UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/533,030	09/19/2006	Vincent Cedric Colnot	P1987	3809

24739 7590 11/06/2014

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

EXAMINER	
KAPLAN, BENJAMIN A	
ART UNIT	PAPER NUMBER
2434	

NOTIFICATION DATE	DELIVERY MODE
11/06/2014	ELECTRONIC

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

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

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

officeactions@CENTRALCOASTPATENT.COM
plambuth@centralcoastpatent.com

Notice of Abandonment	Application No.	Applicant(s)
	11/533,030	COLNOT, VINCENT CEDRIC
	Examiner	Art Unit
	BENJAMIN KAPLAN	2434

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

This application is abandoned in view of:

1. ☐ Applicant's failure to timely file a proper reply to the Office letter mailed on _____.
   (a) ☐ A reply was received on _____ (with a Certificate of Mailing or Transmission dated _____), which is after the expiration of the period for reply (including a total extension of time of _____ month(s)) which expired on _____.
   (b) ☐ A proposed reply was received on _____, but it does not constitute a proper reply under 37 CFR 1.113 to the final rejection.
   (A proper reply under 37 CFR 1.113 to a final rejection consists only of: (1) a timely filed amendment which places the application in condition for allowance; (2) a timely filed Notice of Appeal (with appeal fee); or (3) a timely filed Request for Continued Examination (RCE) in compliance with 37 CFR 1.114).
   (c) ☐ A reply was received on _____ but it does not constitute a proper reply, or a bona fide attempt at a proper reply, to the non-final rejection. See 37 CFR 1.85(a) and 1.111. (See explanation in box 7 below).
   (d) ☐ No reply has been received.

2. ☐ Applicant's failure to timely pay the required issue fee and publication fee, if applicable, within the statutory period of three months from the mailing date of the Notice of Allowance (PTOL-85).
   (a) ☐ The issue fee and publication fee, if applicable, was received on _____ (with a Certificate of Mailing or Transmission dated _____), which is after the expiration of the statutory period for payment of the issue fee (and publication fee) set in the Notice of Allowance (PTOL-85).
   (b) ☐ The submitted fee of $_____ is insufficient. A balance of $_____ is due.
   The issue fee required by 37 CFR 1.18 is $_____. The publication fee, if required by 37 CFR 1.18(d), is $_____.
   (c) ☐ The issue fee and publication fee, if applicable, has not been received.

3. ☐ Applicant's failure to timely file corrected drawings as required by, and within the three-month period set in, the Notice of Allowability (PTO-37).
   (a) ☐ Proposed corrected drawings were received on _____ (with a Certificate of Mailing or Transmission dated _____), which is after the expiration of the period for reply.
   (b) ☐ No corrected drawings have been received.

4. ☐ The letter of express abandonment which is signed by the attorney or agent of record or other party authorized under 37 CFR 1.33(b). See 37 CFR 1.138(b).

5. ☐ The letter of express abandonment which is signed by an attorney or agent (acting in a representative capacity under 37 CFR 1.34) upon the filing of a continuing application.

6. ☒ The decision by the Board of Patent Appeals and Interference rendered on *29 August 2014* and because the period for seeking court review of the decision has expired and there are no allowed claims.

7. ☐ The reason(s) below:

/KAMBIZ ZAND/ Supervisory Patent Examiner, Art Unit 2434	/BENJAMIN KAPLAN/ Examiner, Art Unit 2434

Petitions to revive under 37 CFR 1.137, or requests to withdraw the holding of abandonment under 37 CFR 1.181, should be promptly filed to minimize any negative effects on patent term.

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/533,030	09/19/2006	Vincent Cedric Colnot	P1987	3809

24739 7590 08/29/2014

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

EXAMINER	
KAPLAN, BENJAMIN A	
ART UNIT	PAPER NUMBER
2434	

NOTIFICATION DATE	DELIVERY MODE
08/29/2014	ELECTRONIC

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

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

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

officeactions@CENTRALCOASTPATENT.COM
plambuth@centralcoastpatent.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte VINCENT CEDRIC COLNOT

Appeal 2012-004535
Application 11/533,030
Technology Center 2400

Before JOHNNY A. KUMAR, JOHN G. NEW, and
CATHERINE SHIANG, *Administrative Patent Judges*.

KUMAR, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

Appellant appeals under 35 U.S.C. § 134(a) from the Examiner's final rejection of claims 21, 23, 26, 29, and 52–55. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm.

Appellants' Invention

Appellant's invention relates to electronic transactions carried out over a network connection while ensuring identity security for the transaction parties. *See* Spec. 1, ll. 15–17.

Representative Claim on Appeal

Claim 21 is exemplary with key disputed language highlighted:

> 21. A system enabling secure transacting over a network comprising:
>
> a network server having an application storing client information and configured to activate a client for secure transacting in the network, the client connecting to the server through a network-connected digital appliance;
>
> a software driver configured to perform authentication, the software driver accessible to and executable by the network server application;
>
> *a software applet configured to create a secure data record and for managing transmission and update of the contents of the record*; and
>
> a token comprising an encrypted text string, the token stored on a data storage device coupled to the client's digital appliance, and also in a data repository coupled to the server;
>
> wherein, upon a client seeking authorization from the server, the server downloads the software applet and a *timestamp of the request time to the client*, the applet executes at the client, retrieves the token from the data storage device,

> concatenates the token file and the time stamp, hashes the result creating the secure data record, sends the secure data record to the server, and the server, executing the software driver, compares the secure data record to a similarly hashed result of the time stamp and token value taken from the data repository coupled to the server, authorizing the client with a match.

Rejection on Appeal

The Examiner rejected claims 21, 23, 26, 29, and 52–55 under 35 U.S.C. § 103(a) as being unpatentable over Colnot (US 2004/0093496 A1, May 13, 2004), Bo (US 2005/0262573 A1, Nov. 24, 2005), and Kocher (US 6,188,766 B1, Feb. 13, 2001). Ans. 4–21.

ISSUES AND ANALYSIS

Based on Appellant's arguments in the Appeal Brief (Br. 11–14), the principal and dispositive issue of whether the Examiner erred in rejecting claims 21, 23, 26, 29, and 52–55 turns on whether the combination of Colnot, Bo, and Kocher teaches or suggests "a software applet configured to create a secure data record and for managing transmission and update of the contents of the record," as recited in independent claim 21.[1]

Appellant has presented several arguments as to why the combination of the references does not teach or suggest the features recited in independent claim 21. The Examiner has provided a comprehensive response to each argument presented by the Appellant on pages 5 through 27 of the Answer. We have reviewed this response and concur with the Examiner's findings and conclusions.

[1] Independent claim 52 was argued together with claim 21. Br. 13.

We observe that no Reply Brief is of record to rebut such findings including the Examiner's responses to Appellant's arguments. Therefore, we adopt as our own (1) the findings and reasons set forth by the Examiner in the action from which this appeal is taken and (2) the reasons set forth by the Examiner in the Examiner's Answer in response to Appellant's Appeal Brief. We concur with the conclusions reached by the Examiner.

Appellant's first argument is that paragraphs 237 and 238 of Bo do not teach "a software applet configured to create a secure data record and for managing transmission and update of the contents of the record" (hereinafter "software applet" limitation). Br. 11. The Examiner finds, and we agree, that paragraphs 242, 243, and 253 of Bo teach the software applet limitation. Ans. 22.

Appellant's next argument is that in Kocher "all time stamping of documents occur at the receiving computer or via a request to a remote device for the time stamp," and that "Kocher fails to teach the actions taken at the client, as claimed, or communication from the client to the server of the hash result, or a comparison of the data at the server," and thus, Kocher would not be properly combinable with Colnot and Bo. Br. 13.

The Examiner finds "Kocher was cited to show that trusted time stamping was a well known well established function in the art at the time of invention was made" (Ans. 25), and "[w]hile the comparison for authentication happens at the time of document retrieval, this is not seen as stopping Kocher from teaching a well known time stamping technique especially as Kocher is being used to demonstrate obviousness as [o]pposed to anticipation." Ans. 26. The Examiner also finds,

> It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the trusted time stamping techniques taught by Kocher in to the method of Colnot and Bo et al. as a timestamping would be particularly helpful in enhancing the integrity of a digital key/encryption system as it provides an extra verification layer without adding a disclosure of a key.

Ans. 11.

We agree with the Examiner's findings because all of the features of the structure in the secondary reference need not be bodily incorporated into the primary reference, but consideration should be given to what the combined teachings, knowledge of one of ordinary skill in the art, and the nature of the problem to be solved as a whole would have suggested to those of ordinary skill in the art. *See In re Keller,* 642 F.2d 413, 425 (CCPA 1981).

In that regard, the Supreme Court has indicated that:

> [It is error to] assum[e] that a person of ordinary skill attempting to solve a problem will be led only to those elements of prior art designed to solve the same problem. . . . Common sense teaches . . . that familiar items may have obvious uses beyond their primary purposes, and in many cases a person of ordinary skill will be able to fit the teachings of multiple patents together like pieces of a puzzle.

KSR Int'l Co. v. Teleflex Inc., 550 U.S. 398, 420 (2007) (citation omitted).

Furthermore, the artisan is not compelled to blindly follow the teaching of one prior art reference over the other without the exercise of independent judgment. *See Lear Siegler, Inc. v. Aeroquip Corp.,* 733 F.2d 881, 889 (Fed. Cir. 1984). As such, Colnot and Bo would have been adjusted to accommodate teachings from Kocher by one of ordinary skill in the art. In particular, the combination as a whole would have taught one of

ordinary skill in the art to enhance the integrity of the digital key/encryption system.

For the above reasons, the Examiner's 35 U.S.C. § 103(a) rejection of independent claims 21 and 52 and dependent claims 23, 26, 29, and 53–55, not separately argued by Appellant, is sustained.

CONCLUSION

The Examiner did not err in rejecting claims 21, 23, 26, 29, and 52–55 under 35 U.S.C. § 103(a) as being unpatentable over Colnot, Bo, and Kocher.

DECISION

We affirm the Examiner's decision to reject claims 21, 23, 26, 29, and 52–55.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

msc

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/533,030	09/19/2006	Vincent Cedric Colnot	P1987	3809

24739 7590 02/10/2012

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

EXAMINER	
KAPLAN, BENJAMIN A	
ART UNIT	PAPER NUMBER
2434	

NOTIFICATION DATE	DELIVERY MODE
02/10/2012	ELECTRONIC

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

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

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

officeactions@CENTRALCOASTPATENT.COM
plambuth@centralcoastpatent.com

United States Patent and Trademark Office

Under Secretary of Commerce for Intellectual Property and
Director of the United States Patent and Trademark Office
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

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

Appeal No: 2012-004535
Application: 11/533,030
Appellant: Vincent Cedric Colnot

Board of Patent Appeals and Interferences
Docketing Notice

Application 11/533,030 was received from the Technology Center at the Board on February 06, 2012 and has been assigned Appeal No: 2012-004535.

In all future communications regarding this appeal, please include both the application number and the appeal number.

The mailing address for the Board is:

BOARD OF PATENT APPEALS AND INTERFERENCES
UNITED STATES PATENT AND TRADEMARK OFFICE
P.O. BOX 1450
ALEXANDRIA, VIRGINIA 22313-1450

The facsimile number of the Board is 571-273-0052. Because of the heightened security in the Washington D.C. area, facsimile communications are recommended. Telephone inquiries can be made by calling 571-272-9797 and referencing the appeal number listed above.

By order of the Board of Patent Appeals and Interferences.

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/533,030	09/19/2006	Vincent Cedric Colnot	P1987	3809

24739 7590 11/02/2011

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

EXAMINER	
KAPLAN, BENJAMIN A	
ART UNIT	PAPER NUMBER
2434	

NOTIFICATION DATE	DELIVERY MODE
11/02/2011	ELECTRONIC

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

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

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

officeactions@CENTRALCOASTPATENT.COM
plambuth@centralcoastpatent.com

UNITED STATES PATENT AND TRADEMARK OFFICE

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

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 11/533,030
Filing Date: September 19, 2006
Appellant(s): COLNOT, VINCENT CEDRIC

Donald R. Boys
Registration Number 35074
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 11 August 2011 appealing from the Office action mailed 6 July 2011.

(1) Real Party in Interest

The examiner has no comment on the statement, or lack of statement, identifying by name the real party in interest in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The following is a list of claims that are rejected and pending in the application:

Claims 21, 23, 26, 29 & 52-55 are rejected and pending in the application.

(4) Status of Amendments After Final

The examiner has no comment on the appellant's statement of the status of amendments after final rejection contained in the brief.

(**5) Summary of Claimed Subject Matter**

The examiner has no comment on the summary of claimed subject matter contained in the brief.

(6) Grounds of Rejection to be Reviewed on Appeal

The examiner has no comment on the appellant's statement of the grounds of rejection to be reviewed on appeal. Every ground of rejection set forth in the Office action from which the appeal is taken (as modified by any advisory actions) is being maintained by the examiner except for the grounds of rejection (if any) listed under the

subheading "WITHDRAWN REJECTIONS." New grounds of rejection (if any) are provided under the subheading "NEW GROUNDS OF REJECTION."

(7) Claims Appendix

The examiner has no comment on the copy of the appealed claims contained in the Appendix to the appellant's brief.

(8) Evidence Relied Upon

2004/0093496	Colnot	10-2003
2005/0262573	Bo et el.	5-2005
6,188,766	Kocher	3-1997

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

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

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim(s) 21, 23, 26, 29 and 52-55 is/are rejected under 35 U.S.C. 103(a) as being unpatentable over United States Patent Application Publication No.: US 20040093496 A1 (Colnot) in view of United States Patent Application Publication No.: US 2005/0262573 A1 (Bo et al.) in further view of United States Patent No.: US 6,188,766 B1 (Kocher).

As Per Claim 21: Colnot teaches: **A system enabling secure transacting over a network comprising:**

- a network server having an application storing client information and configured to activate a client for secure transacting in the network, the client connecting to the server through a network-connected digital appliance;

(Colnot, Drawings, Figure. 1. "

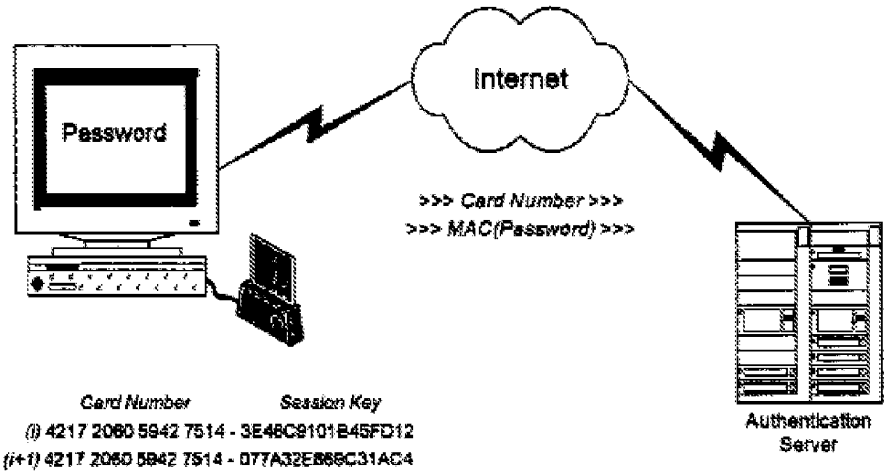


FIG. 1

").

(Colnot, Paragraphs [0011]-[0014], "The method, as detailed in FIG. 1, carries out the user authentication on the Internet. The apparatus comprises a smart card with a modulation output, a card reader plugged into the microphone input, and a PC applet. The user inserts his card in the reader and enters his password on the PC keyboard.

When activated in the card reader, the smart card transmits an identification sequence to the PC in the form of a modulated signal, which is demodulated by the PC

applet. The identification sequence comprises an 8-byte card number and an 8-byte random number valid only once. The card number is unique and identifies the card issuer, application version and user account. The random number is a session key (Ki) which is a function of the previous one (Ki-1) emitted by the card such as: Ki=G(Ki-1), G is a one-way function also known by the authentication server.

The session key (Ki) is used by the PC applet to generate a message authentication code (MAC) of the password entered by the user, using the DES algorithm for instance. This first MAC is transmitted to the authentication server along with the card number, allowing the server to retrieve the previous session key (Ki-1) and the password stored in the authentication server database.

The authentication server deduces from (Ki-1) the session key used by the card, and generates a second MAC of the password stored in the database. The authentication is valid only if the first and second MAC are identical, which means the PC and the authentication server have used the same session key (Ki) to generate a MAC of the same password. If this is the case, the authentication server replaces (Ki-1) by (Ki) in the database. The session key (Ki) cannot be reused, even though the session key (Ki) has not been transmitted to the authentication server.").

- a token comprising an encrypted text string, the token stored on a data storage device coupled to connect to the client's digital appliance, and also in a data repository coupled to the server;

(Colnot, Paragraphs [0011]-[0014], "The method, as detailed in FIG. 1, carries out the user authentication on the Internet. The apparatus comprises a smart card with a modulation output, a card reader plugged into the microphone input, and a PC applet. The user inserts his card in the reader and enters his password on the PC keyboard.

