



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/524,842	04/07/2015	9003508	P1987.01	4129

24739 7590 03/18/2015
CENTRAL COAST PATENT AGENCY, INC
3 HANGAR WAY SUITE D
WATSONVILLE, CA 95076

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

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

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

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

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

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

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

Vincent Cedric Colnot, Milpitas, CA;
OHVA, Inc., San Jose, CA, Assignee (with 37 CFR 1.172 Interest);
Ty Fellers, Little Mountain, SC;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

PART B - FEE(S) TRANSMITTAL

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

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

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

24739 7590 01/13/2015
CENTRAL COAST PATENT AGENCY, INC
3 HANGAR WAY SUITE D
WATSONVILLE, CA 95076

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

Certificate of Mailing or Transmission

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

Sheri Beasley (Depositor's name)
Sheri Beasley (Signature)
03-02-2015 (Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/524,842	10/27/2014	Vincent Cedric Colnot	P1987.01	4/29

TITLE OF INVENTION: METHODS AND APPARATUS FOR ENABLING SECURE NETWORK-BASED TRANSACTIONS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$480	\$0	\$0	\$480	04/13/2015

EXAMINER	ART UNIT	CLASS-SUBCLASS
PYZOCHA, MICHAEL J	2437	726-010000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
 (1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
 (2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 *Donald R. Boys*
 2 *Central Coast*
 3 *Patent Agent, Inc.*

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

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

(A) NAME OF ASSIGNEE

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

OHVA, Inc.

San Jose, CA

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

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

☒ Issue Fee
☐ Publication Fee (No small entity discount permitted)
☐ Advance Order - # of Copies _____

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

☐ A check is enclosed.
☐ Payment by credit card. Form PTO-2038 is attached.
☒ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number *500534* (enclose an extra copy of this form).

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

☐ Applicant certifying micro entity status. See 37 CFR 1.29
☐ Applicant asserting small entity status. See 37 CFR 1.27
☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature *Donald R. Boys*

Date *03-02-2015*

Typed or printed name *Donald R. Boys*

Registration No. *35,074*

Electronic Patent Application Fee Transmittal				
Application Number:	14524842			
Filing Date:	27-Oct-2014			
Title of Invention:	METHODS AND APPARATUS FOR ENABLING SECURE NETWORK-BASED TRANSACTIONS			
First Named Inventor/Applicant Name:	Vincent Cedric Colnot			
Filer:	Donald Rex Boys/Sheri Beasley			
Attorney Docket Number:	P1987.01			
Filed as Small Entity				
Filing Fees for Utility under 35 USC 111(a)				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl Issue Fee	2501	1	480	480

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				480

Electronic Acknowledgement Receipt	
EFS ID:	21638156
Application Number:	14524842
International Application Number:	
Confirmation Number:	4129
Title of Invention:	METHODS AND APPARATUS FOR ENABLING SECURE NETWORK-BASED TRANSACTIONS
First Named Inventor/Applicant Name:	Vincent Cedric Colnot
Customer Number:	24739
Filer:	Donald Rex Boys/Sheri Beasley
Filer Authorized By:	Donald Rex Boys
Attorney Docket Number:	P1987.01
Receipt Date:	02-MAR-2015
Filing Date:	27-OCT-2014
Time Stamp:	14:38:17
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$480
RAM confirmation Number	1121
Deposit Account	500534
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	ISSUE1987_01.pdf	566433 170da81e9597d54da9fb08845f3e2743aae12336	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30606 1e47cc5c5e013326d155b2566ab9608e8254ee8	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			597039		
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.					



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/524,842	10/27/2014	Vincent Cedric Colnot	P1987.01

CONFIRMATION NO. 4129

24739

CENTRAL COAST PATENT AGENCY, INC
3 HANGAR WAY SUITE D
WATSONVILLE, CA 95076

PUBLICATION NOTICE



OC000000073387742

Title:METHODS AND APPARATUS FOR ENABLING SECURE NETWORK-BASED TRANSACTIONS

Publication No.US-2015-0047007-A1

Publication Date:02/12/2015

NOTICE OF PUBLICATION OF APPLICATION

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

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

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

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

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

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



UNITED STATES PATENT AND TRADEMARK OFFICE

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

NOTICE OF ALLOWANCE AND FEE(S) DUE

24739 7590 01/13/2015
CENTRAL COAST PATENT AGENCY, INC
3 HANGAR WAY SUITE D
WATSONVILLE, CA 95076

EXAMINER

PYZOCHA, MICHAEL J

ART UNIT

PAPER NUMBER

2437

DATE MAILED: 01/13/2015

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/524,842	10/27/2014	Vincent Cedric Colnot	P1987.01	4129

TITLE OF INVENTION: METHODS AND APPARATUS FOR ENABLING SECURE NETWORK-BASED TRANSACTIONS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$480	\$0	\$0	\$480	04/13/2015

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

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

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

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

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

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

PART B - FEE(S) TRANSMITTAL

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

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

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

24739 7590 01/13/2015
CENTRAL COAST PATENT AGENCY, INC
3 HANGAR WAY SUITE D
WATSONVILLE, CA 95076

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

Certificate of Mailing or Transmission

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

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/524,842	10/27/2014	Vincent Cedric Colnot	P1987.01	4129

TITLE OF INVENTION: METHODS AND APPARATUS FOR ENABLING SECURE NETWORK-BASED TRANSACTIONS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$480	\$0	\$0	\$480	04/13/2015

EXAMINER	ART UNIT	CLASS-SUBCLASS
PYZOCHA, MICHAEL J	2437	726-010000

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

- ☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

- (1) The names of up to 3 registered patent attorneys or agents OR, alternatively, 1 _____
- (2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. 2 _____
- 3 _____

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

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

(A) NAME OF ASSIGNEE

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

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

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

- ☐ Issue Fee
- ☐ Publication Fee (No small entity discount permitted)
- ☐ Advance Order - # of Copies _____

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

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

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

- ☐ Applicant certifying micro entity status. See 37 CFR 1.29
- ☐ Applicant asserting small entity status. See 37 CFR 1.27
- ☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/524,842	10/27/2014	Vincent Cedric Colnot	P1987.01	4129
24739	7590	01/13/2015	EXAMINER	
CENTRAL COAST PATENT AGENCY, INC			PYZOCHA, MICHAEL J	
3 HANGAR WAY SUITE D			ART UNIT	PAPER NUMBER
WATSONVILLE, CA 95076			2437	

DATE MAILED: 01/13/2015

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

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

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

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

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

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

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

Notice of Allowability	Application No. 14/524,842	Applicant(s) COLNOT ET AL.	
	Examiner MICHAEL PYZOGHA	Art Unit 2437	AIA (First Inventor to File) Status No

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

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

1. ☒ This communication is responsive to the claims filed 10/27/2014.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are 1-8. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
Certified copies:
a) ☐ All b) ☐ Some *c) ☐ None of the:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).
* Certified copies not received: _____.

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

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

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

/MICHAEL PYZOGHA/ Primary Examiner, Art Unit 2437	
--	--

DETAILED ACTION

1. The present application is being examined under the pre-AIA first to invent provisions.
2. Claims 1-8 are pending.

EXAMINER'S AMENDMENT

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

Authorization for this examiner's amendment was given in a telephone interview with Donald R. Boys (Reg. No. 35,074) on 01/07/2015.

The application has been amended as follows:

Art Unit: 2437

Claim 4. The process of claim 1, wherein ~~the software applet is a Java applet and the~~ token is ~~a Java~~ an archive.

Claim 6. The system of claim ~~[[1]]~~ 5, wherein the data storage device coupled to the client's computer where the compatible token is found is a flash thumb drive.

Claim 7. The system of claim ~~[[1]]~~ 5, wherein the token is unique to a client and includes an identification number, a password or personal identification code, a session key, and a secrete data seed.

Claim 8. The system of claim ~~[[1]]~~ 5, wherein ~~the software applet is a Java applet and~~ the token is ~~a Java~~ an archive.

Allowable Subject Matter

4. Claims 1-8 are allowed.
5. The following is an examiner's statement of reasons for allowance: The prior art generally teaches the use of a plurality of authentication/log-in methods to authorize a user access to a server but fails to teach the explicit details in combination as recited in the independent claims.

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

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. The references on the PTO-892 form relate to various authentication methods for controlling user access to services.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL PYZOCHA whose telephone number is (571)272-3875. The examiner can normally be reached on Monday-Thursday, 7:30am - 3:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Eleni Shiferaw can be reached on (571) 272-3867. 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.

/MICHAEL PYZOCHA/
Primary Examiner, Art Unit 2437

Notice of References Cited	Application/Control No. 14/524,842	Applicant(s)/Patent Under Reexamination COLNOT ET AL.	
	Examiner MICHAEL PYZOSHA	Art Unit 2437	Page 1 of 2

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,188,766 B1	02-2001	Kocher, Paul C.	380/246
*	B	US-6,282,653 B1	08-2001	Berstis et al.	726/26
*	C	US-6,385,729 B1	05-2002	DiGiorgio et al.	726/9
*	D	US-2003/0005118 A1	01-2003	Williams, Ronald B.	709/225
*	E	US-2003/0046551 A1	03-2003	Brennan, Sean	713/185
*	F	US-2003/0065919 A1	04-2003	Albert et al.	713/168
*	G	US-2003/0177354 A1	09-2003	CARTER, GEORGE E.	713/164
*	H	US-2004/0093496 A1	05-2004	Colnot, Vincent Cedric	713/168
*	I	US-2004/0107356 A1	06-2004	Shamoon et al.	713/193
*	J	US-2005/0262573 A1	11-2005	Bo et al.	726/027
*	K	US-7,234,059 B1	06-2007	Beaver et al.	713/170
*	L	US-7,233,948 B1	06-2007	Shamoon et al.	1/1
*	M	US-7,359,883 B2	04-2008	Namba et al.	705/59

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.

Notice of References Cited	Application/Control No. 14/524,842	Applicant(s)/Patent Under Reexamination COLNOT ET AL.	
	Examiner MICHAEL PYZOCHA	Art Unit 2437	Page 2 of 2

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-7,900,245 B1	03-2011	Geddes et al.	726/9
*	B	US-8,146,141 B1	03-2012	Grandcolas et al.	726/5
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

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

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



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. 4129

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.		
14/524,842	10/27/2014	726	2437	P1987.01		
APPLICANTS OHVA, Inc., San Jose, CA, Assignee (with 37 CFR 1.172 Interest); INVENTORS Vincent Cedric Colnot, Milpitas, CA; Ty Fellers, Little Mountain, SC; ** CONTINUING DATA ***** This application is a CON of 11/533,030 09/19/2006 ABN which claims benefit of 60/719,273 09/20/2005 ** FOREIGN APPLICATIONS ***** ** IF REQUIRED, FOREIGN FILING LICENSE GRANTED *** SMALL ENTITY ** 11/04/2014						
Foreign Priority claimed ☐ Yes ☒ No 35 USC 119(a-d) conditions met ☐ Yes ☒ No Verified and /MICHAEL J Acknowledged PYZOCHA/ Examiner's Signature		☐ Met after Allowance Initials	STATE OR COUNTRY CA	SHEETS DRAWINGS 15	TOTAL CLAIMS 8	INDEPENDENT CLAIMS 2
ADDRESS CENTRAL COAST PATENT AGENCY, INC 3 HANGAR WAY SUITE D WATSONVILLE, CA 95076 UNITED STATES						
TITLE Methods and Apparatus for Enabling Secure Network-Based Transactions						
FILING FEE RECEIVED 730	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		

Issue Classification 	Application/Control No. 14524842	Applicant(s)/Patent Under Reexamination COLNOT ET AL.	
	Examiner MICHAEL PYZOGHA	Art Unit 2437	

CPC					
Symbol				Type	Version
H04L	63	0853		F	2013-01-01
H04L	63	083		I	2013-01-01
H04L	9	3213		I	2013-01-01
H04L	63	10		I	2013-01-01

CPC Combination Sets				
Symbol	Type	Set	Ranking	Version

NONE		Total Claims Allowed:	
		8	
(Assistant Examiner)	(Date)		
/MICHAEL PYZOGHA/ Primary Examiner.Art Unit 2437	01/07/2015	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	14

Issue Classification 	Application/Control No. 14524842	Applicant(s)/Patent Under Reexamination COLNOT ET AL.
	Examiner MICHAEL PYZOGHA	Art Unit 2437

US ORIGINAL CLASSIFICATION						INTERNATIONAL CLASSIFICATION											
CLASS			SUBCLASS			CLAIMED					NON-CLAIMED						
726			10			H	0	4	L	29 / 00 (2006.01.01)		H	0	4	L	29 / 00 (2006.01.01)	
CROSS REFERENCE(S)																	
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)																
726	9																
713	184																

NONE		Total Claims Allowed:	
		8	
(Assistant Examiner)	(Date)		
/MICHAEL PYZOGHA/ Primary Examiner.Art Unit 2437	01/07/2015	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	14

Search Notes 	Application/Control No. 14524842	Applicant(s)/Patent Under Reexamination COLNOT ET AL.
	Examiner MICHAEL PYZOGHA	Art Unit 2437

CPC- SEARCHED		
Symbol	Date	Examiner
H04L 63/0853	1/7/15	MJP
H04L 63/083	1/7/15	MJP
H04L 63/10	1/7/15	MJP
H04L 9/3213	1/7/15	MJP

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	10	1/7/15	MJP
726	9	1/7/15	MJP
713	184	1/7/15	BRS

SEARCH NOTES		
Search Notes	Date	Examiner
BRS search in USPAT, USPGPUB, EPO, JPO, IBM, DERWENT, see attached search history; inventor name search; consulted Michael Simitoski & David Pearson	1/7/15	MJP

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
726	10	1/7/15	MJP
726	9	1/7/15	MJP
713	184	1/7/15	MJP
H04L	63/0853	1/7/15	MJP
H04L	63/083	1/7/15	MJP

--	--

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
H04L	63/10	1/7/15	MJP
H04L	9/3213	1/7/15	MJP

--	--

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	12	(Colnot near Vincent) (Fellers near Ty)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/01/07 09:58
S2	1713	726/10.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/01/07 10:07
S3	2371	713/185.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/01/07 10:08
S4	3216	726/9.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/01/07 10:08
S5	8038	H04L63/10.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/01/07 10:14
S6	5530	H04L63/083.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/01/07 10:14
S7	4122	H04L63/0853.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/01/07 10:14
S8	945	H04L9/3213.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/01/07 10:14
S9	0	(website web-site webpage web-page (web adj (page site))) same applet same decrypt\$4 with token	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/01/07 10:15
S10	111	(website web-site webpage web-page (web adj (page site))) same applet and decrypt\$4 with token	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/01/07 10:16

S11	35	(website web-site webpage web-page (web adj (page site))) same applet and decrypt\$4 with token same (PIN password)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/01/07 10:16
S12	4	S11 and @ad<"20050920"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/01/07 10:16
S13	0	decrypt\$4 with token with (PIN password) same (timestamp\$4 time-stamp\$4 time adj stamp\$4) same domain	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/01/07 10:18
S14	3	decrypt\$4 with token same (timestamp\$4 time-stamp\$4 time adj stamp\$4) same domain	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/01/07 10:19
S15	2	S14 and @ad<"20050920"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/01/07 10:19
S16	27	token same (timestamp\$4 time-stamp\$4 time adj stamp\$4) same domain same hash\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/01/07 10:20
S17	10	S16 and @ad<"20050920"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/01/07 10:21
S18	1	(website web-site webpage web-page (web adj (page site))) same (login logon log-in log-on signin signon sign-in sign-on) and applet same PIN same (keypad key-pad)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/01/07 10:23
S19	98	("5586166" "5665951" "6038367").PN. OR ("6385729").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2015/01/07 10:24
S20	57	S19 and @ad<"20050920"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/01/07 10:24
S21	24	S20 and token	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/01/07 10:25
S22	139	(website web-site webpage web-page (web adj (page site))) same (multi-factor two-factor ((two multi\$4) adj factor)) and PIN same token	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/01/07 10:27
S23	20	S22 and @ad<"20050920"	US-PGPUB;	OR	ON	2015/01/07

			USPAT; EPO; JPO; DERWENT; IBM_TDB			10:28
S24	10	(website web-site webpage web-page (web adj (page site))) same (multi-factor two-factor ((two multi\$4) adj factor)) and token same domain	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/01/07 10:31
S25	0	S24 and @ad<"20050920"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/01/07 10:31
S26	7	(website web-site webpage web-page (web adj (page site))) same (multi-factor two-factor ((two multi\$4) adj factor)) and token same (timestamp\$4 time-stamp\$4 time adj stamp\$4)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/01/07 10:33
S27	0	S26 and @ad<"20050920"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/01/07 10:33
S28	9	((("20030177354") or ("20040107356") or ("7233948") or ("7359883") or ("20030065919") or ("20040093496") or ("6282653") or ("6188766") or ("20050262573")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2015/01/07 10:34
S29	5	((("20080056496") or ("20080240447") or ("20100180120") or ("20110040964") or ("20110246766")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2015/01/07 10:38
S30	0	applet with determin\$4 with domain same token	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/01/07 10:44
S31	14	applet with domain same token	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/01/07 10:45
S32	0	S31 and @ad<"20050920"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/01/07 10:45
S33	14	applet same domain with token	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/01/07 10:47
S34	2	S33 and @ad<"20050920"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/01/07 10:47

