections Under 35 U.S.C. § 101

Claims 21-40 stand rejected under 35 U.S.C. § 101 because "[t]he steps of authenticating an individual ... do not involve or tied to a particular machine." (See Office Action, page 2). Claims 21, 26 and 34 have been amended to clarify that the method is tied to a particular computer that receives an authentication request message containing both static and dynamic keys over the communication network and authenticates the individual based on the static and dynamic keys. In fact, it can be clearly seen in Figures 2a and 2b that the authentication message is sent over the communication network to a Trusted-Authenticator server, or computer, for authentication of the individual. Accordingly, the Applicant respectfully requests that the rejection under 35 U.S.C. § 101 be withdrawn.

II. Rejections Under 35 U.S.C. § 102(e)

Claims 21-40 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Johnson (US Patent No. 6,529,885) ("Johnson"). The rejection is respectfully traversed.

Claims 26 and 34 have been amended to incorporate the subject matter of dependent claims 32, 33, 39 and 40, respectfully. Claims 21, 26 and 34 have further been amended to clarify that the business, organization, or another

individual is a non-fiduciary entity. The business, organization, or another individual disclosed in the present specification is *different* from the trusted-authenticator (which plays a different role in the current authentication framework). Although not explicitly stated previously, the business, organization, or another individual disclosed in the specification *does not share a trusted relationship* with the individual, and is therefore non-fiduciary. By definition, in order for the business, organization or another individual to be a *fiduciary* entity, a relationship must exist with the individual - and that relationship must necessarily be based on trust. Since the entire present disclosure is directed toward remedying this *missing* trusted relationship between the individual and the business, organization, or another individual at the consumer level (without having to redirect the individual to another site), the business, organization, or another individual is inherently non-fiduciary. Claims 21, 26 and 34 have therefore been amended to clarify this previous implicit distinction. Illustrations of such non-fiduciary entities provided by the present specification include: online merchants, creditors, car dealerships, etc. See, for example, pages 20-26 of the specification.

Claim 21 now recites *inter alia*, "[a] method for a non-fiduciary business, organization or another individual to directly authenticate an individual," "[t]he individual providing a combination of the calculated dynamic key and an existing static key to the business, organization, or another individual," and "[t]he business, organization, or another individual constructing an authentication request message containing the static and dynamic keys and communicating the authentication request message to a computer associated with a second trusted authenticator."

Claims 26 and 34 now recite similar limitations - the business, organization, or another individual - or website, respectively "[c]reating an authentication request message containing the received static and dynamic keys and providing the authentication request message to a computer associated with a trusted-authenticator."

Applicant respectfully submits that the above limitations are not taught or even remotely suggested by Johnson.

In contrast to the claimed invention, Johnson discloses that a fiduciary, or trusted, entity (bank or government institution) is required to receive the buyer's password, certificate, etc. Johnson is completely silent regarding the buyer submitting a dynamic key to the seller. This is because the entire password-based authentication framework of Johnson *necessitates* authentication to take place on the "front-end" (i.e., via a trusted party). Johnson does not envision a "back-end" authentication framework - where a non-fiduciary business, organization, or another individual receives and *then* submits an individual's static and dynamic keys to a trusted-authority for authentication – as disclosed by the present invention. In fact, Johnson makes it clear that the buyer's personal information (required for authentication) is **never** communicated to the seller (col. 12 lines 56-58). Thus, Johnson cannot teach or suggest a non-fiduciary entity generating an authentication request message containing both static and dynamic keys as claimed.

Moreover, the "front-end" authentication framework of Johnson precludes the *seller* from directly authenticating the buyer. This is because the seller of Johnson is required to redirect the buyer to the bank for authentication (see, col. 12 line 65 – col. 13 line 3, where the web seller causes the web buyer to be connected to their home bank for authentication). However, such redirection undesirably increases security risks because redirecting the customer to another site increases the likelihood of phishing and pharming attacks.

In contrast to Johnson, present claims 21, 26 and 34 state that the business, organization, or another individual directly authenticates the individual. In other words, the present invention provides a "back-end" authentication framework which allows the combined static and dynamic keys to be directly communicated to the business, organization, or another individual. In turn, the

business, organization, or another individual then submits an authentication request message containing the keys to a trusted-authority for authentication. As a result, an individual shopping online can conveniently and securely submit their static and dynamic keys directly to the online merchant without being redirected to another website for authentication, or having to first enter a secure portal. Consequently, the possibility of phishing and pharming attacks are avoided and security is further improved.

For at least the above reasons, Applicant submits that Johnson fails to anticipate independent claims 21, 26, and 34 as well as their dependent claims under 35 USC 102(e) and respectfully request that the rejection of claims 21-31, and 34-38 be withdrawn.

III. Conclusion

Since it is believed that all aspects of the rejections set forth in the Non-Final Office Action mailed 06/23/2009 have been addressed and overcome, Applicants' submit that the present application is now in condition for allowance. If the examiner believes that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at (571) 228-2938.

Dated: 09/22/2009

Respectfully submitted,

/Shawna J. Shaw/

Shawna J. Shaw
Agent for Applicants
Registration No. 57,091

FACSIMILE TRANSMITTAL SHEET

TO: Examiner Nobahar	FROM: Shawna J. Shaw
COMPANY:	DATE: 9/22/2009
FAX NUMBER:	TOTAL NO. OF PAGES INCLUDING COVER: 10
PHONE NUMBER: (571) 228-2938	SENDER'S REFERENCE NUMBER:
RE: 11/333,400	YOUR REFERENCE NUMBER:

☐ URGENT ☐ FOR REVIEW ☐ PLEASE COMMENT ☐ PLEASE REPLY ☐ PLEASE RECYCLE

NOTES/COMMENTS:

Please find attached an amendment and response to the office action dated 06/23/09.

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	09/22/2009	(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))	* 16	Minus	** 26	= 0	X $26 =	0	OR	X $ =	
	Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $110 =	0	OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

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:
/MYRTLE B. LEIGH/

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		4456

7590 06/23/2009

Nader Asghari-Kamrani
6558 Palisades Drive
Centreville, VA 20121

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
06/23/2009	PAPER

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

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

Office Action Summary	Application No.	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 *08 June 2009*.

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

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

Disposition of Claims

4)☒ Claim(s) *21-40* 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) *21-40* is/are rejected.

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

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

Application Papers

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

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

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

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

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

Priority under 35 U.S.C. § 119

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

a)☐ All b)☐ Some * c)☐ None of:

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

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

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

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

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to applicant's amendment filed on 06/08/2009.

2. Claims 21-40 are pending.

3. Claims 1-20 are cancelled.

Claim Rejections - 35 USC § 101

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

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

Claims 21-40 are rejected under 35 U.S.C. 101 as not falling within one of the four statutory categories of invention. While the claims recite a series of steps or acts to be performed, a statutory "process" under 35 U.S.C. 101 must (1) be tied to particular machine, or (2) transform underlying subject matter (such as an article or material) to a different state or thing. See page 10 of In Re Bilski 88 USPQ2d 1385.

The instant claims are neither positively tied to a particular machine that accomplishes the claimed method steps nor transform underlying subject matter, and therefore do not qualify as a statutory process. The steps of authenticating an individual recited by these claims do not involve or tied to a particular machine and could be completely performed mentally, verbally or without a machine. Thus, the claims are non-statutory.

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 –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claims 21-40 are rejected under 35 U.S.C. 102(e) as being anticipated by Johnson (6,529,885).

Regarding claims 21, 26 and 34, Johnson discloses:

A method for a business, organization, or another individual to directly authenticate an individual over a communication network without redirecting the individual to another site and without requiring previous information about the individual, the method comprising:

The individual communicating with a business, organization, or another individual, over a communication network (see, e.g., Fig. 3, where the web buyer 301 communicates with the web seller 304_1 over the network 308);

The business, organization, or another individual communicating a request for both a static key and a dynamic key from the individual (see, e.g., col. 4 , lines 61-65 and col. 12 , lines 44-67, where the identification information corresponds to the recited static key and a dynamic key; col. 14, lines 5-8);

In response to the business, organization, or another individual's request, the individual communicating a request for a dynamic key from a first trusted-authenticator (see, e.g., col. 9, lines 9-16 and lines 29-37, col. 20, lines 5-10, where the one-time, specific-transaction certificate authorization corresponds to the recited a dynamic key);

In response to the individual's request, the first trusted-authenticator calculating a dynamic key and providing it to the individual (see, e.g., col. 9, lines 9-16 and lines 29-37, col. 20, lines 5-10, where the one-time, specific-transaction certificate authorization corresponds to the recited a dynamic key);

The individual providing a combination of the calculated dynamic key and an existing static key to the business, organization, or another individual (see, e.g., col. 12 , lines 44-67 and col. 13, lines 42-60 and col. 20, lines 5-10, where the iDraft includes static key and dynamic key);

The business, organization, or another individual constructing an authentication request message containing the static and dynamic keys and communicating the authentication request message to a second trusted-authenticator (see, e.g., col. 15,

lines 61-63, where the Web seller 304_2 causes an LDAP-formatted query to be sent to the Web seller's home bank corresponds to the recited constructing an authentication request message containing the static and dynamic keys and communicating the authentication request message to a second trusted-authenticator); and

The second trusted-authenticator verifying the individual's identity and sending a confirmation or denial authentication message to the business, organization, or another individual (col. 16, lines 1-17, where the Web buyer's home bank and the Web seller's home bank correspond to the recited first and second trusted-authenticators; see also Fig. 2, steps 24-28).

Regarding claim 22, Johnson discloses:

The method of claim 21, wherein the first and second trusted-authenticator are the same entity (see, e.g., col. 15, lines 57-60).

Regarding claim 23, Johnson discloses:

The method of claim 21, wherein the first and second trusted-authenticator are different entities (see, e.g., Fig. 3, where Web buyer's and Web seller's banks are different entities).

Regarding claims 24, 28 and 36, Johnson discloses:

The method of claim 21, wherein the dynamic key includes a non-predictable and time-dependent SecureCode (see, e.g., col. 9, lines 9-13, col. 20, lines 5-10).

Regarding claims 25, 29 and 37, Johnson discloses:

The method of claim 21, wherein at least the dynamic key is encrypted (see, e.g., col. 4, lines 61-67; col. 8, lines 64-67).

Regarding claims 27 and 35, Johnson discloses:

The method of claim 26, wherein the static and dynamic keys contain credentials for verifying the individual's identity (see, e.g., col. 8, lines 45-57; col. 11, lines 37-41).

Regarding claim 30, Johnson discloses:

The method of claim 26, wherein the entity corresponds to a business, organization, or another individual (see, e.g., Fig. 3, where the home banks or the web seller correspond to the recited entity).

Regarding claims 31 and 38, Johnson discloses:

The method of claim 26, wherein a first trusted-authenticator calculates the dynamic key and provides it to the individual for each authentication session (see, e.g., col. 12 , lines 44-67 and col. 13, lines 42-60 and col. 20, lines 5-10, where the iDraft includes static key and dynamic key).

Regarding claims 32 and 39, Johnson discloses:

The method of claim 31, the entity creating an authentication request message containing the received static and dynamic keys and providing the authentication request message to the first trusted-authenticator for authentication of the individual (see, e.g., col. 15, lines 57-63, where the Web seller 304_2 causes an LDAP-formatted query to be sent to the Web seller's home bank corresponds to the recited creating an authentication request message containing the static and dynamic keys and communicating the authentication request message to a first trusted-authenticator).

Regarding claims 33 and 40, Johnson discloses:

The method of claim 31, the entity creating an authentication request message containing the received static and dynamic keys and providing the authentication request message to a second trusted-authenticator for authentication of the individual (see, e.g., col. 15, lines 61-63, where the Web seller 304_2 causes an LDAP-formatted query to be sent to the Web seller's home bank corresponds to the recited creating an authentication request message containing the static and dynamic keys and communicating the authentication request message to a second trusted-authenticator).

Conclusion

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

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

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

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

/A. N./
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-2002/0120587 A1	08-2002	D'Agostino, John	705/78
*	B	US-2002/0083347 A1	06-2002	Taguchi, Akira	713/202
*	C	US-2002/0046187 A1	04-2002	Vargas et al.	705/67
*	D	US-7,324,972 B1	01-2008	Oliver et al.	705/40
*	E	US-7,236,956 B1	06-2007	Ogg et al.	705/50
*	F	US-7,171,694 B1	01-2007	Jespersen et al.	726/27
*	G	US-7,096,204 B1	08-2006	Chen et al.	705/74
*	H	US-7,065,786 B2	06-2006	Taguchi, Akira	726/18
	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						
	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						
	37			✓						
	38			✓						
	39			✓						
	40			✓						

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		

SEARCH NOTES		
Search Notes	Date	Examiner

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

/A. N./ Examiner.Art Unit 2132	

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	10725	(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	2009/06/17 15:07
L2	520	L1 and (static dynamic fixed unchanging constant invariable unvarying variable time-depend $4 changeable changing unpredictable predictable non predictable temp temporar$3 onetime provision$4 intrim transi$4 short single) adj2 (key password code passcode passphrase phrase ID identification identify$3 identity PIN secret securecode) same (authenticat$3 authoriz$5 verify $3 verification valid$4 validat $3 match$3 compar$5 check$3 examin$5) same (authority trust$3 bank$3 issuing institution organization authenticator center$3 central $5 centre centralization or broker$4 authoritative or authorized official$3) same (user client consum$3 customer subscrib$3 buy$3 purchas$3 shop$4 trad$3 partner counterpart member individual person party entity recipient receiver)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/17 15:07
L3	410	2 and (static dynamic fixed unchanging constant invariable unvarying variable time-depend $4 changeable changing unpredictable predictable non predictable temp temporar$3 onetime provision$4 intrim transi$4 short single) adj2 (key password code passcode passphrase phrase ID identification identify$3 identity PIN secret securecode) same (authenticat$3 authoriz$5 verif $4 verification valid$4 validat $3 match$3 compar$5 check$3 examin$5) adj5 (key password code passcode passphrase phrase ID identification identif	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/17 15:24

		$4 identity PIN secret securecode user client consum $3 customer subscrib$3 buy$3 purchas$3 shop$4 trad$3 partner counterpart member individual person party entity recipient receiver) same (authority trust$3 bank$3 issuing institution organization authenticator center$3 central $5 centre centralization or broker$4 authoritative or authorized official$3)				
L4	172	3 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)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/17 15:29
L5	171	4 and (key password code passcode passphrase phrase ID identification identify$3 identity PIN secret securecode) near5 (authenticat$3 verify$3 verification valid$4 validat$3 match$3 compar$5 check$3 examin$5)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/17 15:34
L6	167	5 and (user client consum$3 customer subscrib$3 buy$3 purchas$3 shop$4 trad$3 partner counterpart member individual person party entity recipient receiver business) near5 (register$5 apply$4 application request$4 enlist$4 enroll$4 sign$3 ask$3)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/17 16:03
L7	165	6 and (user client consum$3 customer subscrib$3 buy$3 purchas$3 shop$4 trad$3 partner counterpart member individual person party entity recipient receiver business) near5 (register$5 apply$4 application request$4 enlist$4 enroll$4 sign$3 ask$3) same (key password code passcode passphrase phrase ID identification identify$3 identity PIN secret securecode)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/17 16:11

L8	146	7 and (user client consum$3 customer subscrib$3 buy$3 purchas$3 shop$4 trad$3 partner counterpart member individual person party entity recipient receiver business) same (key password code passcode passphrase phrase ID identification identify$3 identity PIN secret securecode) same (deny$4 den$4 reject$4 approv$4 disapprov$4 accept $4 allow$4 permit$4 permision authoriz$5) same (match$3 compar$4 checkS3 examin$5 verif$4 verification valid$5)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/17 16:28
L9	138	7 and (user client consum$3 customer subscrib$3 buy$3 purchas$3 shop$4 trad$3 partner counterpart member individual person party entity recipient receiver business) same (key password code passcode passphrase phrase ID identification identify$3 identity PIN secret securecode) same (deny$4 den$4 reject$4 approv$4 disapprov$4 allow$4 permit$4 permision) same (match$3 compar$4 check$3 examin$5 verif$4 verification valid$5)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/17 16:30
L10	99	7 and (user client consum$3 customer subscrib$3 buy$3 purchas$3 shop$4 trad$3 partner counterpart member individual person party entity recipient receiver business) same (match$3 compar$4 check$3 examin$5 verif$4 verification valid$5) near4 (key password code passcode passphrase phrase ID identification identify$3 identity PIN secret securecode) same (deny$4 den$4 reject$4 approv $4 disapprov$4 allow$4 permit $4 permision)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/17 16:31

6/17/2009 4:51:46 PM
C:\Documents and Settings\hnobahar\My Documents\EAST\Workspaces\11333400.wsp

1 Fm RCE $ ✓

PTO/SB/30 (06-09)
Approved for use through 06/30/2009. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Request for Continued Examination (RCE) Transmittal

Address to:
Mail Stop RCE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Application Number	11/333,400
Filing Date	01/18/06
First Named Inventor	Kamrani et al.
Art Unit	2132
Examiner Name	Nobahar
Attorney Docket Number	

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. See Instruction Sheet for RCEs (not to be submitted to the USPTO) on page 2.