When activated in the card reader, the smart card transmits an identification sequence to the PC in the form of a modulated signal, which is demodulated by the PC applet. The identification sequence comprises an 8-byte card number and an 8-byte random number valid only once. The card number is unique and identifies the card issuer, application version and user account. The random number is a session key (Ki) which is a function of the previous one (Ki-1) emitted by the card such as: Ki=G(Ki-1), G is a one-way function also known by the authentication server.

The session key (Ki) is used by the PC applet to generate a message authentication code (MAC) of the password entered by the user, using the DES algorithm for instance. This first MAC is transmitted to the authentication server along with the card number, allowing the server to retrieve the previous session key (Ki-1) and the password stored in the authentication server database.

The authentication server deduces from (Ki-1) the session key used by the card, and generates a second MAC of the password stored in the database. The authentication is valid only if the first and second MAC are identical, which means the PC and the authentication server have used the same session key (Ki) to generate a MAC of the same password. If this is the case, the authentication server replaces (Ki-1)

by (Ki) in the database. The session key (Ki) cannot be reused, even though the session key (Ki) has not been transmitted to the authentication server.").

Colnot does not explicitly teach the following limitations however Bo et al in analogous are does teach the following limitations:

- a software driver configured to perform authentication, the software driver accessible to and executable by the network server application;

- a software applet configured to create a secure data record and for managing transmission and update of the contents of the record; and

(Bo et al., Paragraphs [0242]-[0243], "c) With the agreement of the user, an application of the client 23 is downloaded from the web server 13 as S27 shows. The application is, for example, a Java applet. The user installs the application on the end station as S28 shows. Thus, the application of the client 23 is implemented.

d) With the agreement of the user, the application of the client 23 establishes an SSL connection (an SSL link) with the web server 13 for further transactions as S29 shows.").

(Bo et al., Paragraph [0253], "FIG. 16 shows a method of user authentication and digital audio-visual content encryption key(s) distribution. Each time a registered user wants to enjoy the services from the content provider, the user may be authenticated.").

The driver is the inherent underlying software that makes it possible for a system to operate with its underlying hardware and functions thereof.

- wherein upon a client seeking authorization from the server, the server downloads the software applet

(Bo et al., Paragraphs [0242]-[0243], "c) With the agreement of the user, an application of the client 23 is downloaded from the web server 13 as S27 shows. The application is, for example, a Java applet. The user installs the application on the end station as S28 shows. Thus, the application of the client 23 is implemented.

d) With the agreement of the user, the application of the client 23 establishes an SSL connection (an SSL link) with the web server 13 for further transactions as S29 shows.").

(Bo et al., Paragraph [0253], "FIG. 16 shows a method of user authentication and digital audio-visual content encryption key(s) distribution. Each time a registered user wants to enjoy the services from the content provider, the user may be authenticated.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Colnot in to the method of Bo et al. in order to take advantage of being able to inexpensively add the enhancements of smart card authentication (Colnot, Paragraph [0005]). On in reverse to incorporate the teaching of Bo et al. in to the method of Colnot in order to take advantage of the authentication enhancements provided by Bo et al. (Bo et al., Paragraph [0011]).

Colnot and Bo et al. do not explicitly teach the following limitations however Kocher in analogous are does teach the following limitations:

- the server downloads a timestamp of the request time to the client, the applet executes at the client, retrieves the token from the data storage device, concatenates the token file and the time stamp, hashes the result creating the secure data record, sends the secure data record to the server, and the server, executing the software driver, compares the secure data record to a similarly hashed result of the time stamp and token value taken from the data repository coupled to the server, authorizing the client with a match.

(Kocher, Column 7, Lines 47-64, "If the sender identification at step 220 is satisfactory, the system proceeds to step 230, where the digital data are cryptographically timestamped using digital timestamp computation apparatus 170. In one preferred embodiment, timestamp computation involves obtaining the date and time from a trusted clock and performing a verifiable cryptographic operation on the digital document data plus the date/time (e.g., combining the hash of the digital data with the date and time, hashing the combination, and digitally signing the result using a private RSA key). As previously described, other techniques, such as the hash tree and catenate timestamping techniques described by Haber et al., may also be used. The apparatus which performs the basic timestamping operation may be, without limitation, the computer which is connected to the modem, or a smart-card or other cryptographic token connected to said computer, or a separate timestamping device or service connected to said computer via a computer network.").

(Kocher, Column 10, Lines 32-46, "If the document was stored in encrypted form, the TTS decrypts the document (if necessary, employing a cryptographic token,

networked secure decrypting system, or other decryption mechanism), optionally using a decryption key included with or in the DIV or TTI. The digital timestamp stored with the data is then cryptographically verified as appropriate for the timestamping technique. For example, a timestamp constructed using an RSA signature may be verified by operating on the timestamp with the public key corresponding to the digital signing key used by the timestamp computation apparatus 170, then verifying that the result corresponds to the cryptographic hash of the combination of the archived digital document data and time indicator. An error is returned if document retrieval or timestamp verification fails.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the trusted time stamping techniques taught by Kocher in to the method of Colnot and Bo et al. as a timestamping would be particularly helpful in enhancing the integrity of a digital key/encryption system as it provides an extra verification layer without adding a disclosure of a key. (RSA Laboratories Frequently Asked Questions About Today's Cryptography version 4.1 Section 7.11 What is digital timestamping?)

As Per Claim 23: The rejection of claim 21 is incorporated and further Colnot, Bo et al. and Kocher do not explicitly teach:

- the data storage device coupled to the client's computer, and storing the token file, is a flash thumb drive

However the examiner is giving official notice the use of flash drives as key sources was well established in the art at the time of invention was made. It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporated the use of flash drives as potential key sources as they provide as highly expedient manner of having a portable connectable/disconnect-able device easily at the ready.

As Per Claim 26: The rejection of claim 21 is incorporated and further Colnot does not explicitly teach the following limitations however Bo et al in analogous art does teach the following limitations:

- 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

(Bo et al., Paragraph [0152], “In one example, the web server 13 is used to transfer user's personal information from the client 23 to the SRM 5 through a pre-established SSL link. The user's personal information includes user's log-in ID and password. The user account manager 35 in the SRM 5 maintains and manages all the user's personal information.”).

(Bo et al., Paragraph [0147], “The encipheror 3 or the encipheror in the encipheror/decipherer module 38 defines a block cipher algorithm, e.g., DES (data encryption standard), AES (advanced encryption standard), or Blowfish. The encipheror 3 or the encipheror in the encipheror/decipherer module 38 also defines the seeds for generating random keys, the preferred key length for the block cipher algorithm that

accepts variable length keys, the preferred plaintext block size, e.g., 64 bits, 128 bits, or 256 bits. Otherwise, a default encryption strategy is to be used.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Colnot in to the method of Bo et al. in order to take advantage of being able to inexpensively add the enhancements of smart card authentication (Colnot, Paragraph [0005]). On in reverse to incorporate the teaching of Bo et al. in to the method of Colnot in order to take advantage of the authentication enhancements provided by Bo et al. (Bo et al., Paragraph [0011]).

As Per Claim 29: The rejection of claim 21 is incorporated and further Colnot does not explicitly teach the following limitations however Bo et al in analogous art does teach the following limitations:

- the software applet is a Java applet and the secure data record token is a Java archive

(Bo et al., Paragraphs [0242]-[0243], "c) With the agreement of the user, an application of the client 23 is downloaded from the web server 13 as S27 shows. The application is, for example, a Java applet. The user installs the application on the end station as S28 shows. Thus, the application of the client 23 is implemented.

d) With the agreement of the user, the application of the client 23 establishes an SSL connection (an SSL link) with the web server 13 for further transactions as S29 shows.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Colnot in to the method of Bo et al. in order to take advantage of being able to inexpensively add the enhancements of smart card authentication (Colnot, Paragraph [0005]). On in reverse to incorporate the teaching of Bo et al. in to the method of Colnot in order to take advantage of the authentication enhancements provided by Bo et al. (Bo et al., Paragraph [0011]).

As Per Claim 52: Colnot teaches: **A method enabling secure transacting over a network comprising:**

(b) executing the applet at the client, retrieving a token file from a data storage device coupled to the client appliance, the token file comprising an encrypted text string;

(Colnot, Drawings, Figure. 1. "

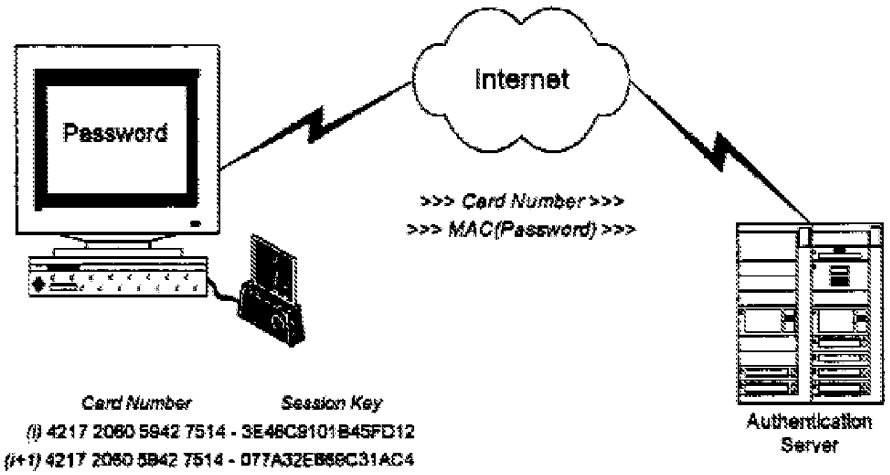


FIG. 1

").

(Colnot, Paragraphs [0011]-[0014], "The method, as detailed in FIG. 1, carries out the user authentication on the Internet. The apparatus comprises a smart card with a modulation output, a card reader plugged into the microphone input, and a PC applet. The user inserts his card in the reader and enters his password on the PC keyboard.

When activated in the card reader, the smart card transmits an identification sequence to the PC in the form of a modulated signal, which is demodulated by the PC applet. The identification sequence comprises an 8-byte card number and an 8-byte random number valid only once. The card number is unique and identifies the card issuer, application version and user account. The random number is a session key (Ki) which is a function of the previous one (Ki-1) emitted by the card such as: Ki=G(Ki-1), G is a one-way function also known by the authentication server.

The session key (Ki) is used by the PC applet to generate a message authentication code (MAC) of the password entered by the user, using the DES algorithm for instance. This first MAC is transmitted to the authentication server along with the card number, allowing the server to retrieve the previous session key (Ki-1) and the password stored in the authentication server database.

The authentication server deduces from (Ki-1) the session key used by the card, and generates a second MAC of the password stored in the database. The authentication is valid only if the first and second MAC are identical, which means the PC and the authentication server have used the same session key (Ki) to generate a MAC of the same password. If this is the case, the authentication server replaces (Ki-1)

by (Ki) in the database. The session key (Ki) cannot be reused, even though the session key (Ki) has not been transmitted to the authentication server.").

Colnot does not explicitly teach the following limitations however Bo et al in analogous are does teach the following limitations:

-(a) upon a client seeking authorization from a network server, the server downloading a software applet

(Bo et al., Paragraphs [0242]-[0243], "c) With the agreement of the user, an application of the client 23 is downloaded from the web server 13 as S27 shows. The application is, for example, a Java applet. The user installs the application on the end station as S28 shows. Thus, the application of the client 23 is implemented.

d) With the agreement of the user, the application of the client 23 establishes an SSL connection (an SSL link) with the web server 13 for further transactions as S29 shows.").

(Bo et al., Paragraph [0253], "FIG. 16 shows a method of user authentication and digital audio-visual content encryption key(s) distribution. Each time a registered user wants to enjoy the services from the content provider, the user may be authenticated.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Colnot in to the method of Bo et al. in order to take advantage of being able to inexpensively add the enhancements of smart card authentication (Colnot, Paragraph [0005]). On in reverse to incorporate the

teaching of Bo et al. in to the method of Colnot in order to take advantage of the authentication enhancements provided by Bo et al. (Bo et al., Paragraph [0011]).

Colnot and Bo et al. do not explicitly teach the following limitations however Kocher in analogous are does teach the following limitations:

- a timestamp of the request time to a client digital appliance;

(c) concatenating the token file and the timestamp and hashing the result, creating a secure data record;

(d) sending the secure data record to the server;

(e) comparing the secure data record to a similarly hashed result of the time stamp and token value taken from a data repository coupled to the server; and

(f) authorizing the client with a match.

(Kocher, Column 7, Lines 47-64, "If the sender identification at step 220 is satisfactory, the system proceeds to step 230, where the digital data are cryptographically timestamped using digital timestamp computation apparatus 170. In one preferred embodiment, timestamp computation involves obtaining the date and time from a trusted clock and performing a verifiable cryptographic operation on the digital document data plus the date/time (e.g., combining the hash of the digital data with the date and time, hashing the combination, and digitally signing the result using a private RSA key). As previously described, other techniques, such as the hash tree and catenate timestamping techniques described by Haber et al., may also be used. The apparatus which performs the basic timestamping operation may be, without limitation,

the computer which is connected to the modem, or a smart-card or other cryptographic token connected to said computer, or a separate timestamping device or service connected to said computer via a computer network.").

(Kocher, Column 10, Lines 32-46, "If the document was stored in encrypted form, the TTS decrypts the document (if necessary, employing a cryptographic token, networked secure decrypting system, or other decryption mechanism), optionally using a decryption key included with or in the DIV or TTI. The digital timestamp stored with the data is then cryptographically verified as appropriate for the timestamping technique. For example, a timestamp constructed using an RSA signature may be verified by operating on the timestamp with the public key corresponding to the digital signing key used by the timestamp computation apparatus 170, then verifying that the result corresponds to the cryptographic hash of the combination of the archived digital document data and time indicator. An error is returned if document retrieval or timestamp verification fails.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the trusted time stamping techniques taught by Kocher in to the method of Colnot and Bo et al. as a timestamping would be particularly helpful in enhancing the integrity of a digital key/encryption system as it provides an extra verification layer without adding a disclosure of a key. (RSA Laboratories Frequently Asked Questions About Today's Cryptography version 4.1 Section 7.11 What is digital timestamping?)

As Per Claim 53: The rejection of claim 52 is incorporated and further Colnot, Bo et al. and Kocher do not explicitly teach:

- data storage device coupled to the client's appliance, and storing the token file, is a flash thumb drive

However the examiner is giving official notice the use of flash drives as key sources was well established in the art at the time of invention was made. It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporated the use of flash drives as potential key sources as they provide as highly expedient manner of having a portable connectable/disconnect-able device easily at the ready.

As Per Claim 54: The rejection of claim 52 is incorporated and further Colnot does not explicitly teach the following limitations however Bo et al in analogous art does teach the following limitations:

- 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

(Bo et al., Paragraph [0152], “In one example, the web server 13 is used to transfer user's personal information from the client 23 to the SRM 5 through a pre-established SSL link. The user's personal information includes user's log-in ID and password. The user account manager 35 in the SRM 5 maintains and manages all the user's personal information.”).

(Bo et al., Paragraph [0147], "The encipheror 3 or the encipheror in the encipheror/decipherer module 38 defines a block cipher algorithm, e.g., DES (data encryption standard), AES (advanced encryption standard), or Blowfish. The encipheror 3 or the encipheror in the encipheror/decipherer module 38 also defines the seeds for generating random keys, the preferred key length for the block cipher algorithm that accepts variable length keys, the preferred plaintext block size, e.g., 64 bits, 128 bits, or 256 bits. Otherwise, a default encryption strategy is to be used.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Colnot in to the method of Bo et al. in order to take advantage of being able to inexpensively add the enhancements of smart card authentication (Colnot, Paragraph [0005]). On in reverse to incorporate the teaching of Bo et al. in to the method of Colnot in order to take advantage of the authentication enhancements provided by Bo et al. (Bo et al., Paragraph [0011]).

As Per Claim 55: The rejection of claim 52 is incorporated and further Colnot does not explicitly teach the following limitations however Bo et al in analogous art does teach the following limitations:

- the software applet is a Java applet and the secure data record token is a Java archive

(Bo et al., Paragraphs [0242]-[0243], "c) With the agreement of the user, an application of the client 23 is downloaded from the web server 13 as S27 shows. The

application is, for example, a Java applet. The user installs the application on the end station as S28 shows. Thus, the application of the client 23 is implemented.

d) With the agreement of the user, the application of the client 23 establishes an SSL connection (an SSL link) with the web server 13 for further transactions as S29 shows.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Colnot in to the method of Bo et al. in order to take advantage of being able to inexpensively add the enhancements of smart card authentication (Colnot, Paragraph [0005]). On in reverse to incorporate the teaching of Bo et al. in to the method of Colnot in order to take advantage of the authentication enhancements provided by Bo et al. (Bo et al., Paragraph [0011]).

(10) Response to Argument

On page 11 Appellant in substance argues that:

Appellant points out that the art of Colnot is the same inventor as the present application and is valid art by only a few months.

United States Patent Application Publication No.: US 20040093496 A1 (Colnot) is from the same inventor however it is valid art under 35 U.S.C. § 102(b) representing a statutory bar to patentability. (MPEP 2141.01 Scope and Content of the Prior Art [R-6] - 2100 Patentability).