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	0	(applet with time adj stamp with domain with PIN with token with encrypt\$4 with hash\$4).clm. and (726/10.ccls. 713/184.ccls. 726/9.ccls. H04L63/10.cpc. H04L63/083.cpc. H04L63/0853.cpc. H04L9/3213.cpc.)	USPAT; UPAD	OR	ON	2015/01/07 13:30
L2	0	(applet with time adj stamp with domain with PIN with token with encrypt\$4 with hash\$4).clm.	USPAT; UPAD	OR	ON	2015/01/07 13:30
L3	0	(applet with time adj stamp with domain with PIN with token with encrypt\$4).clm. and (726/10.ccls. 713/184.ccls. 726/9.ccls. H04L63/10.cpc. H04L63/083.cpc. H04L63/0853.cpc. H04L9/3213.cpc.)	USPAT; UPAD	OR	ON	2015/01/07 13:30
L4	0	(applet with time adj stamp with domain with PIN with token with encrypt\$4).clm.	USPAT; UPAD	OR	ON	2015/01/07 13:30
L5	0	(applet with time adj stamp with domain with PIN with token with decrypt\$4).clm. and (726/10.ccls. 713/184.ccls. 726/9.ccls. H04L63/10.cpc. H04L63/083.cpc. H04L63/0853.cpc. H04L9/3213.cpc.)	USPAT; UPAD	OR	ON	2015/01/07 13:30
L6	0	(applet with time adj stamp with domain with PIN with token with decrypt\$4).clm.	USPAT; UPAD	OR	ON	2015/01/07 13:30
L7	0	(applet with time adj stamp with domain with token).clm. and (726/10.ccls. 713/184.ccls. 726/9.ccls. H04L63/10.cpc. H04L63/083.cpc. H04L63/0853.cpc. H04L9/3213.cpc.)	USPAT; UPAD	OR	ON	2015/01/07 13:31
L8	0	(applet with time adj stamp with domain with token).clm.	USPAT; UPAD	OR	ON	2015/01/07 13:31
L9	0	(applet with domain with token).clm. and (726/10.ccls. 713/184.ccls. 726/9.ccls. H04L63/10.cpc. H04L63/083.cpc. H04L63/0853.cpc. H04L9/3213.cpc.)	USPAT; UPAD	OR	ON	2015/01/07 13:31
L10	0	(applet with domain with token).clm.	USPAT; UPAD	OR	ON	2015/01/07 13:31

1/ 7/ 2015 1:42:52 PM

C:\Users\mpyzocha1\Documents\EAST\Workspaces\14524842.wsp

<i>Index of Claims</i> 	Application/Control No. 14524842	Applicant(s)/Patent Under Reexamination COLNOT ET AL.
	Examiner MICHAEL PYZOGHA	Art Unit 2437

✓	Rejected
=	Allowed

-	Cancelled
÷	Restricted

N	Non-Elected
I	Interference

A	Appeal
O	Objected

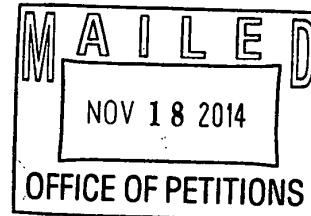
☒ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47										
CLAIM		DATE								
Final	Original	01/07/2015								
	1	=								
	2	=								
	3	=								
	4	=								
	5	=								
	6	=								
	7	=								
	8	=								



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

CENTRAL COAST PATENT AGENCY, INC
3 HANGAR WAY SUITE D
WATSONVILLE CA 95076



Doc Code: TRACK1.GRANT

Decision Granting Request for Prioritized Examination (Track I or After RCE)	Application No.: 14/524,842
1. THE REQUEST FILED <u>10/27/14</u> IS GRANTED. The above-identified application has met the requirements for prioritized examination A. ☒ for an original nonprovisional application (Track I). B. ☐ for an application undergoing continued examination (RCE). 2. The above-identified application will undergo prioritized examination. The application will be accorded special status throughout its entire course of prosecution until one of the following occurs: A. filing a petition for extension of time to extend the time period for filing a reply; B. filing an amendment to amend the application to contain more than four independent claims, more than thirty total claims, or a multiple dependent claim; C. filing a request for continued examination; D. filing a notice of appeal; E. filing a request for suspension of action; F. mailing of a notice of allowance; G. mailing of a final Office action; H. completion of examination as defined in 37 CFR 41.102; or I. abandonment of the application. Telephone inquiries with regard to this decision should be directed to Cheryl Gibson-Baylor at (571)272-3213, Office of Petitions. In his/her absence, calls may be directed to Brian W. Brown, (571)272-5338. Cheryl Gibson-Baylor <u>/Cheryl Gibson-Baylor/</u> [Signature] <u>Petitions Paralegal Specialist</u> (Title)	



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO.	TOT CLAIMS	IND CLAIMS
14/524,842	10/27/2014	2431	730	P1987.01	8	2

CONFIRMATION NO. 4129

24739
CENTRAL COAST PATENT AGENCY, INC
3 HANGAR WAY SUITE D
WATSONVILLE, CA 95076

FILING RECEIPT



OC000000071701946

Date Mailed: 11/05/2014

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

Inventor(s)

Vincent Cedric Colnot, Milpitas, CA;
Ty Fellers, Little Mountain, SC;

Applicant(s)

OHVA, Inc., San Jose, CA

Power of Attorney: The patent practitioners associated with Customer Number 24739

Domestic Priority data as claimed by applicant

This application is a CON of 11/533,030 09/19/2006 ABN
which claims benefit of 60/719,273 09/20/2005

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see <http://www.uspto.gov> for more information.) - None.

Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access - A proper **Authorization to Permit Access to Application by Participating Offices** (PTO/SB/39 or its equivalent) has been received by the USPTO.

If Required, Foreign Filing License Granted: 11/04/2014

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/524,842**

Projected Publication Date: 02/12/2015

Non-Publication Request: No

Early Publication Request: No

**** SMALL ENTITY ****

Title

Methods and Apparatus for Enabling Secure Network-Based Transactions

Preliminary Class

726

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

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

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

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

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

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

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

LICENSE FOR FOREIGN FILING UNDER
Title 35, United States Code, Section 184
Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

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

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

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

NOT GRANTED

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

SelectUSA

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

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875						Application or Docket Number 14/524,842	
APPLICATION AS FILED - PART I							
(Column 1)		(Column 2)		SMALL ENTITY		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	70		N/A	
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A	300		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	360		N/A	
TOTAL CLAIMS (37 CFR 1.16(j))	8	minus 20 = *	x 40 =	0.00	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	2	minus 3 = *	x 210 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	730		TOTAL	
APPLICATION AS AMENDED - PART II							
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY	
AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		OTHER THAN SMALL ENTITY
	Total (37 CFR 1.16(i))	*	Minus **	=	x =		RATE(\$)
	Independent (37 CFR 1.16(h))	*	Minus ***	=	x =		ADDITIONAL FEE(\$)
	Application Size Fee (37 CFR 1.16(s))						
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
TOTAL ADD'L FEE					OR	TOTAL ADD'L FEE	
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY	
AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		OTHER THAN SMALL ENTITY
	Total (37 CFR 1.16(i))	*	Minus **	=	x =		RATE(\$)
	Independent (37 CFR 1.16(h))	*	Minus ***	=	x =		ADDITIONAL FEE(\$)
	Application Size Fee (37 CFR 1.16(s))						
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
TOTAL ADD'L FEE					OR	TOTAL ADD'L FEE	
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.							

**CERTIFICATION AND REQUEST FOR PRIORITIZED EXAMINATION
UNDER 37 CFR 1.102(e) (Page 1 of 1)**

First Named Inventor:	Vincent Cedric Colnot	Nonprovisional Application Number (if known):	
Title of Invention:	Methods and Apparatus for Enabling Secure Network-Based Transactions		

APPLICANT HEREBY CERTIFIES THE FOLLOWING AND REQUESTS PRIORITIZED EXAMINATION FOR THE ABOVE-IDENTIFIED APPLICATION.

1. The processing fee set forth in 37 CFR 1.17(i)(1), the prioritized examination fee set forth in 37 CFR 1.17(c), and if not already paid, the publication fee set forth in 37 CFR 1.18(d) have been filed with the request. The basic filing fee, search fee, examination fee, and any required excess claims and application size fees are filed with the request or have been already been paid.
2. The application contains or is amended to contain no more than four independent claims and no more than thirty total claims, and no multiple dependent claims.
3. The applicable box is checked below:
 - I. ☒ **Original Application (Track One) - Prioritized Examination under § 1.102(e)(1)**
 - i. (a) The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a). This certification and request is being filed with the utility application via EFS-Web.
---OR---
(b) The application is an original nonprovisional plant application filed under 35 U.S.C. 111(a). This certification and request is being filed with the plant application in paper.
 - ii. The executed inventor's oath or declaration is filed with the application. (37 CFR 1.63 and 1.64)
 - II. ☐ **Request for Continued Examination - Prioritized Examination under § 1.102(e)(2)**
 - i. A request for continued examination has been filed with, or prior to, this form.
 - ii. If the application is a utility application, this certification and request is being filed via EFS-Web.
 - iii. The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a), or is a national stage entry under 35 U.S.C. 371.
 - iv. This certification and request is being filed prior to the mailing of a first Office action responsive to the request for continued examination.
 - v. No prior request for continued examination has been granted prioritized examination status under 37 CFR 1.102(e)(2).

Signature /Donald R. Boys/	Date 10/27/2014
Name (Print/Typed) Donald R. Boys	Practitioner Registration Number 35074
Note: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. Submit multiple forms if more than one signature is required.*	
☐ *Total of _____ forms are submitted.	

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.

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

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	P1987.01
		Application Number	
Title of Invention	Methods and Apparatus for Enabling Secure Network-Based Transactions		
The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76. This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.			

Secrecy Order 37 CFR 5.2

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

Inventor Information:

Inventor 1					Remove	
Legal Name						
Prefix	Given Name	Middle Name	Family Name	Suffix		
	Vincent	Cedric	Colnot			
Residence Information (Select One) ☒ US Residency ☐ Non US Residency ☐ Active US Military Service						
City	Milpitas	State/Province	CA	Country of Residence i	US	
Mailing Address of Inventor:						
Address 1		803 Kevenaire Drive				
Address 2						
City	Milpitas	State/Province	CA			
Postal Code	95035	Country i	US			
Inventor 2					Remove	
Legal Name						
Prefix	Given Name	Middle Name	Family Name	Suffix		
	Ty		Fellers			
Residence Information (Select One) ☒ US Residency ☐ Non US Residency ☐ Active US Military Service						
City	Little Mountain	State/Province	SC	Country of Residence i	US	
Mailing Address of Inventor:						
Address 1		1970 Mill Road				
Address 2						
City	Little Mountain	State/Province	SC			
Postal Code	29075	Country i	US			
All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the Add button.					Add	

Correspondence Information:

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

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	P1987.01
		Application Number	
Title of Invention	Methods and Apparatus for Enabling Secure Network-Based Transactions		

☐ An Address is being provided for the correspondence information of this application.			
Customer Number	24739		
Email Address	info@centralcoastpatent.com	Add Email	Remove Email

Application Information:

Title of the Invention	Methods and Apparatus for Enabling Secure Network-Based Transactions		
Attorney Docket Number	P1987.01	Small Entity Status Claimed	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	15	Suggested Figure for Publication (if any)	

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)
☐ Request Not to Publish. I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application has not and will not be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32). Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.			
Please Select One: ☒ Customer Number ☐ US Patent Practitioner ☐ Limited Recognition (37 CFR 11.9)			
Customer Number	24739		

Domestic Benefit/National Stage Information:

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

When referring to the current application, please leave the application number blank.

Prior Application Status	Pending	Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation of	11533030	2006-09-19
Prior Application Status	Expired	Remove	

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	P1987.01
		Application Number	
Title of Invention	Methods and Apparatus for Enabling Secure Network-Based Transactions		
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
11533030	Claims benefit of provisional	60719273	2005-09-20
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the Add button.			Add

Foreign Priority Information:

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

			Remove
Application Number	Country ⁱ	Filing Date (YYYY-MM-DD)	Access Code ^j (if applicable)
Additional Foreign Priority Data may be generated within this form by selecting the Add button.			Add

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

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.

NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Authorization to Permit Access:

☒ Authorization to Permit Access to the Instant Application by the Participating Offices
--

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	P1987.01
		Application Number	
Title of Invention	Methods and Apparatus for Enabling Secure Network-Based Transactions		

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

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

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

Applicant Information:

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

Applicant 1

[Remove](#)

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

[Clear](#)

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

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

Name of the Deceased or Legally Incapacitated Inventor :

If the Applicant is an Organization check here. ☒

Organization Name OHVA, Inc.

Mailing Address Information:

Address 1	945 Whitehall Avenue		
Address 2			
City	San Jose	State/Province	CA
Country ⁱ	US	Postal Code	95128
Phone Number		Fax Number	

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	P1987.01
		Application Number	
Title of Invention	Methods and Apparatus for Enabling Secure Network-Based Transactions		
Email Address			
Additional Applicant Data may be generated within this form by selecting the Add button.			Add

Assignee Information including Non-Applicant Assignee Information:

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

Assignee 1				
Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.				
				Remove
If the Assignee or Non-Applicant Assignee is an Organization check here.				☐
Prefix	Given Name	Middle Name	Family Name	Suffix
Mailing Address Information For Assignee including Non-Applicant Assignee:				
Address 1				
Address 2				
City		State/Province		
Country i		Postal Code		
Phone Number		Fax Number		
Email Address				
Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button.				Add

Signature:

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications					
Signature	/Donald R. Boys/			Date (YYYY-MM-DD)	2014-10-27
First Name	Donald	Last Name	Boys	Registration Number	35074
Additional Signature may be generated within this form by selecting the Add button.					Add

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

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	P1987.01
		Application Number	
Title of Invention	Methods and Apparatus for Enabling Secure Network-Based Transactions		

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

Privacy Act Statement

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

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

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

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B or equivalent) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5. If the Power of Attorney by Applicant form is not accompanied by this transmittal form or an equivalent, the Power of Attorney will not be recognized in the application.

Application Number			
Filing Date			
First Named Inventor	Vincent Cedric Colnot		
Title	Methods and Apparatus for Enabling Secure Network-Based Transactions		
Art Unit			
Examiner Name			
Attorney Docket Number	P1987.01		
SIGNATURE of Applicant or Patent Practitioner			
Signature	/Donald R. Boys/	Date	10/27/2014
Name	Donald R. Boys	Telephone	831-768-1755
Registration Number	35,074		
NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications.			
☐ *Total of _____ 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.

POWER OF ATTORNEY BY APPLICANT

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

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

24739

OR

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

Name	Registration Number	Name	Registration Number

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

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

OR

- ☐ The address associated with Customer Number:

OR

☐ Firm or Individual Name

Address

City

State

Zip

Country

Telephone

Email

I am the Applicant:

- ☐ Inventor or Joint Inventor
- ☐ Legal Representative of a Deceased or Legally Incapacitated Inventor
- ☒ Assignee or Person to Whom the Inventor is Under an Obligation to Assign
- ☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document)

SIGNATURE of Applicant for Patent

Signature	<i>Mike Angelinovich</i>	Date	10/27/14
Name	Mike Angelinovich	Telephone	
Title and Company	CEO OHVA, Inc.		

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

- ☐ *Total of _____ 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.

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.

**SUBSTITUTE STATEMENT IN LIEU OF AN OATH OR DECLARATION FOR UTILITY
OR DESIGN PATENT APPLICATION (35 U.S.C. 115(d) AND 37 CFR 1.64)**

Title of Invention	Methods and Apparatus for Enabling Secure Network-Based Transactions		
This statement is directed to:			
☒ The attached application,			
OR			
☐ United States application or PCT international application number _____ filed on _____			
LEGAL NAME of inventor to whom this substitute statement applies:			
(E.g., Given Name (first and middle (if any)) and Family Name or Surname)			
Vincent Cedric Colnot			
Residence (except for a deceased or legally incapacitated inventor):			
City	Milpitas	State	CA US
Mailing Address (except for a deceased or legally incapacitated inventor):			
803 Kevenaire Drive			
City	Milpitas	State	CA 95035 US
I believe the above-named inventor or joint inventor to be the original inventor or an original joint inventor of a claimed invention in the application.			
The above-identified application was made or authorized to be made by me.			
I hereby acknowledge that any willful false statement made in this statement is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.			
Relationship to the inventor to whom this substitute statement applies:			
☐ Legal Representative (for deceased or legally incapacitated inventor only),			
☒ Assignee,			
☐ Person to whom the inventor is under an obligation to assign,			
☐ Person who otherwise shows a sufficient proprietary interest in the matter (petition under 37 CFR 1.46 is required), or			
☐ Joint Inventor.			

[Page 1 of 2]

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

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.

SUBSTITUTE STATEMENT

Circumstances permitting execution of this substitute statement:

- ☐ Inventor is deceased,
☐ Inventor is under legal incapacity,
☒ Inventor cannot be found or reached after diligent effort, or
☐ Inventor has refused to execute the oath or declaration under 37 CFR 1.63.

If there are joint inventors, please check the appropriate box below:

- ☒ An application data sheet under 37 CFR 1.76 (PTO/AIA/14 or equivalent) naming the entire inventive entity has been or is currently submitted.

OR

- ☐ An application data sheet under 37 CFR 1.76 (PTO/AIA/14 or equivalent) has not been submitted. Thus, a Substitute Statement Supplemental Sheet (PTO/AIA/11 or equivalent) naming the entire inventive entity and providing inventor information is attached. See 37 CFR 1.64(b).

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.

PERSON EXECUTING THIS SUBSTITUTE STATEMENT:Name: **Mike Angelinovich**

Date (Optional):

Signature: **APPLICANT NAME AND TITLE OF PERSON EXECUTING THIS SUBSTITUTE STATEMENT:**

If the applicant is a juristic entity, list the applicant name and the title of the signer:

OHVA, Inc.

Applicant Name:

Title of Person Executing
This Substitute Statement: **CEO**

The signer, whose title is supplied above, is authorized to act on behalf of the applicant.