1. Submission required under 37 CFR 1.114 Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

   a. ☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

      i. ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____

      ii. ☐ Other _____

   b. ☑ Enclosed

      i. ☑ Amendment/Reply

      ii. ☐ Affidavit(s)/ Declaration(s)

      iii. ☐ Information Disclosure Statement (IDS)

      iv. ☐ Other _____

2. Miscellaneous

   a. ☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of _____ months. (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

   b. ☐ Other _____

3. Fees The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.

   a. ☐ The Director is hereby authorized to charge the following fees, any underpayment of fees, or credit any overpayments, to Deposit Account No. _____.

      i. ☐ RCE fee required under 37 CFR 1.17(e)

      ii. ☐ Extension of time fee (37 CFR 1.136 and 1.17)

      iii. ☐ Other _____

   b. ☑ Check in the amount of $ 405 enclosed

   c. ☐ Payment by credit card (Form PTO-2038 enclosed)

06/09/2009 SMOHAMME 00000003 11333400
01 FC:2801 405.00 OP

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.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

Signature		Date	6/6/09
Name (Print/Type)	Shawna J. Shaw	Registration No.	57,091

CERTIFICATE OF MAILING OR TRANSMISSION

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 RCE, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450 or facsimile transmitted to the U.S. Patent and Trademark Office on the date shown below.

Signature			
Name (Print/Type)		Date	

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Mail Stop RCE, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Nader Ashgari-Kamrani et al.

Application No.: 11/333,400 Confirmation No.: 4456

Filed: 01/18/2006 Art Unit: 2132

For: Direct Authentication System and Method via Trusted Authenticators Examiner: A. Nobahar

REQUEST FOR CONTINUED EXAMINATION (RCE)

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

INTRODUCTORY COMMENTS

In response to the Final Office Action mailed 03/06/2009, the Applicants respectfully request reconsideration based on the new claims which follow. Support for the new claims can be found, for example, on page 13 line 14 – page 15 line 13, page 19 line 15 – page 21 line 21 and page 25 lines 12-14.

In the claims:

Please cancel claims 1-20.

21. (New) A method for a business, organization, or another individual to directly authenticate an individual over a communication network without redirecting the individual to another site and without requiring previous information about the individual, the method comprising:

The individual communicating with a business, organization, or another individual, over a communication network;

The business, organization, or another individual communicating a request for both a static key and a dynamic key from the individual;

In response to the business, organization, or another individual's request, the individual communicating a request for a dynamic key from a first trusted-authenticator;

In response to the individual's request, the first trusted-authenticator calculating a dynamic key and providing it to the individual;

The individual providing a combination of the calculated dynamic key and an existing static key to the business, organization, or another individual;

The business, organization, or another individual constructing an authentication request message containing the static and dynamic keys and communicating the authentication request message to a second trusted-authenticator; and

The second trusted-authenticator verifying the individual's identity and sending a confirmation or denial authentication message to the business, organization, or another individual.

22. (New) The method of claim 21, wherein the first and second trusted-authenticator are the same entity.

23. (New) The method of claim 21, wherein the first and second trusted-authenticator are different entities.

24. (New) The method of claim 21, wherein the dynamic key includes a non-predictable and time-dependent SecureCode.

25. (New) The method of claim 21, wherein at least the dynamic key is encrypted.

26. (New) A method for an entity to directly authenticate an individual over a communication network without redirecting the individual to another site and without requiring previous information about the individual, the method comprising:

Requesting both a static key and a dynamic key from the individual over the communication network in order to validate the individual's identity;

Receiving both the static and dynamic keys from the individual over the communication network; and

Authenticating the individual based on a combination of the received static and dynamic keys.

27. (New) The method of claim 26, wherein the static and dynamic keys contain credentials for verifying the individual's identity.

28. (New) The method of claim 26, wherein the dynamic key includes a non-predictable and time-dependent SecureCode.

29. (New) The method of claim 26, wherein at least the dynamic key is encrypted.

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

31. (New) The method of claim 26, wherein a first trusted-authenticator calculates the dynamic key and provides it to the individual for each authentication session.

32. (New) The method of claim 31, the entity creating an authentication request message containing the received static and dynamic keys and providing the authentication request message to the first trusted-authenticator for authentication of the individual.

33. (New) The method of claim 31, the entity creating an authentication request message containing the received static and dynamic keys and providing the authentication request message to a second trusted-authenticator for authentication of the individual.

34. (New) A method for a website to directly authenticate an individual over a communication network such that the individual is not redirected to another site and without requiring previous information about the individual, the method comprising:

Requesting both a static key and a dynamic key from the individual in order to validate the individual's identity; and

Receiving both the static and dynamic keys from the individual over the communication network; and

Authenticating the individual based on a combination of the received static and dynamic keys.

35. (New) The method of claim 34, wherein the static and dynamic keys contain credentials for verifying the individual's identity.

36. (New) The method of claim 34, wherein the dynamic key includes a non-predictable and time-dependent SecureCode.

37. (New) The method of claim 34, wherein at least the dynamic key is encrypted.

38. (New) The method of claim 34, wherein a first-trusted authenticator calculates the dynamic key and provides it to the individual for each authentication session.

39. (New) The method of claim 38, the website creating an authentication request message containing the received static and dynamic keys and providing the authentication request message to the first trusted-authenticator for authentication of the individual.

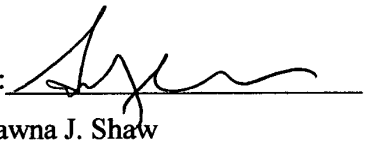
40. (New) The method of claim 38, the website creating an authentication request message containing the received static and dynamic keys and providing the authentication request message to a second trusted-authenticator for authentication of the individual.

Conclusion

The Applicant's believe that new claims 21-40 are allowable over the prior art and are therefore in condition for allowance. If the examiner believes that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at (571) 228-2938.

Respectfully submitted,

Dated: 06/06/2009

By: 

Shawna J. Shaw
Agent for Applicants
Registration No. 57,091

Doc code: RCEX
Doc description: Request for Continued Examination (RCE)

PTO/SB/30EFS (06-09)
Approved for use through 06/30/2009. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	11/333,400	Filing Date	2006-01-18	Docket Number (if applicable)		Art Unit	2132
First Named Inventor	Kamrani et al.			Examiner Name	A. Nobahar		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

- ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____
- ☐ Other _____

☒ Enclosed

- ☒ Amendment/Reply
- ☐ Information Disclosure Statement (IDS)
- ☐ Affidavit(s)/ Declaration(s)
- ☐ Other _____

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____
(Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other _____

FEES

The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.

☐ The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No _____

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature

☐ Applicant Signature

PTO/SB/30EFS (06-09)
Approved for use through 06/30/2009. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Signature of Registered U.S. Patent Practitioner			
Signature	/Shawna J. Shaw/	Date (YYYY-MM-DD)	2009-06-06
Name	Shawna J. Shaw	Registration Number	57091

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

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

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Nader Ashgari-Kamrani et al.

Application No.: 11/333,400 Confirmation No.: 4456

Filed: 01/18/2006 Art Unit: 2132

For: Direct Authentication System and Method via Trusted Authenticators Examiner: A. Nobahar

REQUEST FOR CONTINUED EXAMINATION (RCE)

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

INTRODUCTORY COMMENTS

In response to the Final Office Action mailed 03/06/2009, the Applicants respectfully request reconsideration based on the new claims which follow. Support for the new claims can be found, for example, on page 13 line 14 – page 15 line 13, page 19 line 15 – page 21 line 21 and page 25 lines 12-14.

In the claims:

Please cancel claims 1-20.

21. (New) A method for a business, organization, or another individual to directly authenticate an individual over a communication network without redirecting the individual to another site and without requiring previous information about the individual, the method comprising:

The individual communicating with a business, organization, or another individual, over a communication network;

The business, organization, or another individual communicating a request for both a static key and a dynamic key from the individual;

In response to the business, organization, or another individual's request, the individual communicating a request for a dynamic key from a first trusted-authenticator;

In response to the individual's request, the first trusted-authenticator calculating a dynamic key and providing it to the individual;

The individual providing a combination of the calculated dynamic key and an existing static key to the business, organization, or another individual;

The business, organization, or another individual constructing an authentication request message containing the static and dynamic keys and communicating the authentication request message to a second trusted-authenticator; and

The second trusted-authenticator verifying the individual's identity and sending a confirmation or denial authentication message to the business, organization, or another individual.

22. (New) The method of claim 21, wherein the first and second trusted-authenticator are the same entity.

23. (New) The method of claim 21, wherein the first and second trusted-authenticator are different entities.

24. (New) The method of claim 21, wherein the dynamic key includes a non-predictable and time-dependent SecureCode.

25. (New) The method of claim 21, wherein at least the dynamic key is encrypted.

26. (New) A method for an entity to directly authenticate an individual over a communication network without redirecting the individual to another site and without requiring previous information about the individual, the method comprising:

Requesting both a static key and a dynamic key from the individual over the communication network in order to validate the individual's identity;

Receiving both the static and dynamic keys from the individual over the communication network; and

Authenticating the individual based on a combination of the received static and dynamic keys.

27. (New) The method of claim 26, wherein the static and dynamic keys contain credentials for verifying the individual's identity.

28. (New) The method of claim 26, wherein the dynamic key includes a non-predictable and time-dependent SecureCode.

29. (New) The method of claim 26, wherein at least the dynamic key is encrypted.

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

31. (New) The method of claim 26, wherein a first trusted-authenticator calculates the dynamic key and provides it to the individual for each authentication session.

32. (New) The method of claim 31, the entity creating an authentication request message containing the received static and dynamic keys and providing the authentication request message to the first trusted-authenticator for authentication of the individual.

33. (New) The method of claim 31, the entity creating an authentication request message containing the received static and dynamic keys and providing the authentication request message to a second trusted-authenticator for authentication of the individual.

34. (New) A method for a website to directly authenticate an individual over a communication network such that the individual is not redirected to another site and without requiring previous information about the individual, the method comprising:

Requesting both a static key and a dynamic key from the individual in order to validate the individual's identity; and

Receiving both the static and dynamic keys from the individual over the communication network; and

Authenticating the individual based on a combination of the received static and dynamic keys.

35. (New) The method of claim 34, wherein the static and dynamic keys contain credentials for verifying the individual's identity.

36. (New) The method of claim 34, wherein the dynamic key includes a non-predictable and time-dependent SecureCode.

37. (New) The method of claim 34, wherein at least the dynamic key is encrypted.

38. (New) The method of claim 34, wherein a first-trusted authenticator calculates the dynamic key and provides it to the individual for each authentication session.

39. (New) The method of claim 38, the website creating an authentication request message containing the received static and dynamic keys and providing the authentication request message to the first trusted-authenticator for authentication of the individual.

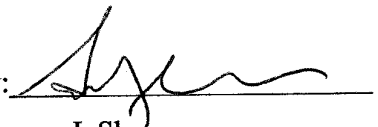
40. (New) The method of claim 38, the website creating an authentication request message containing the received static and dynamic keys and providing the authentication request message to a second trusted-authenticator for authentication of the individual.

Conclusion

The Applicant's believe that new claims 21-40 are allowable over the prior art and are therefore in condition for allowance. If the examiner believes that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at (571) 228-2938.

Respectfully submitted,

Dated: 06/06/2009

By: 

Shawna J. Shaw
Agent for Applicants
Registration No. 57,091

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:	Shawna Jeannine Shaw
Attorney Docket Number:	

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility Search Fee	2111	1	270	270
Utility Examination Fee	2311	1	110	110
Utility filing Fee(efiling)-Small Entity	2011	1	165	165
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**545**

Electronic Acknowledgement Receipt	
EFS ID:	5468304
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
Correspondence Address:	Nader Asghari-Kamrani - 6558 Palisades Drive - Centreville VA 20121 US 7032225104 kamrani@delphinustechnology.com
Filer:	Shawna Jeannine Shaw
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	06-JUN-2009
Filing Date:	18-JAN-2006
Time Stamp:	07:13:38
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Continued Examination (RCE)	SB30.pdf	779506 8a83b910b8924c595aaa3583dccba1bf3ea3bfc6	no	3
Warnings:					
Information:					
2	Amendment Submitted/Entered with Filing of CPA/RCE	RCE.pdf	383839 811a8c2fd86d9157701ebdfba98f3b2eeb865e70	no	6
Warnings:					
Information:					
3	Fee Worksheet (PTO-875)	fee-info.pdf	32427 0528fb1abeed1bbc6c301bd4ae8941f112349ddf	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1195772		

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

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

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

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

Doc code: RCEX
Doc description: Request for Continued Examination (RCE)

PTO/SB/30EFS (06-09)
Approved for use through 06/30/2009. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	11/333,400	Filing Date	2006-01-18	Docket Number (if applicable)		Art Unit	2132
First Named Inventor	Kamrani et al.			Examiner Name	A. Nobahar		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

- ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____
- ☐ Other _____

☒ Enclosed

- ☒ Amendment/Reply
- ☐ Information Disclosure Statement (IDS)
- ☐ Affidavit(s)/ Declaration(s)
- ☐ Other _____

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____
(Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other _____

FEES

The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.

☐ The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No _____

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature

☐ Applicant Signature

PTO/SB/30EFS (06-09)
Approved for use through 06/30/2009. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Signature of Registered U.S. Patent Practitioner			
Signature	/Shawna J. Shaw/	Date (YYYY-MM-DD)	2009-06-06
Name	Shawna J. Shaw	Registration Number	57091

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

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

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Nader Ashgari-Kamrani et al.

Application No.: 11/333,400 Confirmation No.: 4456

Filed: 01/18/2006 Art Unit: 2132

For: Direct Authentication System and Method via Trusted Authenticators Examiner: A. Nobahar

REQUEST FOR CONTINUED EXAMINATION (RCE)

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

INTRODUCTORY COMMENTS

In response to the Final Office Action mailed 03/06/2009, the Applicants respectfully request reconsideration based on the new claims which follow. Support for the new claims can be found, for example, on page 13 line 14 – page 15 line 13, page 19 line 15 – page 21 line 21 and page 25 lines 12-14.

In the claims:

Please cancel claims 1-20.

21. (New) A method for a business, organization, or another individual to directly authenticate an individual over a communication network without redirecting the individual to another site and without requiring previous information about the individual, the method comprising:

The individual communicating with a business, organization, or another individual, over a communication network;

The business, organization, or another individual communicating a request for both a static key and a dynamic key from the individual;

In response to the business, organization, or another individual's request, the individual communicating a request for a dynamic key from a first trusted-authenticator;

In response to the individual's request, the first trusted-authenticator calculating a dynamic key and providing it to the individual;

The individual providing a combination of the calculated dynamic key and an existing static key to the business, organization, or another individual;

The business, organization, or another individual constructing an authentication request message containing the static and dynamic keys and communicating the authentication request message to a second trusted-authenticator; and

The second trusted-authenticator verifying the individual's identity and sending a confirmation or denial authentication message to the business, organization, or another individual.

22. (New) The method of claim 21, wherein the first and second trusted-authenticator are the same entity.

23. (New) The method of claim 21, wherein the first and second trusted-authenticator are different entities.

24. (New) The method of claim 21, wherein the dynamic key includes a non-predictable and time-dependent SecureCode.

25. (New) The method of claim 21, wherein at least the dynamic key is encrypted.

26. (New) A method for an entity to directly authenticate an individual over a communication network without redirecting the individual to another site and without requiring previous information about the individual, the method comprising:

Requesting both a static key and a dynamic key from the individual over the communication network in order to validate the individual's identity;

Receiving both the static and dynamic keys from the individual over the communication network; and

Authenticating the individual based on a combination of the received static and dynamic keys.

27. (New) The method of claim 26, wherein the static and dynamic keys contain credentials for verifying the individual's identity.

28. (New) The method of claim 26, wherein the dynamic key includes a non-predictable and time-dependent SecureCode.

29. (New) The method of claim 26, wherein at least the dynamic key is encrypted.

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

31. (New) The method of claim 26, wherein a first trusted-authenticator calculates the dynamic key and provides it to the individual for each authentication session.

32. (New) The method of claim 31, the entity creating an authentication request message containing the received static and dynamic keys and providing the authentication request message to the first trusted-authenticator for authentication of the individual.

33. (New) The method of claim 31, the entity creating an authentication request message containing the received static and dynamic keys and providing the authentication request message to a second trusted-authenticator for authentication of the individual.

34. (New) A method for a website to directly authenticate an individual over a communication network such that the individual is not redirected to another site and without requiring previous information about the individual, the method comprising:

Requesting both a static key and a dynamic key from the individual in order to validate the individual's identity; and

Receiving both the static and dynamic keys from the individual over the communication network; and

Authenticating the individual based on a combination of the received static and dynamic keys.

35. (New) The method of claim 34, wherein the static and dynamic keys contain credentials for verifying the individual's identity.

36. (New) The method of claim 34, wherein the dynamic key includes a non-predictable and time-dependent SecureCode.

37. (New) The method of claim 34, wherein at least the dynamic key is encrypted.

38. (New) The method of claim 34, wherein a first-trusted authenticator calculates the dynamic key and provides it to the individual for each authentication session.

39. (New) The method of claim 38, the website creating an authentication request message containing the received static and dynamic keys and providing the authentication request message to the first trusted-authenticator for authentication of the individual.

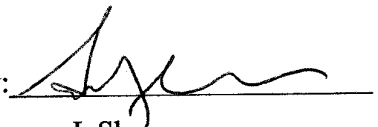
40. (New) The method of claim 38, the website creating an authentication request message containing the received static and dynamic keys and providing the authentication request message to a second trusted-authenticator for authentication of the individual.

Conclusion

The Applicant's believe that new claims 21-40 are allowable over the prior art and are therefore in condition for allowance. If the examiner believes that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at (571) 228-2938.