On page 11 Appellant in substance further argues that:

Regarding claim 21, the Examiner states that Bo teaches, "a software applet configured to create a secure data record and for managing transmission and update of the contents of the record;" Appellant argues that the art of Bo teaches ([237-238] that an SSL is created between the user and the server in order to secure data during manual registration prior to downloading the applet to client 23.

Examiner did not cite paragraphs [0237]-[0238] from Bo et al. rather Examiner cited paragraphs [0242]-[0243] & [0253] from Bo et al.

Additional teachings of Bo et al. do not remove other teaching of Bo et al. Referring back to the cited portions of Bo et al.

(Bo et al., Paragraphs [0242]-[0243], "c) With the agreement of the user, an application of the client 23 is downloaded from the web server 13 as S27 shows. The application is, for example, a Java applet. The user installs the application on the end station as S28 shows. Thus, the application of the client 23 is implemented.

d) With the agreement of the user, the application of the client 23 establishes an SSL connection (an SSL link) with the web server 13 for further transactions as S29 shows.").

(Bo et al., Paragraph [0253], "FIG. 16 shows a method of user authentication and digital audio-visual content encryption key(s) distribution. Each time a registered user wants to enjoy the services from the content provider, the user may be authenticated.").

On pages 11-13 Appellant expresses the claim limitation:

- the server downloads a timestamp of the request time to the client, the applet executes at the client, retrieves the token from the data storage device, concatenates the token file and the time stamp, hashes the result creating the secure data record, sends the secure data record to the server, and the server, executing the software driver, compares the secure data record to a similarly hashed result of the time stamp and token value taken from the data repository coupled to the server, authorizing the client with a match.

and alleges:

The Examiner provides the following portion of Kocher to teach said limitations:

(Kocher, Column 10, Lines 10-46)

Referring now to FIG. 3, the timestamp verification process, as performed by the TTS in a facsimile-based embodiment, will be described. A requester (the document sender or a third party) who wishes to verify the timestamp on a document contacts the TTS, which, at step 300, receives a DIV or TTI. For example, this may be accomplished by receiving via facsimile a document (such as the first page of a document submission receipt) containing a DIV or a representation thereof in machine-readable form. The DIV is automatically detected and decoded using bar code scanning techniques, optical character recognition, etc. Alternate DIV and TTI submission channels may be used including, without limitation: detection of DTMF (touch tone) signals, electronic submission via a computer network (e.g., Internet or world wide web), a voice call to a live operator who enters the DIV or TTI using a computer terminal, a voice recognition system, wireless radio or pager, traditional or certified mail, modem, and electronic mail. At step 310, the TTS determines whether the DIV or TTI corresponds to a document stored in storage subsystem 150. If not, an error is reported to the user at step 315. Otherwise, at step 320, the TTS retrieves the digital document from storage subsystem 150. If the document was stored in encrypted form, the TTS decrypts the document (if necessary, employing a cryptographic token, networked secure decrypting system, or other decryption mechanism), optionally using a decryption key included with or in the DIV or TTI. The digital timestamp stored with the data is then cryptographically verified as appropriate for the timestamping technique. For example, a timestamp constructed using an RSA signature may be verified by operating on the timestamp with the public key corresponding to the digital signing key used by

the timestamp computation apparatus 170, then verifying that the result corresponds to the cryptographic hash of the combination of the archived digital document data and time indicator. An error is returned if document retrieval or timestamp verification fails.

Appellant points out that the DIV is a document identification value generated by the server and printed on a receipt sent to the sender of the telecopier transmission received at the TTS. The TTI is a transmission identifier for the transmission used when the sender sent the telecopier transmission. The requestor uses one or the other previously issued identifiers in order to identify the document stored at the TTS. The TTS may encrypt the document at the time of storage, and if so, will decrypt the document using known methods before applying the time verification process. The TTS decrypts, hashes and verifies the timestamp of the document for the requestor without teaching or suggesting a similar function at the user's station or any comparison of data for authentication. The only input by the requestor is the identifier of the document, the balance of Kocher's teaching occurs at the TTS.

The arguments largely revolve around alleging deficiencies in (Kocher, Column 10, Lines 10-46). In particular Appellant argues:

The TTS decrypts, hashes and verifies the timestamp of the document for the requestor without teaching or suggesting a similar function at the user's station or any comparison of data for authentication.

The segments of Kocher that were cited in the office action were actually (Kocher, Column 7, Lines 47-64) and (Kocher, Column 10, Lines 32-46).

(Kocher, Column 7, Lines 47-64, "If the sender identification at step 220 is satisfactory, the system proceeds to step 230, where the digital data are cryptographically timestamped using digital timestamp computation apparatus 170. In one preferred embodiment, timestamp computation involves obtaining the date and time from a trusted clock and performing a verifiable cryptographic operation on the digital document data plus the date/time (e.g., combining the hash of the digital data with the date and time, hashing the combination, and digitally signing the result using a private RSA key). As previously described, other techniques, such as the hash tree and catenate timestamping techniques described by Haber et al., may also be used. The apparatus which performs the basic timestamping operation may be, without limitation, the computer which is connected to the modem, or a smart-card or other cryptographic token connected to said computer, or a separate timestamping device or service connected to said computer via a computer network.").

Demonstrated the obtaining of the time stamp and creation of a secure data record.

(Kocher, Column 10, Lines 32-46, "If the document was stored in encrypted form, the TTS decrypts the document (if necessary, employing a cryptographic token, networked secure decrypting system, or other decryption mechanism), optionally using a decryption key included with or in the DIV or TTI. The digital timestamp stored with the data is then cryptographically verified as appropriate for the timestamping technique. For example, a timestamp constructed using an RSA signature may be verified by operating on the timestamp with the public key corresponding to the digital signing key used by the timestamp computation apparatus 170, then verifying that the result corresponds to the cryptographic hash of the combination of the archived digital document data and time indicator. An error is returned if document retrieval or timestamp verification fails.").

Shows a verification operation of a secure data record if the function does not have a corresponding result then the match fails indicating improper activity.

Kocher was cited to show that trusted time stamping was a well known well established function in the art at the time of invention was made. The specific environment it would be used in and configuration thereof was established by Colnot and Bo et al. earlier in the rejection.

On Page 13 Appellant questions motivation to combine Kocher with Colnot and Bo et al. arguing:

The Examiner states:

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the trusted time stamping techniques taught by Kocher in to the method of Colnot and Bo et al. as a timestamping would be particularly helpful in enhancing the integrity of a digital key/encryption system as it provides an extra verification layer without adding a disclosure of a key. (RSA Laboratories Frequently Asked Questions About Today's Cryptography version 4.1 Section 7.11 What is digital timestamping?)

Appellant argues one with skill in the art would not look to the simplified timestamp verification process of Kocher to teach or suggest the entire functional wherein clause of appellant's claimed invention. There is no motivation provided in Kocher to make the combination because all hashing, etc. occurs at the receiver or server in Kocher. Therefore, no comparison for authenticating a user need occur in this stage of the process.

The form of the creation of a time stamped record in Kocher is the same as that of the claimed invention. While the comparison for authentication happens at the time of document retrieval, this is not seen as stopping Kocher from teaching a well know timestamping technique especially as Kocher is being used to demonstrate obviousness as apposed to anticipation. Motivation for combination also referred back to extrinsic

evidentiary document RSA Laboratories Frequently Asked Questions About Today's Cryptography version 4.1 (Section 7.11 What is digital timestamping?) From May 2000. For viewing this use of timestamping technique as an obvious variation of well established usage of timestamping techniques.

On page 13 Appellant declairs that:

Claim 52 is appellant's method claim corresponding to claim 21

And

The dependant claims fall or stand with their corresponding independent claim.

As such all presented arguments are have been responded to in the discussion of claim 21.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Benjamin A Kaplan/

Examiner, Art Unit 2434

Conferees:

/PETER POLTORAK/

Primary Examiner, Art Unit 2434

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2434

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES
GROUP ART UNIT: 2434 **EXAMINER:** KAPLAN, BENJAMIN A

In Re:	Vincent Cedric Colnot
Case:	P1987
Serial No.:	11/533,030
Filed:	September 19, 2006
Subject:	Methods and Apparatus for Enabling Secure Network-Based Transactions

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Dear Sirs:

APPEAL BRIEF

Table of Contents

1.0	Real Party in Interest	3
2.0	Related Appeals and Interferences	4
3.0	Status of the Claims	5
4.0	Status of Amendments	6
5.0	Summary of the Claimed Subject Matter	7
6.0	Grounds of Rejection to be Reviewed on Appeal	10
7.0	Argument	11
8.0	Claims Appendix	15
9.0	Evidence Appendix	17
10.0	Related Proceedings Appendix	18

1.0 Real Party in Interest

All inventions in the disclosure in the present case are assigned to or assignable to: OHVA, Inc.

2.0 Related Appeals and Interferences

There are no related appeals and interferences.

3.0 Status of the Claims

Following is the status of the claims in the instant case:

1 - 20. Cancelled

21. Rejected, independent - appealed in this brief

22. Cancelled

23. Rejected, dependent - appealed in this brief

24 - 25. Cancelled

26. Rejected, dependent - appealed in this brief

27 - 28. Cancelled

29. Rejected, dependent - appealed in this brief

30 - 51. Cancelled

52. Rejected, dependent - appealed in this brief

53. Rejected, dependent - appealed in this brief

54. Rejected, independent - appealed in this brief

55. Rejected, dependent - appealed in this brief

4.0 Status of Amendments

No amendments have been filed subsequent to filing a Notice of Appeal.

5.0 Summary of the Claimed Subject Matter

5.1 Independent claim 21

21. A system enabling secure transacting over a network **{Fig. 2, 202; pg. 9, ll. 13-14}** comprising:

a network server **{Fig. 2, 201; pg. 9, ll. 1-10}** having an application storing client information and configured to activate a client **{Fig. 2, 203}** for secure transacting in the network, the client connecting to the server through a network-connected digital appliance **{pg. 9, ll. 12-16}**;

a software driver configured to perform authentication, the software driver accessible to and executable by the network server application **{Fig. 14, pg. 23, ll. 10-15}**;

a software applet **{Pg, 23, ll. 16-17}** configured to create a secure data record and for managing transmission and update of the contents of the record; and

a token comprising an encrypted text string, the token stored on a data storage device coupled to the client's digital appliance, and also in a data repository coupled to the server **{Fig. 14, 1402; ll. 16-17}** ;

wherein, upon a client seeking authorization from the server, the server downloads the software applet and a timestamp of the request time to the client, the applet executes at the client, retrieves the token from the data storage device, concatenates the token file and the time stamp, hashes the result creating the secure data record, sends the secure data record to the server, and the server, executing the software driver, compares the secure data record to a similarly hashed result of the time stamp and token value taken from the data repository coupled to the server, authorizing the client with a match **{Fig. 15, pg. 25, line 14 to pg. 26, line 23}**.

In summary, claim 21 provides a unique system for providing authorization for executing secure transactions within a network. A client, connected to the network via a network appliance seeks authorization from a server, the server downloads a software

applet and a timestamp of the request time to the client, the applet executes at the client, retrieves the token from a data storage device coupled to the appliance, concatenates the token file and the time stamp, hashes the result creating the secure data record, sends the secure data record to the server, and the server, executing a software driver, compares the secure data record to a similarly hashed result of the time stamp and token value taken from the data repository coupled to the server, authorizing the client with a match

5.2 Dependent claims 23, 26 and 29

Dependent claims **23, 26 and 29** stand or fall with the independent claim.

5.3 Independent claim 52

52. (Previously presented) A method enabling secure transacting over a network comprising **{Fig. 15, pg. 25, line 14 to pg. 26, line 23}**:

(a) upon a client seeking authorization from a network server, the server downloading a software applet and a timestamp of the request time to a client digital appliance **{Fig. 15, 1502}**;

(b) executing the applet at the client, retrieving a token file from a data storage device coupled to the client appliance, the token file comprising an encrypted text string **{Fig. 15, 1504 - 1513}**;

(c) concatenating the token file and the timestamp and hashing the result, creating a secure data record **{Fig. 15, 1514}**;

(d) sending the secure data record to the server **{Fig. 15, 1515}**;

(e) comparing the secure data record to a similarly hashed result of the time stamp and token value taken from a data repository coupled to the server **{Fig. 15, 1516-1517}**; and

(f) authorizing the client with a match **{Fig. 15, 1518}**.

In summary, appellant's invention provides a method for improving system performance at a second enterprise by monitoring the second enterprise from a first enterprise. The method establishes, at the second enterprise, a management server managing overall system activities at the second enterprise, a data gathering engine controlled by the management server collecting and integrating data from a plurality of data sources accessible by the data gathering engine, storing collected and integrated data at a local database, and a client interface enabling clients of the second enterprise to access services at the second enterprise and submit specific requests for data. The first enterprise establishes a system server connected by a data link to at least the management server at the second enterprise, the system server remotely monitoring, troubleshooting and enhancing the system activities at the second enterprise including at least services related to the specific requests for data made by the clients.

5.4 Dependent claims 53-55

Dependent claims 53-55 stand or fall with the independent claim.

6.0 Grounds of Rejection to be Reviewed on Appeal

The following grounds are founded in the final Office Action mailed 07/06/2011.

6.1 Whether the Examiner presented a valid rejection for claims 21, 23, 26, 29, and 52-55 under 35 U.S.C. 103(a) as being unpatentable over United States Patent Application Publication No.: US 20040093496 A1 (Colnot) in view of United States Patent Application Publication No.: US 2005/0262573 A1 (Bo et al.) in further view of United States Patent No.: US 6,188,766 B1 (Kocher).

7.0 Argument

Regarding claims 21 and 52 of the rejection appellant argues that the Examiner errs in the interpretation of the art when applying the art to appellant's claims and as used in the reason for obviousness provided by the Examiner. Appellant points out that the art of Colnot is the same inventor as the present application and is valid art by only a few months. Bo teaches a system for validating a user and system to download and view audio/digital content presentations and Kocher is a system for validating a timestamp for a document sent to a server via a fax or other telecopier.

Regarding claim 21, the Examiner states that Bo teaches, "a software applet configured to create a secure data record and for managing transmission and update of the contents of the record;" Appellant argues that the art of Bo teaches ([237-238] that an SSL is created between the user and the server in order to secure data during manual registration prior to downloading the applet to client 23. Therefore, appellant argues that the Examiner has failed to teach that the downloaded applet creates a secure data record and manages transmission and update of the contents of the record, as claimed. The Examiner errs in the rejection when proceeding with the explanation of obviousness while neglecting to show said limitation in the art.

The Examiner states Kocher teaches appellant's limitations including:

- the server downloads a timestamp of the request time to the client, the applet executes at the client, retrieves the token from the data storage device, concatenates the token file and the time stamp, hashes the result creating the secure data record, sends the secure data record to the server, and the server, executing the software driver, compares the secure data record to a similarly hashed result of the time stamp and token value taken from the data repository coupled to the server, authorizing the client with a match.

The Examiner provides the following portion of Kocher to teach said limitations:

Referring now to FIG. 3, the timestamp verification process, as performed by the TTS in a facsimile-based embodiment, will be described. A requester (the document sender or a third party) who wishes to verify the timestamp on a document contacts the TTS, which, at step 300, receives a DIV or TTI. For example, this may be accomplished by receiving via facsimile a document (such as the first page of a document submission receipt) containing a DIV or a representation thereof in machine-readable form. The DIV is automatically detected and decoded using bar code scanning 20 techniques, optical character recognition, etc. Alternate DIV and TTI submission channels may be used including, without limitation: detection of DTMF (touch tone) signals, electronic submission via a computer network (e.g., Internet or world wide web), a voice call to a live operator who enters 25 the DIV or TTI using a computer terminal, a voice recognition system, wireless radio or pager, traditional or certified mail, modem, and electronic mail. At step 310, the TTS determines whether the DIV or TTI corresponds to a document stored in storage subsystem 150. If not, an error is 30 reported to the user at step 315. Otherwise, at step 320, the TTS retrieves the digital document from storage subsystem 150. If the document was stored in encrypted form, the TTS decrypts the document (if necessary, employing a cryptographic token, networked secure decrypting system, or other decryption mechanism), optionally using a decryption key included with or in the DIV or TTI. The digital timestamp stored with the data is then cryptographically verified as appropriate for the time stamping technique. For example, a timestamp constructed using an RSA signature may be 40 verified by operating on the timestamp with the public key corresponding to the digital signing key used by the time transmission stamp computation apparatus 170, then verifying that the result corresponds to the cryptographic hash of the combination of the archived digital document data and time indicator. An error is returned if document retrieval or timestamp verification fails.

Appellant points out that the DIV is a document identification value generated by the server and printed on a receipt sent to the sender of the telecopier transmission received at the TTS. The TTI is a transmission identifier for the transmission used when the sender sent the telecopier transmission. The requestor uses one or the other previously issued identifiers in order to identify the document stored at the TTS. The TTS may encrypt the document at the time of storage, and if so, will decrypt the document using known methods before applying the time verification process. The TTS decrypts, hashes and verifies the timestamp of the document for the requestor without teaching or suggesting a similar function at the user's station or any comparison of data for authentication. The only input by the requestor is the identifier of the document, the

balance of Kocher's teaching occurs at the TTS.