Residence of the signer (unless provided in an application data sheet, PTO/AIA/14 or equivalent):

City

State

Country

Mailing Address of the signer (unless provided in an application data sheet, PTO/AIA/14 or equivalent)

City

State

Zip

Country

Note: Use an additional PTO/AIA/02 form for each inventor who is deceased, legally incapacitated, cannot be found or reached after diligent effort, or has refused to execute the oath or declaration under 37 CFR 1.63.

[Page 2 of 2]

ASSIGNMENT-STATEMENT (1987.01)

This Declaration and Assignment is directed to the invention: **Methods and Apparatus for Enabling Secure Network-Based Transactions**

I, **Ty Fellers**, believe I am the original inventor or an original joint inventor of a claimed invention in the application; and the application for the invention was made or was authorized to be made by me. I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years , or both.

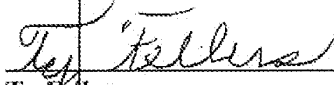
For good and valuable consideration, receipt of which is hereby acknowledged, I, **Ty Fellers**, do hereby sell, assign and transfer unto the **OHVA, Inc.**, (having its principal place of business **945 Whitehall Ave, San Jose, CA 95128**, hereinafter called the "Assignee"), its successors and assigns, the entire world-wide title, interest and right, including the right of priority controlled by me, in, to and under Letters Patent of the United States, the patent application, docket number **1987.01**, which bears application serial number _____, filed _____, ("I hereby authorize and request the agent(s) of record under customer number 24739, Central Coast Patent Agency, Inc., 3 Hangar Way, Suite D, Watsonville, CA 95076, to insert above the serial number and filing date of said application when known"), and the invention and any of them therein set forth and described, and any and all Letters Patent of the United States and of countries foreign thereto which may be granted thereon or therefore based on the original application for said U.S. Letters Patent, and all divisions, reissues, substitutions, continuations, and extensions thereof which may be granted relating thereto in any country; **and**

For the above consideration I agree promptly upon request of the Assignee, its successors or assigns, to execute and deliver without further compensation any power of attorney, assignment, application, whether original, continuation, divisional or reissue, or other papers which may be necessary or desirable fully to secure to the Assignee, its successors and assigns, the inventions and any of them, described in said application and all patent rights therein, in the

United States and in any country foreign thereto, and to cooperate and assist in the prosecution of appeal and interference proceedings involving said inventions and in the adjudication or re-examination of said Letters Patent provided the expenses which may be incurred by me in lending such cooperation and assistance be paid by the Assignee.

For the additional consideration of one dollar (\$1), receipt of which is hereby acknowledged, I, Ty Fellers, do hereby sell, assign and transfer unto the OHVA, Inc., any residual rights, including all moral rights, related to the patent application, docket number 1987.01, which bears application serial number _____, filed _____, the invention and any of them therein set forth and described, and any and all Letters Patent of the United States and of countries foreign thereto which may be granted thereon or therefore based on the original application for said U.S. Letters Patent, and all divisions, reissues, substitutions, continuations, and extensions thereof which may be granted relating thereto in any country.

Signature of Assignor:


Ty Fellers

10-27-14
Date

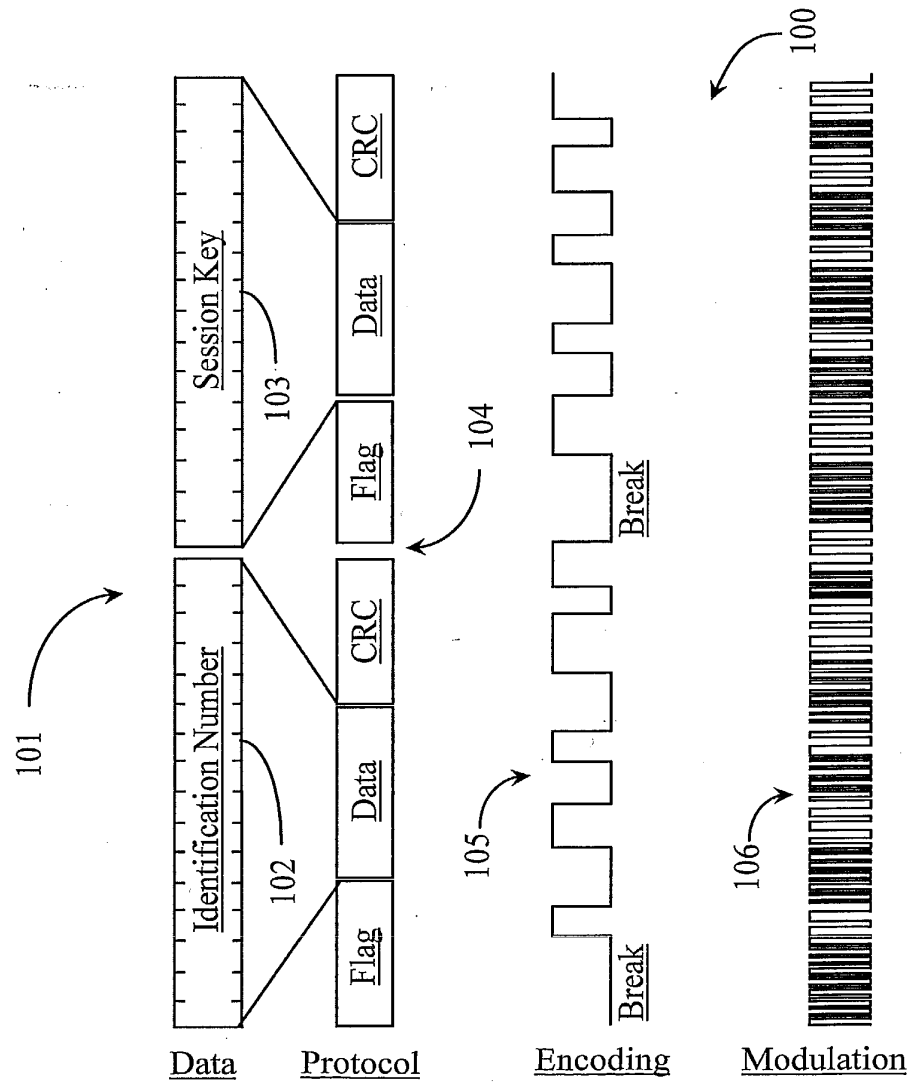


Fig. 1

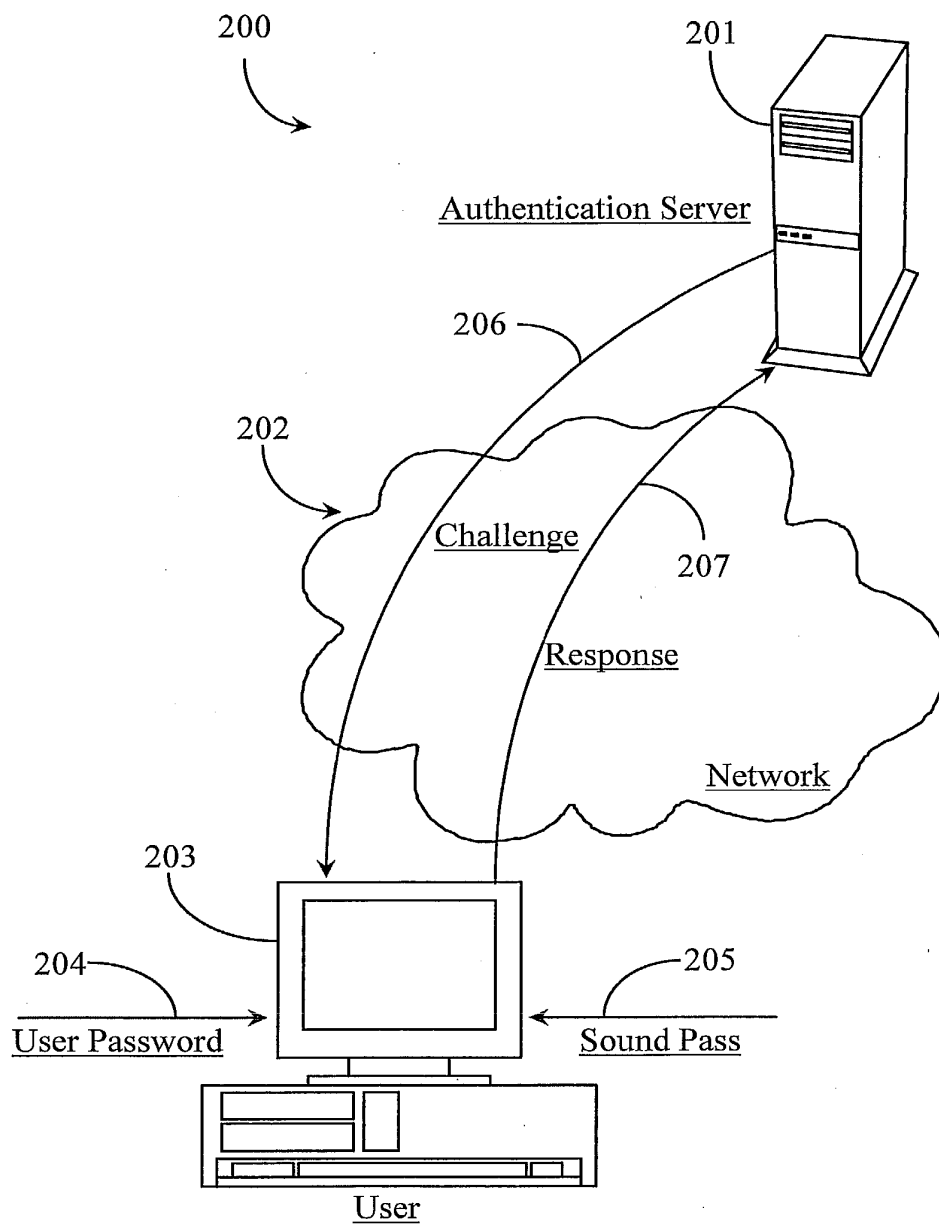


Fig. 2

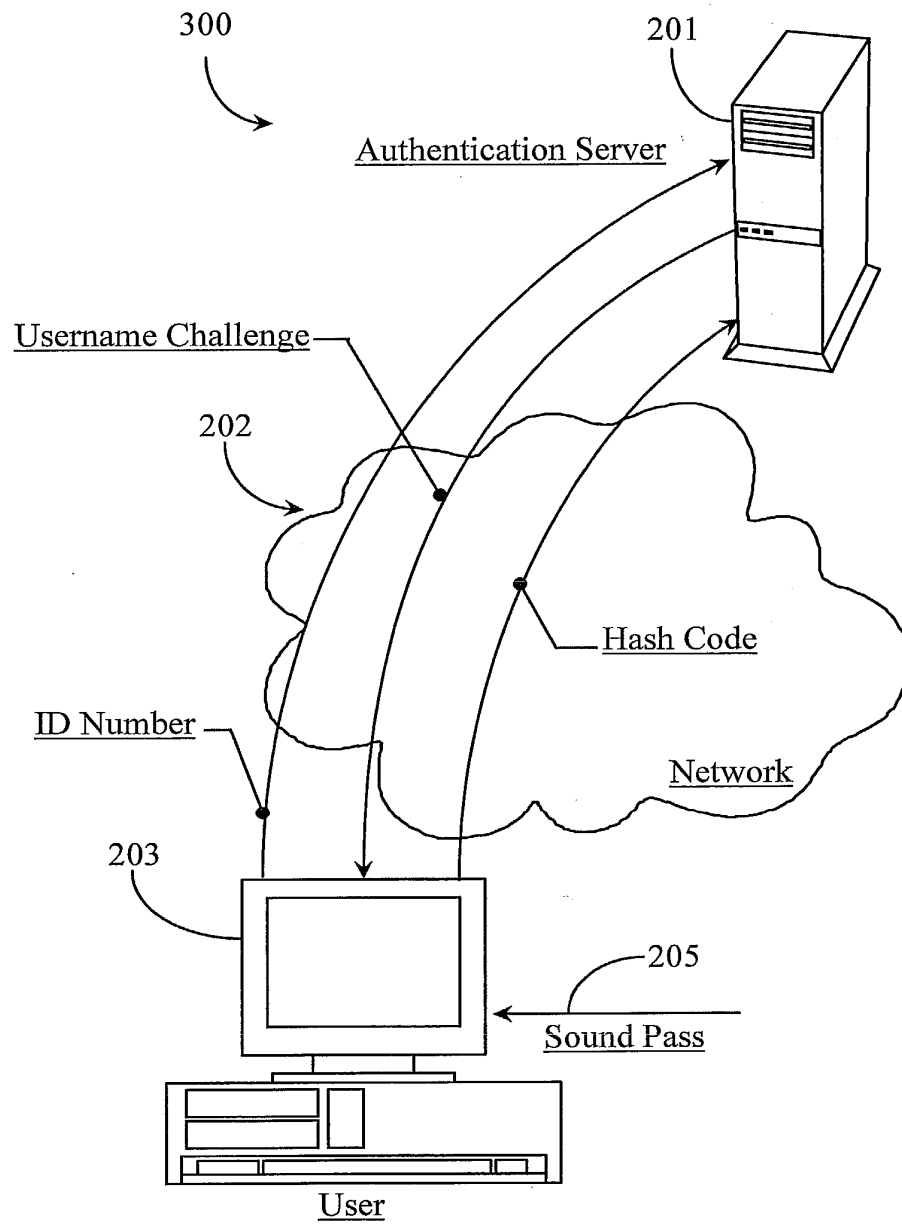


Fig. 3

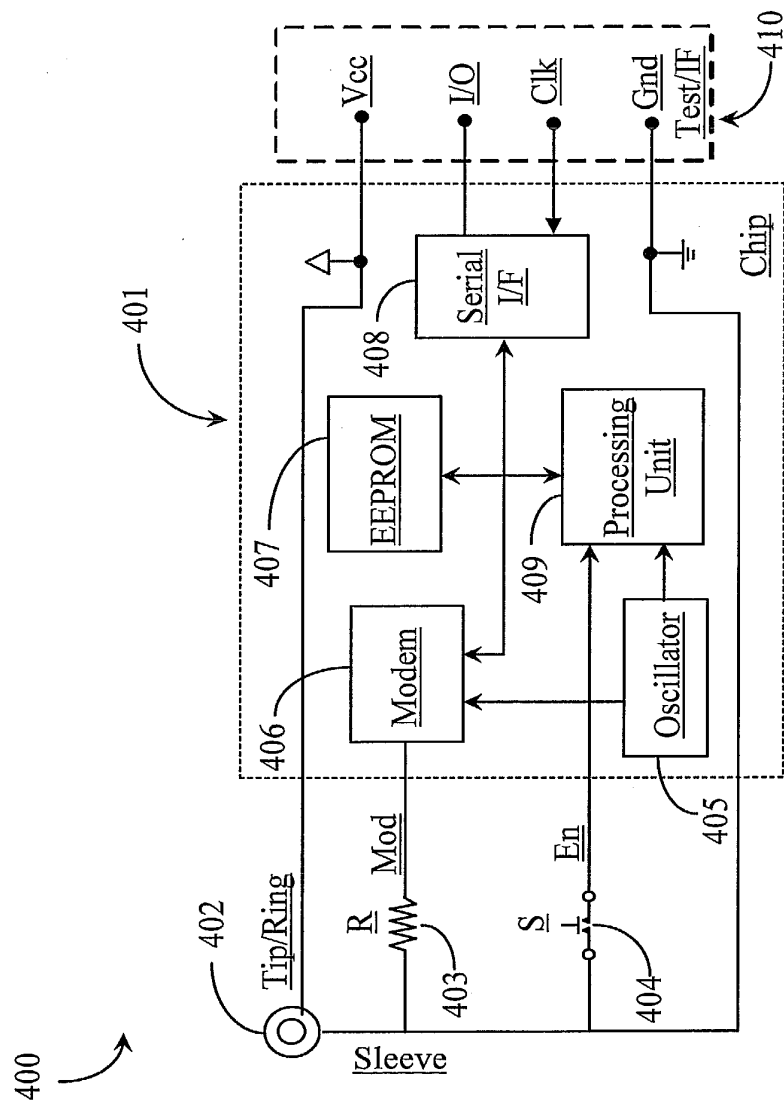


Fig. 4

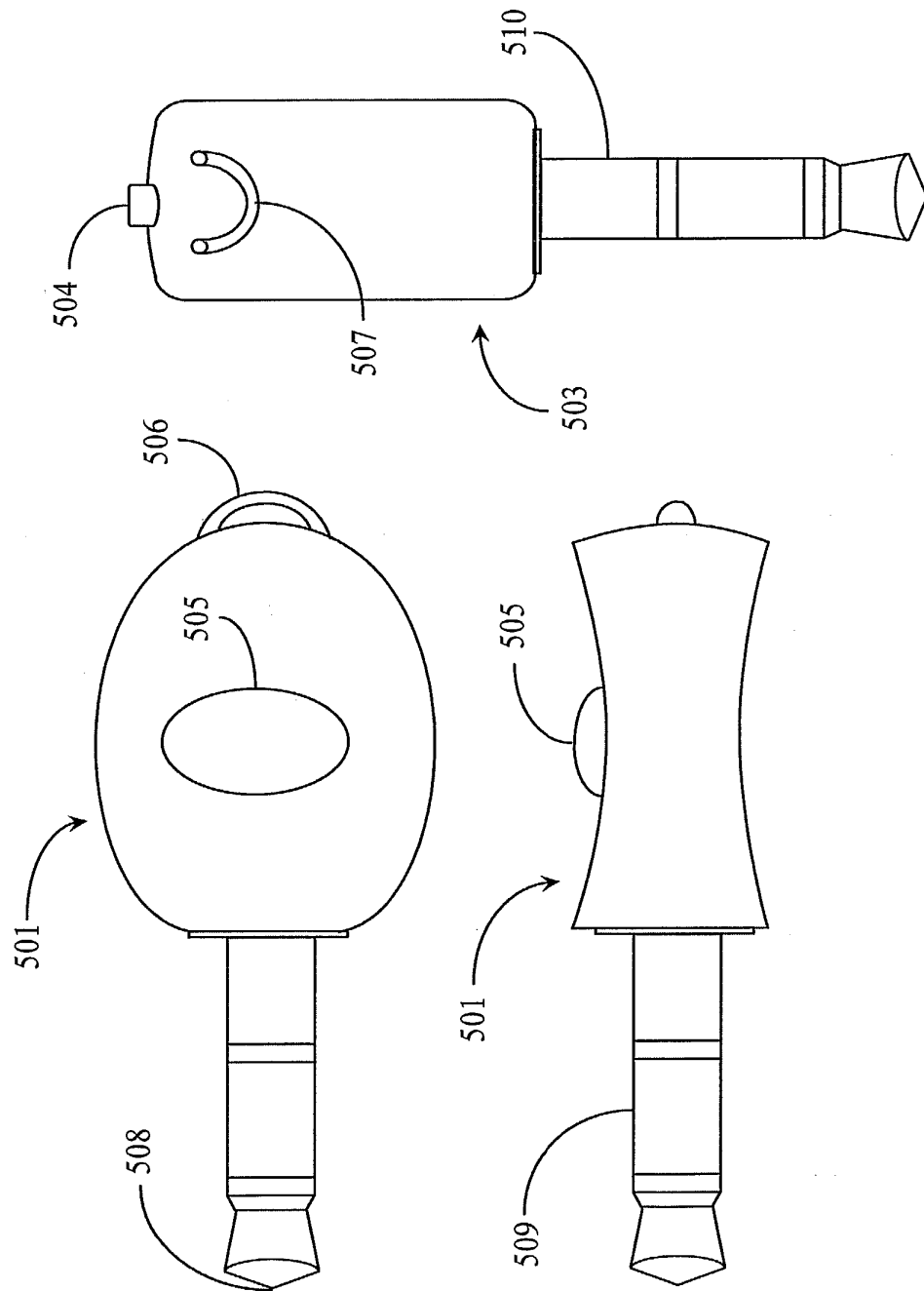


Fig. 5

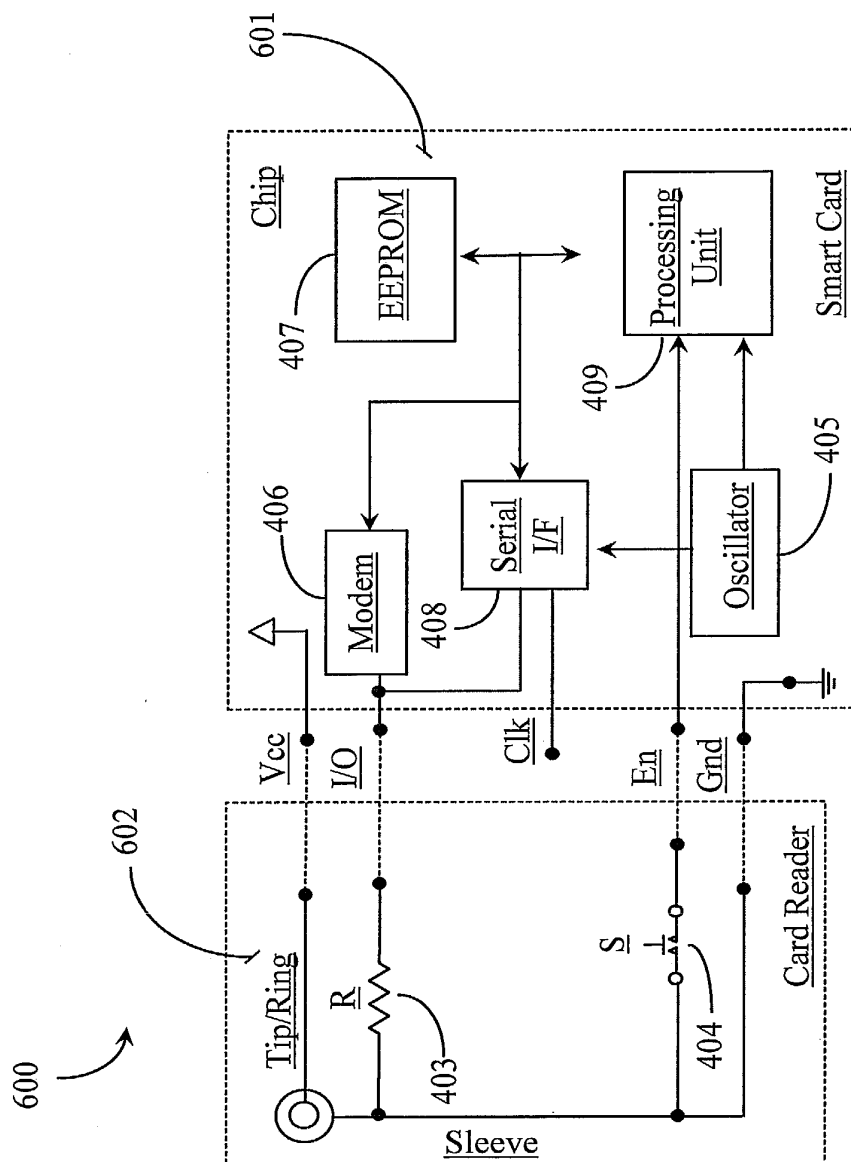


Fig.6

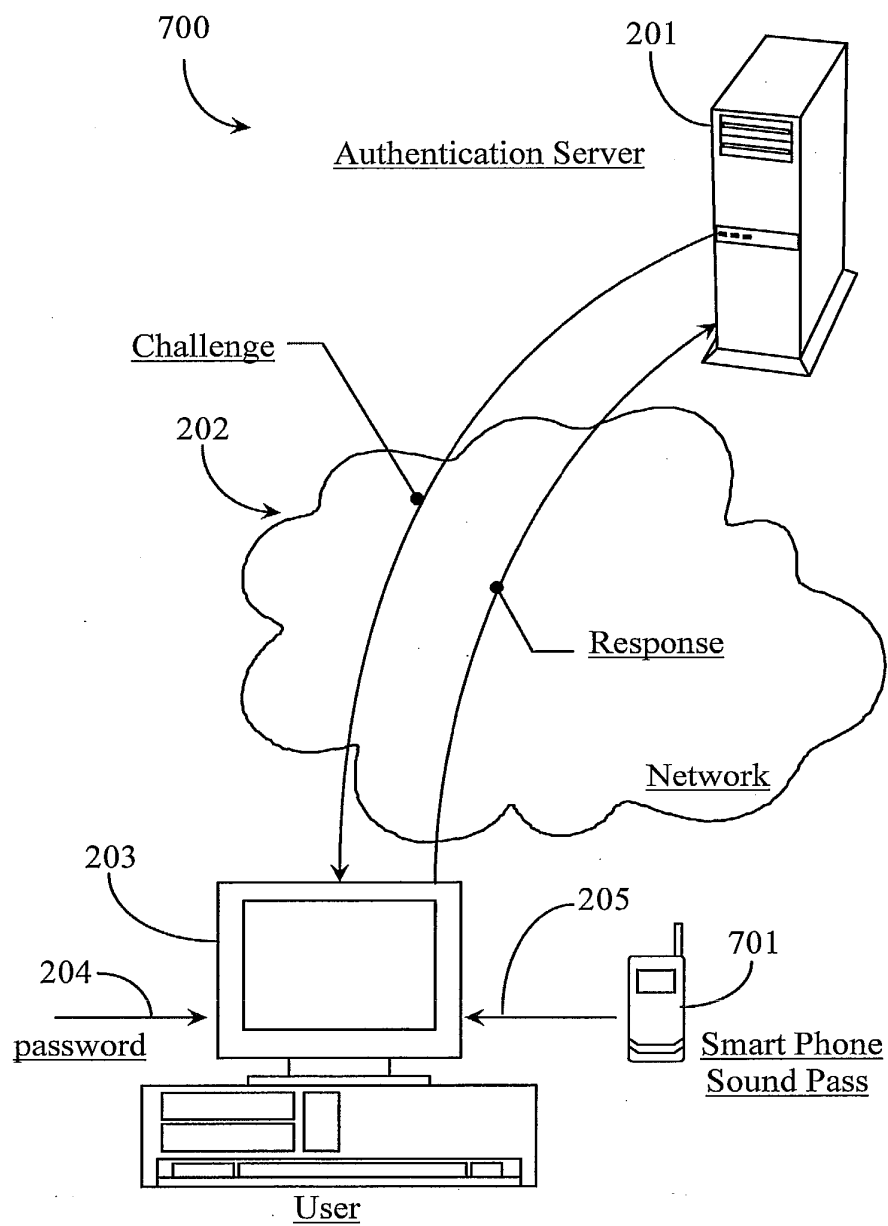


Fig.7

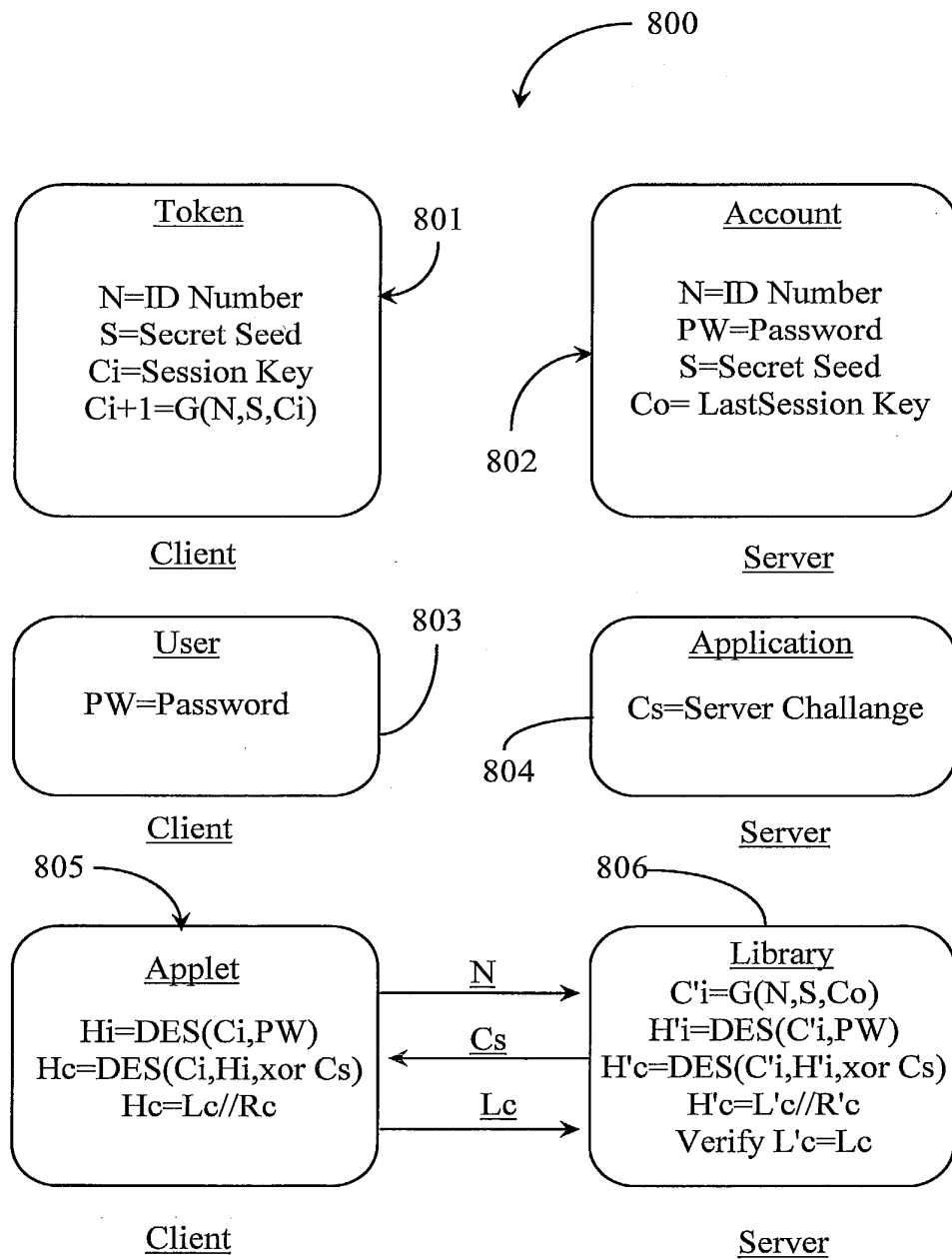


Fig. 8

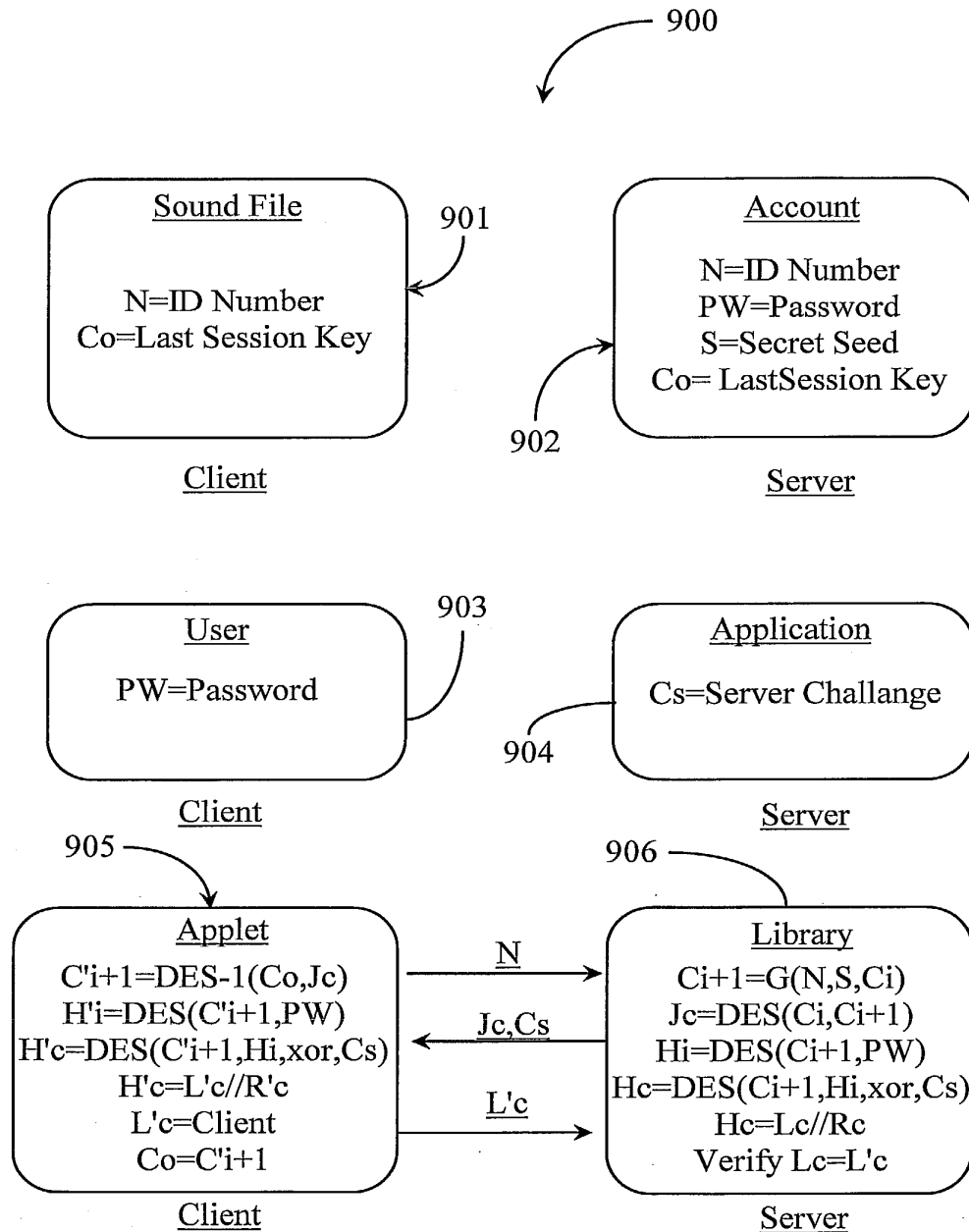


Fig. 9

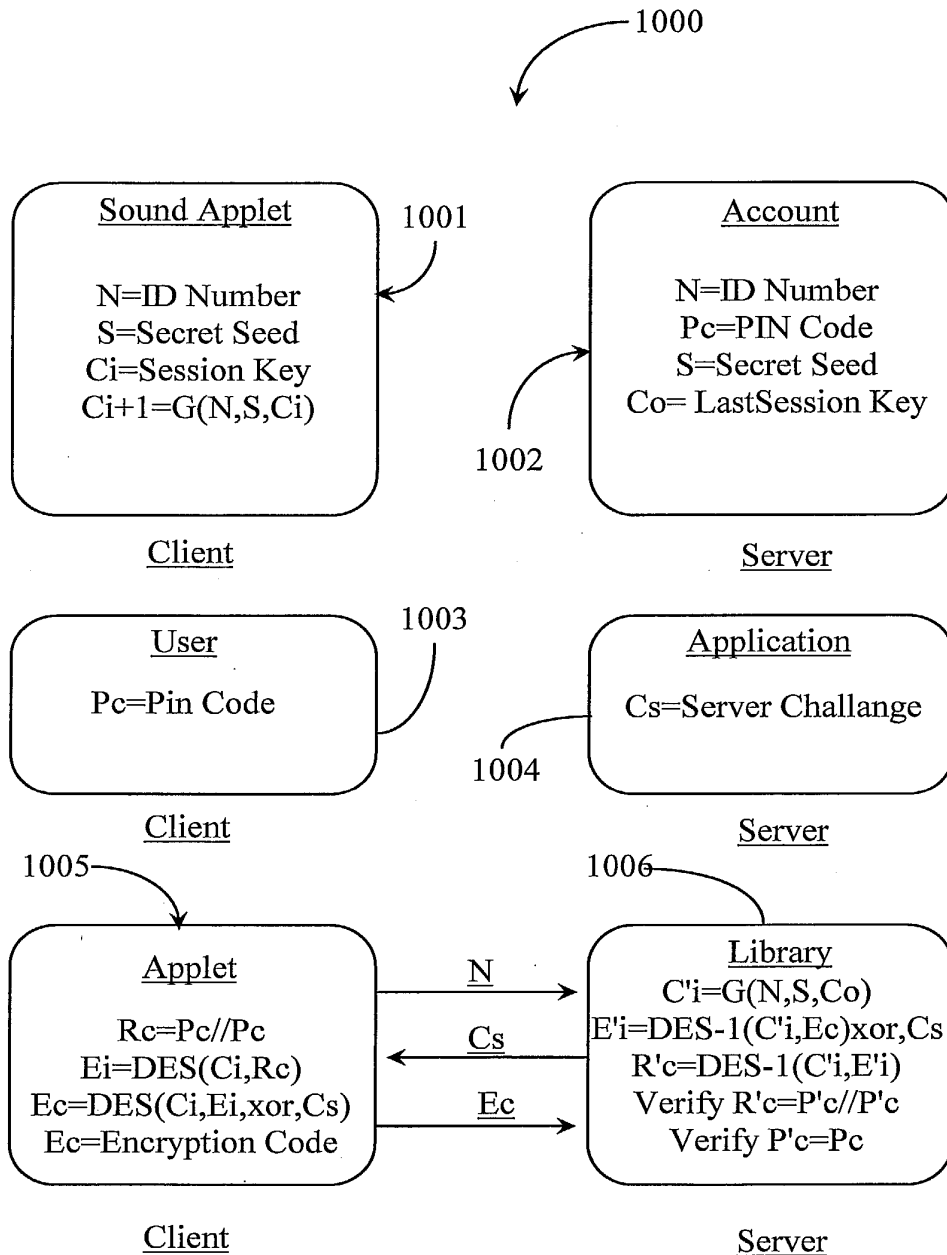


Fig. 10

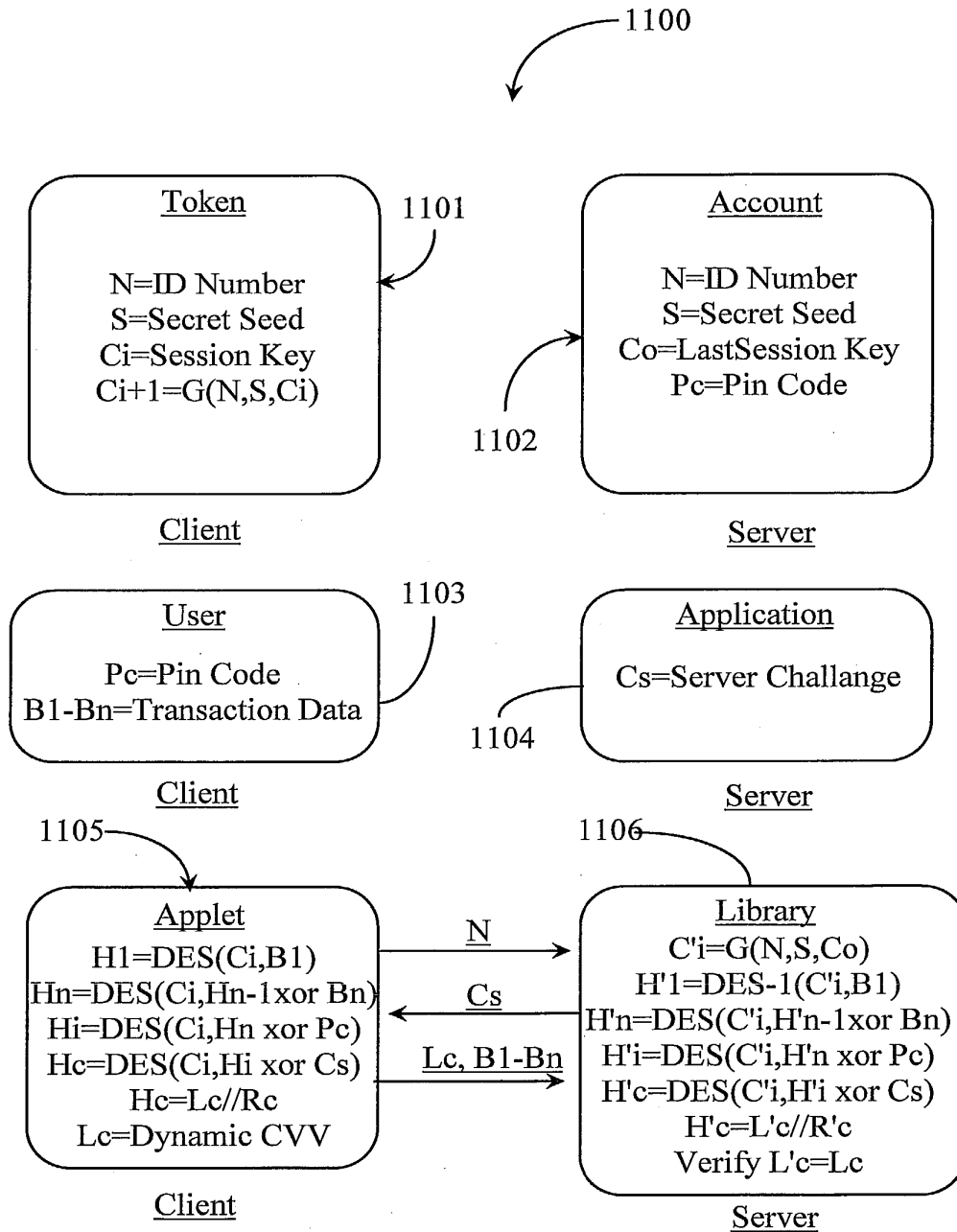


Fig. 11

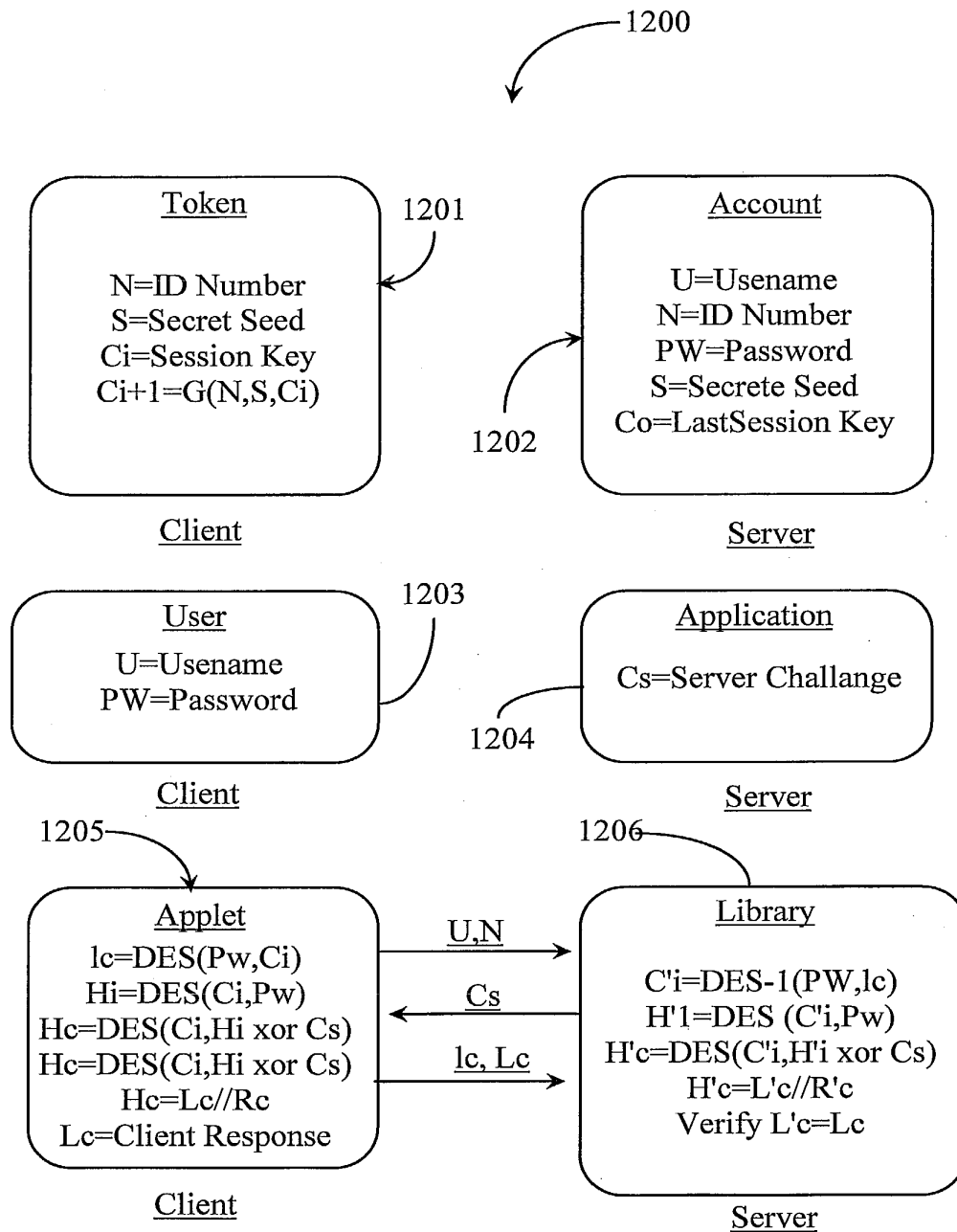


Fig. 12

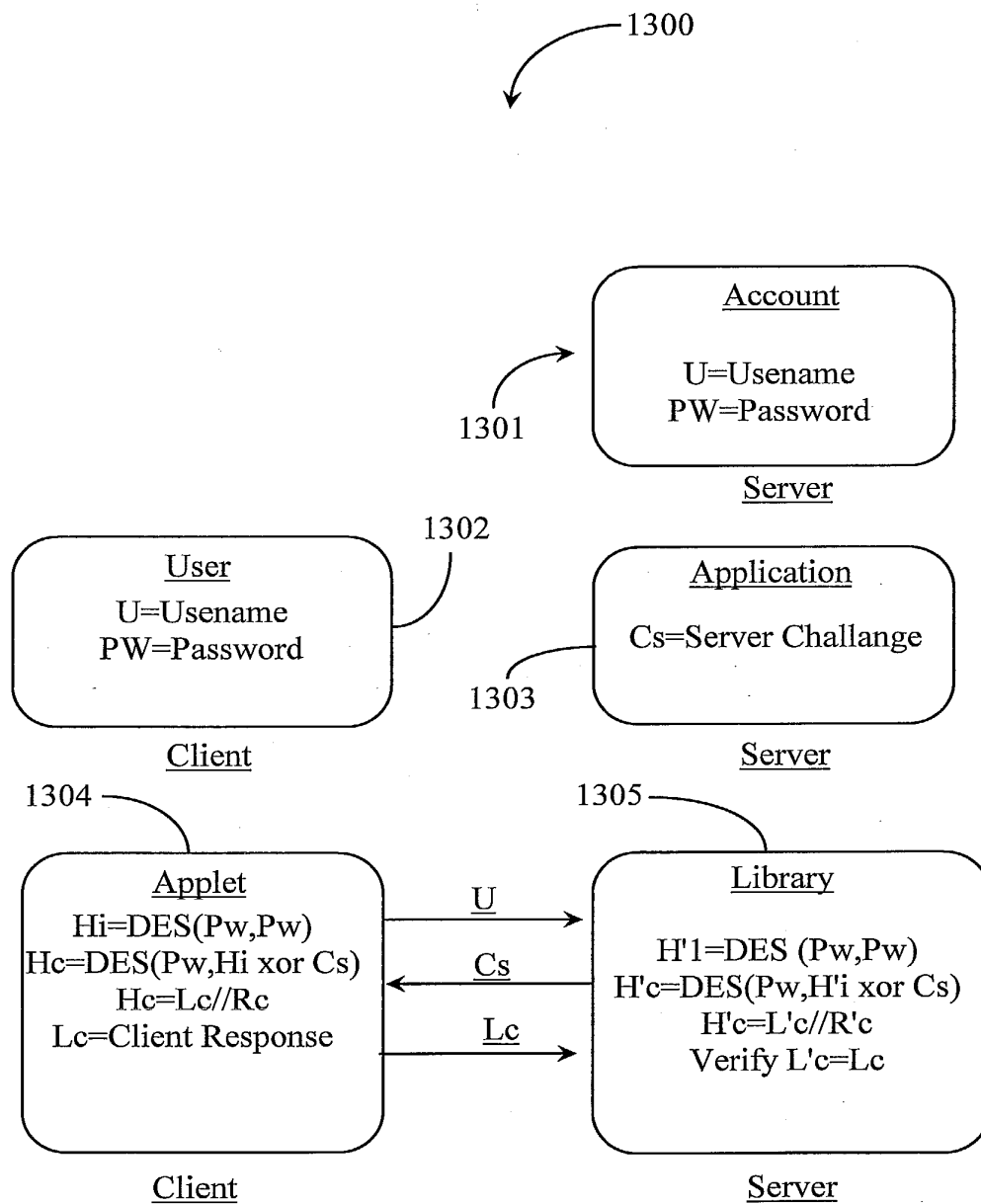


Fig. 13

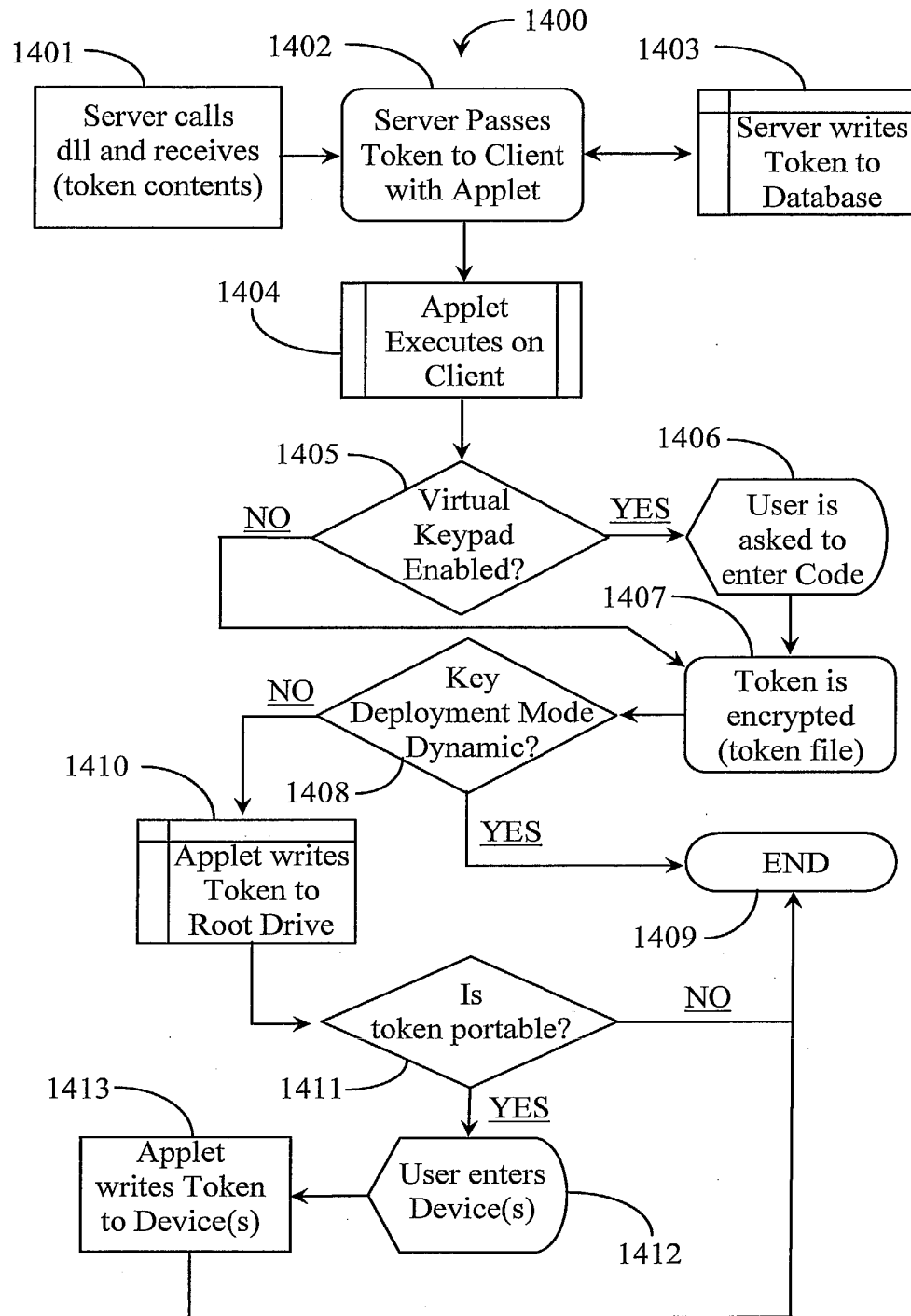


Fig. 14

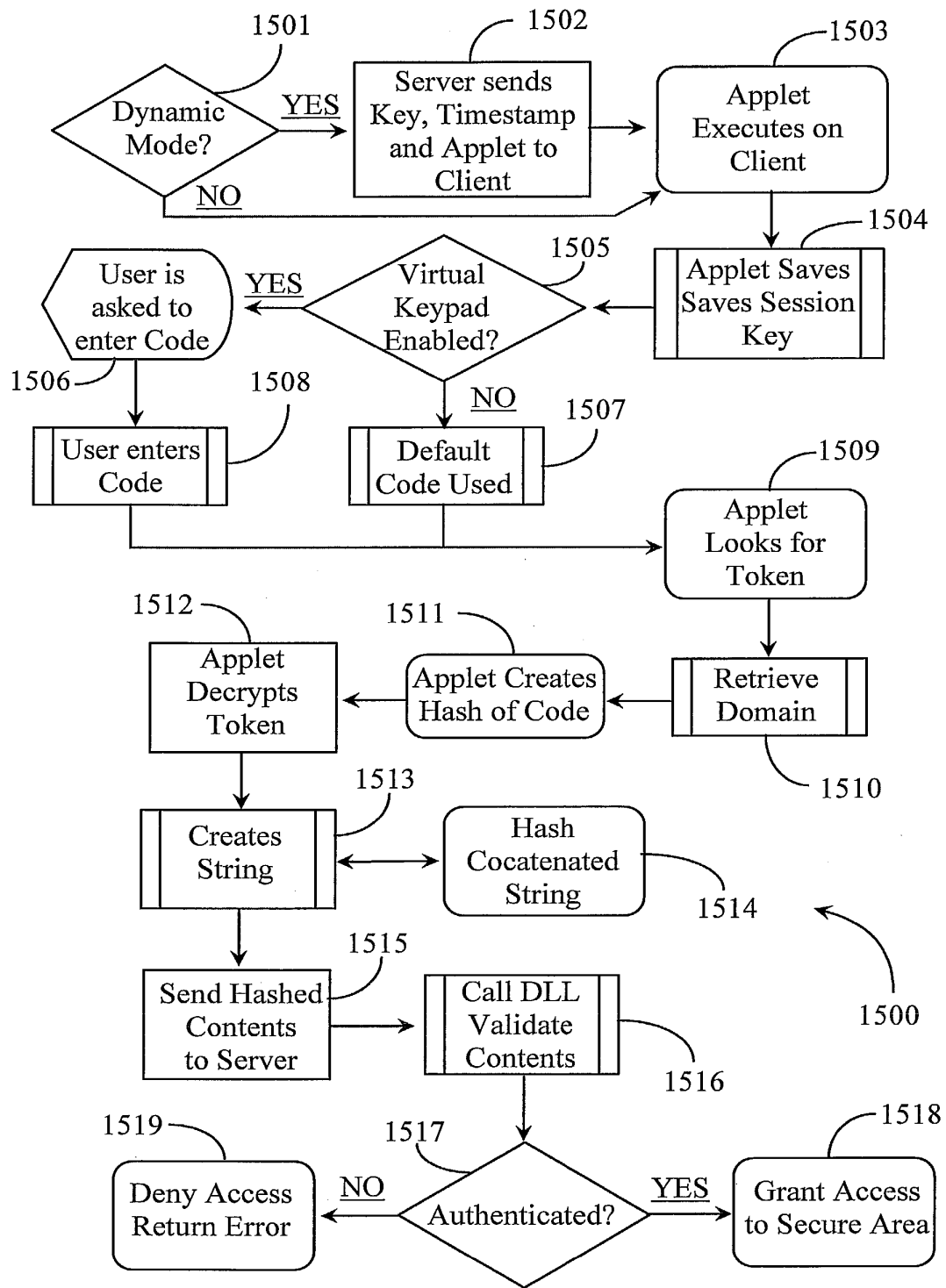


Fig. 15

METHODS AND APPARATUS FOR ENABLING SECURE NETWORK-BASED TRANSACTIONS

5 CROSS-REFERENCE TO RELATED APPLICATIONS

The present invention claims is a Continuation of US application 11/533,030,
filed 09/19/2006, which claims priority to a U.S. provisional patent application serial
number 60/719,273 filed on 09/20/2005. The referenced applications are included herein
10 at least by reference.

BACKGROUND OF THE INVENTION

1. Field of the Invention

15 The present invention is in the field of electronic transactions carried out over a
network connection and pertains particularly to methods and apparatus for ensuring
identity security for the transaction parties.

2. Discussion of the State of the Art

20 Integrated circuit cards, commonly referred to as smart cards, are widely used in
stores to secure electronic payments. The online market has not adopted smart cards,
although they provide the best security to conduct electronic commerce. The main reasons
are the high cost of the card reader and the complexity of the system for most people. Not
only a card but also a reader must be provided to the millions of potential end-users who
25 comprise this market base.

The inventor is aware of a method and apparatus to secure online transactions on
the Internet. The system includes a smart card transmitting an identification sequence to
a PC in the form of a modulated signal, a card reader plugged into the microphone input

of the **PC** sound card, and a **PC** applet demodulating the identification sequence. The card reader is characterized by the absence of processing means.

The inventor is also aware of a secure memory device for a smart card with a modem interface. The secure memory includes a rewritable memory such as an
5 EEPROM, a processing unit or a microprocessor, an on-chip oscillator, an ISO 7816 interface, and a one-wire modem interface. The memory is characterized in that both communication interfaces are bi-directional and share the same terminal. The modem interface is exchanging data with the host in the form of a modulated signal by means of a card reader characterized by the absence of processing means.

10 The inventor is further aware of a method and apparatus to secure online transactions over the phone. The method includes a smart card transmitting an identification sequence to an IVR server in the form of a modulated signal, a card reader plugged into the telephone line, and an IVR applet demodulating the identification sequence. The card reader is characterized by the absence of processing means.

15 What is clearly needed is improved and more secure client/server methods including transmission packaging of secure authentication over a network aided in some case by user-friendly peripherals and devices for performing secure transactions over a data-packet-network.

20 BRIEF SUMMARY OF THE INVENTION

In one embodiment of the invention an access security process is provided, comprising opening a connection to an interactive web site executing on a processor of an Internet-connected server by a client computerized appliance asserting a URL in a web
25 browser, displaying a log-in mechanism to the client computerized appliance by the interactive web site, enabling a user operating the client computerized appliance to enter log-in information, in response to a successful log-in, sending to the client computerized device, data including a time stamp of the time of the log-in, and a page location of an applet to be run by the client computerized appliance to continue the security process,

through executing the applet on the client computerized device, determining the domain of the server by querying the page that includes the applet, and searching data storage devices coupled to the client computerized device for an encrypted token compatible with the security process, on finding the token, rendering a virtual keypad on a display of the client computerized appliance, enabling the user to enter a PIN known to the user for decrypting the encrypted token, if the PIN does not successfully decrypt the token, suspending the security process, in the event the PIN successfully decrypts the token, salting the decrypted token value with the time stamp and the domain by adding the domain on one end of the token string and the time stamp on the other end, and hashing the result by a specific hash function, sending the hash value of the decrypted, salted token value to the interactive web page at the server, invoking a dll at the server, retrieving a token stored at the server, salting that token with the domain of the server and the original time stamp sent to the client computerized appliance, and hashing the result by the specific hash function, comparing the hash value received from the client computerized appliance with the hash value generated by the dll at the server, and determining passage of time from the time of the original time stamp to present time, if the passage of time is greater than a preprogrammed time, or if the hash values do not match, denying access by the user at the server, and if the passage of time is within the time window and the hash values do match, granting access to the user at the server.

In one embodiment the data storage device coupled to the client's computer where the compatible token is found is a flash thumb drive. Also in one embodiment the token is unique to a client and includes an identification number, a password or personal identification code, a session key, and a secret data seed. Also in one embodiment the software applet is a Java applet and the token is a Java archive.

In another aspect of the invention an access security system is provided, comprising an Internet-connected server coupled to a data repository and having a processor, and software executing on the processor from a non-transitory medium, the software providing a process of opening a connection to an interactive web site executing on the processor of the Internet-connected server by a client computerized appliance