Respectfully submitted,

Dated: 06/06/2009

By: 

Shawna J. Shaw
Agent for Applicants
Registration No. 57,091

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:	Shawna Jeannine Shaw
Attorney Docket Number:	

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility Search Fee	2111	1	270	270
Utility Examination Fee	2311	1	110	110
Utility filing Fee(efiling)-Small Entity	2011	1	165	165
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**545**

Electronic Acknowledgement Receipt	
EFS ID:	5468305
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
Correspondence Address:	Nader Asghari-Kamrani - 6558 Palisades Drive - Centreville VA 20121 US 7032225104 kamrani@delphinustechnology.com
Filer:	Shawna Jeannine Shaw
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	06-JUN-2009
Filing Date:	18-JAN-2006
Time Stamp:	07:27:10
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Continued Examination (RCE)	SB30.pdf	779506 8a83b910b8924c595aaa3583dccba1bf3ea3bfc6	no	3
Warnings:					
Information:					
2	Amendment Submitted/Entered with Filing of CPA/RCE	RCE.pdf	383839 811a8c2fd86d9157701ebdfba98f3b2eeb865e70	no	6
Warnings:					
Information:					
3	Fee Worksheet (PTO-875)	fee-info.pdf	32427 05e0816ae7b730755ad4a1a6b8b0e429d464e0c0	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1195772		

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

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

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

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

Doc code: RCEX
Doc description: Request for Continued Examination (RCE)

PTO/SB/30EFS (06-09)
Approved for use through 06/30/2009. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	11/333,400	Filing Date	2006-01-18	Docket Number (if applicable)		Art Unit	2132
First Named Inventor	Kamrani et al.			Examiner Name	A. Nobahar		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

- ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____
- ☐ Other _____

☒ Enclosed

- ☒ Amendment/Reply
- ☐ Information Disclosure Statement (IDS)
- ☐ Affidavit(s)/ Declaration(s)
- ☐ Other _____

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____
(Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other _____

FEES

The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.

☐ The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No _____

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature

☐ Applicant Signature

PTO/SB/30EFS (06-09)
Approved for use through 06/30/2009. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Signature of Registered U.S. Patent Practitioner			
Signature	/Shawna J. Shaw/	Date (YYYY-MM-DD)	2009-06-06
Name	Shawna J. Shaw	Registration Number	57091

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

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

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Nader Ashgari-Kamrani et al.

Application No.: 11/333,400 Confirmation No.: 4456

Filed: 01/18/2006 Art Unit: 2132

For: Direct Authentication System and Method via Trusted Authenticators Examiner: A. Nobahar

REQUEST FOR CONTINUED EXAMINATION (RCE)

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

INTRODUCTORY COMMENTS

In response to the Final Office Action mailed 03/06/2009, the Applicants respectfully request reconsideration based on the new claims which follow. Support for the new claims can be found, for example, on page 13 line 14 – page 15 line 13, page 19 line 15 – page 21 line 21 and page 25 lines 12-14.

In the claims:

Please cancel claims 1-20.

21. (New) A method for a business, organization, or another individual to directly authenticate an individual over a communication network without redirecting the individual to another site and without requiring previous information about the individual, the method comprising:

The individual communicating with a business, organization, or another individual, over a communication network;

The business, organization, or another individual communicating a request for both a static key and a dynamic key from the individual;

In response to the business, organization, or another individual's request, the individual communicating a request for a dynamic key from a first trusted-authenticator;

In response to the individual's request, the first trusted-authenticator calculating a dynamic key and providing it to the individual;

The individual providing a combination of the calculated dynamic key and an existing static key to the business, organization, or another individual;

The business, organization, or another individual constructing an authentication request message containing the static and dynamic keys and communicating the authentication request message to a second trusted-authenticator; and

The second trusted-authenticator verifying the individual's identity and sending a confirmation or denial authentication message to the business, organization, or another individual.

22. (New) The method of claim 21, wherein the first and second trusted-authenticator are the same entity.

23. (New) The method of claim 21, wherein the first and second trusted-authenticator are different entities.

24. (New) The method of claim 21, wherein the dynamic key includes a non-predictable and time-dependent SecureCode.

25. (New) The method of claim 21, wherein at least the dynamic key is encrypted.

26. (New) A method for an entity to directly authenticate an individual over a communication network without redirecting the individual to another site and without requiring previous information about the individual, the method comprising:

Requesting both a static key and a dynamic key from the individual over the communication network in order to validate the individual's identity;

Receiving both the static and dynamic keys from the individual over the communication network; and

Authenticating the individual based on a combination of the received static and dynamic keys.

27. (New) The method of claim 26, wherein the static and dynamic keys contain credentials for verifying the individual's identity.

28. (New) The method of claim 26, wherein the dynamic key includes a non-predictable and time-dependent SecureCode.

29. (New) The method of claim 26, wherein at least the dynamic key is encrypted.

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

31. (New) The method of claim 26, wherein a first trusted-authenticator calculates the dynamic key and provides it to the individual for each authentication session.

32. (New) The method of claim 31, the entity creating an authentication request message containing the received static and dynamic keys and providing the authentication request message to the first trusted-authenticator for authentication of the individual.

33. (New) The method of claim 31, the entity creating an authentication request message containing the received static and dynamic keys and providing the authentication request message to a second trusted-authenticator for authentication of the individual.

34. (New) A method for a website to directly authenticate an individual over a communication network such that the individual is not redirected to another site and without requiring previous information about the individual, the method comprising:

Requesting both a static key and a dynamic key from the individual in order to validate the individual's identity; and

Receiving both the static and dynamic keys from the individual over the communication network; and

Authenticating the individual based on a combination of the received static and dynamic keys.

35. (New) The method of claim 34, wherein the static and dynamic keys contain credentials for verifying the individual's identity.

36. (New) The method of claim 34, wherein the dynamic key includes a non-predictable and time-dependent SecureCode.

37. (New) The method of claim 34, wherein at least the dynamic key is encrypted.

38. (New) The method of claim 34, wherein a first-trusted authenticator calculates the dynamic key and provides it to the individual for each authentication session.

39. (New) The method of claim 38, the website creating an authentication request message containing the received static and dynamic keys and providing the authentication request message to the first trusted-authenticator for authentication of the individual.

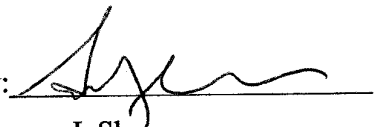
40. (New) The method of claim 38, the website creating an authentication request message containing the received static and dynamic keys and providing the authentication request message to a second trusted-authenticator for authentication of the individual.

Conclusion

The Applicant's believe that new claims 21-40 are allowable over the prior art and are therefore in condition for allowance. If the examiner believes that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at (571) 228-2938.

Respectfully submitted,

Dated: 06/06/2009

By: 

Shawna J. Shaw
Agent for Applicants
Registration No. 57,091

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:	Shawna Jeannine Shaw
Attorney Docket Number:	

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility Search Fee	2111	1	270	270
Utility Examination Fee	2311	1	110	110
Utility filing Fee(efiling)-Small Entity	2011	1	165	165
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**545**

Electronic Acknowledgement Receipt	
EFS ID:	5468483
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
Correspondence Address:	Nader Asghari-Kamrani - 6558 Palisades Drive - Centreville VA 20121 US 7032225104 kamrani@delphinustechnology.com
Filer:	Shawna Jeannine Shaw
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	06-JUN-2009
Filing Date:	18-JAN-2006
Time Stamp:	21:42:34
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Continued Examination (RCE)	SB30.pdf	779506 8a83b910b8924c595aaa3583dccba1bf3ea3bfc6	no	3
Warnings:					
Information:					
2	Amendment Submitted/Entered with Filing of CPA/RCE	RCE.pdf	383839 811a8c2fd86d9157701ebdfba98f3b2eeb865e70	no	6
Warnings:					
Information:					
3	Fee Worksheet (PTO-875)	fee-info.pdf	32427 3c72823723111e061faad895e74153a837fc7f76	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1195772		

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	06/06/2009	(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))	* 20	Minus	** 26	= 0	X $26 =	0	OR	X $ =	
	Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $110 =	0	OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

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:
/DONNA D. SMALLS LOGAN/

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		4456

7590 03/06/2009

Nader Asghari-Kamrani
6558 Palisades Drive
Centreville, VA 20121

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	PAPER NUMBER
2432	
MAIL DATE	DELIVERY MODE
03/06/2009	PAPER

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

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

Office Action Summary	Application No.	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 2008*.

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

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

Disposition of Claims

4)☒ Claim(s) *1,3-12 and 14-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-12 and 14-20* is/are rejected.

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

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

Application Papers

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

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

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

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

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

Priority under 35 U.S.C. § 119

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

a)☐ All b)☐ Some * c)☐ None of:

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

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

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

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

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to applicant's amendment filed on 11/17/2008.

2. Claims 1, 3-12 and 14-20 are pending.

3. Claims 2 and 13 are cancelled.

4. Claims 1 and 12 are amended.

5. Applicant's arguments have been fully considered but they are not persuasive.

Response to Arguments

1. Applicants on page 8 of the remarks argue that "However, nowhere does Johnson disclose that the transaction-specific certificate is provided to an individual in response to a request."

Examiner respectfully disagrees and asserts that Johnson discloses:

"The trusted party may be a financial institution (such as the buyer's home bank, for example), a corporate entity with fiduciary characteristics and established accounts (such as the seller's real estate agency, for example) or some other public or governmental institution (such as the post office, for example) (see, col. 19, lines 29-34)."

"The visit to the trusted party may be carried out physically (in person) or may be carried out by visiting the trusted party's Web site and providing evidence of identity, to the satisfaction of the trusted party. Each of the notified parties to the iTX transaction 500, therefore, may receive a unique ID and may select or be assigned a password, in the manner described above. Alternatively, biometric data or bank-controlled certificates

may supplant or supplement the ID-password combination. Indeed, additional advanced security measure (such as the use of certificates, for example) may be required in the buyer-seller-bank relationship when, for example, large sums of money are transferred via iDraft.TM. or iDraft-C.TM. transactions or any other instance wherein the bank requires added measures of security. Such certificates may then be one-time, transaction-specific certificates authorizing the transaction or may be multiple time certificates applied in special circumstances to determine the limits of the transactions (see col. 19, line 58-col. 20, line 9)."

The fact that the buyer, as one option, visits the trusted party's web site and the buyer, as one option, receives a one-time, transaction-specific certificate corresponds to the recited "a dynamic key provided to the individual, upon request, by the trusted authenticator over a communication network".

2. Applicants on page 8 of the remarks argue that "Thus, the Applicants' submit that Johnson does not teach or suggest a business, organization, or another individual that receives both static and dynamic keys from the individual as claimed."

Examiner respectfully disagrees and asserts that Johnson discloses:

"The Web buyer and the Web seller may then establish a secure communication channel… software at Web seller's site… may then request the Web buyer' identification information. Such identification information includes the Web buyer's ID, may include the identification of the Web buyer's home bank (if this is the first time the Web buyer has made a purchase from this Web seller), selected biometric data and/or other security information requested by the Web buyer's home bank…The identification

information may be sent over the secure communication channel established… Before, the iDraft.TM. transaction is honored by the Web buyer's home bank, however, the Web buyer must be authenticated (col. 12 lines 42-60)". This Indicates that sufficient security information is sent to enables the trusted party to authenticate the Web buyer and it is clear to a person of ordinary skill in the art that a single ID (i.e., one information) related to the Web buyer would not be suffice for authentication.

Johnson further discloses:

"the iDraft.TM. software of the Web buyer's home bank requests the Web buyer's password from the Web buyer…the Web buyer's password is then immediately encrypted… The Web buyer-provided password, therefore, is immediately encrypted within the iDraft.TM. software at the Web buyer's home bank in a manner that is wholly transparent to the Web buyer. Although there may be a short period of time (on the order of nano- or milliseconds) between the receipt of the unencrypted, clear password from the Web buyer and its later encryption, the unencrypted password is never accessible to or displayed by the Web seller or the Web buyer's home bank, their employees or other individuals (col. 13, lines 6-20)." Since buyer submits his or her password immediately after submitting an ID as though he or she submits them together (i.e., two information).

Johnson and discloses:

"The Web buyer is authenticated by his or her home bank for one session only: the Web buyer will need to be authenticated again the next time he or she logs on to the Web seller's Web site." This indicates that the nature of the authentication is dynamic.

Therefore, for authentication the buyer submits one ID which is static and one password which corresponds to the recited dynamic key which is only known to the buyer and his or her home bank, because the buyer selects the password every time visits the home bank (see also col. 2, lines 9-17; Fig. 1A, S11A and S12A), which indicates that the system of Johnson functionally is equivalent to the invention claimed by the applicants.

3. Examiner, however, in light of the above submission maintains the previous rejections while considering the amendments to the claims 1 and 12 as follows:

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claims 1, 3-12 and 14-20 are rejected under 35 U.S.C. 102(e) as being anticipated by Johnson (6,529,885).

Regarding claims 1 and 12, Johnson discloses:

A system for direct authentication of an individual, comprising:

a trusted authenticator with whom the individual has an existing relationship (see, e.g., Fig. 3, col. 9, lines 9-16 and lines 29-37, where the web buyer's home bank is the trusted authenticator and maintaining a checking account corresponds to the recited an existing relationship);

a static key shared between the individual and the trusted authenticator (see, e.g., col. 9, lines 9-16 and lines 29-37, where the buyer's checking account number or ID (either one) corresponds to the recited a static key);

a dynamic key provided to the individual, upon request, by the trusted authenticator over a communication network (see, e.g., col. 9, lines 9-16 and lines 29-37, col. 20, lines 5-10, where the one-time, specific-transaction certificate authorization corresponds to the recited a dynamic key); and

a business, organization or another individual (see, e.g., Fig. 3, where the web seller web site is the business) that receives the static and dynamic keys from the individual and is able to authenticate the individual via the trusted authenticator over a communication network using the dynamic and static keys (see, e.g., col. 12 , lines 44-67 and col. 13, lines 42-60 and col. 20, lines 5-10, where the iDraft includes static key and dynamic key).

an authentication request message created by the business, organization or another

individual including the static and dynamic keys and communicated to the trusted authenticator (see, e.g., Fig. 2, steps S23 and S24); and

an authentication confirmation, or denial, message created by the trusted authenticator based on the received authentication request message and communicated back to the business, organization or another individual for authentication, or non-authentication, of the individual (see, e.g., Fig. 2, steps S25 through S28).

Regarding claims 3 and 14, Johnson discloses:

The system of claim 1, wherein the business, organization or another individual is able to authenticate the individual in substantially real-time (see, e.g., col. 14, lines 5-10, where the authentication is performed in real time).

Regarding claim 4, Johnson discloses:

The system of claim 1, wherein the business, organization or another individual is able to authenticate the individual without having a pre-existing relationship with the individual (see, e.g., col. 7, lines 2531, where the diverse web seller indicates that the web buyer does not have a pre-existing relationship to at least some of web seller).

Regarding claims 5 and 18, Johnson discloses:

The system of claim 1, wherein the individual and the business, organization or another individual communicate face-to-face or over a communication network (see, e.g., col. 9, lines 9-16 and col. 7, lines 25-45, where diverse sellers implies the inclusion of sellers

selling goods online and through physical and traditional outlets and locations to buyers).

Regarding claim 6, Johnson discloses:

The system of claim 1, wherein the business, organization or another individual is in direct, or indirect, communication with the trusted authenticator (see, e.g., Figs. 3 and 7).

Regarding claims 7 and 15, Johnson discloses:

The system of claim 6, wherein the business, organization or another individual is in communication with a second trusted authenticator over a communication network, and the second trusted authenticator communicates with the trusted authenticator over a communication network for authentication of the individual (see, e.g., Figs. 3, where the web seller bank corresponds to the recited a second trusted authenticator and the web seller home bank corresponds to the recited the trusted authenticator).

Regarding claims 8 and 16, Johnson discloses:

The system of claim 1, wherein the static key includes pre-shared information between the individual and the trusted authenticator and may be encrypted (see, e.g., col. 9, lines 9-16 and lines 29-37, where the buyer's checking account number, password or ID (either one) corresponds to the recited a static key; col. 8, lines 59-67).

Regarding claims 9 and 17, Johnson discloses:

The system of claim 1, wherein the dynamic key includes a SecureCode that is dynamic, non-predictable and time dependent and may be encrypted (see, e.g., col. 9, lines 9-13, col. 20, lines 5-10).

Regarding claims 10 and 19, Johnson discloses:

The system of claim 1, wherein the communication network(s) include(s): private and/or public networks such as the Internet (see, e.g., Fig. 3).

Regarding claims 11 and 20, Johnson discloses:

The system of claim 1, wherein the communication network(s) include(s): wireless networks (see, e.g., col. 15, lines 35-45).

Regarding claim 15, this claim is rejected as applied to the like elements of claims 1, 12 and 7.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

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

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

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

/A. N./
Examiner, Art Unit 2432

March 1, 2009

/Benjamin E Lanier/
Primary 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							
	1	✓	✓							
	2	✓	-							
	3	✓	✓							
	4	✓	✓							
	5	✓	✓							
	6	✓	✓							
	7	✓	✓							
	8	✓	✓							
	9	✓	✓							
	10	✓	✓							
	11	✓	✓							
	12	✓	✓							
	13	✓	-							
	14	✓	✓							
	15	✓	✓							
	16	✓	✓							
	17	✓	✓							
	18	✓	✓							
	19	✓	✓							
	20	✓	✓							

FACSIMILE TRANSMITTAL SHEET

TO:	FROM:
Examiner Nobahar	Shawna J. Shaw
COMPANY:	DATE: 11/16/2008
FAX NUMBER:	TOTAL NO. OF PAGES INCLUDING COVER: 12
PHONE NUMBER: (571) 228-2938	SENDER'S REFERENCE NUMBER:
RE: 11/333,400	YOUR REFERENCE NUMBER:

☐ URGENT ☐ FOR REVIEW ☐ PLEASE COMMENT ☐ PLEASE REPLY ☐ PLEASE RECYCLE

NOTES/COMMENTS:

Please find attached an Amendment and Remarks in response to the Non-final Office Action mailed 09/15/2008.

RECEIVED
CENTRAL FAX CENTER
NOV 17 2008

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Nader Ashgari-Kamrani et al.