Appellant believes that because similar terms are used, the Examiner assumes a similar process occurs, which is an error. The art must teach or suggest the claimed subject matter. Appellant points out that all time stamping of documents occur at the receiving computer or via a request to a remote device for the time stamp. Appellant argues that the requestor and the client, as claimed are equated by the Examiner. Kocher fails to teach the actions taken at the client, as claimed, or communication from the client to the server of the hash result, or a comparison of the data at the server, as claimed.

The Examiner states:

> *It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the trusted time stamping techniques taught by Kocher in to the method of Colnot and Bo et al. as a timestamping would be particularly helpful in enhancing the integrity of a digital key/encryption system as it provides an extra verification layer without adding a disclosure of a key. (RSA Laboratories Frequently Asked Questions About Today's Cryptography version 4.1 Section 7.11 What is digital timestamping?)*

Appellant argues one with skill in the art would not look to the simplified timestamp verification process of Kocher to teach or suggest the entire functional wherein clause of appellant's claimed invention. There is no motivation provided in Kocher to make the combination because all hashing, etc. occurs at the receiver or server in Kocher. Therefore, no comparison for authenticating a user need occur in this stage of the process.

Appellant believes it has been fairly shown that the Examiner erred in the current examination process when not showing all of appellant's claimed limitations taught or suggested in the art. Therefore, claim 21 is patentable over the art presented by the Examiner. Claim 52 is appellant's method claim corresponding to claim 21 and is rejected using the same rational by the Examiner. Therefore, appellant believes claim 52 is also patentable over the combination of art provided by the Examiner. The dependent

claims fall or stand with their corresponding independent claim.

Appellant respectfully requests the Board allow the case, as appellant has diligently filed and argued on behalf of the invention, overcoming the Examiner's rejections in every round of prosecution.

5

8.0 Claims Appendix

The claims involved in the appeal are:

21. A system enabling secure transacting over a network comprising:

a network server having an application storing client information and configured to activate a client for secure transacting in the network, the client connecting to the server through a network-connected digital appliance;

a software driver configured to perform authentication, the software driver accessible to and executable by the network server application;

a software applet configured to create a secure data record and for managing transmission and update of the contents of the record; and

a token comprising an encrypted text string, the token stored on a data storage device coupled to the client's digital appliance, and also in a data repository coupled to the server;

wherein, upon a client seeking authorization from the server, the server downloads the software applet and a timestamp of the request time to the client, the applet executes at the client, retrieves the token from the data storage device, concatenates the token file and the time stamp, hashes the result creating the secure data record, sends the secure data record to the server, and the server, executing the software driver, compares the secure data record to a similarly hashed result of the time stamp and token value taken from the data repository coupled to the server, authorizing the client with a match.

23. The system of claim 21 wherein the data storage device coupled to the client's computer, and storing the token file, is a flash thumb drive.

26. The system of claim 21, 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 secret data seed.

29. The system of claim 21, wherein the software applet is a Java applet and the token is a Java archive.

52. (Previously presented) A method enabling secure transacting over a network comprising:

(a) upon a client seeking authorization from a network server, the server downloading a software applet and a timestamp of the request time to a client digital appliance;

(b) executing the applet at the client, retrieving a token file from a data storage device coupled to the client appliance, the token file comprising an encrypted text string;

(c) concatenating the token file and the timestamp and hashing the result, creating a secure data record;

(d) sending the secure data record to the server;

(e) comparing the secure data record to a similarly hashed result of the time stamp and token value taken from a data repository coupled to the server; and

(f) authorizing the client with a match.

53. (Previously presented) The method of claim 52 wherein data storage device coupled to the client's appliance, and storing the token file, is a flash thumb drive.

54. (Previously presented) The method of claim 52, wherein 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.

55. (Previously presented) The system of claim 52, wherein the software applet is a Java applet and the token is a Java archive.

9.0 Evidence Appendix

Not applicable.

10.0 Related Proceedings Appendix

There are no related proceedings in the present application.

Respectfully Submitted,
Vincent Cedric Colnot

By */Donald R. Boys/*
Donald R. Boys
Reg. No. 35,074

Central Coast Patent Agency, Inc.
3 Hangar Way, Suite D
Watsonville, CA 95076
831-768-1755
rexboys@centralcoastpatent.com

Electronic Patent Application Fee Transmittal

Application Number:	11533030
Filing Date:	19-Sep-2006
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

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Filing a brief in support of an appeal	2402	1	270	270
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
		Total in USD ($)		**270**

Electronic Acknowledgement Receipt

EFS ID:	10714383
Application Number:	11533030
International Application Number:	
Confirmation Number:	3809
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
Receipt Date:	11-AUG-2011
Filing Date:	19-SEP-2006
Time Stamp:	13:10:52
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$270
RAM confirmation Number	11234
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	Appeal Brief Filed	1987ApplBrf.pdf	150359 3d639757c80748fa7f2331ff38e13a2d7fe0ef62	no	18
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30425 11310a0764f5dd87811f413bd51844e553e41c2e	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	180784		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

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

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

Docket Number (Optional): P1987

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]
on _____

Signature _____

Typed or printed name _____

In re Application of: Vincent Cedric Colnot

Application Number	Filed
11/533,030	09/19/2006

For: Methods and Apparatus for Enabling Secure Network-Based Transactions

Art Unit	Examiner
2434	Benjamin A. Kaplan

Applicant hereby **appeals** to the Board of Patent Appeals and Interferences from the last decision of the examiner.

The fee for this Notice of Appeal is (37 CFR 41.20(b)(1)) $ 540.00

☑ Applicant claims small entity status. See 37 CFR 1.27. Therefore, the fee shown above is reduced by half, and the resulting fee is: $ 270.00

☐ A check in the amount of the fee is enclosed.

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

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. 50-0534 .

☐ A petition for an extension of time under 37 CFR 1.136(a) (PTO/SB/22) is enclosed.

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

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest.
See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed.
(Form PTO/SB/96)

☑ attorney or agent of record.
Registration number 35074.

☐ attorney or agent acting under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34. _____

/Donald R. Boys/
Signature

Donald R. Boys
Typed or printed name

831-768-1755
Telephone number

08/04/2011
Date

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

☐ *Total of _____ forms are submitted.

This collection of information is required by 37 CFR 41.31. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Privacy Act Statement

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

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

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

Electronic Patent Application Fee Transmittal

Application Number:	11533030
Filing Date:	19-Sep-2006
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

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Notice of appeal	2401	1	270	270
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
		Total in USD ($)		**270**

Electronic Acknowledgement Receipt

EFS ID:	10667113
Application Number:	11533030
International Application Number:	
Confirmation Number:	3809
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
Receipt Date:	04-AUG-2011
Filing Date:	19-SEP-2006
Time Stamp:	14:12:10
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$270
RAM confirmation Number	403
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	Notice of Appeal Filed	Noticeappeal.pdf	257196 e2443a99bbd0287399535557dffa89a5d9044bef	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30410 faa92d8118a8857a6c85d11d3ab72a42679a77bb	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	287606		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE
COMMISSIONER FOR PATENTS
P.O.BOX 1450
ALEXANDRIA VA 22313-1451

PRESORTED
FIRST-CLASS MAIL
U.S. POSTAGE PAID
POSTEDIGITAL
NNNNN

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

Courtesy Reminder for
Application Serial No: 11/533,030

Attorney Docket No: P1987
Customer Number: 24739
Date of Electronic Notification: 07/06/2011

This is a courtesy reminder that new correspondence is available for this application. The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

An email notification regarding the correspondence was sent to the following email address(es) associated with your customer number:
officeactions@CENTRALCOASTPATENT.COM
plambuth@centralcoastpatent.com
Please verify that these email addresses are correct.

To view your correspondence online or update your email addresses, please visit us anytime at **https://sportal.uspto.gov/secure/myportal/privatepair.** If you have any questions, please email the Electronic Business Center (EBC) at EBC@uspto.gov or call 1-866-217-9197.

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11533030	COLNOT, VINCENT CEDRIC
	Examiner	Art Unit
	BENJAMIN A KAPLAN	2434

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

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

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

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11533030	COLNOT, VINCENT CEDRIC
	Examiner	**Art Unit**
	BENJAMIN A KAPLAN	2434

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

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

CLAIM		DATE								
Final	Original	08/28/2009	05/22/2010	11/18/2010	06/29/2011					
	37		✓	-	-					
	38		✓	-	-					
	39		✓	-	-					
	40		✓	-	-					
	41		✓	-	-					
	42		✓	-	-					
	43		✓	-	-					
	44		✓	-	-					
	45		✓	-	-					
	46		✓	-	-					
	47		✓	-	-					
	48		✓	-	-					
	49		✓	-	-					
	50		✓	-	-					
	51		✓	-	-					
	52			✓	✓					
	53			✓	✓					
	54			✓	✓					
	55			✓	✓					

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	1	11/533,030.app.	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/18 13:57
S2	296	(("20010037461") or ("20010042124") or ("20020031225") or ("20020099940") or ("20020099942") or ("20020191765") or ("20030009676") or ("20030009692") or ("20030033545") or ("20030056096") or ("20030065919") or ("20030100371") or ("20030126457") or ("20030169713") or ("20030177354") or ("20030233450") or ("20030233583") or ("20040054794") or ("20040127279") or ("20040133789") or ("20040218897") or ("20050010777") or ("20050021613") or ("20050233811") or ("20060006230") or ("20060059265") or ("20060112213") or ("20060155601") or ("20060161775") or ("20060205394") or ("20060272023") or ("20060288407") or ("20070022469") or ("20070067833") or ("20070098175") or ("20070130334") or ("20070190975") or ("20070232355") or ("20070282909") or ("20080177998") or ("20090125717") or ("20090150977") or ("20090198996") or	US-PGPUB; USPAT; USOCR	OR	OFF	2009/08/27 18:23

		("4295155") or					
		("4386233") or					
		("4423287") or					
		("4755940") or					
		("4783798") or					
		("4888801") or					
		("4890323") or					
		("4897875") or					
		("4905766") or					
		("4910773") or					
		("4956862") or					
		("4997288") or					
		("5008936") or					
		("5016277") or					
		("5022076") or					
		("5202921") or					
		("5204961") or					
		("5210794") or					
		("5210795") or					
		("5226079") or					
		("5237614") or					
		("5239294") or					
		("5241594") or					
		("5261002") or					
		("5272754") or					
		("5276735") or					
		("5311596") or					
		("5313521") or					
		("5347387") or					
		("5349643") or					
		("5353353") or					
		("5369705") or					
		("5371794") or					
		("5410602") or					
		("5412726") or					
		("5425130") or					
		("5444780") or					
		("5454000") or					
		("5469507") or					
		("5479341") or					
		("5481613") or					
		("5485196") or					
		("5491752") or					
		("5499297") or					
		("5500897") or					
		("5502766") or					
		("5535276") or					
		("5557686") or					
		("5587809") or					
		("5588060") or					
		("5590196") or					
		("5590199") or					
		("5590200") or					
		("5592555") or					

("5598459") or
("5602915") or
("5602918") or
("5604663") or
("5604803") or
("5619657") or
("5623601") or
("5633933") or
("5633934") or
("5638448") or
("5643086") or
("5655077") or
("5657390") or
("5666412") or
("5668877") or
("5671279") or
("5673318") or
("5675651") or
("5684950") or
("5687235") or
("5689566") or
("5692400") or
("5699513") or
("5719941") or
("5721779") or
("5724168") or
("5724423") or
("5729594") or
("5732137") or
("5734718") or
("5742756") or
("5745574") or
("5745576") or
("5748736") or
("5754659") or
("5757913") or
("5757918") or
("5764890") or
("5768378") or
("5778065") or
("5778071") or
("5778313")).PN. or
(("5781550") or
("5781724") or
("5784463") or
("5787172") or
("5790669") or
("5796833") or
("5799082") or
("5802178") or
("5802497") or
("5805712") or
("5805803") or
("5809117") or

("5812664") or
("5812669") or
("5812764") or
("5812955") or
("5818936") or
("5822431") or
("5825300") or
("5825877") or
("5825890") or
("5828832") or
("5832209") or
("5832228") or
("5841120") or
("5841864") or
("5850442") or
("5850445") or
("5864665") or
("5870473") or
("5870475") or
("5870544") or
("5872915") or
("5875296") or
("5875394") or
("5875395") or
("5883956") or
("5887063") or
("5887250") or
("5889861") or
("5892829") or
("5892838") or
("5892902") or
("5894552") or
("5903721") or
("5907620") or
("5909491") or
("5913175") or
("5918228") or
("5922074") or
("5923756") or
("5926624") or
("5930362") or
("5931947") or
("5947571") or
("5953422") or
("5963644") or
("5963915") or
("5966441") or
("5967466") or
("5970144") or
("5974144") or
("5978475") or
("5978918") or
("5983350") or
("5995624") or

("5996077") or
("6002767") or
("6009524") or
("6012144") or
("6012632") or
("6017004") or
("6021497") or
("6023764") or
("6026167") or
("6026293") or
("6032150") or
("6032260") or
("6038551") or
("6038892") or
("6044155") or
("6044468") or
("6047072") or
("6047325") or
("6047572") or
("6049878") or
("6052785") or
("6055236") or
("6055636") or
("6061346") or
("6061448") or
("6061448") or
("6061449") or
("6061790") or
("6061796") or
("6061796") or
("6061799") or
("6061799") or
("6065120") or
("6067620") or
("6075860") or
("6081900") or
("6088451") or
("6098056") or
("6119233") or
("6141752") or
("6144848") or
("6148405") or
("6151590") or
("6158007") or
("6178089") or
("6185612") or
("6192474") or
("6198824") or
("6199113") or
("6202081") or
("6216231") or
("6216231") or
("6230266") or
("6233608") or

		("6233687") or ("6233688") or ("6247129") or ("6249867") or ("6249873") or ("6263313") or ("6272633") or ("6282653") or ("6301667") or ("6314468") or ("6345256") or ("6374402") or ("6389403") or ("6389538") or ("6418421") or ("6438600") or ("6449367") or ("6453416") or ("6463537") or ("6678826") or ("6732105") or ("6763370") or ("6907530") or ("6912653") or ("6945870") or ("6973566") or ("7017188") or ("7028182") or ("7073055") or ("7100054")).PN. or (("7103770") or ("7152160") or ("7171467") or ("7184999") or ("7188179") or ("7231025") or ("7287271") or ("7496950") or ("7502928") or ("7509119") or ("7533735")).PN.				
S3	300	(("20010034716") or ("20020014054") or ("20020017079") or ("20020020752") or ("20020032746") or ("20020036114") or ("20020052797") or ("20020073036") or ("20020077992") or ("20020091646") or ("20020103857") or ("20020116274") or ("20020141576") or	US-PGPUB; USPAT; USOCR	OR	OFF	2009/08/27 18:24

("20020157019") or
("20020178364") or
("20020191790") or
("20030014669") or
("20030018916") or
("20030023578") or
("20030028491") or
("20030046586") or
("20030046587") or
("20030046889") or
("20030055733") or
("20030056054") or
("20030056092") or
("20030061173") or
("20030061275") or
("20030061387") or
("20030061506") or
("20030065919") or
("20030081783") or
("20030088426") or
("20030097592") or
("20030100372") or
("20030111266") or
("20030115455") or
("20030126192") or
("20030126483") or
("20030163423") or
("20030163723") or
("20030177348") or
("20030177354") or
("20030182574") or
("20030188003") or
("20030188156") or
("20030188165") or
("20030191932") or
("20030208689") or
("20030221118") or
("20030226014") or
("20030226022") or
("20030229802") or
("20030233550") or
("20030236997") or
("20040002381") or
("20040020164") or
("20040065501") or
("20040068648") or
("20040068726") or
("20040073151") or
("20040083184") or
("20040083375") or
("20040088252") or
("20040089482") or
("20040095083") or
("20040098740") or

		("20040103165") or ("20040111578") or ("20040114182") or ("20040117623") or ("20040117627") or ("20040117635") or ("20040117661") or ("20040121787") or ("20040128517") or ("20040139019") or ("20040158635") or ("20040167465") or ("20040168081") or ("20040182126") or ("20040192303") or ("20040221168") or ("20040224769") or ("20040224771") or ("20040228063") or ("20040230809") or ("20040231594") or ("20040243853") or ("20050002328") or ("20050028487") or ("20050030151") or ("20050031136") or ("20050033980") or ("20050044404") or ("20050050342") or ("20050051448") or ("20050054445") or ("20050055588") or ("20050055815") or ("20050061878") or ("20050081063") or ("20050085931") or ("20050086509") or ("20050091364") or ("20050091527") or ("20050097350") or ("20050102535") or ("20050105736") or ("20050111380") or ("20050114687") or ("20050116026") or ("20050121339") or ("20050132031") or ("20050138356") or ("20050138423") or ("20050144493") or ("20050145695")).PN. or (("20050159203") or ("20050160417") or ("20050172132") or					