asserting a URL in a web browser, displaying a log-in mechanism to the client computerized appliance by the interactive web site, enabling a user operating the client computerized appliance to enter log-in information, in response to a successful log-in, sending to the client computerized device, data including a time stamp of the time of the log-in, and a page location of an applet to be run by the client computerized appliance to continue the security process, through executing the applet on the client computerized device, determining the domain of the server by querying the page that includes the applet, and searching data storage devices coupled to the client computerized device for an encrypted token compatible with the security process, on finding the token, rendering a virtual keypad on a display of the client computerized appliance, enabling the user to enter a PIN known to the user for decrypting the encrypted token, if the PIN does not successfully decrypt the token, suspending the security process, in the event the PIN successfully decrypts the token, salting the decrypted token value with the time stamp and the domain by adding the domain on one end of the token string and the time stamp on the other end, and hashing the result by a specific hash function, sending the hash value of the decrypted, salted token value to the interactive web page at the server, invoking a dll at the server, retrieving a token stored at the server, salting that token with the domain of the server and the original time stamp sent to the client computerized appliance, and hashing the result by the specific hash function, comparing the hash value received from the client computerized appliance with the hash value generated by the dll at the server, and determining passage of time from the time of the original time stamp to present time, if the passage of time is greater than a preprogrammed time, or if the hash values do not match, denying access by the user at the server, and if the passage of time is within the time window and the hash values do match, granting access to the user at the server.

In one embodiment of the system the data storage device coupled to the client's computer where the compatible token is found is a flash thumb drive. Also in one embodiment the token is unique to a client and includes an identification number, a password or personal identification code, a session key, and a secret data seed. And in one embodiment the software applet is a Java applet and the token is a Java archive.

BRIEF DESCRIPTION OF THE DRAWING FIGURES

5 Fig. 1 is a block-diagram illustrating a secure transmission package of a secure identification number and session key according to an embodiment of the invention.

 Fig. 2 is an architectural overview of interaction between a user and an authentication server according to an embodiment of the present invention.

 Fig. 3 is an architectural overview of interaction using the system of the invention according to another embodiment of the present invention.

10 Fig. 4 is a block diagram illustrating basic electronics of a key jack sound pass generator according to an embodiment of the present invention.

 Fig. 5 is a plan view of design options for a key jack signal generator according to embodiments of the present invention.

15 Fig. 6 is a block-diagram illustrating basic electronics of a smart card signal generator coupled to a card reader according to another embodiment of the present invention.

 Fig. 7 is an architectural overview of interaction using the system of the invention including authentication server and a mobile device for signal generation according to yet another embodiment of the present invention.

20 Fig. 8 is a block diagram illustrating user authentication and generation of a new session key by the token for use according to an embodiment of the present invention.

 Fig. 9 is a block diagram illustrating user authentication and update to a sound file token and a server-transmitted session key according to an embodiment of the present invention.

25 Fig. 10 is a block diagram illustrating user authentication and a method for generating a new session key for a user according to another embodiment of the present invention.

 Fig. 11 is a block diagram illustrating user authentication using a card verification value (CVV) code according to yet another embodiment of the invention.

Fig. 12 is a block diagram illustrating user account activation on a server according to an embodiment of the present invention.

Fig. 13 is a block diagram illustrating user authentication using a password as a session key according to yet another embodiment of the invention.

5 Fig. 14 is a process flow chart illustrating acts for creating a soft token for authentication for a user according to embodiments of the present invention.

Fig. 15 is a process flow chart illustrating acts for retrieving or activating a soft token for authentication according to embodiments of the present invention.

10 DETAILED DESCRIPTION

The inventors provide a system that may be used in a variety of ways using hardware and/or software to provide secure authentication over a network for users and user groups. The present invention is described according to various embodiments and in enabling detail supporting each of those embodiments. More particularly, the system uses
15 a modulated sound consisting at least in part of an identification number and a session key.

It is important to note herein that in one embodiment, the identification number may, for example, contain 16 digits of data and may be a fixed identification number (ID)
20 or on that is dynamically assigned. It may also be encoded to include an error detection bit. In this case the identification number may also be encrypted with a proprietary key to ensure the provider authorized to provide the software of the invention may practice the invention in a way that is functional.

The following example demonstrates a configuring and encryption of a 16-digit
25 ID number for use according to an embodiment of the invention. The ID number may contain fewer or more than 16 digits. The number 16 is exemplary. ID number = 1 2 3 4
5 6 7 8 9 0 0 1 2 3 4 5: The 16 digits are grouped into 8 decimal numbers value from 00-99 and these are 12, 34, 56, 78, 90, 01, 23, and 45. Each of the decimal numbers are converted into hexadecimal numbers value from \$00-\$63 and these are \$0C, \$22,

\$B8, \$4E, \$5A, \$81, \$17, \$2D. The most significant bit of each byte of data is reserved for storing an error detection or parity bit. The string of hexadecimal values after conversion is \$0C, \$22, \$B8, \$4E, \$5A, \$81, \$17, and \$2D.