Application No.: 11/333,400 Confirmation No.:

Filed: 01/18/2006 Art Unit: 2132

For: Direct Authentication System and Method via Trusted Authenticators Examiner: A. Nobahar

AMENDMENT AND RESPONSE

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

INTRODUCTORY COMMENTS

In response to the Non-final Office Action mailed 09/15/2008, the Applicants respectfully request reconsideration based on the Amendment and Remarks which follow.

1. (Currently amended) A system for direct authentication of an individual, comprising:

a trusted authenticator with whom the individual has an existing relationship;

a static key shared between the individual and the trusted authenticator;

a dynamic key provided to the individual, upon request, by the trusted authenticator over a communication network; [[and]]

a business, organization or another individual that receives the static and dynamic keys from the individual and is able to authenticate the individual via the trusted authenticator over a communication network using the dynamic and static keys[[.]];

an authentication request message created by the business, organization or another individual including the static and dynamic keys and communicated to the trusted authenticator; and

an authentication confirmation, or denial, message created by the trusted authenticator based on the received authentication request message and communicated back to the business, organization or another individual for authentication, or non-authentication, of the individual.

2. (Canceled)

3. (Original) The system of claim 1, wherein the business, organization or another individual is able to authenticate the individual in substantially real-time.

4. (Original) The system of claim 1, wherein the business, organization or another individual is able to authenticate the individual without having a pre-existing relationship with the individual.

5. (Original) The system of claim 1, wherein the individual and the business, organization or another individual communicate face-to-face or over a communication network.

6. (Original) The system of claim 1, wherein the business, organization or another individual is in direct, or indirect, communication with the trusted authenticator.

7. (Original) The system of claim 6, wherein the business, organization or another individual is in communication with a second trusted authenticator over a communication network, and the second trusted authenticator communicates with the trusted authenticator over a communication network for authentication of the individual.

8. (Original) The system of claim 1, wherein the static key includes pre-shared information between the individual and the trusted authenticator and may be encrypted.

9. (Original) The system of claim 1, wherein the dynamic key includes a SecureCode that is dynamic, non-predictable and time dependent and may be encrypted.

10. (Previously presented) The system of claim 1, wherein the communication network(s) include(s): private and/or public networks such as the Internet.

11. (Previously presented) The system of claim 1, wherein the communication network(s) include(s): wireless networks.

12. (Currently amended) A method for directly authenticating an individual, comprising the steps of:

an individual who needs to be authenticated by a business, organization or another individual, requests a dynamic key from a trusted authenticator over a communication network;

the trusted authenticator calculates a dynamic key and provides it to the individual;

the individual provides the business, organization or another individual with the calculated dynamic key and a static key already known to the individual and trusted authenticator;

the business, organization or another individual communicates the static and dynamic keys to the trusted authenticator, either directly or indirectly, over a communication network for validation and authentication of the individual[[.]];

wherein the step of communicating includes sending an authentication request message including the static and dynamic keys to the trusted authenticator and receiving an authentication confirmation, or denial, message back from the trusted authenticator.

13. (Canceled)

14. (Original) The method of claim 12, wherein authentication of the individual is performed in substantially real time.

15. (Original) The method of claim 12, wherein the business, organization or another individual submits the static and dynamic keys to a second trusted authenticator, and the second trusted authenticator submits the static and dynamic keys to the first trusted authenticator for validation and authentication of the individual.

16. (Original) The method of claim 12, wherein the static key includes pre-shared information between the individual and the trusted authenticator and may be encrypted.

17. (Original) The method of claim 12, wherein the dynamic key includes a SecureCode that is dynamic, non-predictable and time dependent and may be encrypted.

18. (Original) The method of claim 12, wherein the individual and the business, organization, or another individual communicate face-to-face or over a communication network.

19. (Previously presented) The method of claim 12, wherein the communication network(s) include: private and/or public networks such as the Internet.

20. (Previously presented) The method of claim 12, wherein the communication network(s) include: wireless networks.

REMARKS

Currently claims 1, 3-12 and 14-20 are pending. Claims 1-20 stand rejected. Claims 1 and 12 have been amended to incorporate the subject matter of canceled dependent claims 2 and 13. Accordingly, no new matter has been added and new issues have not been raised. Applicants respectfully request reconsideration based on the remarks that follow.

I. Rejections Under 35 U.S.C. § 102(e)

Claims 1-20 are rejected under 35 U.S.C. § 102(e) as being anticipated by Johnson (US Patent No. 6,529,885, hereinafter "Johnson"). Applicants respectfully traverse.

Independent claim 1, as amended, recites: "a dynamic key provided to the individual, upon request", "a business, organization or another individual that receives the static and dynamic keys from the individual" and "an authentication request message created by the business, organization or another individual including the static and dynamic keys." According to MPEP § 2131, a claim is anticipated "only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." The Applicants' submit that Johnson does not disclose all the elements of claim 1, and therefore fails to anticipate the claim.

Johnson is directed to a system and method for carrying out Directory-Authenticated electronic transactions. To perform a transaction, a web buyer submits a user ID and password to their home bank (S12B, col. 10 lines 8-11). The home bank immediately encrypts the password and authenticates the buyer by comparing the received encrypted password with other encrypted passwords stored in the directory (S14B, col. 10 lines 22-27). For each transaction, the

buyer uses the same password. The security of Johnson relies on the fact that the password is never sent to the seller (col. 12 lines 56-58).

The Office asserts that a one-time, transaction-specific certificate authorization used to supplement the password of Johnson corresponds to the recited dynamic key (Office Action, page 3). However, nowhere does Johnson disclose that the transaction-specific certificate is provided to an individual in response to a request. The fact that Johnson clearly states certificates should be relegated to "special" circumstances and that use of such certificates may "unduly burden the free-flow of e-commerce" (col. 20 lines 5-11), suggests that Johnson does not inherently provide a dynamic key to an individual for a transaction upon request as claimed.

The Office further asserts that the web seller web site of Johnson corresponds to the recited business, organization, or another individual that receives the static and dynamic keys from the individual (Office Action, page 3). The Applicants' disagree. Johnson does not disclose where the web seller website receives either the password or the one-time, transaction-specific certificate from the individual. Johnson does disclose, however, that the buyer's password is never sent to the seller (col. 12 lines 56-58). Moreover, the Office does not provide any explanation how such a feature is necessarily inherently present in Johnson. Thus, the Applicants' submit that Johnson does not teach or suggest a business, organization, or another individual that receives both static and dynamic keys from the individual as claimed.

The Office also asserts that steps 23 and 24 of Johnson correspond to "an authentication request message created by the business, organization, or another individual including the static and dynamic keys." (Office Action, page 3). Applicants disagree. In steps 23 and 24 of Johnson, only the Web buyer's ID (corresponding to the "static" key) is received by the Web seller - but not the dynamic key. Steps 25 and 26 of Johnson only disclose that the Web buyer's password is received by the home Bank. Thus, Applicants' maintain that Johnson does not disclose "an authentication request message created by the

business, organization, or another individual including the static and dynamic keys" as claimed.

For at least the above reasons, Applicants' submit that Johnson fails to anticipate independent claim 1 and its dependents under 35 USC 102(e) and respectfully request that the rejection of claims 1 and 3-11 be withdrawn.

Independent claim 12, as amended, recites: "an individual who ... requests a dynamic key from a trusted authenticator," "the trusted authenticator calculates a dynamic key and provides it to the individual", "the individual provides the business, organization or another individual with the calculated dynamic key and a static key," and "an authentication request message created by the business, organization or another individual including the static and dynamic keys." According to MPEP § 2131, a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." The Applicants' submit that Johnson does not disclose all the elements of claim 12, and therefore fails to anticipate the claim.

Johnson is directed to a system and method for carrying out Directory-Authenticated electronic transactions. To perform a transaction, a web buyer submits a user ID and password to their home bank (S12B, col. 10 lines 8-11). The home bank immediately encrypts the password and authenticates the buyer by comparing the received encrypted password with other encrypted passwords stored in the directory (S14B, col. 10 lines 22-27). For each transaction, the buyer uses the same password. The security of Johnson relies on the fact that the password is never sent to the seller (col. 12 lines 56-58).

The Office asserts that a one-time, transaction-specific certificate authorization used to supplement the password of Johnson corresponds to the recited dynamic key (Office Action, page 3). However, Johnson does not disclose where the home bank calculates a dynamic key in response to a request from the web buyer. The fact that Johnson clearly states certificates should be relegated to "special" circumstances and that use of such certificates may

"unduly burden the free-flow of e-commerce" (col. 20 lines 5-11), suggests that Johnson does not inherently provide a dynamic key in response to an individual's request as claimed.

The Office further asserts that the web seller web site of Johnson corresponds to the recited business, organization, or another individual that receives the static and dynamic keys from the individual (Office Action, page 3). The Applicants' disagree. Johnson does not disclose where the web seller website receives either the password or the one-time, transaction-specific certificate from the individual. Johnson does disclose, however, that the buyer's password is never sent to the seller (col. 12 lines 56-58). Moreover, the Office does not provide any explanation how such a feature is necessarily inherently present in Johnson. Thus, the Applicants' submit that Johnson does not teach or suggest a business, organization, or another individual that receives both static and dynamic keys from the individual as claimed.

The Office also asserts that steps 23 and 24 of Johnson correspond to an authentication request message created by the business, organization or another individual including the static and dynamic keys and communicated to the trusted authenticator (Office Action, page 3). The Applicants' disagree. In steps 23 and 24 of Johnson, the Web buyer's ID (corresponding to the "static" key) is received by the Web seller - but not the dynamic key. Steps 25 and 26 of Johnson only disclose that the Web buyer's password is received by the home Bank. Thus, the Applicants' maintain that Johnson does not disclose "an authentication request created by the business, organization or another individual including the static and dynamic keys" as claimed.

For at least the above reasons, the Applicants' respectfully submit that Johnson fails to anticipate independent claim 12 and its dependents under 35 USC 102(e) and request that the rejection of claims 12 and 14-20 be withdrawn.

In contrast to Johnson, the present invention provides a dynamic key to the individual upon authentication (p. 19 lines 19-21). In response to a request, the trusted-authenticator calculates and sends a dynamic key to the individual (p.

21 lines 1-3). The individual then provides the dynamic key and static key to a business, organization, or another individual (p. 19 lines 15-17). An online merchant, for example, may receive both static and dynamic keys from the individual and forward them to the trusted authenticator to validate the individual's identity. Therefore, one of several advantages of the present invention is that an online merchant does not need to redirect the individual away from its own website to be authenticated, and thereby risk losing the individual's business.

Conclusion

The Applicants' respectfully request reconsideration of the claim rejections based on the above remarks. Since it is believed that all aspects of the rejections set forth in the Office Action mailed 09/15/2008 have been addressed and overcome, the Applicants' submit that the present application is now in condition for allowance. If the examiner believes that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at (571) 228-2938.

Respectfully submitted,

Dated: 11/17/2008

Shawna J. Shaw
Agent for Applicants
Registration No. 57,091

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	150		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	150		TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	11/17/2008	(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))	* 18	Minus	** 26	= 0	X $26 =	0	OR	X $ =	
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $110 =	0	OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

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:
/FELICIA ALLEN-JENKINS/

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		4456

7590 09/15/2008

Nader Asghari-Kamrani
6558 Palisades Drive
Centreville, VA 20121

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
09/15/2008	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	2132	

-- 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 *28 April 2006*.

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

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

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* 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 *18 January 2006* 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 *01/18/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

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 –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claims 1-20 and 12-14 are rejected under 35 U.S.C. 102(e) as being anticipated by Johnson (6,529,885).

Regarding claims 1 and 12, Johnson discloses:

A system for direct authentication of an individual, comprising:

a trusted authenticator with whom the individual has an existing relationship (see, e.g., Fig. 3, col. 9, lines 9-16 and lines 29-37, where the web buyer's home bank is the trusted authenticator and maintaining a checking account corresponds to the recited an existing relationship);

a static key shared between the individual and the trusted authenticator (see, e.g., col.

9, lines 9-16 and lines 29-37, where the buyer's checking account number or ID (either one) corresponds to the recited a static key);

a dynamic key provided to the individual, upon request, by the trusted authenticator over a communication network (see, e.g., col. 9, lines 9-16 and lines 29-37, col. 20, lines 5-10, where the one-time, specific-transaction certificate authorization corresponds to the recited a dynamic key); and

a business, organization or another individual (see, e.g., Fig. 3, where the web seller web site is the business) that receives the static and dynamic keys from the individual and is able to authenticate the individual via the trusted authenticator over a communication network using the dynamic and static keys (see, e.g., col. 12 , lines 44-67 and col. 13, lines 42-60 and col. 20, lines 5-10, where the iDraft includes static key and dynamic key).

Regarding claims 2 and 13, Johnson discloses:

The system of claim 1, further including:

an authentication request message created by the business, organization or another individual including the static and dynamic keys and communicated to the trusted authenticator (see, e.g., Fig. 2, steps S23 and S24); and

an authentication confirmation, or denial, message created by the trusted authenticator based on the received authentication request message and communicated back to the business, organization or another individual for authentication, or non-authentication, of the individual (see, e.g., Fig. 2, steps S25 through S28).

Regarding claims 3 and 14, Johnson discloses:

The system of claim 1, wherein the business, organization or another individual is able to authenticate the individual in substantially real-time (see, e.g., col. 14, lines 5-10, where the authentication is performed in real time).

Regarding claim 4, Johnson discloses:

The system of claim 1, wherein the business, organization or another individual is able to authenticate the individual without having a pre-existing relationship with the individual (see, e.g., col. 7, lines 2531, where the diverse web seller indicates that the web buyer does not have a pre-existing relationship to at least some of web seller).

Regarding claims 5 and 18, Johnson discloses:

The system of claim 1, wherein the individual and the business, organization or another individual communicate face-to-face or over a communication network (see, e.g., col. 9, lines 9-16 and col. 7, lines 25-45, where diverse sellers implies the inclusion of sellers selling goods online and through physical and traditional outlets and locations to buyers).

Regarding claim 6, Johnson discloses:

The system of claim 1, wherein the business, organization or another individual is in direct, or indirect, communication with the trusted authenticator (see, e.g., Figs. 3 and 7).

Regarding claim 7, Johnson discloses:

The system of claim 6, wherein the business, organization or another individual is in communication with a second trusted authenticator over a communication network, and the second trusted authenticator communicates with the trusted authenticator over a communication network for authentication of the individual (see, e.g., Figs. 3, where the

web seller bank corresponds to the recited a second trusted authenticator and the web seller home bank corresponds to the recited the trusted authenticator).

Regarding claims 8 and 16, Johnson discloses:

The system of claim 1, wherein the static key includes pre-shared information between the individual and the trusted authenticator and may be encrypted (see, e.g., col. 9, lines 9-16 and lines 29-37, where the buyer's checking account number, password or ID (either one) corresponds to the recited a static key; col. 8, lines 59-67).

Regarding claims 9 and 17, Johnson discloses:

The system of claim 1, wherein the dynamic key includes a SecureCode that is dynamic, non-predictable and time dependent and may be encrypted (see, e.g., col. 9, lines 9-13, col. 20, lines 5-10).

Regarding claims 10 and 19, Johnson discloses:

The system of claim 1, wherein the communication network(s) include(s): private and/or public networks such as the Internet (see, e.g., Fig. 3).

Regarding claims 11 and 20, Johnson discloses:

The system of claim 1, wherein the communication network(s) include(s): wireless networks (see, e.g., col. 15, lines 35-45).

Regarding claim 15, this claim is rejected as applied to the like elements of claims 1, 12 and 7.

Conclusion

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

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

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

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

September 02/08

/Abdulhakim Nobahar/
Examiner, Art Unit 2132

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132

Notice of References Cited	Application/Control No. 11/333,400	Applicant(s)/Patent Under Reexamination ASGHARI-KAMRANI ET AL.	
	Examiner ABDULHAKIM NOBAHAR	Art Unit 2132	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,529,885 B1	03-2003	Johnson, Richard C.	705/64
*	B	US-5,883,810 A	03-1999	Franklin et al.	705/39
*	C	US-6,748,367 B1	06-2004	Lee, Joonho John	705/66
*	D	US-2002/0087483 A1	07-2002	Harif, Shlomi	705/76
*	E	US-6,233,565 B1	05-2001	Lewis et al.	705/35
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 4456

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
11/333,400	01/18/2006 RULE	713	2132	

APPLICANTS

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

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

This application is a CIP of 09/940,635 08/29/2001 PAT 7,356,837
and claims benefit of 60/650,137 02/07/2005

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

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **
03/07/2006

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☐ No Verified and Acknowledged /ABDULHAKIM NOBAHAR/ Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		VA	4	20	2

ADDRESS

Nader Asghari-Kamrani
6558 Palisades Drive
Centreville, VA 20121
UNITED STATES

TITLE

Direct authentication system and method via trusted authenticators

FILING FEE RECEIVED		
500	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

BIB (Rev. 05/07).