		("20050182938") or ("20050185647") or ("20050188251") or ("20050188731") or ("20050198461") or ("20050209006") or ("20050209842") or ("20050213768") or ("20050223220") or ("20050226175") or ("20050240685") or ("20050240712") or ("20050251685") or ("20050251852") or ("20050256806") or ("20050257245") or ("20050268336") or ("20060004964") or ("20060005072") or ("20060015947") or ("20060019657") or ("20060025147") or ("20060026573") or ("20060036693") or ("20060039305") or ("20060039306") or ("20060039321") or ("20060039339") or ("20060039340") or ("20060039360") or ("20060039562") or ("20060039563") or ("20060041750") or ("20060041761") or ("20060042882") or ("20060047784") or ("20060050887") or ("20060056630") or ("20060059543") or ("20060074983") or ("20060085370") or ("20060087192") or ("20060095377") or ("20060111165") or ("20060111794") or ("20060136742") or ("20060143700") or ("20060155589") or ("20060156019") or ("20060156399") or ("20060179308") or ("20060184524") or ("20060189382") or ("20060193474") or					

		("20060197403") or ("20060200660") or ("20060270346") or ("20070041110") or ("20070067833") or ("20070294085") or ("20080098872") or ("20080161951") or ("20080188182") or ("20080228865") or ("20080240468") or ("3683325") or ("4526115") or ("5051564") or ("5282247") or ("5406039") or ("5493767") or ("5656799") or ("5657388") or ("5695183") or ("5749253") or ("5825752") or ("6022009") or ("6038590") or ("6105042") or ("6118732") or ("6178550") or ("6209095") or ("6226697") or ("6233620") or ("6254366") or ("6282653") or ("6298336") or ("6328149") or ("6339827") or ("6382516") or ("6389541") or ("6393569") or ("6442532") or ("6502746") or ("6507908") or ("6520285") or ("6615194") or ("6620047") or ("6671810") or ("6701304") or ("6710893") or ("6722466") or ("6748532") or ("6769068") or ("6789147") or ("6823452") or ("6836795") or ("6845905") or						

		("6901251") or ("6915437") or ("6916247") or ("6920557") or ("6928707") or ("6934848") or ("6945458") or ("6957343") or ("6961759") or ("6970918") or ("6976164") or ("6976172") or ("6996841") or ("7013387") or ("7020476") or ("7024377") or ("7063615") or ("7069442") or ("7084734") or ("7085933") or ("7089587")).PN. or (("7095150") or ("7101296") or ("7103529") or ("7135968") or ("7137016") or ("7143280") or ("7146640") or ("7149821") or ("7152245") or ("7154628") or ("7155615") or ("7159242") or ("7185365") or ("7197644") or ("7207481") or ("7219480") or ("7228566") or ("7237717") or ("7245726") or ("7266703") or ("7290287") or ("7313679") or ("7333717") or ("7336789") or ("7343411") or ("7346929") or ("7350230") or ("7371952") or ("7383193") or ("7401230") or ("7418504") or ("7424610") or ("7428754") or					

		("7441153") or ("7452278") or ("7455590") or ("7458075") or ("7469341") or ("7469368") or ("7496097") or ("7502475") or ("7506170") or ("7509487") or ("7516331") or ("7530103") or ("7539651") or ("7540516") or ("7549922") or ("7574509") or ("7577258")).PN.				
S4	283	S2 @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:25
S5	285	S3 @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:25
S6	3	S4 S5	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:25
S7	29905	server client authentication @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:52
S8	21050	server client authentication key @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:52
S9	14617	server client authentication key secure @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:52
S10	4843	server client authentication key secure java @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:53
S11	2219	server client authentication key secure java applet @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:53
S12	604	server client authentication key secure java applet archive @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:53
S13	322	server client authentication key secure java applet archive sound card @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:53

S14	322	server client authentication key secure java applet archive sound card network @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:54
S15	283	server client authentication key secure java applet archive sound card network password @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:54
S16	279	server client authentication key secure java applet archive sound card network password session @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:54
S17	30	server client authentication key secure java applet archive sound card network password session seed @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:54
S18	0	server client authentication key secure java applet archive (sound adj source) @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 19:15
S19	1	server client authentication key secure java applet archive (sound same password) @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 19:17
S20	1	10/696,650.app.	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 19:26
S21	244	server client authentication key secure java applet archive (smart adj card) @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 18:48
S22	244	server client authentication key secure java applet archive (smart adj card) network @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 18:48
S23	234	server client authentication key secure java applet archive (smart adj card) network password @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 18:48

S24	225	server client authentication key secure java applet archive (smart adj card) network password session @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 18:49
S25	27	server client authentication key secure java applet archive (smart adj card) network password session seed @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 18:49
S26	1546	(726/2).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2009/08/28 20:32
S27	694	(726/9).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2009/08/28 20:32
S28	2232	(726/26).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2009/08/28 20:32
S29	1545	(726/27).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2009/08/28 20:32
S30	1033	S26 @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 20:32
S31	453	S27 @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 20:32
S32	1688	S28 @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 20:32
S33	1050	S29 @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 20:32
S34	1	S30 S31 S32 S33	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 20:33
S35	3732	S30 or S31 or S32 or S33	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 20:33
S36	1446	key source flash thumb drive @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/05/21 17:21
S37	0	(key adj source) (flash adj thumb adj drive) @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/05/21 17:21

S38	0	(key adj source) (thumb adj drive) @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/05/21 17:21
S39	3	(key adj source) (flash adj drive) @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/05/21 17:21
S40	128	(key) same (flash adj drive) @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/05/21 17:23
S41	6623	(726/2,9,26,27).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2010/05/22 19:21
S42	4273	S41 @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/05/22 19:21
S43	538	S42 @pd>"20090824"	US-PGPUB; USPAT; USOCR	AND	ON	2010/05/22 19:21
S44	15	(key) same (flash adj drive) (time adj stamp) @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/16 17:44
S45	34820	time adj stamp @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/16 17:45
S46	4062	time adj stamp hash @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/16 17:51
S47	954	(time adj stamp) same hash @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/16 17:51
S48	12	(key) same (flash adj drive) (time adj stamp) hash @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/16 17:51
S49	12	S47 S48	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/16 17:52
S50	195	((time adj stamp) same hash) (java or applet) @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/16 17:59
S51	5	((time adj stamp) same hash) (java or applet) concatenate @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/16 18:01
S52	12	(key) same (flash adj drive) (time adj stamp) hash @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/17 18:37

S53	200	Trusted timestamping @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/17 19:43
S54	8	Trusted adj timestamping @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/17 19:43
S55	4062	hash (time adj stamp) hash @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/17 19:48
S56	954	hash same (time adj stamp) hash @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/17 19:48
S57	130	hash near (time adj stamp) hash @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/17 19:48
S58	442	data same hash same (time adj stamp) hash @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/17 19:49
S59	2	data near hash near (time adj stamp) hash @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/17 19:50
S60	1	("7716488").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2010/11/17 19:56
S61	442	data same hash same (time adj stamp) hash @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/18 18:12
S62	129	hash near (time adj stamp) data @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/18 19:41
S63	130	hash near (time adj stamp) @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/18 19:42
S64	2027	hash secure data timestamp @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/18 20:03
S65	894	hash secure data timestamp token @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/18 20:03
S66	3	(hash secure data timestamp token) and @ad<"20050920"	US-PGPUB; USPAT; USOCR	SAME	ON	2010/11/18 20:03
S67	7571	(726/2,9,26,27).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2010/11/18 21:27
S68	4570	S67 @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/18 21:27

S69	297	S68 @pd>"20100518"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/18 21:27
S70	8616	(726/2,9,26,27).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2011/06/29 15:00
S71	4792	S70 @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2011/06/29 15:00
S72	219	S71 @pd>"20101118"	US-PGPUB; USPAT; USOCR	AND	ON	2011/06/29 15:00

EAST Search History (Interference)

< This search history is empty>

6/29/2011 3:03:18 PM
C:\Documents and Settings\bkaplan\My Documents\EAST\Workspaces\11533030.wsp

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/533,030	09/19/2006	Vincent Cedric Colnot	P1987	3809

24739 7590 07/06/2011

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

EXAMINER	
KAPLAN, BENJAMIN A	
ART UNIT	PAPER NUMBER
2434	

NOTIFICATION DATE	DELIVERY MODE
07/06/2011	ELECTRONIC

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

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

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

officeactions@CENTRALCOASTPATENT.COM
plambuth@centralcoastpatent.com

Office Action Summary	Application No.	Applicant(s)	
	11/533,030	COLNOT, VINCENT CEDRIC	
	Examiner	Art Unit	
	BENJAMIN KAPLAN	2434	

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

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

Status

1)☒ Responsive to communication(s) filed on *20 April 2011*.

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

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

Disposition of Claims

4)☒ Claim(s) *21,23,26,29 and 52-55* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *21,23,26,29 and 52-55* is/are rejected.

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

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

Application Papers

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

10)☒ The drawing(s) filed on *19 September 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

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

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

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

Priority under 35 U.S.C. § 119

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

a)☐ All b)☐ Some * c)☐ None of:

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

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

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

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

Attachment(s)

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

DETAILED ACTION

1. This Office Action is responsive to the most recent papers filed on 20 April 2011.

2. Claims 21, 23, 26, 29 and 52-55 are rejected.

Continued Examination Under 37 CFR 1.114

3. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 9/27/2010 has been entered.

Response to Arguments and Amendments

4. The rejection of claims 52, 54 & 55 under 35 U.S.C. § 101 is withdrawn.

5. Applicant's arguments filed 20 April 2011 have been considered but are not persuasive.

6. Applicant argued in substance that **It is important in the claimed invention that the secure data record is created at the client using the applet and time stamp from the server. The server also creates one using the same ingredients. Authorization (also not a function in Kocher) is a matter of the data records being independently created by the server and the client machine, and the data records matching. This is simply not in Kocher, and cannot be inferred from Kocher. In**

Kocher, any similar data record involving a token and time stamp is just created at the server side, not the sender side, and there is no comparison of independently-created data records, as claimed.

7. The arguments as presented are not sufficient to render the claimed invention non-obvious as the points noted fall in the range of predictable obvious variations to one of ordinary skill in the art as understood after *KSR International Co. v. Teleflex Inc. 550 U.S. 398 (2007)*.

8. As noted in (Kocher, Column 7, Lines 47-64) timestamp computation involves obtaining the date and time from a trusted clock and performing a verifiable cryptographic operation the server would be a obvious fit for a "trusted clock"

9. As noted in (Kocher, Column 10, Lines 32-46) The digital timestamp stored with the data is cryptographically verified as appropriate for the timestamping technique. Verifying a time stamp involves at minimum some sort of comparison of a similarly created record.

10. The arguments presented are also appear slightly narrower then the claim limitations themselves. The real question that should be answered in arguments is what is the key to applicants invention that advances it over what is know in the prior art.

Claim Rejections - 35 USC § 103

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

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

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

12. Claim(s) 21, 23, 26, 29 and 52-55 is/are rejected under 35 U.S.C. 103(a) as being unpatentable over United States Patent Application Publication No.: US 20040093496 A1 (Colnot) in view of United States Patent Application Publication No.: US 2005/0262573 A1 (Bo et al.) in further view of United States Patent No.: US 6,188,766 B1 (Kocher).

As Per Claim 21: Colnot teaches: **A system enabling secure transacting over a network comprising:**

- a network server having an application storing client information and configured to activate a client for secure transacting in the network, the client connecting to the server through a network-connected digital appliance;

(Colnot, Drawings, Figure. 1. "

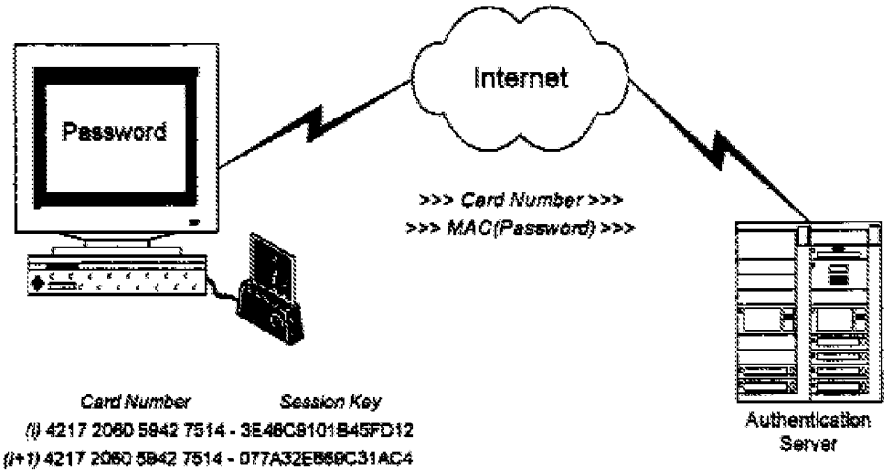


FIG. 1

").

(Colnot, Paragraphs [0011]-[0014], "The method, as detailed in FIG. 1, carries out the user authentication on the Internet. The apparatus comprises a smart card with a modulation output, a card reader plugged into the microphone input, and a PC applet. The user inserts his card in the reader and enters his password on the PC keyboard.

When activated in the card reader, the smart card transmits an identification sequence to the PC in the form of a modulated signal, which is demodulated by the PC applet. The identification sequence comprises an 8-byte card number and an 8-byte random number valid only once. The card number is unique and identifies the card issuer, application version and user account. The random number is a session key (Ki) which is a function of the previous one (Ki-1) emitted by the card such as: Ki=G(Ki-1), G is a one-way function also known by the authentication server.

The session key (Ki) is used by the PC applet to generate a message authentication code (MAC) of the password entered by the user, using the DES algorithm for instance. This first MAC is transmitted to the authentication server along with the card number, allowing the server to retrieve the previous session key (Ki-1) and the password stored in the authentication server database.

The authentication server deduces from (Ki-1) the session key used by the card, and generates a second MAC of the password stored in the database. The authentication is valid only if the first and second MAC are identical, which means the PC and the authentication server have used the same session key (Ki) to generate a MAC of the same password. If this is the case, the authentication server replaces (Ki-1)

by (Ki) in the database. The session key (Ki) cannot be reused, even though the session key (Ki) has not been transmitted to the authentication server.").

- a token comprising an encrypted text string, the token stored on a data storage device coupled to connect to the client's digital appliance, and also in a data repository coupled to the server;

(Colnot, Paragraphs [0011]-[0014], "The method, as detailed in FIG. 1, carries out the user authentication on the Internet. The apparatus comprises a smart card with a modulation output, a card reader plugged into the microphone input, and a PC applet. The user inserts his card in the reader and enters his password on the PC keyboard.

When activated in the card reader, the smart card transmits an identification sequence to the PC in the form of a modulated signal, which is demodulated by the PC applet. The identification sequence comprises an 8-byte card number and an 8-byte random number valid only once. The card number is unique and identifies the card issuer, application version and user account. The random number is a session key (Ki) which is a function of the previous one (Ki-1) emitted by the card such as: Ki=G(Ki-1), G is a one-way function also known by the authentication server.

The session key (Ki) is used by the PC applet to generate a message authentication code (MAC) of the password entered by the user, using the DES algorithm for instance. This first MAC is transmitted to the authentication server along with the card number, allowing the server to retrieve the previous session key (Ki-1) and the password stored in the authentication server database.

The authentication server deduces from (Ki-1) the session key used by the card, and generates a second MAC of the password stored in the database. The authentication is valid only if the first and second MAC are identical, which means the PC and the authentication server have used the same session key (Ki) to generate a MAC of the same password. If this is the case, the authentication server replaces (Ki-1) by (Ki) in the database. The session key (Ki) cannot be reused, even though the session key (Ki) has not been transmitted to the authentication server.").

Colnot does not explicitly teach the following limitations however Bo et al in analogous are does teach the following limitations:

- a software driver configured to perform authentication, the software driver accessible to and executable by the network server application;

- a software applet configured to create a secure data record and for managing transmission and update of the contents of the record; and

(Bo et al., Paragraphs [0242]-[0243], "c) With the agreement of the user, an application of the client 23 is downloaded from the web server 13 as S27 shows. The application is, for example, a Java applet. The user installs the application on the end station as S28 shows. Thus, the application of the client 23 is implemented.

d) With the agreement of the user, the application of the client 23 establishes an SSL connection (an SSL link) with the web server 13 for further transactions as S29 shows.").

(Bo et al., Paragraph [0253], "FIG. 16 shows a method of user authentication and digital audio-visual content encryption key(s) distribution. Each time a registered user wants to enjoy the services from the content provider, the user may be authenticated.").

The driver is the inherent underlying software that makes it possible for a system to operate with its underlying hardware and functions thereof.

- wherein upon a client seeking authorization from the server, the server downloads the software applet

(Bo et al., Paragraphs [0242]-[0243], "c) With the agreement of the user, an application of the client 23 is downloaded from the web server 13 as S27 shows. The application is, for example, a Java applet. The user installs the application on the end station as S28 shows. Thus, the application of the client 23 is implemented.

d) With the agreement of the user, the application of the client 23 establishes an SSL connection (an SSL link) with the web server 13 for further transactions as S29 shows.").