5 The ID number is then encrypted by adding an exclusive logical operator (XOR) that in this example is a proprietary 8-byte applet key. An example of the applet key is \$99, \$AA, \$BB, \$CC, \$DD, \$EE, \$FF, \$55. The resulting encrypted ID string is \$95, \$88, \$03, \$82, \$87, \$6F, \$E8, \$78. In this example, a session key is provided to generate a hash of the user password. The hashed password is valid only for one session.

10 In a variation of this embodiment, a new session key is generated each time a user attempts authentication and the user token is activated. An iterative algorithm [$C_{i+1} = G(N, S, C_i)$] is used to generate a new key. G = a one way function such as one based on a stream cipher, an encryption method that works on a continuous stream of data rather than individual data blocks. N = the client or user ID number described above whether encrypted or not. S = a proprietary seed known only to the issuer. C_i = the current session
15 key. The session key may be 8 bytes or longer depending on the token capabilities. The inventor provides the above information for clarity relative to encryption methods only that are described in detail further below according to several embodiments. Other variants may be used without departing from the spirit and scope of the present invention. However, the function of a two factor authentication where one factor is an identification
20 number and the other is a modulated sound is important in several aspects of the present invention as will be seen further below.

Fig. 1 is a block-diagram illustrating a secure transmission package 100 of a secure identification number and session key according to an embodiment of the invention. Package 100 represents an encoded and sound modulated transmission
25 carrying a data payload 101 including a secure identification number 102 and a session key 103 comprising 2 data frames. Package 100 includes a protocol layer 104, an encoding layer 105, and a sound modulation layer 106. Package 100 is assembled at a client-operated personal computing appliance (PC) and is transmittable over a data-packet-network such as a local area network (LAN) or a wide area network (WAN) where

it is decipherable at the other end, typically at a server adapted to authenticate secure access to some network-based resource.

Data payload 101 includes ID number 102, typically in an encrypted state. However, encryption of ID number 102 is not specifically required in order to practice the present invention. Session key 103 is used to encrypt a user password and is a unique key provided by a key issuer. A session key may be a dynamic key good only for one session as described further above. However, in some cases it may be a static key good for more than one session.

ID number 102 and Session key 103 are embedded into protocol layer 104 each chunk of data starts with a flag byte indicating the type of data enclosed and ends with a cyclical redundancy-checking (CRC) bit for transmission error detection comprising a data frame of a data type. The data frames carrying the ID number and session key are encoded with encoding breaks.

In this example, the frames are encoded using a Miller code known to the inventors. This encoding creates transitions every 1 elementary time unit (etu), every 1.5 etus, and every 2 etus even if the data doesn't change. Any other known code could be used in place of the Miller code, although other codes might create more transitions. The Manchester code for instance creates transitions every 0.5 etu and every 1 etu.

The encoding process in this example transmits the data (ID number and session key) and bit clock together in a same signal. The flag byte contains an encoding break, which is a longer time without data transition (3 etu for instance), signaling the beginning of a frame.

In this embodiment, the encoded bit flow is modulated as demonstrated by modulation layer 106 using a frequency-shift keying (FSK) modulation technique creating an analog waveform for representing logic 1 and another for representing logic 0 each wave form at different frequencies. The FSK modulation of the data is performed by a soft modem that is provided in an applet downloaded to a client practicing the present invention. The modem generates an audible sound compatible with PC sound card capabilities. The modulation frequency may be in the range of 0 Hz to 20 kHz for PC

server application or in the range of 300 Hz to 3 kHz, which is compatible with telephone networks (wired and mobile). The modulated signal is demodulated by an FSK modem at the server.

5 Fig. 2 is an architectural overview 200 of interaction between a user and an authentication server according to an embodiment of the present invention. Overview 200 includes an authentication server adapted to authenticate a user 203 for access to a secure resource. Server 201 may be any type of server including a transaction portal authenticating transaction for a group of web merchants or banks. It may also be any server adapted to handle secure transactions for individuals. The server may simply
10 provide secure login services to a secure area instead of enabling transactions. A secure authentication may be for the purpose of authentication one or more transactions or for granting network access to one or more than one secure resource. Likewise one server may perform both secure login services and secure transaction services.

15 In this example, user 203 is operating a PC having a network connection to server 201 over a network 202. Network 202 may be an Internet network, an Intranet network, or a wireless telephone network without departing from the spirit and scope of the present invention. In this example, to be authenticated user 203 has a password or personal identification number (PIN) and a token that generates a session key that is useable only once in this embodiment.

20 Before practicing the invention for the first time, user 203 receives an applet from server 201. The applet contains a modem and a session key issued by the server. The modem demodulates and decodes the signal and includes an encryption algorithm for handling the challenge/response interaction between the user and server. In this example, user 203 enters a password or pin code locally and inserts the sound token, which
25 generates the modulated sound into an audio input on the PC. The session key automatically encrypts the password or PIN ensuring a permanent password encryption state meaning that the password or PIN is never transmitted over the network to the server in a clear or unencrypted state.