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L2	2	"20020188481".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/02 09:23
L3	6	"5757917".pn. "5826241".pn. "5890137".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/02 09:25
L4	2	"5557516".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/02 09:27
L5	68086	(713/155,156).ccls. (726/4,5).ccls. (705/39,,64,74,77,78).ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/02 10:11
L6	5370	5 and (realtime time dynamic$6 temporar$5 single onetime on-the-fly) near1 (identity identification identif$5 ID DID password passphrase)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/02 10:12
L7	3878	6 and ((user customer consumer client origina$4 receiv $3 buy$3 purchas$3 initiat$3) near1 (identity identification identif$5 ID DID))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/02 10:12
L8	1262	7 and ((financ$6 commerc$6 bank$3 credit$3 sale electronic $5) adj1 transaction)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/02 10:12
L9	846	8 and ((center$4 main authorized) adj1 (institution entity financ$6 commerc$6 bank $4 office) authority CA official)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/02 10:13
L10	658	9 and ((center$4 main authorized institution entity financ$6 commerc$6 bank$4 office authority CA official) with (authenticat$4 authoriz$4 verification verify$3 validat$4) with (user customer consumer client origina$4 receiv$3 buy$3 purchas$3 initiat$3))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/02 10:13

L11	261	10 and ((trusted protected secure private local) adj network)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/02 10:14
L12	240	11 and ((authenticat$4 authoriz $5 verification verify$3 validat $4) near2 (identity identification identif$5 ID DID certificat))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/02 10:14
L13	83	12 and @ad<"20010901"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/09/02 10:15

9/2/2008 10:15:57 AM
C:\Documents and Settings\hnobahar\My Documents\EAST\Workspaces\11239046.wsp

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11333400	ASGHARI-KAMRANI ET AL.
	Examiner	Art Unit
	ABDULHAKIM NOBAHAR	2132

✓	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								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11333400	ASGHARI-KAMRANI ET AL.
	Examiner	Art Unit
	ABDULHAKIM NOBAHAR	2132

SEARCHED			
Class	Subclass	Date	Examiner
713	155,156	9/2/2008	AN
726	4,5	9/2/2008	AN
705	39,64,74,77,78	9/2/2008	AN

SEARCH NOTES		
Search Notes	Date	Examiner

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

/A. N./ Examiner.Art Unit 2132	

PTO/SB/08A (07-05)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	
Filing Date	
First Named Inventor	Asghari-Kamrani et al.
Art Unit	
Examiner Name	
Attorney Docket Number	

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/08B (07-05)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 2

Complete if Known	
Application Number	
Filing Date	
First Named Inventor	Asghari-Kamrani et al.
Art Unit	
Examiner Name	
Attorney Docket Number	

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
/H.N./		LOPUCKI, "Human Identification Theory and the Identity Theft Problem," Texas Law Review, Vol. 80, pp. 89-134 (2001)	
/H.N./		SOLOVE, "Identity Theft, Privacy, and the Architechture of Vulnerability," Hastings Law Journal, Vol. 54 No. 4, p.1251 (2003)	

Examiner Signature	/Abdulhakim Nobahar/	Date Considered	09/09/2008

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

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

IFW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Nader Ashgari-Kamrani et al.

Application No.: 11/333,400 — Confirmation No.:

Filed: 01/18/2006 — Art Unit: 2132

For: DIRECT AUTHENTICATION SYSTEM AND METHOD VIA TRUSTED AUTHENTICATORS — Examiner:

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

PRELIMINARY AMENDMENT

In response to the Notice to File Missing Parts mailed 03/07/2006, please 'cancel the additional claims for which fees are due' by way of the attached preliminary amendment beginning on page 2 of this communication.

Respectfully Submitted,

Shawna J. Shaw
Agent for Applicants
Registration No.: 57,091

In the Claims:

1. (Original) A system for direct authentication of an individual, comprising:

a trusted authenticator with whom the individual has an existing relationship;

a static key shared between the individual and the trusted authenticator;

a dynamic key provided to the individual, upon request, by the trusted authenticator over a communication network; and

a business, organization or another individual that receives the static and dynamic keys from the individual and is able to authenticate the individual via the trusted authenticator over a communication network using the dynamic and static keys.

2. (Original) The system of claim 1, further including:

an authentication request message created by the business, organization or another individual including the static and dynamic keys and communicated to the trusted authenticator; and

an authentication confirmation, or denial, message created by the trusted authenticator based on the received authentication request message and communicated back to the business, organization or another individual for authentication, or non-authentication, of the individual.

3. (Original) The system of claim 1, wherein the business, organization or another individual is able to authenticate the individual in substantially real-time.

4. (Original) The system of claim 1, wherein the business, organization or another individual is able to authenticate the individual without having a pre-existing relationship with the individual.

5. (Original) The system of claim 1, wherein the individual and the business, organization or another individual communicate face-to-face or over a communication network.

6. (Original) The system of claim 1, wherein the business, organization or another individual is in direct, or indirect, communication with the trusted authenticator.

7. (Original) The system of claim 6, wherein the business, organization or another individual is in communication with a second trusted authenticator over a communication network, and the second trusted authenticator communicates with the trusted authenticator over a communication network for authentication of the individual.

8. (Original) The system of claim 1, wherein the static key includes pre-shared information between the individual and the trusted authenticator and may be encrypted.

9. (Original) The system of claim 1, wherein the dynamic key includes a SecureCode that is dynamic, non-predictable and time dependent and may be encrypted.

10. (Currently Amended) The system of claim 1, ~~5 or 7,~~ wherein the communication network(s) include(s): private and/or public networks such as the Internet.

11. (Currently Amended) The system of claim 1, ~~5, or 7,~~ wherein the communication network(s) include(s): wireless networks.

12. (Original) A method for directly authenticating an individual, comprising the steps of:

an individual who needs to be authenticated by a business, organization or another individual, requests a dynamic key from a trusted authenticator over a communication network;

the trusted authenticator calculates a dynamic key and provides it to the individual;

the individual provides the business, organization or another individual with the calculated dynamic key and a static key already known to the individual and trusted authenticator;

the business, organization or another individual communicates the static and dynamic keys to the trusted authenticator, either directly or indirectly, over a communication network for validation and authentication of the individual.

13. (Original) The method of claim 12, wherein the step of communicating includes sending an authentication request message including the static and dynamic keys to the trusted authenticator and receiving an authentication confirmation, or denial, message back from the trusted authenticator.

14. (Original) The method of claim 12, wherein authentication of the individual is performed in substantially real time.

15. (Original) The method of claim 12, wherein the business, organization or another individual submits the static and dynamic keys to a second trusted authenticator, and the second trusted authenticator submits the static and dynamic keys to the first trusted authenticator for validation and authentication of the individual.

16. (Original) The method of claim 12, wherein the static key includes pre-shared information between the individual and the trusted authenticator and may be encrypted.

17. (Original) The method of claim 12, wherein the dynamic key includes a SecureCode that is dynamic, non-predictable and time dependent and may be encrypted.

18. (Original) The method of claim 12, wherein the individual and the business, organization, or another individual communicate face-to-face or over a communication network.

19. (Currently Amended) The method of claim 12 ~~or 18~~, wherein the communication network(s) include: private and/or public networks such as the Internet.

20. (Currently Amended) The method of claim 12 ~~or 18~~, wherein the communication network(s) include: wireless networks.

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	04/28/2006	(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))	* 20	Minus	** 26	= 0	X $25 =	0	OR	X $ =	
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $100 =	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:
/STEFANIE BRYCE/

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371 (c) DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NUMBER
11/333,400	01/18/2006	Nader Asghari-Kamrani	

CONFIRMATION NO. 4456

Nader Asghari-Kamrani
6558 Palisades Drive
Centreville, VA 20121

FORMALITIES LETTER

Date Mailed: 03/07/2006

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

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

- Additional claim fees of **$330** as a small entity, including any required multiple dependent claim fee, are required. Applicant must submit the additional claim fees or cancel the additional claims for which fees are due.

SUMMARY OF FEES DUE:

Total additional fee(s) required for this application is **$330** for a Small Entity

- Total additional claim fee(s) for this application is **$330**
  - **$150** for **6** total claims over 20.
  - **$180** for multiple dependent claim surcharge.

Replies should be mailed to: Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

A copy of this notice MUST be returned with the reply.

Cont

Office of Initial Patent Examination (571) 272-4000, or 1-800-PTO-9199, or 1-800-972-6382
PART 3 - OFFICE COPY

PTO/SB/05 (04-05)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office. U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	
First Inventor	Asghari-Kamrani et al.
Title	Direct Authentication System and Me
Express Mail Label No.	

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

1. [✓] **Fee Transmittal Form** (e.g., PTO/SB/17) *(Submit an original and a duplicate for fee processing)*
2. [✓] **Applicant claims small entity status.** See 37 CFR 1.27.
3. [✓] **Specification** [*Total Pages* ~~28~~ 33] Both the claims and abstract must start on a new page *(For information on the preferred arrangement, see MPEP 608.01(a))*
4. [✓] **Drawing(s)** (*35 U.S.C. 113*) [*Total Sheets* 4]
5. **Oath or Declaration** [*Total Sheets* 3]
   a. [✓] Newly executed (original or copy)
   b. [ ] A copy from a prior application (37 CFR 1.63(d)) *(for continuation/divisional with Box 18 completed)*
      i. [ ] DELETION OF INVENTOR(S) Signed statement attached deleting inventor(s) name in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
6. [ ] **Application Data Sheet.** See 37 CFR 1.76
7. [ ] **CD-ROM or CD-R** in duplicate, large table or Computer Program *(Appendix)* [ ] Landscape Table on CD
8. **Nucleotide and/or Amino Acid Sequence Submission** *(if applicable, items a. – c. are required)*
   a. [ ] Computer Readable Form (CRF)
   b. Specification Sequence Listing on:
      i. [ ] CD-ROM or CD-R (2 copies); or
      ii. [ ] Paper
   c. [ ] Statements verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

9. [ ] **Assignment Papers** (cover sheet & document(s))
   Name of Assignee _____
10. [ ] **37 CFR 3.73(b) Statement** *(when there is an assignee)* [ ] **Power of Attorney**
11. [ ] **English Translation Document** *(if applicable)*
12. [ ] **Information Disclosure Statement** (PTO/SB/08 or PTO-1449) [ ] Copies of citations attached
13. [ ] **Preliminary Amendment**
14. [ ] **Return Receipt Postcard** (MPEP 503) *(Should be specifically itemized)*
15. [ ] **Certified Copy of Priority Document(s)** *(if foreign priority is claimed)*
16. [ ] **Nonpublication Request** under 35 U.S.C. 122(b)(2)(B)(i). Applicant must attach form PTO/SB/35 or equivalent.
17. [ ] Other: _____

18. If a CONTINUING APPLICATION, *check appropriate box, and supply the requisite information below and in the first sentence of the specification following the title, or in an Application Data Sheet under 37 CFR 1.76:*

[ ] Continuation [ ] Divisional [✓] Continuation-in-part (CIP) of prior application No.: 09/940,635

Prior application information: *Examiner* A. Nobahar *Art Unit:* 2132

19. CORRESPONDENCE ADDRESS

[ ] The address associated with Customer Number: [ ] *OR* [✓] Correspondence address below

Name	Nader Asghari-Kamrani				
Address	6558 Palisades Drive				
City	Centreville	State	VA	Zip Code	20121
Country	U.S.A.	Telephone	(703) 222-~~1570~~ 5104	Email	kamrani@delphinustechnology.com

Signature		Date	01/18/06
Name (Print/Type)	Nader, Asghari Kamrani	Registration No. (Attorney/Agent)	

This collection of information is required by 37 CFR 1.53(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

PTO/SB/17 (12-04v2)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Effective on 12/08/2004.
Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).

FEE TRANSMITTAL
For FY 2005

☑ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($)

Complete if Known	
Application Number	
Filing Date	
First Named Inventor	Asghari-Kamrani et al.
Examiner Name	
Art Unit	
Attorney Docket No.	

METHOD OF PAYMENT (check all that apply)

☑ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): _____

☐ Deposit Account Deposit Account Number: _____ Deposit Account Name: _____

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☐ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, except for the filing fee

☐ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17 ☐ Credit any overpayments

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.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

	FILING FEES		SEARCH FEES		EXAMINATION FEES		
		Small Entity		Small Entity		Small Entity	
Application Type	Fee ($)	Fee ($)	Fee ($)	Fee ($)	Fee ($)	Fee ($)	Fees Paid ($)
Utility	300	150	500	250	200	100	500
Design	200	100	100	50	130	65	
Plant	200	100	300	150	160	80	
Reissue	300	150	500	250	600	300	
Provisional	200	100	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 (including Reissues)	50	25
Each independent claim over 3 (including Reissues)	200	100
Multiple dependent claims	360	180

Total Claims	Extra Claims	Fee ($)	Fee Paid ($)
_____ - 20 or HP =	_____ x	_____ =	_____

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims	Extra Claims	Fee ($)	Fee Paid ($)
_____ - 3 or HP =	_____ x	_____ =	_____

HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims	
Fee ($)	Fee Paid ($)
_____	_____

3. APPLICATION SIZE FEE

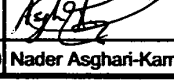
If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets	Extra Sheets	Number of each additional 50 or fraction thereof	Fee ($)	Fee Paid ($)
_____ - 100 =	_____ / 50 =	_____ (round up to a whole number) x	_____ =	_____

4. OTHER FEE(S)

	Fees Paid ($)
Non-English Specification, $130 fee (no small entity discount)	
Other (e.g., late filing surcharge): _____	

SUBMITTED BY

Signature		Registration No. (Attorney/Agent)	Telephone
Name (Print/Type)	Nader Asghari-Kamrani		Date 01/18/06

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.

Direct Authentication System and Method via Trusted Authenticators

U.S. Patent Application of

Nader Asghari-Kamrani

and

Kamran Asghari-Kamrani

Direct Authentication System and Method
via Trusted Authenticators

This application is a continuation-in-part of U.S. Patent Application No. 09/940,635 filed August 31, 2001, and claims priority to U.S. Provisional Application No. 60/650,137 filed February 7, 2005.

BACKGROUND OF THE INVENTION

1. FIELD OF THE INVENTION

The present invention generally relates to a direct authentication system and method, more particularly, to a new two-factor authentication method used by a business to authenticate its customers' identity utilizing trusted-authenticators.

2. DESCRIPTION OF THE RELATED ART

Fraud and Identity theft, the taking of a person's identity for the purpose of committing a criminal act, is a growing national concern, both in terms of its affect on its victims, and its potential national security implications. Checking account fraud costs US banks USD 698 million in 2002, according to the American

Bankers' Association, while those perpetrating the fraud attempted to take USD 4.3 billion in total. Identity theft costs financial institutions USD 47.6 billion in 2002-2003. A report issued in September 2003 by the Federal Trade Commission estimates that almost 10 million Americans were victims of some type of identity theft within the previous year. Especially unnerving are the numerous accounts of the ordeals that victims endure as they attempt to deal with the results of this crime. They are assumed to be responsible for the debts incurred by the thief until they can demonstrate that they have been victims of fraud. They are targeted by collection agencies trying to collect on debts generated by thieves who open new accounts in their name. They have to deal with damaging information placed in their credit files as a result of the imposter's actions. It's well known how this can happen. Fraudulent charges may be posted to someone's checking account if the thief knows the account number and banks routing number. Identity thieves can "take over" an existing account and withdraw money, as well as change other account information such as mailing address, if the thief knows a few pieces of sensitive personal information, especially the account holder's Social Security Number (SSN). Perhaps worst of all, a thief can easily open a new account in someone else's name by completing an application for a new credit account, using the victim's name and SSN, but with a different address. The credit grantor, whether it be a retailer offering instant credit accounts via their website, a telecommunications company offering a new cell phone account, a bank offering a credit card, or an auto dealership offering a new car loan, uses the information provided by the thief to obtain a credit report on the person named in the account application. If the report indicates that the person named in the application is a good credit risk, a new account will likely be opened in the victim's name. But the victim never knows about the late and unpaid bills, until his credit is ruined.

Online Fraud happens because online businesses such as retailers assume that the person shopping online is the same person whose personal or financial information are given. Identity theft happens because creditors assume that the person filling the application is the same person whose name and personal information are used in the application, unless there is clear evidence to the contrary. A business "authenticates" a customer by matching personal and financial information provided, such as name, SSN, birth date, etc., with information contained in third party databases (indirect authentication). If there is a match on at least a few items of information, it is assumed that the person is the same person who he says he is. This assumption itself is a direct result of a belief that sensitive personal and financial information can be kept secret and out of the hands of thieves. Yet the widespread incidence of fraud and identity theft, as detailed by the personal stories of its many victims, clearly demonstrates that this notion is false. A recent paper by Prof. Daniel Solove ("Identity Theft, Privacy, and the Architecture of Vulnerability", Hastings Law Journal, Vol 54, N o. 4 (2003), page 1251) of the Seton Hall Law School aptly points out that "*The identity thief's ability to so easily access and use our personal and financial data stems from an architecture that does not provide adequate security to our personal and financial information and that does not afford us with a sufficient degree of participation in the collection, dissemination, and use of that information."* He further goes on to say "*The problem, however, runs deeper than the public disclosure of Social Security Numbers (SSN), personal and financial information. The problem stems not only from the government's creation of a de facto identifier and lax protection of it, but also from the private sector's inadequate security measures in handling personal information*". "*Further, identity thieves can obtain personal and financial information simply by paying a small*

fee to various database companies and obtaining a detailed dossier about their victims." There's only a certain amount that an individual can do to prevent sensitive information from getting into the wrong hands, such as keeping a tight grip on one's purse or wallet. Beyond that, the information is easily available to a thief in numerous other ways. It may be available through certain public records. It can be purchased from publicly available databases for a nominal fee. It can be copied from medical claims forms lying around in a doctor's office. Other methods include breaking into various commercial databases containing sensitive information about business's customers, many times with the help of an insider. As long as the authentication of new credit applications is based upon knowledge of a few items of personal information that are supposed to be confidential, the only way to truly prevent this type of identity theft is to keep one's personal information out of the hands of thieves, an impossible task. This is also true in the case of identity theft involving account takeovers, in which the thief uses knowledge of personal information about the victim to obtain information needed to take over someone's existing account.

There have been many attempts to solve above issues and concerns. One being the recent paper by Prof. Lynn LoPucki of the UCLA School of Law (www.ssrn.com/abstract=263213). The paper addresses many of these concerns, and suggests an approach to the identity theft problem that addresses the fundamental flaws in the process. This approach does not depend on keeping personal information secret, asking out-of-wallet questions, or computing fraud scores based on historical data and analytical fraud models. LoPucki's approach, which he calls the Public Identity System (PIDS), would establish a voluntary list of people concerned about identity theft, and who consent to be directly contacted for verification when someone applies for credit in their name.