(Bo et al., Paragraph [0253], "FIG. 16 shows a method of user authentication and digital audio-visual content encryption key(s) distribution. Each time a registered user wants to enjoy the services from the content provider, the user may be authenticated.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Colnot in to the method of Bo et al. in order to take advantage of being able to inexpensively add the enhancements of smart card authentication (Colnot, Paragraph [0005]). On in reverse to incorporate the

teaching of Bo et al. in to the method of Colnot in order to take advantage of the authentication enhancements provided by Bo et al. (Bo et al., Paragraph [0011]).

Colnot and Bo et al. do not explicitly teach the following limitations however Kocher in analogous are does teach the following limitations:

- the server downloads a timestamp of the request time to the client, the applet executes at the client, retrieves the token from the data storage device, concatenates the token file and the time stamp, hashes the result creating the secure data record, sends the secure data record to the server, and the server, executing the software driver, compares the secure data record to a similarly hashed result of the time stamp and token value taken from the data repository coupled to the server, authorizing the client with a match.

(Kocher, Column 7, Lines 47-64, "If the sender identification at step 220 is satisfactory, the system proceeds to step 230, where the digital data are cryptographically timestamped using digital timestamp computation apparatus 170. In one preferred embodiment, timestamp computation involves obtaining the date and time from a trusted clock and performing a verifiable cryptographic operation on the digital document data plus the date/time (e.g., combining the hash of the digital data with the date and time, hashing the combination, and digitally signing the result using a private RSA key). As previously described, other techniques, such as the hash tree and catenate timestamping techniques described by Haber et al., may also be used. The apparatus which performs the basic timestamping operation may be, without limitation,

the computer which is connected to the modem, or a smart-card or other cryptographic token connected to said computer, or a separate timestamping device or service connected to said computer via a computer network.").

(Kocher, Column 10, Lines 32-46, "If the document was stored in encrypted form, the TTS decrypts the document (if necessary, employing a cryptographic token, networked secure decrypting system, or other decryption mechanism), optionally using a decryption key included with or in the DIV or TTI. The digital timestamp stored with the data is then cryptographically verified as appropriate for the timestamping technique. For example, a timestamp constructed using an RSA signature may be verified by operating on the timestamp with the public key corresponding to the digital signing key used by the timestamp computation apparatus 170, then verifying that the result corresponds to the cryptographic hash of the combination of the archived digital document data and time indicator. An error is returned if document retrieval or timestamp verification fails.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the trusted time stamping techniques taught by Kocher in to the method of Colnot and Bo et al. as a timestamping would be particularly helpful in enhancing the integrity of a digital key/encryption system as it provides an extra verification layer without adding a disclosure of a key. (RSA Laboratories Frequently Asked Questions About Today's Cryptography version 4.1 Section 7.11 What is digital timestamping?)

As Per Claim 23: The rejection of claim 21 is incorporated and further Colnot, Bo et al. and Kocher do not explicitly teach:

- the data storage device coupled to the client's computer, and storing the token file, is a flash thumb drive

However the examiner is giving official notice the use of flash drives as key sources was well established in the art at the time of invention was made. It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporated the use of flash drives as potential key sources as they provide as highly expedient manner of having a portable connectable/disconnect-able device easily at the ready.

As Per Claim 26: The rejection of claim 21 is incorporated and further Colnot does not explicitly teach the following limitations however Bo et al in analogous art does teach the following limitations:

- 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

(Bo et al., Paragraph [0152], "In one example, the web server 13 is used to transfer user's personal information from the client 23 to the SRM 5 through a pre-established SSL link. The user's personal information includes user's log-in ID and password. The user account manager 35 in the SRM 5 maintains and manages all the user's personal information.").

(Bo et al., Paragraph [0147], "The encipheror 3 or the encipheror in the encipheror/decipherer module 38 defines a block cipher algorithm, e.g., DES (data encryption standard), AES (advanced encryption standard), or Blowfish. The encipheror 3 or the encipheror in the encipheror/decipherer module 38 also defines the seeds for generating random keys, the preferred key length for the block cipher algorithm that accepts variable length keys, the preferred plaintext block size, e.g., 64 bits, 128 bits, or 256 bits. Otherwise, a default encryption strategy is to be used.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Colnot in to the method of Bo et al. in order to take advantage of being able to inexpensively add the enhancements of smart card authentication (Colnot, Paragraph [0005]). On in reverse to incorporate the teaching of Bo et al. in to the method of Colnot in order to take advantage of the authentication enhancements provided by Bo et al. (Bo et al., Paragraph [0011]).

As Per Claim 29: The rejection of claim 21 is incorporated and further Colnot does not explicitly teach the following limitations however Bo et al in analogous art does teach the following limitations:

- the software applet is a Java applet and the secure data record token is a Java archive

(Bo et al., Paragraphs [0242]-[0243], "c) With the agreement of the user, an application of the client 23 is downloaded from the web server 13 as S27 shows. The

application is, for example, a Java applet. The user installs the application on the end station as S28 shows. Thus, the application of the client 23 is implemented.

d) With the agreement of the user, the application of the client 23 establishes an SSL connection (an SSL link) with the web server 13 for further transactions as S29 shows.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Colnot in to the method of Bo et al. in order to take advantage of being able to inexpensively add the enhancements of smart card authentication (Colnot, Paragraph [0005]). On in reverse to incorporate the teaching of Bo et al. in to the method of Colnot in order to take advantage of the authentication enhancements provided by Bo et al. (Bo et al., Paragraph [0011]).

As Per Claim 52: Colnot teaches: **A method enabling secure transacting over a network comprising:**

(b) executing the applet at the client, retrieving a token file from a data storage device coupled to the client appliance, the token file comprising an encrypted text string;

(Colnot, Drawings, Figure. 1. "

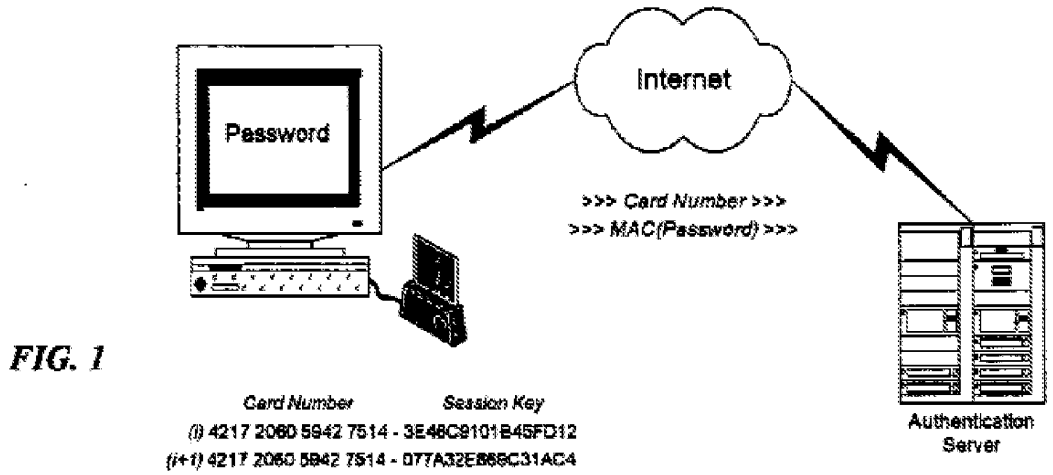


FIG. 1

").

(Colnot, Paragraphs [0011]-[0014], "The method, as detailed in FIG. 1, carries out the user authentication on the Internet. The apparatus comprises a smart card with a modulation output, a card reader plugged into the microphone input, and a PC applet. The user inserts his card in the reader and enters his password on the PC keyboard.

When activated in the card reader, the smart card transmits an identification sequence to the PC in the form of a modulated signal, which is demodulated by the PC applet. The identification sequence comprises an 8-byte card number and an 8-byte random number valid only once. The card number is unique and identifies the card issuer, application version and user account. The random number is a session key (Ki) which is a function of the previous one (Ki-1) emitted by the card such as: Ki=G(Ki-1), G is a one-way function also known by the authentication server.

The session key (Ki) is used by the PC applet to generate a message authentication code (MAC) of the password entered by the user, using the DES algorithm for instance. This first MAC is transmitted to the authentication server along

with the card number, allowing the server to retrieve the previous session key (Ki-1) and the password stored in the authentication server database.

The authentication server deduces from (Ki-1) the session key used by the card, and generates a second MAC of the password stored in the database. The authentication is valid only if the first and second MAC are identical, which means the PC and the authentication server have used the same session key (Ki) to generate a MAC of the same password. If this is the case, the authentication server replaces (Ki-1) by (Ki) in the database. The session key (Ki) cannot be reused, even though the session key (Ki) has not been transmitted to the authentication server.").

Colnot does not explicitly teach the following limitations however Bo et al in analogous are does teach the following limitations:

-(a) upon a client seeking authorization from a network server, the server downloading a software applet

(Bo et al., Paragraphs [0242]-[0243], "c) With the agreement of the user, an application of the client 23 is downloaded from the web server 13 as S27 shows. The application is, for example, a Java applet. The user installs the application on the end station as S28 shows. Thus, the application of the client 23 is implemented.

d) With the agreement of the user, the application of the client 23 establishes an SSL connection (an SSL link) with the web server 13 for further transactions as S29 shows.").

(Bo et al., Paragraph [0253], "FIG. 16 shows a method of user authentication and digital audio-visual content encryption key(s) distribution. Each time a registered user wants to enjoy the services from the content provider, the user may be authenticated.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Colnot in to the method of Bo et al. in order to take advantage of being able to inexpensively add the enhancements of smart card authentication (Colnot, Paragraph [0005]). On in reverse to incorporate the teaching of Bo et al. in to the method of Colnot in order to take advantage of the authentication enhancements provided by Bo et al. (Bo et al., Paragraph [0011]).

Colnot and Bo et al. do not explicitly teach the following limitations however Kocher in analogous are does teach the following limitations:

- a timestamp of the request time to a client digital appliance;

(c) concatenating the token file and the timestamp and hashing the result, creating a secure data record;

(d) sending the secure data record to the server;

(e) comparing the secure data record to a similarly hashed result of the time stamp and token value taken from a data repository coupled to the server; and

(f) authorizing the client with a match.

(Kocher, Column 7, Lines 47-64, "If the sender identification at step 220 is satisfactory, the system proceeds to step 230, where the digital data are cryptographically timestamped using digital timestamp computation apparatus 170. In

one preferred embodiment, timestamp computation involves obtaining the date and time from a trusted clock and performing a verifiable cryptographic operation on the digital document data plus the date/time (e.g., combining the hash of the digital data with the date and time, hashing the combination, and digitally signing the result using a private RSA key). As previously described, other techniques, such as the hash tree and catenate timestamping techniques described by Haber et al., may also be used. The apparatus which performs the basic timestamping operation may be, without limitation, the computer which is connected to the modem, or a smart-card or other cryptographic token connected to said computer, or a separate timestamping device or service connected to said computer via a computer network.").

(Kocher, Column 10, Lines 32-46, "If the document was stored in encrypted form, the TTS decrypts the document (if necessary, employing a cryptographic token, networked secure decrypting system, or other decryption mechanism), optionally using a decryption key included with or in the DIV or TTI. The digital timestamp stored with the data is then cryptographically verified as appropriate for the timestamping technique. For example, a timestamp constructed using an RSA signature may be verified by operating on the timestamp with the public key corresponding to the digital signing key used by the timestamp computation apparatus 170, then verifying that the result corresponds to the cryptographic hash of the combination of the archived digital document data and time indicator. An error is returned if document retrieval or timestamp verification fails.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the trusted time stamping techniques taught by Kocher in to the method of Colnot and Bo et al. as a timestamping would be particularly helpful in enhancing the integrity of a digital key/encryption system as it provides an extra verification layer without adding a disclosure of a key. (RSA Laboratories Frequently Asked Questions About Today's Cryptography version 4.1 Section 7.11 What is digital timestamping?)

As Per Claim 53: The rejection of claim 52 is incorporated and further Colnot, Bo et al. and Kocher do not explicitly teach:

- data storage device coupled to the client's appliance, and storing the token file, is a flash thumb drive

However the examiner is giving official notice the use of flash drives as key sources was well established in the art at the time of invention was made. It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporated the use of flash drives as potential key sources as they provide as highly expedient manner of having a portable connectable/disconnect-able device easily at the ready.

As Per Claim 54: The rejection of claim 52 is incorporated and further Colnot does not explicitly teach the following limitations however Bo et al in analogous art does teach the following limitations:

- 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

(Bo et al., Paragraph [0152], “In one example, the web server 13 is used to transfer user's personal information from the client 23 to the SRM 5 through a pre-established SSL link. The user's personal information includes user's log-in ID and password. The user account manager 35 in the SRM 5 maintains and manages all the user's personal information.”).

(Bo et al., Paragraph [0147], “The encipheror 3 or the encipheror in the encipheror/decipherer module 38 defines a block cipher algorithm, e.g., DES (data encryption standard), AES (advanced encryption standard), or Blowfish. The encipheror 3 or the encipheror in the encipheror/decipherer module 38 also defines the seeds for generating random keys, the preferred key length for the block cipher algorithm that accepts variable length keys, the preferred plaintext block size, e.g., 64 bits, 128 bits, or 256 bits. Otherwise, a default encryption strategy is to be used.”).

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Colnot in to the method of Bo et al. in order to take advantage of being able to inexpensively add the enhancements of smart card authentication (Colnot, Paragraph [0005]). On in reverse to incorporate the teaching of Bo et al. in to the method of Colnot in order to take advantage of the authentication enhancements provided by Bo et al. (Bo et al., Paragraph [0011]).

As Per Claim 55: The rejection of claim 52 is incorporated and further Colnot does not explicitly teach the following limitations however Bo et al in analogous art does teach the following limitations:

- the software applet is a Java applet and the secure data record token is a Java archive

(Bo et al., Paragraphs [0242]-[0243], "c) With the agreement of the user, an application of the client 23 is downloaded from the web server 13 as S27 shows. The application is, for example, a Java applet. The user installs the application on the end station as S28 shows. Thus, the application of the client 23 is implemented.

d) With the agreement of the user, the application of the client 23 establishes an SSL connection (an SSL link) with the web server 13 for further transactions as S29 shows.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Colnot in to the method of Bo et al. in order to take advantage of being able to inexpensively add the enhancements of smart card authentication (Colnot, Paragraph [0005]). On in reverse to incorporate the teaching of Bo et al. in to the method of Colnot in order to take advantage of the authentication enhancements provided by Bo et al. (Bo et al., Paragraph [0011]).

Conclusion

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BENJAMIN KAPLAN whose telephone number is (571)270-3170. The examiner can normally be reached on 7:30 a.m. - 5:00 p.m. E.S.T..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. 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.

/Benjamin A Kaplan/
Examiner, Art Unit 2434

/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2434

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11533030	COLNOT, VINCENT CEDRIC
	Examiner	Art Unit
	BENJAMIN A KAPLAN	2434

SEARCHED			
Class	Subclass	Date	Examiner
726	2,9,26,27	6/29/2011	BK

SEARCH NOTES		
Search Notes	Date	Examiner
East, Plus Search, Google	6/29/2011	BK

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Art Unit: 2434 Examiner: Kaplan, Benjamin A

In Re:	Vincent Cedric Colnot
Case:	P1987
Serial No.:	11/533,030
Filed:	September 19, 2006
Subject:	Methods and Apparatus for Enabling Secure Network-Based Transactions

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Response C

In the Claims

All of the claims standing for examination are reproduced below with appropriate status indication.

1-20. (Cancelled)

21. (Previously presented) A system enabling secure transacting over a network comprising:

a network server having an application storing client information and configured to activate a client for secure transacting in the network, the client connecting to the server through a network-connected digital appliance;

a software driver configured to perform authentication, the software driver accessible to and executable by the network server application;

a software applet configured to create a secure data record and for managing transmission and update of the contents of the record; and

a token comprising an encrypted text string, the token stored on a data storage device coupled to the client's digital appliance, and also in a data repository coupled to the server;

wherein, upon a client seeking authorization from the server, the server downloads the software applet and a timestamp of the request time to the client, the applet executes at the client, retrieves the token from the data storage device, concatenates the token file and the time stamp, hashes the result creating the secure data record, sends the secure data record to the server, and the server, executing the software driver, compares the secure data record to a similarly hashed result of the time stamp and token value taken from the data repository coupled to the server, authorizing the client with a match.

22. (Cancelled)

23. (Previously presented) The system of claim 21 wherein the data storage device coupled to the client's computer, and storing the token file, is a flash thumb drive.

24-25. (Cancelled)

26. (Previously presented) The system of claim 21, 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 secret data seed.

27-28. (Cancelled)

29. (Previously presented) The system of claim 21, wherein the software applet is a Java applet and the token is a Java archive.

30-51. (Cancelled)

52. (Previously presented) A method enabling secure transacting over a network comprising:

(a) upon a client seeking authorization from a network server, the server downloading a software applet and a timestamp of the request time to a client digital appliance;

(b) executing the applet at the client, retrieving a token file from a data storage device coupled to the client appliance, the token file comprising an encrypted text string;

(c) concatenating the token file and the timestamp and hashing the result, creating a secure data record;

(d) sending the secure data record to the server;

(e) comparing the secure data record to a similarly hashed result of the time stamp and token value taken from a data repository coupled to the server; and

(f) authorizing the client with a match.