In this example user 203 is not required to enter a username. Server 201 sends the correct user name when it receives the correct ID number from the token on the client PC. Only a valid server can send the correct user name. Therefore user 203 is entering his password safely and securely.

5 Fig. 3 is an architectural overview 300 of interaction using the system of the invention according to another embodiment of the present invention. Overview 300 includes authentication server 201, network 202 and user 203 having the same description and element numbers introduced in the description of Fig. 2 above. In this example user authentication is demonstrated.

10 In this embodiment the applet on PC 203 generates a hash code based on the session key, challenge, and password. The challenge is a random number generated by server 201 for each transaction that requires authentication. Access is granted to the user operating PC 203 if the server authenticates the hash code, which is sent from the PC to the server over the network.

15 The hash code is the session key in this example. As the session key, the hash code is valid only once. The hash code is also the server challenge in this example. As the server challenge, the hash code is valid for a short period of time. In this embodiment server 201 deduces the current session key referred to herein for discussion purposes as (Ci) from the last session key used, which is stored at the server. The previous session
20 key is referred to herein for discussion purposes as (Ci-1) or as (Co) in some embodiments is stored in the server database.

 Server 201 generates a hash code of the user password stored at the server using the session key. In this example, server 201 compares the hash of the user password to the hash received. The user is authenticated for a transaction if both hash codes are
25 identical. This indicates that both PC 203 and server 201 have used the same session key and password. In this case, server 201 stores (Ci-1) by (Ci) in the database and (Ci) cannot then be reused. In this interaction an ID number sent to server 201. The server sends a username challenge. The username challenge is sent in the form of a hash back to PC 203. The PC sends a hash code derived from the demodulated token parameters back

to server 201. The server, in the meantime generates its own hash code and when the server receives the client response, a comparison of the hash codes is performed. If the hash codes are identical, the user is granted access or otherwise is validated as the correct user authorized to complete the transaction during the current session.

5 In a preferred embodiment, the sound signal or sound pass, as referred to by the inventor and illustrated herein as sound pass 205 in Figs. 2 and 3, may be provided in at least three system compatible forms. In fact any hardware device capable of playing a sound may be incorporated as a sound pass token. Therefore, the token may be a hardware device or a software file (soft form) like a Wav file for instance. One device
10 that is disclosed herein and that may serve as a sound pass token is a smart card used in conjunction with a card reader. Another device that may be used as a sound pass token is a unique key device termed a key jack by the inventor. The key jack may be adapted to be inserted into any "audio in" line on a PC such as the microphone port, telephone jack, or any auxiliary port having connection directly or indirectly to the sound card on the PC.
15 The key jack is manipulated to play the modulated sound pass by pressing a button provided on the device when the device is properly inserted into the PC. The applet on the PC makes use of the sound pass token, demodulating the signal and generating the hash code for send to the authentication server.

 Yet another compatible sound token is soft version in the form of a sound file
20 deliverable from a mobile device like a cell phone, a personal digital assistant, or a handheld music player such as a Sony music player or an Ipod™. As long as the sound file can be input into the PC and recognized by the applet running on the PC the present invention can be practiced successfully.

 Fig. 4 is a block diagram illustrating basic electronics 400 of a key jack sound
25 pass generator according to an embodiment of the present invention. In one embodiment a semiconductor chip installed enclosed in a hand-held device like a key jack discussed above that plugs into the microphone input or other line input on a PC generates the sound pass signal. In one embodiment, the key jack may be plugged into the sound input

or headset connector jack associated with a mobile smart telephone or PDA enabling authentication through a telephone network.

In this example, chip circuitry 400 includes an electrically erasable programmable read-only memory (EEPROM) 401. In one embodiment, a re-writable flash memory may
5 be used. A modem circuit 406, an on-chip oscillator 405, a processing unit 409, and a serial input interface 408.

A tip/ring interface for plugging into a microphone jack or other line in is illustrated in reference to the chip circuitry and electrical paths. Chip 400 derives its voltage power from a sound card that provides from +3 to +5V direct current (DC). A
10 testing interface 410 is provided on chip 400 for the purpose of enabling remote access to the chip for erasing and reprogramming and testing. All components on the chip are accessible or may at least be tested through interface 408 without removing the chip from its host. Processing unit 409 may be a small microprocessor. Testing interface 410 includes a connection to power and a connection to ground. A sound pass file may be
15 stored on chip 400 in EEPROM 407 for use as a sound pass token. The file may be any suitable compression format including MP4, Wav, AVI, or others. Modem 406 and oscillator 405 generate the signal in the form of sine waves that are demodulated by a modem provided in the applet on the users PC.

The applet is, of course running when the sound pass token is input for
20 authentication using a key jack. The resistor adapts the impedance between the chip 401 and the microphone or other input. Switch 404 activates the modem 406, which in turn generates the modulated sound pass or signal input to the sound card on the PC. A user pushing a button, switch, or other mechanism on the external surface of the device hosting the chip operates or activates the modem to deliver the modulated sound one
25 time. Test interface 410 is a bi-directional interface. As a mobile device key jack 400 may be used at virtually any PC station or if so adapted any mobile device capable of a bi-directional network connection. Therefore, a user may perform a secure login without physically using a clear text password or username that might later be revealed through a key logger program or the like.

Fig. 5 is a plan view of design options for a key jack signal generator according to embodiments of the present invention. In this example, the circuitry described above is housed within a convenient and mobile key jack device that can be worn around a user's neck or may be placed on a key ring for convenience. A key jack design 501 is illustrated in both a top view and in a side view. Device 501 includes a tip interface 508 adapted to fit into a microphone input on a PC or other computing appliance. The ring interface is illustrated herein as ring 509. In one embodiment another plug interface may be used instead such as a telephone jack or other line in design capable of transmitting audio in to pass the signal into the computing appliance. Device 501 includes the sleeve illustrated in the device to the right as sleeve 510 functioning as ground.

In this case, device 501 is molded from a durable polymer and includes an activation switch in the form of a button 505. A user may insert device 501 into a microphone input and depress button 505 to close switch 404 described further above thereby activating the modem to generate and modulate the sound pass signal. The sound pass signal contains the ID number and session key embedded in the modulated sound.

Key jack device 501 may be updated to change token parameters dynamically through the test interface. Optionally, other designs may be provided such as with a key jack device 503 illustrated in a position rotated 90 degrees from device 501. Device 503 has a user activation button 504 located at the end of the device opposite tip/ring and sleeve assembly 510 in which the sleeve 510 is numbered. A convenient ring attachment 507 provides an interface for attaching the same to a rope or key ring. Device 503 has an alternate shape than device 501. There are many variant design options available.

Fig. 6 is a block-diagram 600 illustrating basic electronics of a smart card signal generator 601 coupled to a card reader 602 according to another embodiment of the present invention. Diagram 600 includes a smart card 601 with the sound pass chip embedded therein. The card plugs into card reader 602, which in turn is plugged into the microphone input of the host commuting appliance or other line input capable of carrying sound and directly or indirectly connected to the sound card on the computing appliance such as a PC.

The components of the chip are essentially identical to those describe in the example of Fig. 5 for the key jack circuitry. Therefore they shall retain the same element numbers and shall not be reintroduced. The difference in this implementation from that of the key jack implementation described above is that the chip 602 is removable from the card reader circuitry 602. In both cases of the smart card/reader and the key jack, the reader has no processing components. The microprocessor 409 is part of the chip. Another variation that separates the two described embodiments is that in this example, modem 406 and the serial interface 408 share the same international standards organization (ISO) contacts.

In still another embodiment of the present invention, a key jack or a smart card coupled to a card reader is not required to successfully practice the present invention. The token may instead be embodied as a sound file containing the ID number and session key that is simply stored on a PC hard drive or, in one embodiment on a USB flash drive or other removable media for better security. In the later case, the sound file token, which may be a wav file or other audio compression format, is entirely mobile (if stored on a removable drive) and may be generated and stored on the removable drive by an applet downloaded to the host PC. It is important to note herein that a user may utilize the token at any station having the required network connection capabilities by plugging the removable drive containing the token into that station. An applet though would have to first be downloaded to that station for updating the session key in one embodiment.

In another embodiment however the applet may also be an executable stored on the same removable drive containing the token. For example, in a preferred embodiment the applet is a Java applet utilizing a java archive (JAR) including the token parameters and current session key. The applet and token parameters may be downloaded to a same removable media wherein session key updates are performed on the removable media instead of on the host appliance.

The only requirement of the host appliance is that it has a version Java installed and accessible to the network browser that recognizes the applet and JAR file on the removable media such as a re-writable (RW) compact disc (CD) or a flash drive. In this

embodiment, extensions may be created to enable older versions of Java installed on older operating systems to recognize the Java applet and JAR file. In this way no initial download of an applet is required of the host PC.

5 The server may dynamically send a new session key upon connection established thereto by the host PC. The session key may be downloaded directly onto the removable media and the applet already on the removable media may automatically update the token for next use. In this way a user may perform a secure transaction from any host station running a compatible version of java or an older version of Java adapted by extension to recognize the latter version applet and JAR file. Moreover, the transaction may occur in a
10 secure manner leaving no trace of the activity on the host PC.

In one embodiment using a sound file, the sound file may be updated by a PC-based applet, which includes a FSK modem generating the modulated signal based on a new session key received from the server. Alternatively, the sound file is updated by the server during a session with the host PC periodically lie every week or month. This is a
15 static or quasi-static implementation of the system since the same session key is used for several authentications instead of being valid only for one authentication.

Fig. 7 is an architectural overview 700 of interaction using the system of the invention including authentication server 201 and a mobile device 701 for signal generation according to yet another embodiment of the present invention. As described
20 above, in one embodiment a sound file may serve as the token that includes the user ID number and session key as previously described.

In this example, a modulated audio signal is generated by a sound-generating applet installed on and executable from mobile device 701, which is a smart phone in this example. In another embodiment, phone 701 may instead be a PDA or a hand-held music
25 player such as an Ipod™.

In one embodiment a user enters a password or PIN on the PC via the keyboard of the PC. The output speaker system of mobile device 701 may be leveraged to play the modulated sound pass into a microphone plugged into PC 203. The microphone is plugged into the sound card on PC 203. The server challenge is a hash of the user

password and the PC response is the modulated sound pass sent to the PC from mobile device 701 acoustically.

5 In another embodiment, mobile device 701 may include a hardwire cable that connects the speaker or headset output to the microphone input accomplishing the same task of inputting the signal. A PC-based applet on the PC demodulates the sound pass signal and communicates with the server to authenticate the user. In this example, the token on the mobile device if a sound file may not be updated by a PC applet or by the server through the host PC. However, in one embodiment the sound file may be updated by the applet on the device if the server sends a new session key to the mobile device
10 directly or by the server contacting the telephone directly and establishing a secure network session with the device to update the file.

Fig. 8 is a block diagram 800 illustrating user authentication and generation of a new session key by the token for use according to an embodiment of the present invention. The token in this example is a hardware token like a key jack or smart card.
15 The authentication process of the present invention may vary slightly according to the form of token used. This embodiment is applicable to the use of either a smart card or a key jack token host described further above.

In this example a client has a token 801 in the form of a key jack or smart card having the secure chip described in the circuitry diagrams above. Token 801 in this
20 example includes the user ID number (N), a secrete seed (S) provided by the authentication service, and a session key (Ci). Ci is the current session key stored on the token. In this case the token generates a new session key. A new session key that is generated by the token is expressed as C_{i+1} which is = to a one-way function (G) of N, S, and Ci. Ci is the previous or current session key stored on the card, which may have been
25 used in the last authenticated transaction made by the user. It is possible that Ci is a current key that has expired but was never used. The secrete seed (S) is a parameter issued to the client by the authentication entity or service and is known only to the issuing service. It is not specifically required in order to successfully practice the invention, but provides yet another enhancement to the hash code generation process.

At the server, an account belonging to the user is known. Server 802, which may be the authenticating entity, has stored therein parameters of the user account including N, a user password (PW), S, and record of the last session key (Co) used in an authentication. Co may or may not be the same key as Ci on the token. In this example
5 the user token generates a new session key (Ci+1) for each subsequent secure transaction that requires authentication of the user. The server deduces the new session key from knowledge of the last-used session key in the same fashion as the token.

The user 803 has a password (PW) that is identical to the password recorded in the account data and that is the only parameter the user manually enters in this
10 embodiment. The server has an application 804 that issues a server challenge among other tasks whenever the ID number (N) is submitted. The user sends N to the server, which identifies the user and the server sends back a sever challenge (Cs) back to the user. The server challenge has described further above may be a hash of the user ID number and password. An applet 805 generates an encrypted version (Hi) of the Ci and
15 PW using a symmetric-key encryption method known as the data encryption standard (DES) available to the inventor. Other methods are possible without departing from the spirit and scope of the present invention.

A Hash code is generated from Hi using the session key again (Ci), adding an xor function, and the server challenge (Cs), which may be hashed or not. The resulting hash
20 code is divided in two and only one of the halves of the code is used as a client response (Lc) in this example that is sent to the server (Rc). The process of encryption and hashing ensues after the server challenge is received at the client because the server challenge is a variable of the final hash code sent back to the server.

As the process unfolds, the server generates its own hash codes using the exact
25 same parameters that the client used with the aid of the software driver (DLL) the codes cached temporarily in a code library 806. Library 806 represents the processing environment that the server uses to temporarily store data and make hash comparisons to validate clients. In the server library 806, the hash code generated by the server is compared to the one received by the client. If the compared codes are identical, $L'c=Lc$,

then it provides absolute assurance that the client and the server used the same session key and the same password.

Fig. 9 is a block diagram 900 illustrating user authentication and update to a sound file token 901 and a server-transmitted session key according to an embodiment of the present invention. In the last embodiment, the token at the client location generates a new session key. In this example, the server generates a new session key.

The client has a sound file token 901 located on a PC or on some external device like a cell phone, PDA, or other handheld device capable of playing the sound file. The current sound file has the user ID number and the last session key sent to the server at the last successful transaction that required authentication. At server side, the client account parameters defining account 902 are known and include N, PW, S, and Co as described with respect to Fig. 8 above.

In this case, a user 903 manually enters a password (PW) known only to the user and to the server. A server application 904 provides a server challenge and a new session key transmission (Jc) to the applet running on the user PC. The server challenge is required by the applet running on the PC in this case to generate the proper hash code for return to the server as L'c and to obtain the new session key for use.

In this case, the server, within the library 906 generates a new session key after the correct identification number (N) is received from the client. The key is expressed in this case as C_{i+1} and is derived from a one way function (G) of N, S, and C_i , or $C_{i+1}=G(N,S,C_i)$. In library 906, the transmission (Jc) is the new session key encrypted with the last session key (C_i) or $Jc=DES(C_i, C_{i+1})$.

The server sends Jc and the server challenge (C_s) together in one transmission back the client. The client generates a first hash ($H'i$), which is an encryption of the new session key sent by the server and the password or $H'i=DES(C'i+1,PW)$. The server performs an identical hash in the library or $H_i=DES(C_{i+1},PW)$.

The applet on the client generates a final hash code ($H'c$) which is an encryption of H_i and the server challenge using the received session key and adding an xor function or $H'c=DES(C_{i+1},H_i,xor,C_s)$. The server performs the same hash

$H_c = \text{DES}(C_{i+1}, H_i, \text{xor}, C_s)$. H'_c then equals the client code to be compared with the server code. The client sends L'_c to the server and stores C'_{i+1} (new session key) as C_o (the last session key used). The last operation occurs after the client is successfully validated. L'_c is compared to L_c at the server and if the hash codes are identical, authentication is successful.

Fig. 10 is a block diagram 1000 illustrating user authentication and a method for generating a new session key for a user 1003 according to another embodiment of the present invention. In this example, the token is a sound file stored on a device like a cell phone or a PDA and a sound applet 1001 is provided to the mobile device to perform the modulation, demodulation and encryption. The client token includes N , S , and C_i . The sound applet 1001 generates a new session key expressed as C_{i+1} , which is = to $G(H, S, C_i)$ where G is a one-way function. The known account parameters of the client account 1002 stored by the server are N (ID number), PW (Password), S (Secret Seed), and C_o (Last Session Key) used by the client.

In this example, user 1003 enters a PIN code (P_c) and plays the modulated sound into the microphone input of the PC acoustically using the speaker system of the mobile device. In one embodiment, the mobile device may be cabled to the microphone input from the speaker output or headset output. The client account 1002 at the server domain includes the parameters N , P_c , S , and C_o .

In this implementation the user entered PIN code is duplicated $R_c = P_c \parallel P_c$. A value E_i is generated and is an encryption of C_i and R_c or $E_i = \text{DES}(C_i, R_c)$. Eventually, the PC applet 1005 creates an encryption code (E_c) that is the encryption of E_i and C_s using the session key (C_i) and adding an xor function. Expressed in this example, it is $E_c = \text{DES}(C_i, E_i, \text{xor}, C_s)$. E_c is decrypted at the server using the session key stored in the account parameters.

Fig. 11 is a block diagram 1100 illustrating user authentication using a card verification value (CVV) code according to yet another embodiment of the invention. In this example, banks or other financial institutions deploy secure smart cards in the form of bank cards having the sound pass token chip embedded thereon. The cards are adapted

as a variation of the smart card used with a card reader plugged into a microphone jack on the user PC as described further above.

In this example the token (bank card) includes the token parameters of N, S, and C_i where C_i is the current session key. N (ID number) is different than the issued card number in this example for better security, but it includes the ID of the card issuing entity and enables the bank to route the transaction along with the CVV number (3-digit number) using existing bank protocols. The client account 1102 includes the ID number (N), the secret seed (S), the last session key used by the client (C_o), and the client PIN code (P_c).