The list would be maintained by a government agency. An individual would voluntarily provide his/her personal information to the list, including name, SSN, and perhaps other identifying information. A thorough authentication process would ensure that new members of the list are truly the persons they claim to be. A personal appearance before the government agency that maintains the list would be required. Individuals participating in PIDS would specify one or more standardized ways that a creditor should contact them when the creditor has received a new account application in their name. Contact methods would likely be limited to a phone call, e-mail (encrypted or unencrypted), or US Mail. When a creditor receives a new account application, the creditor would consult the list to determine if the person named in the application, as identified by a SSN or other information, is a PIDS participant. If the named person is not a participant, the new account application would be processed in the usual manner. If, however, the named person is a PIDS participant, the creditor would contact the individual directly using one or more of the contact methods specified in the instructions provided by the individual.

A PIDS participant may even require, under some circumstances, a personal appearance before the creditor by anyone applying for a new account in his or her name. The reason for contacting the participant would be to verify that the participant is truly the person who submitted the new account application. To significantly reduce identity theft using this approach, creditors would need to have an incentive to consult the list and follow the instructions given, and consumers would need to participate in PIDS in large numbers.

Although Prof. LoPucki's approach addresses the fundamental flaws in the credit granting process responsible for identity theft, it is time consuming for

creditors to verify customer's identity. Also, some difficulties may arise with its implementation. The list of PIDS participants, together with their Social Security Numbers and contact information, would reside on a government website, and the information would be available to the public. This would only be implemented if the laws were changed to prevent knowledge of this information alone as providing "proof" of identity, as well as preventing other types of privacy invasions that might be enabled with public access to such information. Although the legal changes would make one's personal information much less useful to an identity thief, it is not clear how comfortable people would feel about an arrangement that allows their personal information to be made public in such an overt manner. In addition, PIDS participants would also need to personally appear before the government agency managing the list. These factors may inhibit many people from participating in PIDS. Since creditors would be required to directly contact individuals named in an account application if the person's name appears on the list, creditors may find this type of "direct authentication" process to be burdensome, especially if it involves more than a simple phone call or email. This may lead creditors to oppose PIDS. In addition, there is the question of how the creditor should authenticate the person taking the call, or responding to the email. How can the creditor be sure that the person taking the call, or responding to the email, is truly the person who joined PIDS, and who now should be queried about the credit application? Finally, the implementation of PIDS would seem to require the establishment of a new government bureaucracy to perform necessary functions such as establishing and maintaining the PIDS list, meeting with those individuals seeking to participate, verifying their identity credentials, and establishing the standardized methods by which creditors will contact and interact with PIDS participants. Of course, implementing any alternative to PIDS would also require a certain amount of up-front work to develop the necessary

capabilities and infrastructures. And while it is not unreasonable for a government agency (such as a state motor vehicles bureau) to undertake at least some of these tasks, it is not clear whether any federal or state agencies would be ready and willing to fulfill the entire role.

Another possible solution has been suggested to modify Prof. LoPucki's approach (PIDS procedure) somewhat to take advantage of the existing trust relationships that individuals have already established with various organizations that they deal with. Rather than requiring creditors to authenticate applicants for new accounts by contacting them directly, these interactions could instead be performed by a "trusted authenticator." The trusted authenticator would be an entity that already knows the individual, maintains personal information about that individual, and has established a trusted relationship with that person. The advantage of using trusted authenticators is that the authentication process can be built on trust relationships and infrastructures already in place. A reasonable candidate for such a trusted authenticator would be a bank or other financial institution with whom the individual has already established an account. After all, if most people trust a bank to handle their money and keep it safe, trusting that same bank to authenticate their identities in other financial transactions should be natural. Prof. LoPucki's paper hints at such an arrangement in its discussion of how list members may choose to be contacted:

The [e-mail] contact could be directly with the owner or through the owner's trusted intermediary. Instead of creating a new government bureaucracy to implement PIDS, the existing infrastructures and trust relationships within the financial services community could be enhanced to more efficiently derive the same benefits that PIDS provides.

In this modified authentication procedure, a list of all individuals who choose to participate (the "participants") would still be needed. The list would contain a name and SSN of each participant, together with the identity of their trusted authenticator. The list would be maintained by a new organization created by the financial services community specifically for this purpose, rather than by the government. However, the information on the list would not be accessible by the general public, but only by creditors and other members of the financial services community acting as trusted authenticators. The modified authentication procedure works as follows:

The creditor, upon receiving a new account application, checks the list to determine if the person named in the application is a participant. If so, the creditor queries the trusted authenticator designated on the list, and requests verification that the person named in the application is actually the person filing the new account application. If the person is not a participant, the creditor will process the application in the usual way.

Upon receiving a request from a creditor for direct authentication of a participant, who is also one of its customers, the trusted authenticator contacts its customer via a secure email message or phone call, as specified by the customer.

When communication is established, the trusted authenticator must first determine that it is actually communicating with its customer, and not someone else who has intercepted the email or phone call.

An email would contain a link that takes the customer to an authentication screen on the trusted authenticator's website. Here the customer would provide a password or Personal Identification Number (PIN) to authenticate himself/herself. The authentication process may also include an additional biometric factor such as a fingerprint or voiceprint. Most likely, the method of authentication used would be the same as the customer would use for online banking, which provides access to his/her banking accounts online.

A phone call would contain, at least, a request for the customer to provide a PIN or some other secret. A more secure authentication process might include an additional biometric factor, such as a voiceprint. Again, the method of authentication may be the same as the customer may use to perform telephone banking, which provides access to his/her banking accounts over the phone. Once the trusted authenticator has verified the identity of its customer, the trusted authenticator asks its customer whether he/she has filed a specific application for credit, as indicated in the creditor's request for authentication.

If the customer responds affirmatively, the trusted authenticator replies to the creditor that the application appears to be authentic. If the customer responds negatively, the bank responds to the creditor that the application appears to be fraudulent.

The first problem with this solution is the fact that the trusted authenticator contacts its customer via an email message, which allows for phishing or brand spoofing. The customer could receive an email from a user falsely claiming to be the trusted authenticator in an attempt to scam the customer into surrendering private information that will be used for identity theft.

The second problem is the fact that a list of all individuals who choose to participate would still be needed. This will add to privacy and security concerns.

Another problem is the fact that this authentication method lacks the real-time authentication and therefore it is not suited for online transactions.

There have been many attempts to solve the online identification problems using tokens, smart cards or biometrics authentication methods, but these methods failed due to high cost and consumers' dissatisfactions:

Password Generation Tokens – creates custom passwords each time they are activated. The cost of each token makes this type of two-factor authentication method suited only for enterprise spaces and not to the consumer level outside of the enterprise. Another problem with this method is that the passwords are generated using an algorithm that is based on both a unique user ID and the current time, which makes the next generated password guessable. Another drawback of this authentication method is that a consumer has to manage different tokens for different relationships.

Biometrics – measure unique bodily characteristics such as fingerprint as a form of identification. Again, the cost of the devices makes this type of two-factor authentication method suited only for enterprise spaces. For privacy and security reasons, it's not suited to consumer level authentication where biometric images need to be stored and transmitted over a public network such as the Internet for authentication (opens to theft or interception).

Smart Cards and – store information on a tiny computer chip on the card. This type of two-factor authentication method requires a reader device and therefore makes it suited only for enterprise spaces. There have been many attempts to implement this method to the consumer level, but each time it failed because consumers find it difficult to use (Hooking up smart card readers to computer systems), costly and software dependent.

Smart Tokens – are technologically identical to the smart cards with the exception of their form factor and interface. Again, many attempts to implement this type of two-factor authentication method to the consumer level failed due to the same reasons: cost and consumer adoption (difficult to use and difficult to manage).

In view of the foregoing, a need exists for a new and improved direct authentication system and method via trusted-authenticators that validates customers' identity without the deficiencies and disadvantages of the prior arts, mainly the cost and consumer adoption. This new direct authentication system and method via trusted-authenticators will reduce the identity theft, fraud and customer privacy concerns, will be secure, easy to use and manage, will be inexpensive, will offer a high level assurance that an individual is who he/she claims he/she is, and will provide a real-time authentication solution that is suited for the consumer level authentication where real-time identity validation of the consumer is necessary.

SUMMARY OF THE INVENTION

Briefly described, the present invention relates to a direct authentication system and method via trusted-authenticators.

In this invention, direct authentication of an individual would be achieved via a new two-factor authentication method used by businesses to authenticate customers' identity utilizing trusted-authenticators. A trusted-authenticator would be an entity that already knows the individual, maintains information about that individual, and has established a trusted relationship with that individual. A reasonable candidate for such a trusted-authenticator would be bank or other financial institution with whom the individual has already established a relationship. In this invention, the financial services community will have a leading role in implementing stronger forms of authentication for identity theft and fraud prevention.

Experience shows that knowlege-based authentication, where individuals are recognized by demonstrating that they are in possession of information which only that individual would be expected to know, is an inexpensive, easy to use and easy to implement authentication method, where the authentication is beween two entities such as a banks's customer and the bank. It relies on the secret information that is shared between these two entities. Therefore the underlying basis for this method is that only the real individual (bank's customer) would know such identifying information. But, when it comes to direct authentication to the consumer level, where the individual needs to authenticate his/her identity to any other entities with whom the individual does not have an existing relationship, such knowledge-based authentication will not work.

Therefore, it's not secure to share the same secret information that the individual shares with one entity, with other entities for identification purposes. Such information is static and someone who happens to get access to such information could use it for authentication at other entities as well. Therefore, knowledge-based authentication is not secure for direct authentication of individuals.

To eliminate the risks associated with the static nature of the knowledge-based authentication, this invention suggests combining knowledge-based authentication with a dynamic key or information maintained by the trusted-authenticator to create a new two-factor authentication. This new two-factor authentication confirms individual identities using two different credentials:

a) Something the individual knows – This factor is a *static key or information* that the individual shares with his/her trusted-authenticator.

b) Something the individual receives – This factor refers to SecureCode which is a dynamic key or information that the individual requests and receives from his or her trusted-authenticator at the time of authentication through a communication network. It is important to note that the individual's dynamic key is an alphanumeric code and will have a different value each time the individual receives it from his/her trusted-authenticator for authentication purpose.

The strength of this new method of authentication occures when combining two factors. This achieves a high level of assurance that an individual

is who he/she claims he/she is and enhances security and reduces privacy concerns.

The direct authentication of an individual works as follows:

When an individual is on a business's site (offline or online), for successful direct authentication, the business requires the individual to provide his/her static and dynamic keys. The individual requests a dynamic key from his/her trusted-authenticator (using any communication network such as Internet or wireless) and provides it along with his/her static key to the business. When the business receives individual's static and dynamic keys, the business communicates authentication messages including individual's static and dynamic keys to the trusted-authenticator. The trusted-authenticator verifies individual's identity if both static and dynamic keys are valid, otherwise will send a denial authentication message back to the business over the same communication network.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1a is a high-level overview of a direct authentication system and method according to the present invention where the business directly contacts the individual's trusted-authenticator for validation of the individual's identity.

Fig. 1b is another high-level overview of a direct authentication system and method according to the present invention where the business contacts the individual's trusted-authenticator through its own trusted-authenticator to validate the individual's identity.

Fig. 2a illustrates the direct authentication system and method according to the present invention where the business directly contacts the individual's trusted-authenticator for validation of the individual's identity.

Fig. 2b illustrates the direct authentication system and method according to the present invention where the business contacts the individual's trusted-authenticator through its own trusted-authenticator to validate the individual's identity.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Detailed descriptions of the preferred embodiment are provided herein. It is to be understood, however, that the present invention may be embodied in various forms. Therefore, specific details disclosed herein are not to be interpreted as limiting, but rather as a basis for the claims and as a representative basis for teaching one skilled in the art to employ the present invention in virtually any appropriately detailed system, structure or manner.

Furthermore, as used herein, "individual" **10** broadly refers to a person, company or organization that has established a trusted relationship with a trusted-authenticator **30**.

Furthermore, as used herein, "business" **20** broadly refers to a company or organization (online or offline) that has established a trusted relationship with a trusted-authenticator **40** and that needs to authenticate the identity of the individual **10**.

The use of "trusted-authenticator" **30** refers to an entity that already knows the individual **10**, maintains information about that individual **10**, and has established a trusted relationship with that individual **10**. A reasonable candidate for such a trusted-authenticator **30** would be a bank or other financial institution.

The use of "trusted-authenticator" **40** refers to an entity that already knows the business **20**, maintains information about that business **20**, and has established a trusted relationship with that business **20**. A reasonable candidate for such a trusted-authenticator **40** would be a bank or other financial institution.

The use of "static key" refers to pre-shared information between both the individual **10** and individual's trusted-authenticator **30**. The static key of an individual **10** is fixed information that does not change automatically and is used for authentication purposes. A static key might be any identification phrases such as password, name, UserName, SSN, alias, account number, customer number, etc or the combination of this information.

The use of "dynamic key" refers to SecureCode which is a key or information that is variable and is provided to the individual **10** by the individual's trusted-authenticator **30** at the time it is needed for authentication. The dynamic key is an alphanumeric code and will have a different value each time the individual **10** receives it from his/her trusted-authenticator **30** for authentication purposes. To increase security a dynamic key may have a non-repeating value, may be time dependent (valid for some period of time) and may be in an encrypted format.

The use of "communication network" **50** refers to any public or private network, wired or wireless (including cellular) network that exist between individuals **10**, trusted-authenticators **30, 40** and businesses **20** for communication.

The use of "face-to-face communication" **80** refers to a situation when the "communication network" **50** is not required. Meaning that the individual **10** is physically at the location of the business **20** to communicate with the business.

The use of "authentication message" refers to a message that businesses **20**, and trusted-authenticators **30, 40** send and receive to validate individual's identity. An authentication message may include individual's static and dynamic keys and any other information.

With reference to **Fig.1a** and **Fig. 1b**, a direct authentication system **1-1, 1-2** in accordance with the present invention is illustrated. The system **1-1** in Fig. 1a, includes at least one individual **10**, one individual's trusted-authenticator **30**, one business **20** and communication network **50**. The system **1-2** in Fig. 1b, includes at least one individual **10**, one individual's trusted-authenticator **30**, one business **20**, one business's trusted-authenticator **40** and communication network **50**.

The business **20** needs to authenticate the identity of the individual **10** utilizing either the individual's trusted-authenticator **30** or its own trusted-authenticator **40**.

Specifically, when the business **20** desires to validate the individual's **10** identity, the individual **10** is required by the business **20** to provide his/her **static** and **dynamic** keys. A static key is something the individual **10** knows and is a shared secret between the individual and the individual's trusted-authenticator **30**. A dynamic key refers to SecureCode which is an alphanumeric code the individual **10** receives from his/her trusted-authenticator **30** at the time of authentication through a communication network **50**. Each time an individual **10** receives a dynamic key from his/her trusted-authenticator **30**, the dynamic key has a different value.

In accordance with the **first** embodiment of the present invention **Fig.1a,** the business **20** might directly communicate authentication messages with the individual's trusted-authenticator **30** and request the individual's trusted-authenticator **30** to validate the individual's **10** identity. An example would be a creditor **20** who receives customer's **10** static and dynamic keys and directly communicates authentication messages with the customer's bank **30** to validate the customer's **10** identity.

In accordance with the **second** embodiment of the present invention **Fig. 1b**, the business **20** might communicate authentication messages with its own trusted-authenticator **40** and request its own trusted-authenticator **40** to validate the individual's **10** identity by communicating authentication messages with the individual's trusted-authenticator **30**. An example would be an online merchant **20** who receives customer's **10** static and dynamic keys and communicates authentication messages with the merchant's bank **40**. The merchant's bank **40** validates the customer's **10** identity by communicating authentication messages with the customer's bank **30**.

Fig. 2a illustrates the direct authentication method **2-1** in accordance with the first embodiment of the present invention. For two-factor authentication of an individual, the business **20** requests **110** the individual **10** to provide static and dynamic keys for validation of his/her identity. The individual **10** has already his/her static key (not shown). If the individual **10** does not own a valid dynamic key, the individual **10** requests it **100** from his/her trusted-authenticator **30** by communicating over a communication network **50**.

In response to the individual's request **100**, the trusted-authenticator **30** calculates and sends **102** a dynamic key to the individual **10** over a communication network **50**. The trusted-authenticator **30** maintains both the static and dynamic keys in association with the authentication transaction.

Upon receipt of the dynamic key, the individual **10** provides the static key and the dynamic key to the business **20, 112** for validation of his/her **10** identity.

Upon receipt of the individual's **10** static and dynamic keys, the business **20** constructs an authentication message including the individual's **10** keys and communicates it to the trusted-authenticator **30, 120** for validation of the individual's **10** identity over a communication network **50**.

Upon receipt of the authentication message, the trusted-authenticator **30** validates both keys and verifies the individual's **10** identity, and sends **126** either a confirmation message or a denial message back to the business over a communication network **50**. The business **20** will receive **126** a confirmation message from the individual's trusted-authenticator **30** if both keys are valid. A confirmation message means that the individual **10** appears to be authentic and a denial message indicates that the individual's **10** identity has not been authenticated.

Upon receipt of a confirmation message from the individual's **10** trusted-authenticator **30**, the business **20** will be certain that the individual **10** is who he/she **10** says he/she **10** is.

Fig. 2b illustrates the direct authentication method **2-2** in accordance with the second embodiment of the present invention. For two-factor authentication of an individual, the business **20** requests **110** the individual **10** to provide static and dynamic keys for validation of his/her identity. The individual **10** has already his/her static key (not shown). If the individual **10** does not own a valid dynamic key, the individual **10** requests it **100** from his/her trusted-authenticator **30** by communicating over a communication network **50**.

In response to the individual's request **100**, the trusted-authenticator **30** calculates and sends a dynamic key to the individual **10, 102** over a communication network **50**. The trusted-authenticator **30** maintains both the static and dynamic keys in association with the authentication transaction.