53. (Previously presented) The method of claim 52 wherein data storage device coupled to the client's appliance, and storing the token file, is a flash thumb drive.

54. (Previously presented) The method of claim 52, wherein 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.

55. (Previously presented) The system of claim 52, wherein the software applet is a Java applet and the token is a Java archive.

REMARKS

This response is to the Office Action mailed on 11/23/2010.

From the action:

This action is a non-final action in response to communication filed on 01 March 2010. Claims 21,23,26,29 and 52-55 are pending in the application. Claims 21,23,26,29 and 52-55 are rejected. The drawing(s) filed on 19 September 2006 are accepted by the Examiner. This Office Action is responsive to the most recent papers filed on 9/27/2010. Claims 21-51 are rejected.

Applicant's response:

Acknowledged

From the action:

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 9/27/2010 has been entered.

Applicant's response:

Acknowledged

From the action:

Response to Arguments and Amendments

The rejections of canceled claims are moot in view of their cancelation.

The rejection of claims 21-34 under 35 U.S.C. § 112 is withdrawn.

Applicant's arguments that Colnot and Bo et al. do not teach the amended claims as use of time stamps has been accepted new ground(s) of rejection are presented with additional teachings from United States Patent No.: US 6,188,766 B1 (Kocher).

Applicant's response:

Acknowledged

From the action:

Claim Rejections - 35 USC § 101

Claim(s) 52, 54 & 55 fail the machine-or-transformation test which is a two-branched inquiry. It may be shown that a process claim satisfies 35 USC § 101 by showing that a claim is tied to a particular machine or by showing that a claim transforms an article into a different state or thing. See Gottschalk v. Benson, 409 U.S. 63, 67 (1972). As to the first prong (machine), the Examiner cannot find any showing that these claims are attached to a specific machine. As to the second prong (transformation), the process claims do not transform a physical article into a different state or thing. The process claims are merely manipulating abstract data without regard to any physical article or object.

Applicant's response:

The applicant has presented claim 52 just below. The examiner states in the 101 rejection that he cannot find any showing that these claims are attached to a specific machine. The applicant has caused to be **bolded** in the claim at least three instances of a specific apparatus to which the claim attaches, these being a network server, a client digital device, and a data storage device. Server is often interpreted by the Office as possibly software, but a digital appliance cannot be considered to be software, and the method requires (attaches to) the digital appliance.

52. (Previously presented) A method enabling secure transacting over a network comprising:

(a) upon a client seeking authorization from a **network server**, the server downloading a software applet and a timestamp of the request time to a **client digital appliance**;

(b) executing the applet at the client, retrieving a token file from a **data storage device coupled to the client appliance**, the token file comprising an encrypted text string;

(c) concatenating the token file and the timestamp and hashing the result, creating a secure data record;

(d) sending the secure data record to the server;

(e) comparing the secure data record to a similarly hashed result of the time stamp and token value taken from a data repository coupled to the server; and

(f) authorizing the client with a match.

The applicant believes that claim 52 passes the two-prong test, and respectfully asks that the examiner withdraw the 101 rejection. Claims 53-55 depend from claim 52 and are therefore also pass the test for patentable subject matter.

From the action:

Claim Rejections - 35 USC § 103

Claim(s) 21-34 & 41-51 is/are rejected under 35 U.S.C. 103(a) as being unpatentable over United States Patent Application Publication No.: US 20040093496 A1 (Colnot) in view of United States Patent Application Publication No.: US 2005/0262573 A1 (Bo et al.) in further view of United States Patent No.: US 6,188,766 B1 (Kocher).

As Per Claim 21: Colnot teaches: **A system enabling secure transacting over a network comprising:**

- a network server having an application storing client information and configured to activate a client for secure transacting in the network, the client connecting to the server through a network-connected digital appliance;

(Colnot, Drawings, Figure. 1.)

(Colnot, Paragraphs [0011]-[0014], "The method, as detailed in FIG. 1, carries out the user authentication on the Internet. The apparatus comprises a smart card with a modulation output, a card reader plugged into the microphone input, and a PC applet. The user inserts his card in the reader and enters his password on the PC keyboard.

When activated in the card reader, the smart card transmits an identification sequence to the PC in the form of a modulated signal, which is demodulated by the PC applet. The identification sequence comprises an 8-byte card number and an 8-byte random number valid only once. The card number is unique and identifies the card issuer, application version and user account. The random number is a session key (Ki) which is a function of the previous one (Ki-1) emitted by the card such as: Ki=G (Ki-1), G is a one-way function also known by the authentication server.

The session key (Ki) is used by the PC applet to generate a message authentication code (MAC) of the password entered by the user, using the DES algorithm for instance. This first MAC is transmitted to the authentication server along with the card number, allowing the server to retrieve the previous session key (Ki-1) and the password stored in the authentication server database.

The authentication server deduces from (Ki-1) the session key used by the card, and generates a second MAC of the password stored in the database. The authentication is valid only if the first and second MAC are identical, which means the PC and the authentication server have used the same session key (Ki) to generate a MAC of the same password. If this is the case, the authentication server replaces (Ki-1) by (Ki) in the database. The session key (Ki) cannot be reused, even though the session key (Ki) has not been transmitted to the authentication server.").

- a token comprising an encrypted text string, the token stored on a data storage device coupled to connect to the client's digital appliance, and also in a data repository coupled to the server;

(Colnot, Paragraphs [0011]-[0014], "The method, as detailed in FIG. 1, carries out the user authentication on the Internet. The apparatus comprises a smart card with a modulation output, a card reader plugged into the microphone input, and a PC applet.

The user inserts his card in the reader and enters his password on the PC keyboard. When activated in the card reader, the smart card transmits an identification sequence to the PC in the form of a modulated signal, which is demodulated by the PC applet. The identification sequence comprises an 8-byte card number and an 8-byte random number valid only once. The card number is unique and identifies the card issuer, application version and user account. The random number is a session key (Ki) which is a function of the previous one (Ki-1) emitted by the card such as: Ki=G (Ki-1), G is a one-way function also known by the authentication server.

The session key (Ki) is used by the PC applet to generate a message authentication code (MAC) of the password entered by the user, using the DES algorithm for instance. This first MAC is transmitted to the authentication server along with the card number, allowing the server to retrieve the previous session key (Ki-1) and the password stored in the authentication server database.

The authentication server deduces from (Ki-1) the session key used by the card, and generates a second MAC of the password stored in the database. The authentication is valid only if the first and second MAC are identical, which means the PC and the authentication server have used the same session key (Ki) to generate a MAC of the same password. If this is the case, the authentication server replaces (Ki-1) by (Ki) in the database. The session key (Ki) cannot be reused, even though the session key (Ki) has not been transmitted to the authentication server.").

Colnot does not explicitly teach the following limitations however Bo et al in analogous are does teach the following limitations:

- a software driver configured to perform authentication, the software driver accessible to and executable by the network server application;
- a software applet configured to create a secure data record and for managing transmission and update of the contents of the record; and

(Bo et al., Paragraphs [0242]-[0243], "c) With the agreement of the user, an application of the client 23 is downloaded from the web server 13 as S27 shows. The application is, for example, a Java applet. The user installs the application on the end station as S28 shows. Thus, the application of the client 23 is implemented.

d) With the agreement of the user, the application of the client 23 establishes an SSL connection (an SSL link) with the web server 13 for further transactions as S29 shows.").

(Bo et al., Paragraph [0253], "FIG. 16 shows a method of user authentication and digital audio-visual content encryption key(s) distribution. Each time a registered user wants to enjoy the services from the content provider, the user may be authenticated.").

The driver is the inherent underlying software that makes it possible for a system to operate with its underlying hardware and functions thereof.

- wherein upon a client seeking authorization from the server, the server downloads the software applet

(Bo et al., Paragraphs [0242]-[0243], "c) With the agreement of the user, an application of the client 23 is downloaded from the web server 13 as S27 shows. The application is, for example, a Java applet. The user installs the application on the end station as S28 shows. Thus, the application of the client 23 is implemented.

d) With the agreement of the user, the application of the client 23 establishes an SSL connection (an SSL link) with the web server 13 for further transactions as S29 shows.").

(Bo et al., Paragraph [0253], "FIG. 16 shows a method of user authentication and digital audio-visual content encryption key(s) distribution. Each time a registered user wants to enjoy the services from the content provider, the user may be authenticated.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Colnot in to the method of Bo et al. in order to take advantage of being able to inexpensively add the enhancements of smart card authentication (Colnot, Paragraph [0005]). On in reverse to incorporate the teaching of Bo et al. in to the method of Colnot in order to take advantage of the authentication enhancements provided by Bo et al. (Bo et al., Paragraph [0011]).

Colnot and Bo et al. do not explicitly teach the following limitations however Kocher in analogous are does teach the following limitations:

- the server downloads a timestamp of the request time to the client, the applet executes at the client, retrieves the token from the data storage device, concatenates the token file and the time stamp, hashes the result creating the secure data record, sends the secure data record to the server, and the server, executing the software driver, compares the secure data record to a similarly hashed result of the time stamp and token value taken from the data repository coupled to the server, authorizing the client with a match.

(Kocher, Column 7, Lines 47-64, "If the sender identification at step 220 is satisfactory, the system proceeds to step 230, where the digital data are cryptographically timestamped using digital timestamp computation apparatus 170. In one preferred embodiment, timestamp computation involves obtaining the date and time from a trusted clock and performing a verifiable cryptographic operation on the digital document data plus the date/time (e.g., combining the hash of the digital data with the date and time, hashing the combination, and digitally signing the result using a private RSA key). As previously described, other techniques, such as the hash tree and catenate timestamping techniques described by Haber et al., may also be used. The apparatus which performs the basic timestamping operation may be, without limitation, the computer which is connected to the modem, or a smart-card or other cryptographic token connected to said computer, or a separate timestamping device or service connected to said computer via a computer network.").

(Kocher, Column 10, Lines 32-46, "If the document was stored in encrypted form, the TTS decrypts the document (if necessary, employing a cryptographic token, networked secure decrypting system, or other decryption mechanism), optionally using a decryption key included with or in the DIV or TTI. The digital timestamp stored with the data is then cryptographically verified as appropriate for the timestamping technique. For example, a timestamp constructed using an RSA signature may be verified by operating on the timestamp with the public key corresponding to the digital signing key used by the timestamp computation apparatus 170, then verifying that the result corresponds to the cryptographic hash of the combination of the archived digital document data and time indicator. An error is returned if document retrieval or timestamp verification fails.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the trusted time stamping techniques taught by Kocher in to the method of Colnot and Bo et al. as a timestamping would be particularly helpful in enhancing the integrity of a digital key/encryption system as it provides an extra verification layer without adding a disclosure of a key. (RSA Laboratories Frequently Asked Questions About Today's Cryptography version 4.1 Section 7.11 What is digital timestamping?)

As Per Claim 23: The rejection of claim 21 is incorporated and further Colnot, Bo et al. and Kocher do not explicitly teach:

- the data storage device coupled to the client's computer, and storing the token file, is a flash thumb drive

However the examiner is giving official notice the use of flash drives as key sources was well established in the art at the time of invention was made. It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporated the use of flash drives as potential key sources as they provide as highly expedient manner of having a portable connectable/disconnect-able device easily at the ready.

As Per Claim 26: The rejection of claim 21 is incorporated and further Colnot does not explicitly teach the following limitations however Bo et al in analogous art does teach the following limitations:

- 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

(Bo et al., Paragraph [0152], "In one example, the web server 13 is used to transfer user's personal information from the client 23 to the SRM 5 through a pre-established SSL link. The user's personal information includes user's log-in 10 and password. The user account manager 35 in the SRM 5 maintains and manages all the user's personal information.").

(Bo et al., Paragraph [0147], "The encipheror 3 or the encipheror in the encipheror/decipherer module 38 defines a block cipher algorithm, e.g., DES (data encryption standard), AES (advanced encryption standard), or Blowfish. The encipheror 3 or the encipheror in the encipheror/decipherer module 38 also defines the seeds for generating random keys, the preferred key length for the block cipher algorithm that accepts variable length keys, the preferred plaintext block size, e.g., 64 bits, 128 bits, or 256 bits. Otherwise, a default encryption strategy is to be used.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Colnot in to the method of Bo et al. in order to take advantage of being able to inexpensively add the enhancements of smart card authentication (Colnot, Paragraph [0005]). On in reverse to incorporate the teaching of Bo et al. in to the method of Colnot in order to take advantage of the authentication enhancements provided by Bo et al. (Bo et al., Paragraph [0011]).

As Per Claim 29: The rejection of claim 21 is incorporated and further Colnot does not explicitly teach the following limitations however Bo et al in analogous art does teach the following limitations:

- the software applet is a Java applet and the secure data record token is a Java archive

(Bo et al., Paragraphs [0242]-[0243], "c) With the agreement of the user, an application of the client 23 is downloaded from the web server 13 as S27 shows. The application is, for example, a Java applet. The user installs the application on the end station as S28 shows. Thus, the application of the client 23 is implemented.

d) With the agreement of the user, the application of the client 23 establishes an SSL connection (an SSL link) with the web server 13 for further transactions as 829 shows.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Colnot in to the method of Bo et al. in order to take advantage of being able to inexpensively add the enhancements of smart card authentication (Colnot, Paragraph [0005]). On in reverse to incorporate the teaching of Bo et al. in to the method of Colnot in order to take advantage of the authentication enhancements provided by Bo et al. (Bo et al., Paragraph [0011]).

As Per Claim 52: Colnot teaches: **A method enabling secure transacting over a network comprising:**

(b) executing the applet at the client, retrieving a token file from a data storage device coupled to the client appliance, the token file comprising an encrypted text string;

(Colnot, Drawings, Figure. 1.)

(Colnot, Paragraphs [0011]-[0014], "The method, as detailed in FIG. 1, carries out the user authentication on the Internet. The apparatus comprises a smart card with a modulation output, a card reader plugged into the microphone input, and a PC applet. The user inserts his card in the reader and enters his password on the PC keyboard.

When activated in the card reader, the smart card transmits an identification sequence to the PC in the form of a modulated signal, which is demodulated by the PC applet. The identification sequence comprises an 8-byte card number and an 8-byte random number valid only once. The card number is unique and identifies the card issuer,

application version and user account. The random number is a session key (Ki) which is a function of the previous one (Ki-1) emitted by the card such as: Ki=G (Ki-1), G is a one-way function also known by the authentication server.

The session key (Ki) is used by the PC applet to generate a message authentication code (MAC) of the password entered by the user, using the DES algorithm for instance. This first MAC is transmitted to the authentication server along with the card number, allowing the server to retrieve the previous session key (Ki-1) and the password stored in the authentication server database.

The authentication server deduces from (Ki-1) the session key used by the card, and generates a second MAC of the password stored in the database. The authentication is valid only if the first and second MAC are identical, which means the PC and the authentication server have used the same session key (Ki) to generate a MAC of the same password. If this is the case, the authentication server replaces (Ki-1) by (Ki) in the database. The session key (Ki) cannot be reused, even though the session key (Ki) has not been transmitted to the authentication server.").

Colnot does not explicitly teach the following limitations however Bo et al in analogous are does teach the following limitations:

-(a) upon a client seeking authorization from a network server, the server downloading a software applet

(Bo et al., Paragraphs [0242]-[0243], "c) With the agreement of the user, an application of the client 23 is downloaded from the web server 13 as S27 shows. The application is, for example, a Java applet. The user installs the application on the end station as S28 shows. Thus, the application of the client 23 is implemented.

d) With the agreement of the user, the application of the client 23 establishes an SSL connection (an SSL link) with the web server 13 for further transactions as S29 shows.").

(Bo et al., Paragraph [0253], "FIG. 16 shows a method of user authentication and digital audio-visual content encryption key(s) distribution. Each time a registered user wants to enjoy the services from the content provider, the user may be authenticated.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Colnot in to the method of Bo et al. in order to take advantage of being able to inexpensively add the enhancements of smart card authentication (Colnot, Paragraph [0005]). On in reverse to incorporate the teaching of Bo et al. in to the method of Colnot in order to take advantage of the authentication enhancements provided by Bo et al. (Bo et al., Paragraph [0011]).

Colnot and Bo et al. do not explicitly teach the following limitations however Kocher in analogous are does teach the following limitations:

- a timestamp of the request time to a client digital appliance;

(c) concatenating the token file and the timestamp and hashing the result, creating a secure data record;

(d) sending the secure data record to the server;

(e) comparing the secure data record to a similarly hashed result of the time stamp and token value taken from a data repository coupled to the server; and

(f) authorizing the client with a match.