Like the smart card or key jack implementation described further above, the token generates the new session key expressed as $C_{i+1} = G(N, S, C_i)$. The user may enter a PIN code (P_c) and then may perform a series of banking transactions by submitting transaction data B_1 - B_n . For each transaction, a new hash code (H_c) is generated by applet 1205 on the client PC. The final H_c is a dynamic card verification value (CVV) based on the session key, the transaction data (b_1 - B_n) for the instant transaction, and the P_c . In this example, $H_c = L_c$, which is sent to the server for each transaction and must be verified for each transaction.

The server generates its own hash to determine L'_c , which is compared to the received H_c L_c for each transaction wherein the authentication is defined by the compared hash codes being identical. In this example, the server hash operation occurs after the user has entered his or her PIN code and the instant transaction data for that session. Otherwise, the server would not have any knowledge of B_i - B_n and could not match the client hash.

One with skill in the art of encryption will appreciate and understand the multi step encryptions using the session key at the client and the parallel encryption performed at the server so that the final hash codes may be compared. The actual process never reveals any clear text data that could become compromised. In fact, in all of the embodiments of the invention, the server may store the user ID number Username, Password, PIN, etc in permanently encrypted format.

Fig. 12 is a block diagram 1200 illustrating user account activation on a server according to an embodiment of the present invention. An activation protocol is used for clients that are activating their accounts for the first time. The activation protocol automatically activates the system software on the server. In this example, the user 1203 enters his username (U) and password (PW). Token 1201 includes the issued ID number (N), the secreta seed (S), a current session key (Ci) and the token generates the new session key (Ci+1, which is a one way function (G)(N,S,Ci). In initial use, account 1202 includes the username (U) in addition to N, PW, S, and Co. Note that Co is only available to the server after authenticating the client for the first time.

The user 1203 accesses his account 1202 with his username and password. The first time he is using a sound pass token, the ID number and new session key are transmitted to the server and stored in the database only after authentication. The session key is encrypted (Ic) with the password prior to transmission to the server.

Fig. 13 is a block diagram 1300 illustrating user authentication using a password as a session key according to yet another embodiment of the invention. In this case, the client 1302 knows the username (U) and the password (PW) to access account 1301. Account 1301 has U and PW stored as parameters. In this case, user 1302 does not have a token available because he has forgotten it or otherwise does not have access to it.

In this case, user 1302 enters U and PW to access the account. The applet 1304 on the client PC creates a session key from the PW $H_i = \text{DES}(\text{PW}, \text{PW})$. The application 1303 at the server sends a server challenge (Cs) to the client. The applet 1304 on the client PC generates a hash code (Hc), which is a DES encryption of the PW, the previous encryption (Hi) and the server challenge (Cs) adding an xor function. The Hc is the client response (Lc) sent to the server. Although this implementation is less secure because the session key is fixed, the method still ensures a permanent encryption of the password. In a preferred embodiment, this implementation may provide only a limited access to the user account.

Creating and Retrieving a Soft Token

In one embodiment of the present invention the token is not a secure chip but a software file that works with a server driver (dll) and a client applet. The soft token can be made portable and can be duplicated to portable or removable drives. It is important to note herein that the token values are expressed as a modulated sound pass signal and that, in most secure embodiments a new session key is used for each token hash operation. In this way, the token contents never change, but the hash value of those contents sent to the server is never the same.

Fig. 14 is a process flow chart illustrating acts 1400 for creating a soft token for authentication for a user according to embodiments of the present invention. In general use, a soft token is created for the client and the token, which is a sound file or generated sound is used with a session key to produce the hash code that authenticates the user for each transaction that requires authentication.

In act 1401, the server calls a driver or dll at the server or in some connected machine and receives randomly written token contents that provide the basis for future client access of one or of more than on account held for the client by one or more services. It is possible that the token issuer and the authentication entity is a third party to the transaction between a client and a service organization maintaining an account for the client.

In act 1402, the authentication server passes the token contents as clear text string along with a software applet to the client. The applet automatically installs itself either in the clients Web browser as a plug-in or as a separate instance. The applet and the token together may be packaged as a Java-based solution, more particularly an executable Java Archive (JAR) file. The solution includes the domain of the parent application or server-side dll. At act 1403, the server replicates or writes the token contents into a database at the server. Token contents may include, but are not limited to a user ID number, a secret seed, and an initial session key. Account parameters may include a password or PIN in addition to the other components mentioned above.

When the applet is received at the client, it executes on the client for the purpose of creating the token file at act 1404. In one embodiment there is a virtual keypad included as part of the applet program that may be used by the client to enter an encryption code for the purpose of encrypting the token file. In act 1405, it is determined if the virtual keypad is enabled or not. It may be a matter of user preference. If the virtual keypad is enabled at act 1405, then at act 1406, the user is prompted to enter a code to use as an encryption key. In one embodiment, the user-entered code is message-digest algorithm 5 (MD5) hashed and the hash value of the code is used as the encryption key. In a variation of this embodiment, random salts are added on each end of the token string before encryption. Salts are known in the art and used in DES sometimes to strengthen encryption. MD5 is a well-known hash used for many security applications and for file integrity checking. Other known or future-developed hash algorithms may be used in other embodiments without departing from the spirit and scope of the present invention.

At act 1405, if it is determined that a virtual keypad is not available, then a default code is used and the process skips to act 1407 where the token is encrypted using the MD5 hash value described above or some other value derived from a hash operation.

At act 1407, the token contents are encrypted according to either case of user-entered code or default code, and written to a token JAR file in a preferred embodiment. In the preferred implementation the applet is a Java applet leveraging a token file, which is a JAR file. At act 1408, it is determined if the token deployment mode will be dynamic or not. This option may be pre-set as a default by the token issuer or it may be an election granted to the user. Dynamic deployment mode is an option that prevents any storage of the token at the client machine. In the case of dynamic deployment, the user will immediately use the issue token to perform a secure transaction after which the token is no longer valid. In act 1408 if deployment mode is dynamic then the process ends at act 1409.

If at act 1408 the token deployment mode is not dynamic, then at act 1410 the applet writes the token file in encrypted form to the root drive on the client PC. At act

1411 it is determined if the token will be a portable token or not. This option may be a user preference. If at act 1411 the token is not portable, then the process ends at act 1409. If at act 1411 it is determined that the token is a portable token, then at act 1412, the user enters the parameters for the device or devices that will receive the token or a replicate of the token. These parameters may include a device machine address if the device is on a network, or drive letter id the device is directly attached storage (DAS). After the user enters the correct information, the applet writes or replicates the token to the appropriate storage devices at act 1413. The process ends at act 1409.

One with skill in the art of encryption will appreciate that the exact encryption system and methods employed may vary somewhat without departing from the spirit and scope of the present invention. For example, MD4 may replace MD5 as the hash method for the personal or default encryption code. Salts may be used or may not be used. It is reminded here for clarity that the ID number and session key are embedded into the generated sound or sound file or sound pass that is the token, each time the token is activated, a new session key is generated in a preferred embodiment.

Fig. 15 is a process flow chart illustrating acts 1500 for retrieving or activating a soft token for authentication according to embodiments of the present invention. At act 1501, it is determined whether the token deployment is dynamic mode or not. Dynamic mode means that there is no token resident on the client PC. If at act 1501 dynamic mode is enabled, then at act 1502 the server sends a session key, timestamp and applet to the client. If at act 1501, dynamic mode is not enabled, then the process skips to act 1503 wherein the applet executes of the client PC. In either case, the applet executes on the client PC in act 1503 and saves the session key in act 1504.

At act 1505 it is determined whether the virtual keypad is enabled or not. If at act 1505, the virtual keypad is enabled, then at act 1506 the user is asked to enter a code to use in encryption of the session key saved in act 1504. At act 1508 then the user enters the code. If the virtual keypad is not enabled at act 1505, then a default code is used at act 1507. The code is used to decrypt the token contents. In dynamic mode the applet has the token. If the mode is not dynamic then at act 1509, the applet looks for the client

token. The applet will use the first token it finds if there are multiple portable tokens or if the token is otherwise resident in more than one location accessible to the applet at the time.

At act 1510, the applet retrieves the domain of the token issuer to ensure it is the correct token. At act 1511, the PC applet creates an MD5 hash of the user-entered code of act 1508, or of the default code of act 1507. If operating in dynamic mode, the applet also updates the exiting token contents with the passed contents. At act 1512, the PC applet uses the hash to decrypt the token contents including removing any salts from the token contents. At act 1513, the PC applet concatenates the token value domain name and timestamp received from the server if dynamic mode is enabled. At act 1514, the applet performs an MD5 hash on the string of act 1513. At act 1515 the PC applet sends the hashed contents or content string to the authentication server.

At act 1516, the server calls the software driver (dll) to validate the contents of the string received from the client against the token and its domain retrieved from the server database. At act 1517 the dll attempt to authenticate the user by comparing the Parsed contents, which have been MD5 hashed by the client applet to a server hash of the token value, domain, and timestamp from the server. In act 1517, the server also checks to current time stamp against the current time. If it is operating according to dynamic mode. If the time stamp is not more than 2 minutes or so before the current time at the server, and the hashed values match then the user is authenticated in act 1517 and is granted access into the secure area at act 1518. The content string should equal the MD5 hash value of the server database token, the server domain and the original timestamp. Act 1518 may be access to a resource or it may be an approval or other type of user validation for a transaction.

If the hashed values matched but the time stamp window has expired in act 1517 then authentication fails and at act 1519 the server denies access or approval and returns an error to the user. Likewise, if the hashed values do not match identically then the user is not authenticated and the process moves again to act 1519.

It will be apparent to a skilled person that the examples and embodiments described in enabling detail above are not completely limiting to the invention. They are examples of practice of the invention. There may be many alterations that may be made in the described embodiments without departing from the spirit and scope of the invention. For example, readers and tokens may be implemented in many ways, in many shapes, and with a variety of materials, still within the scope of this invention. Further communications protocols may vary, and there are many ways of providing functionality critical to the invention with software beyond the examples give. It is not, for example, strictly limiting that the token generated is a sound file. Tokens may be provided in other ways as well. In one case one might provide a modulated light signal, or infrared signal to be read by an optical reader, the signal modulated to provide the same sort of information provided by the audio token described in detail above. The token might be a modulated vibratory signal. It could also be a character string coded in a fashion to provide the necessary input. Therefore the invention is limited only by the scope of the following claims.

20

What is claimed is:

1. An access security process, comprising:

- 5 opening a connection to an interactive web site executing on a processor of an Internet-connected server by a client computerized appliance asserting a URL in a web browser;
- displaying a log-in mechanism to the client computerized appliance by the interactive web site, enabling a user operating the client computerized appliance to enter log-in information;
- 10 in response to a successful log-in, sending to the client computerized device, data including a time stamp of the time of the log-in, and a page location of an applet to be run by the client computerized appliance to continue the security process;
- through executing the applet on the client computerized device, determining the domain of the server by querying the page that includes the applet, and searching data
- 15 storage devices coupled to the client computerized device for an encrypted token compatible with the security process;
- on finding the token, rendering a virtual keypad on a display of the client computerized appliance, enabling the user to enter a PIN known to the user for decrypting the encrypted token;
- 20 if the PIN does not successfully decrypt the token, suspending the security process;
- in the event the PIN successfully decrypts the token, salting the decrypted token value with the time stamp and the domain by adding the domain on one end of the token string and the time stamp on the other end, and hashing the result by a specific hash
- 25 function;
- sending the hash value of the decrypted, salted token value to the interactive web page at the server;

invoking a dll at the server, retrieving a token stored at the server, salting that token with the domain of the server and the original time stamp sent to the client computerized appliance, and hashing the result by the specific hash function;

5 comparing the hash value received from the client computerized appliance with the hash value generated by the dll at the server, and determining passage of time from the time of the original time stamp to present time;

if the passage of time is greater than a preprogrammed time, or if the hash values do not match, denying access by the user at the server; and

10 if the passage of time is within the time window and the hash values do match, granting access to the user at the server.

2. The process of claim 1 wherein the data storage device coupled to the client's computer where the compatible token is found is a flash thumb drive.

15 3. The process of claim 1, wherein the token is unique to a client and includes an identification number, a password or personal identification code, a session key, and a secrete data seed.

20 4. The process of claim 1, wherein the software applet is a Java applet and the token is a Java archive.

5. An access security system, comprising:

an Internet-connected server coupled to a data repository and having a processor; and

25 software executing on the processor from a non-transitory medium, the software providing a process:

opening a connection to an interactive web site executing on the processor of the Internet-connected server by a client computerized appliance asserting a URL in a web browser;

displaying a log-in mechanism to the client computerized appliance by the interactive web site, enabling a user operating the client computerized appliance to enter log-in information;

5 in response to a successful log-in, sending to the client computerized device, data including a time stamp of the time of the log-in, and a page location of an applet to be run by the client computerized appliance to continue the security process;

through executing the applet on the client computerized device, determining the domain of the server by querying the page that includes the applet, and searching data storage devices coupled to the client computerized device for an encrypted token
10 compatible with the security process;

on finding the token, rendering a virtual keypad on a display of the client computerized appliance, enabling the user to enter a PIN known to the user for decrypting the encrypted token;

15 if the PIN does not successfully decrypt the token, suspending the security process;

in the event the PIN successfully decrypts the token, salting the decrypted token value with the time stamp and the domain by adding the domain on one end of the token string and the time stamp on the other end, and hashing the result by a specific hash function;

20 sending the hash value of the decrypted, salted token value to the interactive web page at the server;

invoking a dll at the server, retrieving a token stored at the server, salting that token with the domain of the server and the original time stamp sent to the client computerized appliance, and hashing the result by the specific hash function;

25 comparing the hash value received from the client computerized appliance with the hash value generated by the dll at the server, and determining passage of time from the time of the original time stamp to present time;

if the passage of time is greater than a preprogrammed time, or if the hash values do not match, denying access by the user at the server; and

if the passage of time is within the time window and the hash values do match,
granting access to the user at the server.

5 6. The system of claim 1 wherein the data storage device coupled to the client's computer
where the compatible token is found is a flash thumb drive.

10 7. The system of claim 1, wherein the token is unique to a client and includes an
identification number, a password or personal identification code, a session key, and a
secrete data seed.

15 8. The system of claim 1, wherein the software applet is a Java applet and the token is a
Java archive.

ABSTRACT OF THE DISCLOSURE

A security process involves log-in and data exchange between a server and a user operating a computerized appliance. The process requires a user-specific token,
5 independent verification of the server execution within a programmed time window. A hash created at the client side is reproduced at the server side from separate data and compared to the client hash. Too much time or incorrect hash denies access.

10

Electronic Patent Application Fee Transmittal				
Application Number:				
Filing Date:				
Title of Invention:		Methods and Apparatus for Enabling Secure Network-Based Transactions		
First Named Inventor/Applicant Name:		Vincent Cedric Colnot		
Filer:		Donald Rex Boys/Sheri Beasley		
Attorney Docket Number:		P1987.01		
Filed as Small Entity				
Track I Prioritized Examination - Nonprovisional Application under 35 USC 111(a) Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Utility filing Fee (Electronic filing)	4011	1	70	70
Utility Search Fee	2111	1	300	300
Utility Examination Fee	2311	1	360	360
Request for Prioritized Examination	2817	1	2000	2000
Pages:				
Claims:				
Miscellaneous-Filing:				
PROCESSING FEE, EXCEPT PROV. APPLS.	2830	1	70	70

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				2800

Electronic Acknowledgement Receipt	
EFS ID:	20528042
Application Number:	14524842
International Application Number:	
Confirmation Number:	4129
Title of Invention:	Methods and Apparatus for Enabling Secure Network-Based Transactions
First Named Inventor/Applicant Name:	Vincent Cedric Colnot
Customer Number:	24739
Filer:	Donald Rex Boys/Sheri Beasley
Filer Authorized By:	Donald Rex Boys
Attorney Docket Number:	P1987.01
Receipt Date:	27-OCT-2014
Filing Date:	
Time Stamp:	17:56:47
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$2800
RAM confirmation Number	7429
Deposit Account	500534
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
-----------------	----------------------	-----------	-------------------------------------	------------------	------------------

1	TrackOne Request	aia0424-track_one.pdf	152659 45244825a044b5e55bfaa3dfc7e121606b8d1a4f	no	2
Warnings:					
Information:					
2	Application Data Sheet	aia0014ADS.pdf	1265547 9a2827a03436a1a6081075fbc7bbb8aeca0f73f5	no	7
Warnings:					
Information:					
3	Power of Attorney	P0A1987_01.pdf	805984 c525b473ca8695c29e23b301f1b1015e2ecd8113	no	2
Warnings:					
Information:					
4	Oath or Declaration filed	STATEMENTINLIEUSIGNED.pdf	866048 cd44184a3a355bccddf7b8c6307b843a5b3ed32c	no	2
Warnings:					
Information:					
5	Oath or Declaration filed	ASSIGNSTATEMENTFELLERSSIGNED.pdf	589616 e121409fe64fe6bdf6d8673e8663373afa1e771f	no	2
Warnings:					
Information:					
6	Drawings-only black and white line drawings	DRAWINGS.pdf	268115 bbe2473c0ae5ba857e8e6c1796fb43001e734c57	no	15
Warnings:					
Information:					
7		1987_01PA.pdf	117646 4356cadbdaf0886570b2899e5a97c5320deb15f8	yes	31
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Specification		1	26	
	Claims		27	30	
	Abstract		31	31	
Warnings:					
Information:					

8	Fee Worksheet (SB06)	fee-info.pdf	38791 8d2c7c7289fad07d2b8bac0136206c7179176617	no	2
Warnings:					
Information:					
Total Files Size (in bytes):				4104406	
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.					