Upon receipt of the dynamic key, the individual **10** provides the static key and the dynamic key to the business **20, 112** for validation of his/her **10** identity.

Upon receipt of the individual's **10** static and dynamic keys, the business **20** constructs an authentication message including the individual's **10** keys and communicates the authentication message **120** to it's trusted-authenticator **40** for validation of the individual's **10** identity over a communications network **50**.

Upon receipt of the authentication message, the business's trusted-authenticator **40** processes the request and forwards the authentication message to the individual's **10** trusted-authenticator **30, 122**.

Upon receipt of the authentication message, the individual's trusted-authenticator **30** validates both keys and verifies the individual's **10** identity, and

sends **124** either a confirmation message or a denial message back to the business's trusted-authenticator **40** over a communication network **50.** The business's trusted-authenticator **40** will receive **124** a confirmation message from the individual's trusted-authenticator **30** if both keys are valid, otherwise, the business's trusted-authenticator **40** will receive **124** a denial message.

Upon receipt of a confirmation or denial message from the individual's trusted-authenticator **30**, the business's trusted-authenticator **40** will process the message and will forward **126** the confirmation or denial message to the business **20**. A confirmation message means that the individual **10** appears to be authentic and a denial message indicates that the individual's **10** identity has not been authenticated.

Upon receipt of a confirmation, the business **20** will be certain that the individual **10** is who he/she **10** says he/she **10** is.

Although not shown specifically in **Fig. 2a** and **Fig. 2b**, it should be understood that one or more additional parties or entities may be introduced along the communication route within the scope of the present invention. Among other things, such additional parties may be useful for calculating and validating dynamic keys or expediting, screening, and correctly routing electronic communications between the various parties

BENEFITS OF THE PRESENT INVENTION

The security benefits of this invention are clear. The security provided by this new two-factor authentication method is the computer equivalent of the security provided by a safety deposit box: the individual's key alone can't open the safety box, and neither can the bank's key; both parties need to make use of both keys at the same time in order to open the safety box. Even if someone gets access to the individual's **10** static key, they cannot get authenticated as that individual **10** without the individual's **10** dynamic key (A key that the individual **10** receives from his/her trusted-authenticator **30** at the time of authentication). This is also true when, for authentication purposes, the individual **10** shares his/her static and dynamic keys with a business **20**. If someone gets access to both keys, they still cannot use it for authentication at other businesses **20** because the dynamic key may expire the moment it gets used and it is no longer valid. Therefore, for authentication over the Internet, it will not matter whether a keystroke logger records what the individual **10** enters, because one of the keys is dynamic and may expire the moment the hacker gets it.

Comparing to other solutions, the present invention differs in several key advantages and offers many benefits:

- In general, the main advantage is the ability to validate individuals' identity for a large number of businesses.

- A very important advantage is that individuals' sensitive information is kept in a decentralized fashion among a large number of trusted-authenticators.

- Further advantage is the high security provided by a new two-factor authentication method.

- Another advantage is that it proofs that the individual is who he/she claims he/she is.

- Another advantage is that it prohibits individuals from falsely denying involvement in a transaction.

- Further advantage is that it enables businesses to validate individuals' identity in real time.

- Another advantage is that it utilizes a secure, inexpensive, easy to use and easy to manage authentication method that reduces the risk of fraud as well as identity theft, therefore offers a long-term security solution.

- Another advantage is that it handles the most difficult identification environment where the individual who is seeking identity verification is unknown to the business.

- Furthermore, It is responsive in any authentication environment, offline, domestically, internationally and electronically (online).

Those skilled in the art appreciate that authentication of individuals **10** may happen online or offline and therefore the communication between the individual **10** and the business **20** could happen either over a communication network **50** or face-to-face **80**. In one embodiment the individual **10** may provide

his/her static and dynamic keys to the business **20** over a communication network **50** such as the Internet or phone. In another embodiment the individual **10** may provide his/her static and dynamic keys to the business **20** in a face-to-face interaction with the business **20**. An example would be when a car dealership needs to validate the individual's **10** identity. In this example, the individual **10** receives his/her dynamic key over a wireless communication network (wireless phone) and provides it along with his/her static key to the dealership for authentication of his/her identity.

Those skilled in the art also appreciate that a third party organization could act as a trusted-authenticator **30, 40**. In one embodiment a trusted-authenticator **30, 40** may outsource the whole authentication process to a third party organization and in another embodiment a trusted-authenticator **30, 40** may outsource part of the authentication process to a third party organization.

Those skilled in the art also appreciate that one or more intermediaries may exist between a business **20** and a trusted-authenticator **30, 40**.

Those skilled in the art also appreciate that for security reasons the individual **10** may receive his/her dynamic key in an encrypted format.

Those skilled in the art also appreciate that for convenience the transfer or communication **102, 112** of the individual's dynamic key from the individual's trusted-authenticator **30** to the business **20** could be done in an automated fashion through the individual's system to eliminate or minimize the involvement of the individual **10** or the interaction with the individual **10**. For example, in an online authentication scenario, the individual's trusted-authenticator **30** might

store the individual's dynamic key on the individual's system (e.g. as Cookie), which would be later accessed by the business **20** when the business **20** requires the individual **10** to provide his/her static key. Those skilled in the art will acknowledge that the options are unlimited.

Those skilled in the art also appreciate that the individual's trusted-authenticator **30** may invalidate the individual's dynamic key after its use and may also make the dynamic key time dependent by invalidating the key after a period of time. If an attacker gains access to the individual's static and dynamic keys, and the dynamic key is still valid, the damages that the individual **10** will receive will be limited only to one transaction, since the dynamic key gets invalidated after its use. But the individual will not receive any damages if the dynamic key has been invalidated.

Those skilled in the art appreciate that the present invention could be used to obtain authorization of financial transactions from individuals **10**. A financial transaction is a payment or funds transfer transaction.

In view of the foregoing detailed description of preferred embodiments of the present invention, it readily will be understood by those persons skilled in the art that the present invention is susceptible of broad utility and application. While various aspects have been described in particular contexts of use, the aspects may be useful in other contexts as well. Many embodiments and adaptations of the present invention other than those herein described, as well as many variations, modifications, and equivalent arrangements, will be apparent from or reasonably suggested by the present invention and the foregoing description thereof, without departing from the substance or scope of the present invention.

Furthermore, any sequence(s) and/or temporal order of steps of various processes described and claimed herein are those considered to be the best mode contemplated for carrying out the present invention. It should also be understood that, although steps of various processes may be shown and described as being in a preferred sequence or temporal order, the steps of any such processes are not limited to being carried out in any particular sequence or order, absent a specific indication of such to achieve a particular intended result. In most cases, the steps of such processes may be carried out in various different sequences and orders, while still falling within the scope of the present inventions. Accordingly, while the present invention has been described herein in detail in relation to preferred embodiments, it is to be understood that this disclosure is only illustrative and exemplary of the present invention and is made merely for purposes of providing a full and enabling disclosure of the invention. The foregoing disclosure is not intended nor is to be construed to limit the present invention or otherwise to exclude any such other embodiments, adaptations, variations, modifications and equivalent arrangements.

We Claim:

1. A system for direct authentication of an individual, comprising:

a trusted authenticator with whom the individual has an existing relationship;

a static key shared between the individual and the trusted authenticator;

a dynamic key provided to the individual, upon request, by the trusted authenticator over a communication network; and

a business, organization or another individual that receives the static and dynamic keys from the individual and is able to authenticate the individual via the trusted authenticator over a communication network using the dynamic and static keys.

2. The system of claim 1, further including:

an authentication request message created by the business, organization or another individual including the static and dynamic keys and communicated to the trusted authenticator; and

an authentication confirmation, or denial, message created by the trusted authenticator based on the received authentication request message and communicated back to the business, organization or another individual for authentication, or non-authentication, of the individual.

3. The system of claim 1, wherein the business, organization or another individual is able to authenticate the individual in substantially real-time.

4. The system of claim 1, wherein the business, organization or another individual is able to authenticate the individual without having a pre-existing relationship with the individual.

5. The system of claim 1, wherein the individual and the business, organization or another individual communicate face-to-face or over a communication network.

6. The system of claim 1, wherein the business, organization or another individual is in direct, or indirect, communication with the trusted authenticator.

7. The system of claim 6, wherein the business, organization or another individual is in communication with a second trusted authenticator over a communication network, and the second trusted authenticator communicates with the trusted authenticator over a communication network for authentication of the individual.

8. The system of claim 1, wherein the static key includes pre-shared information between the individual and the trusted authenticator and may be encrypted.

9. The system of claim 1, wherein the dynamic key includes a SecureCode that is dynamic, non-predictable and time dependent and may be encrypted.

10. The system of claim 1, 5 or 7, wherein the communication network(s) include(s): private and/or public networks such as the Internet.

11. The system of claim 1, 5, or 7, wherein the communication network(s) include(s): wireless networks.

12. A method for directly authenticating an individual, comprising the steps of:

an individual who needs to be authenticated by a business, organization or another individual, requests a dynamic key from a trusted authenticator over a communication network;

the trusted authenticator calculates a dynamic key and provides it to the individual;

the individual provides the business, organization or another individual with the calculated dynamic key and a static key already known to the individual and trusted authenticator;

the business, organization or another individual communicates the static and dynamic keys to the trusted authenticator, either directly or indirectly, over a communication network for validation and authentication of the individual.

13. The method of claim 12, wherein the step of communicating includes sending an authentication request message including the static and dynamic keys to the trusted authenticator and receiving an authentication confirmation, or denial, message back from the trusted authenticator.

14. The method of claim 12, wherein authentication of the individual is performed in substantially real time.

15. The method of claim 12, wherein the business, organization or another individual submits the static and dynamic keys to a second trusted authenticator, and the second trusted authenticator submits the static and dynamic keys to the first trusted authenticator for validation and authentication of the individual.

16. The method of claim 12, wherein the static key includes pre-shared information between the individual and the trusted authenticator and may be encrypted.

17. The method of claim 12, wherein the dynamic key includes a SecureCode that is dynamic, non-predictable and time dependent and may be encrypted.

18. The method of claim 12, wherein the individual and the business, organization, or another individual communicate face-to-face or over a communication network.

19. The method of claim 12 or 18, wherein the communication network(s) include: private and/or public networks such as the Internet.

20. The method of claim 12 or 18, wherein the communication network(s) include: wireless networks.

ABSTRACT OF THE DISCLOSURE

Fraud and identity theft are enabled by two faulty assumptions about the way that the identity of a person is verified in our society. The first is that someone who demonstrates knowledge of certain items of personal or financial information about a particular person is presumed to be that person. The second assumption, which gives rise to the first assumption, is that these items of information can be kept confidential. Because fraudsters and identity thieves often seek to use their victim's personal and financial information, this invention proposes a direct authentication system and method that does not depend on these assumptions. The proposed method enables businesses to determine whether the customer is truly the person who he says he is by adopting a new "two-factor" authentication technique and authenticating customer's identity utilizing customer's trusted authenticator. A customer's trusted authenticator can be found within the financial services community; in particular, a bank or other financial institution with whom the customer has a trusted relationship, such as a bank account.

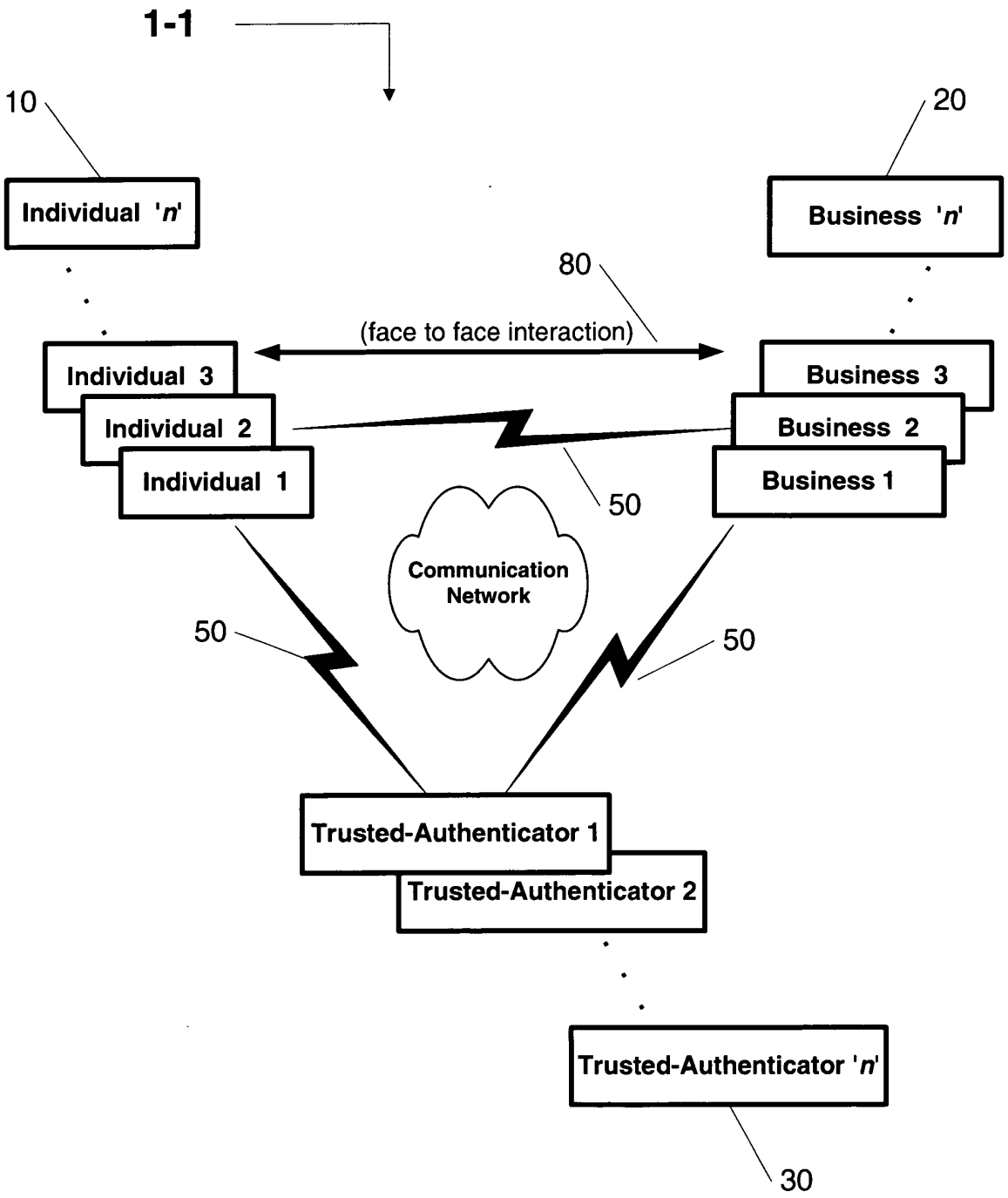

1-1
10
20
Individual 'n'
Business 'n'
80
(face to face interaction)
Individual 3
Individual 2
Individual 1
Business 3
Business 2
Business 1
50
Communication Network
50
50
Trusted-Authenticator 1
Trusted-Authenticator 2
Trusted-Authenticator 'n'
30

Figure 1a

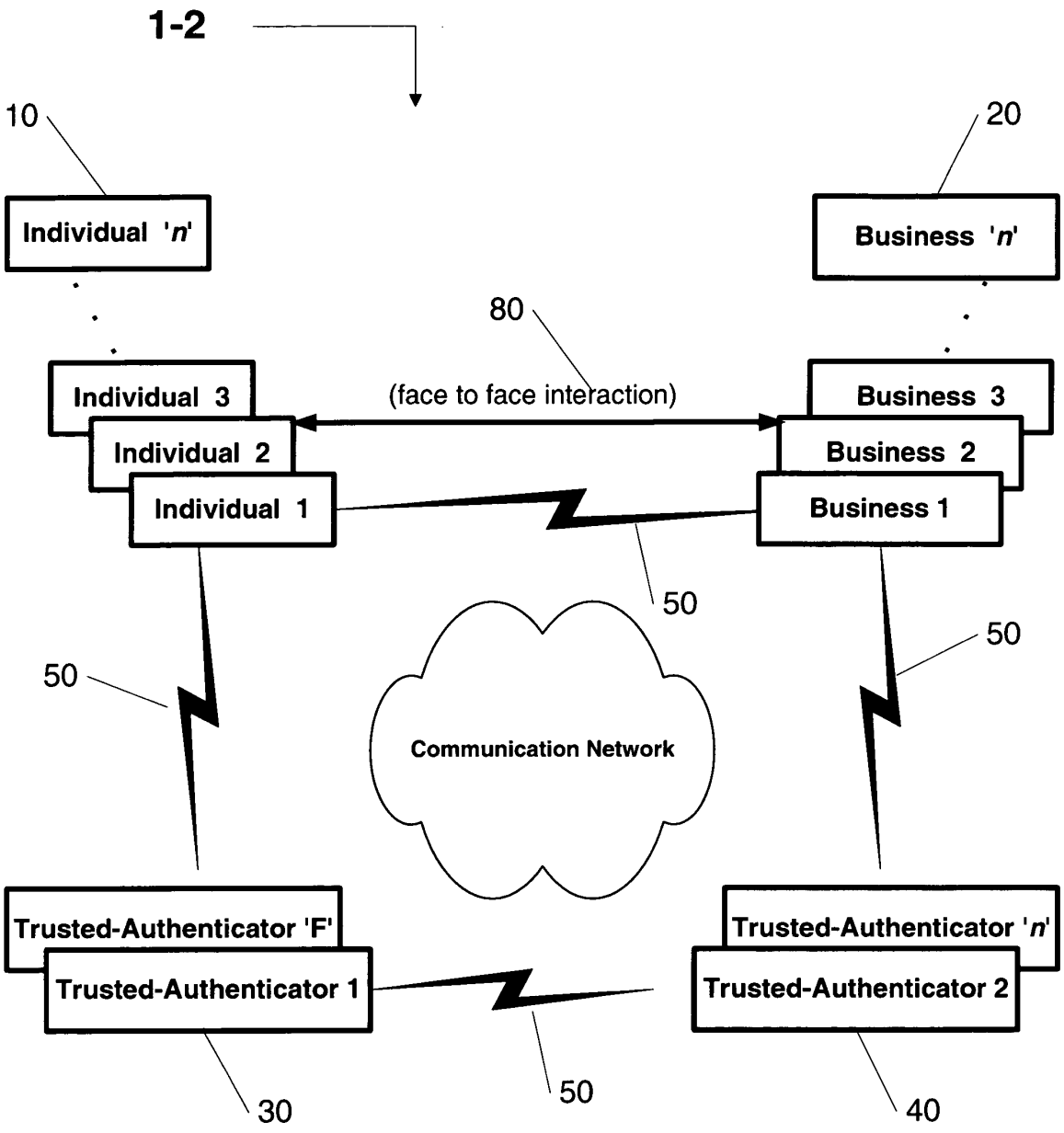
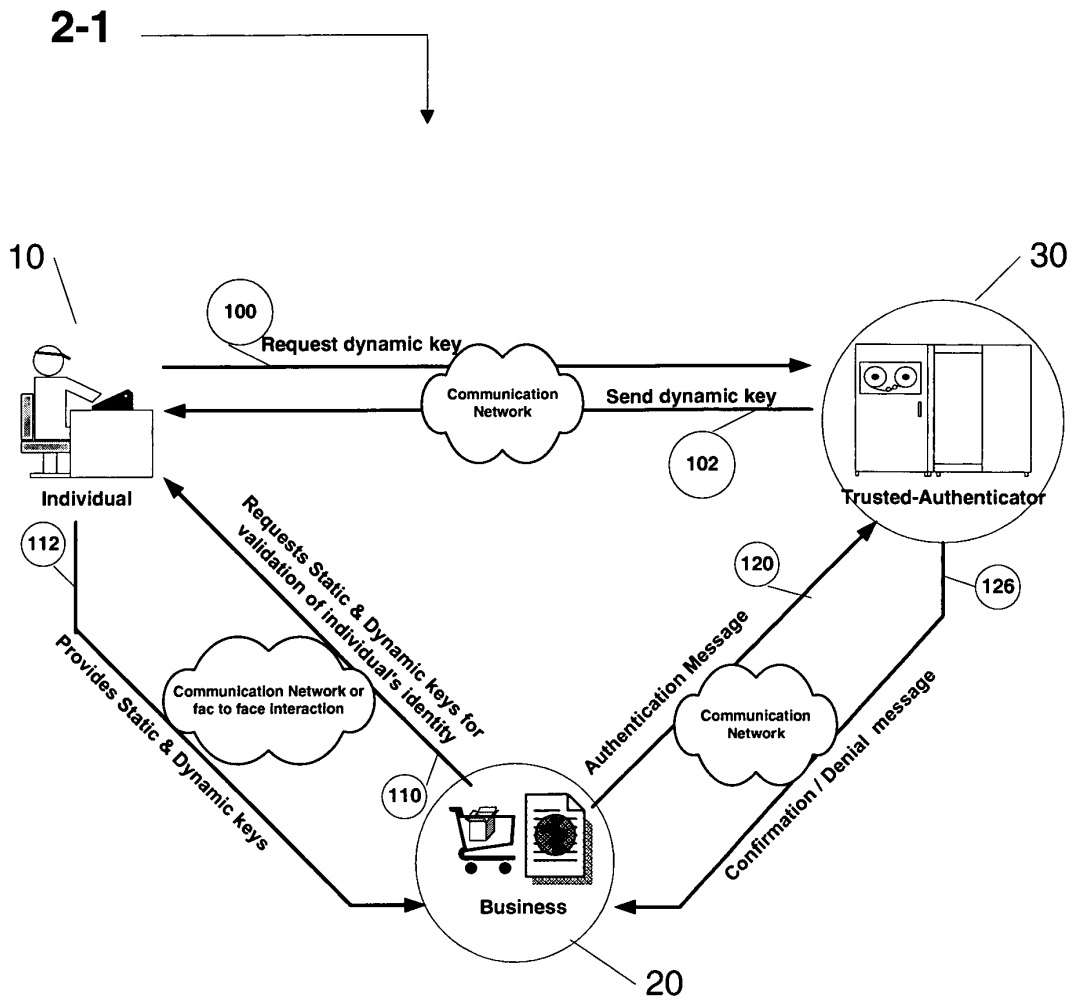

1-2
10
20
Individual 'n'
Business 'n'
80
Individual 3
(face to face interaction)
Business 3
Individual 2
Business 2
Individual 1
Business 1
50
50
50
Communication Network
Trusted-Authenticator 'F'
Trusted-Authenticator 'n'
Trusted-Authenticator 1
Trusted-Authenticator 2
50
30
40

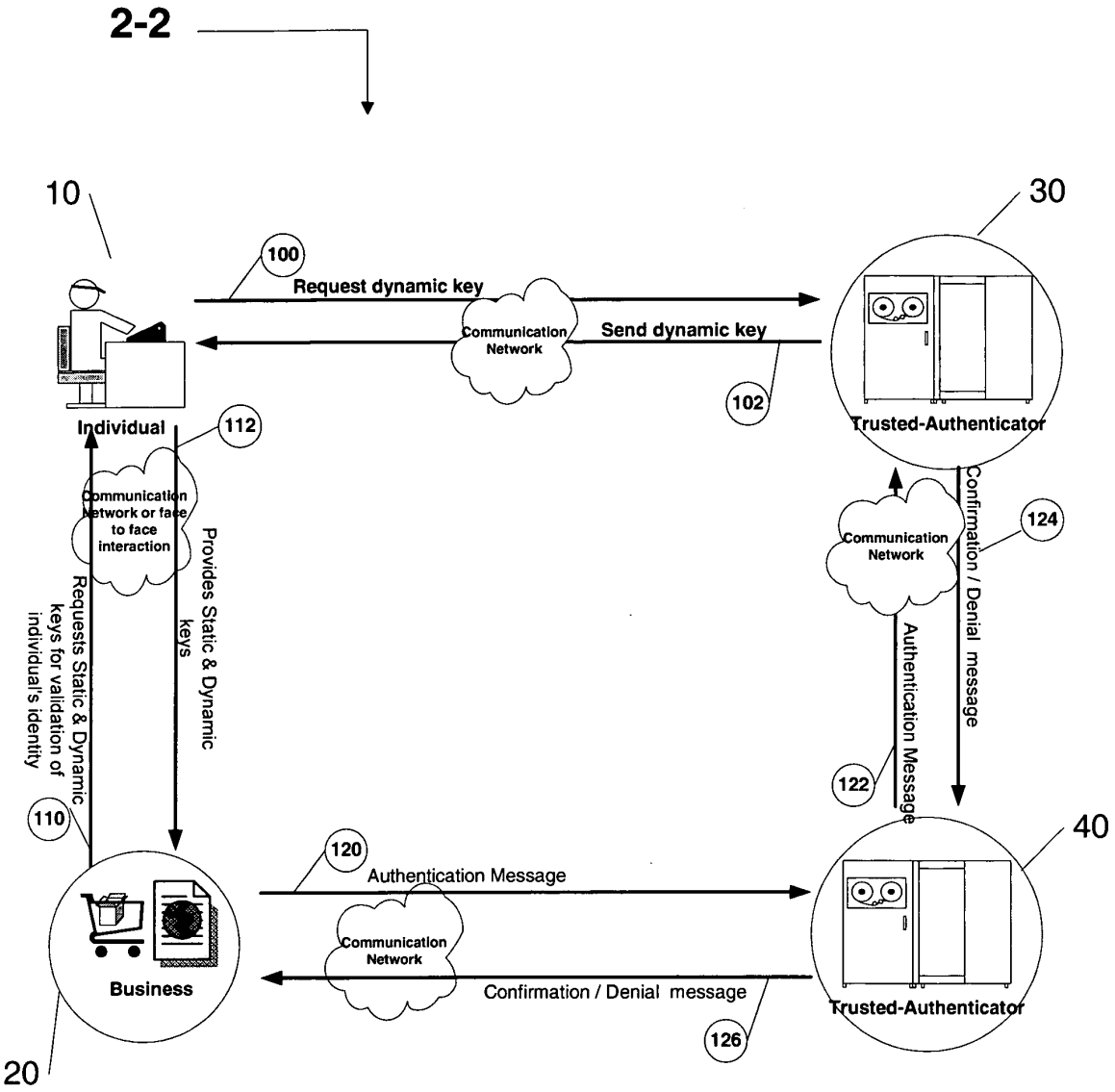
Figure 1b



Request / Receive Dynamic Key (100) (102)

Authentication Steps: (110) (112) (120) (122)

Figure 2a



Request / Receive Dynamic Key (100) (102)

Authentication Steps: (110) (112) (120) (122) (124) (126)

Figure 2b

PTO/SB/01 (10-05)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

DECLARATION FOR UTILITY OR DESIGN PATENT APPLICATION (37 CFR 1.63)

☑ Declaration Submitted With Initial Filing **OR** ☐ Declaration Submitted after Initial Filing (surcharge (37 CFR 1.16 (e)) required)

Attorney Docket Number	
First Named Inventor	Asghari-Kamrani et al.
COMPLETE IF KNOWN	
Application Number	
Filing Date	
Art Unit	
Examiner Name	

I hereby declare that:

Each inventor's residence, mailing address, and citizenship are as stated below next to their name.

I believe the inventor(s) named below to be the original and first inventor(s) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

Direct Authentication System and Method via Trusted Authenticators

(Title of the Invention)

the specification of which

☑ is attached hereto

OR

☐ was filed on (MM/DD/YYYY) ☐ as United States Application Number or PCT International Application Number ☐ and was amended on (MM/DD/YYYY) ☐ (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or (f), or 365(b) of any foreign application(s) for patent, inventor's or plant breeder's rights certificate(s), or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent, inventor's or plant breeder's rights certificate(s), or any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached? YES	NO
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐

☐ Additional foreign application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto.

PTO/SB/01 (10-05)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

DECLARATION — Utility or Design Patent Application

Direct all correspondence to: ☐ The address associated with Customer Number: [ ] OR ☑ Correspondence address below

Name			
Nader Asghari-Kamrani			
Address			
6558 Palisades Drive			
City		**State**	**ZIP**
Centreville		VA	20121
Country	**Telephone**		**Email**
U.S.A.	(703) 222-~~1070~~ 5104		Kamrani@delphinustechnology.com

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

NAME OF SOLE OR FIRST INVENTOR: ☐ A petition has been filed for this unsigned inventor

Given Name (first and middle [if any])	Family Name or Surname	
Nader	Asghari-Kamrani	
Inventor's Signature		**Date**
		01/18/06
Residence: City	**State**	**Country**	**Citizenship**
Centreville	VA	U.S.A.	United States
Mailing Address			
6558 Palisades Dr.			
City	**State**	**Zip**	**Country**
Centreville	VA	20120	U.S.A.

☑ Additional inventors or a legal representative are being named on the 1 supplemental sheet(s) PTO/SB/02A or 02LR attached hereto.

PTO/SB/02A (09-04)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

DECLARATION

ADDITIONAL INVENTOR(S)
Supplemental Sheet

Name of Additional Joint Inventor, if any:	☐ A petition has been filed for this unsigned inventor		
Given Name (first and middle (if any))	Family Name or Surname		
Kamran	Asghari-Kamrani		
Inventor's Signature Kamrani			Date 01/18/06
Centreville Residence: City	VA State	U.S.A. Country	Netherlands Citizenship
6547 Palisades Drive Mailing Address			
Centreville City	VA State	20120 Zip	U.S.A. Country

Name of Additional Joint Inventor, if any:	☐ A petition has been filed for this unsigned inventor		
Given Name (first and middle (if any))	Family Name or Surname		
Inventor's Signature			Date
Residence: City	State	Country	Citizenship
Mailing Address			
City	State	Zip	Country

Name of Additional Joint Inventor, if any:	☐ A petition has been filed for this unsigned inventor		
Given Name (first and middle (if any))	Family Name or Surname		
Inventor's Signature			Date
Residence: City	State	Country	Citizenship
Mailing Address			
City	State	Zip	Country

CLAIMS ONLY	SERIAL NO	FILING DATE
	APPLICANT(S)	

CLAIMS

	AS FILED		AFTER 1ST AMENDMENT		AFTER 2ND AMENDMENT							
	IND	DEP	IND	DEP	IND	DEP		IND	DEP	IND	DEP	IND	DEP
1	1						51						
2							52						
3							53						
4							54						
5							55						
6							56						
7							57						
8							58						
9							59						
10		3					60						
11		3					61						
12	1						62						
13		1					63						
14							64						
15							65						
16							66						
17							67						
18							68						
19		2					69						
20		2					70						
21							71						
22							72						
23							73						
24							74						
25							75						
26							76						
27							77						
28							78						
29							79						
30							80						
31							81						
32							82						
33							83						
34							84						
35							85						
36							86						
37							87						
38							88						
39							89						
40							90						
41							91						
42							92						
43							93						
44							94						
45							95						
46							96						
47							97						
48							98						
49							99						
50							100						
TOTAL IND.	1						TOTAL IND.						
TOTAL DEP.	25						TOTAL DEP.						
TOTAL CLAIMS	26						TOTAL CLAIMS						

PTO-2202 (Replication only) (1/03)

PATENT APPLICATION SERIAL NO. _____

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE
FEE RECORD SHEET

01/19/2006 FFANAEIA 00000055 11333400

01 FC:2011	150.00 OP
02 FC:2111	250.00 OP
03 FC:2311	100.00 OP

PTO-1556
(5/87)

*U.S. Government Printing Office: 2002 — 489-267/69033

PTO/SB/06 (12-04)
Approved for use through 7/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875 Effective December 8, 2004

Application or Docket Number: 11333400

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	150.00		N/A	300.00
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A	$250		N/A	$500
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	$100		N/A	$200
TOTAL CLAIMS (37 CFR 1.16(i))	26 minus 20 =	* 6	X$ 25 =		OR	X$50 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	2 minus 3 =	* 0	X100 =			X200 =	
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))			+180=			+360=	
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	50		TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT A

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X$ 25 =		OR	X$50 =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X100 =		OR	X200 =	
Application Size Fee (37 CFR 1.16(s))									
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					+180=		OR	+360=	
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

AMENDMENT B

	(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$ 25 =		OR	X$50 =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X100 =		OR	X200 =	
Application Size Fee (37 CFR 1.16(s))									
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					+180=		OR	+360=	
					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.

PTO/SB/35 (09-04)
Approved for use through 07/31/2006. 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.

NONPUBLICATION REQUEST UNDER 35 U.S.C. 122(b)(2)(B)(i)

First Named Inventor	Asghari-Kamrani et. al.
Title	Direct Authentication System and Method via Trusted Authenticators
Attorney Docket Number	

I hereby certify that the invention disclosed in the attached application **has not and will not be** the subject of an application filed in another country, or under a multilateral agreement, that requires publication at eighteen months after filing.

I hereby request that the attached application not be published under 35 U.S.C. 122(b).

Signature — 01/18/06 Date

Nader, Asghari Kamrani
Typed or printed name

Registration Number, if applicable

703-222-5104
Telephone Number

This request must be signed in compliance with 37 CFR 1.33(b) and submitted with the application **upon filing.**

Applicant may rescind this nonpublication request at any time. If applicant rescinds a request that an application not be published under 35 U.S.C. 122(b), the application will be scheduled for publication at eighteen months from the earliest claimed filing date for which a benefit is claimed.

If applicant subsequently files an application directed to the invention disclosed in the attached application in another country, or under a multilateral international agreement, that requires publication of applications eighteen months after filing, the applicant **must** notify the United States Patent and Trademark Office of such filing within forty-five (45) days after the date of the filing of such foreign or international application. **Failure to do so will result in abandonment of this application (35 U.S.C. 122(b)(2)(B)(iii)).**

PTO/SB/08A (07-05)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	
Filing Date	
First Named Inventor	Asghari-Kamrani et al.
Art Unit	
Examiner Name	
Attorney Docket Number	

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3]Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4]For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6]Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/08B (07-05)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 2

Complete if Known	
Application Number	
Filing Date	
First Named Inventor	Asghari-Kamrani et al.
Art Unit	
Examiner Name	
Attorney Docket Number	

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		LOPUCKI, "Human Identification Theory and the Identity Theft Problem," Texas Law Review, Vol. 80, pp. 89-134 (2001)	
		SOLOVE, "Identity Theft, Privacy, and the Architechture of Vulnerability," Hastings Law Journal, Vol. 54 No. 4, p.1251 (2003)	

Examiner Signature		Date Considered	

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

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

NOTICE OF FEE DUE

DATE: 01-19-02

TO: Utility

FROM: Office of Initial Patent Examination

SUBJECT: Fee Due

APPLICATION NUMBER 11334400

A fee is due for the attached document submitted to the U.S. Patent and Trademark Office for the following reason. Please check the application for the appropriate authorizations to charge a deposit account if an authorizations is present, please charge the Appropriate Fee. If and authorization is not present, notify the applicant of the fee deficiency.

- ☑ Insufficient fee by check
- ☑ Insufficient funds in deposit amount
- ☐ Insufficient by Credit Card
- ☐ Declined credit card
- ☐ Non-authorization for charge to deposit account
- ☐ No fee submitted per requirement

The correct fee code:	8202-2203	Amount	$ 330
The suspended fee code:	1999	Amount	$
The suspended	1622	Amount	$
The suspended	2622	Amount	$
Fee Due			$ 330

Terminal Operator Paul