(Kocher, Column 7, Lines 47-64, "If the sender identification at step 220 is satisfactory, the system proceeds to step 230, where the digital data are cryptographically timestamped using digital timestamp computation apparatus 170. In one preferred embodiment, timestamp computation involves obtaining the date and time from a trusted clock and performing a verifiable cryptographic operation on the digital document data plus the date/time (e.g., combining the hash of the digital data with the date and time, hashing the combination, and digitally signing the result using a private RSA key). As previously described, other techniques, such as the hash tree and catenate timestamping techniques described by Haber et al., may also be used. The apparatus which performs the basic timestamping operation may be, without limitation, the computer which is connected to the modem, or a smart-card or other cryptographic token connected to said

computer, or a separate timestamping device or service connected to said computer via a computer network.").

(Kocher, Column 10, Lines 32-46, "If the document was stored in encrypted form, the TTS decrypts the document (if necessary, employing a cryptographic token, networked secure decrypting system, or other decryption mechanism), optionally using a decryption key included with or in the DIV or TTL. The digital timestamp stored with the data is then cryptographically verified as appropriate for the timestamping technique. For example, a timestamp constructed using an RSA signature may be verified by operating on the timestamp with the public key corresponding to the digital signing key used by the timestamp computation apparatus 170, then verifying that the result corresponds to the cryptographic hash of the combination of the archived digital document data and time indicator. An error is returned if document retrieval or timestamp verification fails.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the trusted time stamping techniques taught by Kocher in to the method of Colnot and Bo et al. as a timestamping would be particularly helpful in enhancing the integrity of a digital key/encryption system as it provides an extra verification layer without adding a disclosure of a key. (RSA Laboratories Frequently Asked Questions About Today's Cryptography version 4.1 Section 7.11 What is digital timestamping?)

As Per Claim 53: The rejection of claim 52 is incorporated and further Colnot, Bo et al. and Kocher do not explicitly teach:

- data storage device coupled to the client's appliance, and storing the token file, is a flash thumb drive

However the examiner is giving official notice the use of flash drives as key sources was well established in the art at the time of invention was made. It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporated the use of flash drives as potential key sources as they provide as highly

expedient manner of having a portable connectable/disconnect-able device easily at the ready.

As Per Claim 54: The rejection of claim 52 is incorporated and further Colnot does not explicitly teach the following limitations however Bo et al in analogous art does teach the following limitations:

- 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

(Bo et al., Paragraph [0152], "In one example, the web server 13 is used to transfer user's personal information from the client 23 to the SRM 5 through a pre-established SSL link. The user's personal information includes user's log-in 10 and password. The user account manager 35 in the SRM 5 maintains and manages all the user's personal information.").

(Bo et al., Paragraph [0147], "The encipheror 3 or the encipheror in the encipheror/decipherer module 38 defines a block cipher algorithm, e.g., DES (data encryption standard), AES (advanced encryption standard), or Blowfish. The encipheror 3 or the encipheror in the encipheror/decipherer module 38 also defines the seeds for generating random keys, the preferred key length for the block cipher algorithm that accepts variable length keys, the preferred plaintext block size, e.g., 64 bits, 128 bits, or 256 bits. Otherwise, a default encryption strategy is to be used.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Colnot in to the method of Bo et al. in order to take advantage of being able to inexpensively add the enhancements of smart card authentication (Colnot, Paragraph [0005]). On in reverse to incorporate the teaching of Bo et al. in to the method of Colnot in order to take advantage of the authentication enhancements provided by Bo et al. (Bo et al., Paragraph [0011]).

As Per Claim 55: The rejection of claim 52 is incorporated and further Colnot does not explicitly teach the following limitations however Bo et al in analogous art does teach the following limitations:

- the software applet is a Java applet and the secure data record token is a Java archive

(Bo et al., Paragraphs [0242]-[0243], "c) With the agreement of the user, an application of the client 23 is downloaded from the web server 13 as S27 shows. The application is, for example, a Java applet. The user installs the application on the end station as S28 shows. Thus, the application of the client 23 is implemented.

d) With the agreement of the user, the application of the client 23 establishes an SSL connection (an SSL link) with the web server 13 for further transactions as S29 shows.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Colnot in to the method of Bo et al. in order to take advantage of being able to inexpensively add the enhancements of smart card authentication (Colnot, Paragraph [0005]). On in reverse to incorporate the teaching of Bo et al. in to the method of Colnot in order to take advantage of the authentication enhancements provided by Bo et al. (Bo et al., Paragraph [0011]).

Applicant's response:

The examiner seems to have found art (Kocher) that indicates that the applicant's invention is achievable, and presents the art of Kocher in a long and very detailed manner. Unfortunately Kocher does **not** read on the claim language recited.

Claim 21 quite clearly recites that the client requests authorization from the server and the server then downloads the Applet to the client along with a timestamp. **The applet executes at the client. The client retrieves the token from the data storage device, concatenates the token file and the time stamp, hashes the result creating the secure data record**, and **sends the secure data record to the server**. The server, executing the software driver, compares the secure data record (created at the client using the downloaded applet and the time stamp of the time of the request for authorization) to

a similarly hashed result of the time stamp and token value taken from the data repository coupled to the server, authorizing the client with a match.

Kocher just doesn't do most of that. It is important in the claimed invention that the secure data record is created at the client using the applet and time stamp from the server. The server also creates one using the same ingredients. Authorization (also not a function in Kocher) is a matter of the data records being independently created by the server and the client machine, and the data records matching. This is simply not in Kocher, and cannot be inferred from Kocher. In Kocher, any similar data record involving a token and time stamp is just created at the server side, not the sender side, and there is no comparison of independently-created data records, as claimed.

21. (Previously presented) A system enabling secure transacting over a network comprising:

a network server having an application storing client information and configured to activate a client for secure transacting in the network, the client connecting to the server through a network-connected digital appliance;

a software driver configured to perform authentication, the software driver accessible to and executable by the network server application;

a software applet configured to create a secure data record and for managing transmission and update of the contents of the record; and

a token comprising an encrypted text string, the token stored on a data storage device coupled to the client's digital appliance, and also in a data repository coupled to the server;

wherein, upon a client seeking authorization from the server, the server downloads the software applet and a timestamp of the request time to the client, the applet executes at the client, retrieves the token from the data storage device, concatenates the token file and the time stamp, hashes the result creating the secure data record, sends the secure data record to the server, and the server, executing the software driver, compares the secure data record to a similarly hashed result of the time stamp and

token value taken from the data repository coupled to the server, authorizing the client with a match.

Claim 21 is thus clearly patentable over the combination of Colnot, Bo and Kocher. Claim 52 limited identically to claim 21 is patentable by the same reasoning. Claims 23, 26 and 29 depended from patentable claim 21, and claims 53-55 depended from claim 52 are thus patentable on their merits, or at least as depended from a patentable claim.

Summary

As all of the claims, as amended and argued above, have been shown to be patentable over the art presented by the Examiner, applicant respectfully requests reconsideration and the case be passed quickly to issue.

If any fees are due beyond fees paid with this amendment, authorization is made to deduct those fees from deposit account 50-0534. If any time extension is needed beyond any extension requested with this amendment, such extension is hereby requested.

Respectfully Submitted,
Vincent Cedric Colnot

By /Donald R. Boys/
Donald R. Boys
Reg. No. 35,074

Central Coast Patent Agency, Inc.
3 Hangar Way, Suite D
Watsonville, CA 95076
(831) 768-1755

PTO/SB/22 (10-08)
Approved for use through 10/31/2008. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARMENT OF COMMERCE
Under the paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless if displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a) **FY 2009** (*Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).*)	Docket Number (Optional) P1987
Application Number 11/533,030	Filed 09/19/2006
For Vincent Cedric Colnot	
Art Unit 2434	Examiner Benjamin A. Kaplan

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

		Fee	Small Entity Fee	
☐	One month (37 CFR 1.17(a)(1))	$130	$65	$
☑	Two months (37 CFR 1.17(a)(2))	$490	$245	$ 245.00
☐	Three months (37 CFR 1.17(a)(3))	$1110	$555	$
☐	Four months (37 CFR 1.17(a)(4))	$1730	$865	$
☐	Five months (37 CFR 1.17(a)(5))	$2350	$1175	$

☑ Applicant claims small entity status. See 37 CFR 1.27.

☐ A check in the amount of the fee is enclosed.

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

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 50-0534.

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

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest. See 37 CFR 3.71.
Statement under 37 CFR 3.73(b) is enclosed (Form PTO/SB/96).

☑ attorney or agent of record. Registration Number 35,074

☐ attorney or agent under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34 _____

/Donald R. Boys/ — Signature

04/20/2011 — Date

Donald R. Boys — Typed or printed name

831-768-1755 — Telephone Number

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

☐ Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.136(a). 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 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Electronic Patent Application Fee Transmittal

Application Number:	11533030
Filing Date:	19-Sep-2006
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

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 2 months with $0 paid	2252	1	245	245

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
		Total in USD ($)		**245**

Electronic Acknowledgement Receipt

EFS ID:	9921008
Application Number:	11533030
International Application Number:	
Confirmation Number:	3809
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
Receipt Date:	20-APR-2011
Filing Date:	19-SEP-2006
Time Stamp:	15:52:22
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$245
RAM confirmation Number	2391
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	Amendment/Req. Reconsideration-After Non-Final Reject	P1987oar3.pdf	183535 1a0529a2e0d556239ef9e8e21e92b5d7333b363b	no	21
Warnings:					
Information:					
2	Extension of Time	Extension.pdf	201638 45502bc4e6672dd4ae5c04f2d1376ed430203bda	no	1
Warnings:					
Information:					
3	Fee Worksheet (PTO-875)	fee-info.pdf	30483 3becdc79af7586f043617730c34e52e56704a621	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	415656		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

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

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
11/533,030	09/19/2006	

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)	SMALL ENTITY ☒		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	04/20/2011	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 8	Minus	** 20	= 0	X $26 =	0	OR	X $ =	
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $110 =	0	OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

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

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

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

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

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

Legal Instrument Examiner:
/TONI HAKIM/

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE
COMMISSIONER FOR PATENTS
P.O.BOX 1450
ALEXANDRIA VA 22313-1451

PRESORTED
FIRST-CLASS MAIL
U.S. POSTAGE PAID
POSTEDIGITAL
NNNNN

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

Courtesy Reminder for
Application Serial No: 11/533,030

Attorney Docket No: P1987
Customer Number: 24739
Date of Electronic Notification: 11/23/2010

This is a courtesy reminder that new correspondence is available for this application. The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

An email notification regarding the correspondence was sent to the following email address(es) associated with your customer number:

anantha@formulateip.com
officeactions@CENTRALCOASTPATENT.COM
plambuth@centralcoastpatent.com

Please verify that these email addresses are correct.

To view your correspondence online or update your email addresses, please visit us anytime at **https://sportal.uspto.gov/secure/myportal/privatepair.** If you have any questions, please email the Electronic Business Center (EBC) at EBC@uspto.gov or call 1-866-217-9197.

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/533,030	09/19/2006	Vincent Cedric Colnot	P1987	3809

24739 7590 11/23/2010

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

EXAMINER	
KAPLAN, BENJAMIN A	
ART UNIT	PAPER NUMBER
2434	

NOTIFICATION DATE	DELIVERY MODE
11/23/2010	ELECTRONIC

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

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

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

officeactions@CENTRALCOASTPATENT.COM
plambuth@centralcoastpatent.com
anantha@formulateip.com

Office Action Summary	Application No.	Applicant(s)	
	11/533,030	COLNOT, VINCENT CEDRIC	
	Examiner	Art Unit	
	BENJAMIN A. KAPLAN	2434	

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

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

Status

1)☒ Responsive to communication(s) filed on *01 March 2010*.

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

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

Disposition of Claims

4)☒ Claim(s) *21,23,26,29 and 52-55* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *21,23,26,29 and 52-55* is/are rejected.

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

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

Application Papers

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

10)☒ The drawing(s) filed on *19 September 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

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

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

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

Priority under 35 U.S.C. § 119

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

a)☐ All b)☐ Some * c)☐ None of:

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

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

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

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

Attachment(s)

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

DETAILED ACTION

1. This Office Action is responsive to the most recent papers filed on 9/27/2010.

2. Claims 21-51 are rejected.

Continued Examination Under 37 CFR 1.114

3. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 9/27/2010 has been entered.

Response to Arguments and Amendments

4. The rejections of canceled claims are moot in view of their cancelation.

5. The rejection of claims 21-34 under 35 U.S.C. § 112 is withdrawn.

6. Applicant's arguments that Colnot and Bo et al. do not teach the amended claims as use of time stamps has been accepted new ground(s) of rejection are presented with additional teachings from United States Patent No.: US 6,188,766 B1 (Kocher).

Claim Rejections - 35 USC § 101

7. 35 U.S.C. 101 reads as follows:

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

8. Claim(s) 52, 54 & 55 fail the machine-or-transformation test which is a two-branched inquiry. It may be shown that a process claim satisfies 35 USC § 101 by showing that a claim is tied to a particular machine or by showing that a claim transforms an article into a different state or thing. See Gottschalk v. Benson, 409 U.S. 63, 67 (1972). As to the first prong (machine), the Examiner cannot find any showing that these claims are attached to a specific machine. As to the second prong (transformation), the process claims do not transform a physical article into a different state or thing. The process claims are merely manipulating abstract data without regard to any physical article or object.

Claim Rejections - 35 USC § 103

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

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claim(s) 21-34 & 41-51 is/are rejected under 35 U.S.C. 103(a) as being unpatentable over United States Patent Application Publication No.: US 20040093496 A1 (Colnot) in view of United States Patent Application Publication No.: US 2005/0262573 A1 (Bo et al.) in further view of United States Patent No.: US 6,188,766 B1 (Kocher).

As Per Claim 21: Colnot teaches: **A system enabling secure transacting over a network comprising:**

- a network server having an application storing client information and configured to activate a client for secure transacting in the network, the client connecting to the server through a network-connected digital appliance;

(Colnot, Drawings, Figure. 1. "

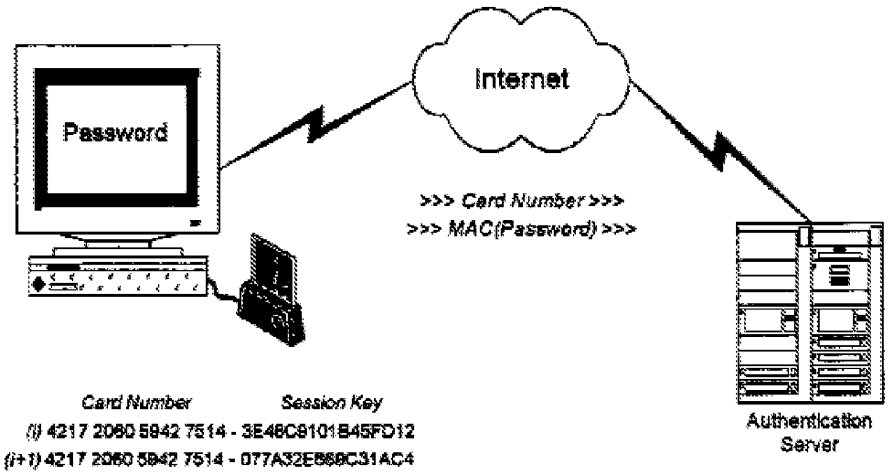


FIG. 1

").

(Colnot, Paragraphs [0011]-[0014], "The method, as detailed in FIG. 1, carries out the user authentication on the Internet. The apparatus comprises a smart card with a modulation output, a card reader plugged into the microphone input, and a PC applet. The user inserts his card in the reader and enters his password on the PC keyboard.

When activated in the card reader, the smart card transmits an identification sequence to the PC in the form of a modulated signal, which is demodulated by the PC applet. The identification sequence comprises an 8-byte card number and an 8-byte

random number valid only once. The card number is unique and identifies the card issuer, application version and user account. The random number is a session key (Ki) which is a function of the previous one (Ki-1) emitted by the card such as: Ki=G(Ki-1), G is a one-way function also known by the authentication server.

The session key (Ki) is used by the PC applet to generate a message authentication code (MAC) of the password entered by the user, using the DES algorithm for instance. This first MAC is transmitted to the authentication server along with the card number, allowing the server to retrieve the previous session key (Ki-1) and the password stored in the authentication server database.

The authentication server deduces from (Ki-1) the session key used by the card, and generates a second MAC of the password stored in the database. The authentication is valid only if the first and second MAC are identical, which means the PC and the authentication server have used the same session key (Ki) to generate a MAC of the same password. If this is the case, the authentication server replaces (Ki-1) by (Ki) in the database. The session key (Ki) cannot be reused, even though the session key (Ki) has not been transmitted to the authentication server.").

- a token comprising an encrypted text string, the token stored on a data storage device coupled to connect to the client's digital appliance, and also in a data repository coupled to the server;

(Colnot, Paragraphs [0011]-[0014], "The method, as detailed in FIG. 1, carries out the user authentication on the Internet. The apparatus comprises a smart card with

a modulation output, a card reader plugged into the microphone input, and a PC applet. The user inserts his card in the reader and enters his password on the PC keyboard.

When activated in the card reader, the smart card transmits an identification sequence to the PC in the form of a modulated signal, which is demodulated by the PC applet. The identification sequence comprises an 8-byte card number and an 8-byte random number valid only once. The card number is unique and identifies the card issuer, application version and user account. The random number is a session key (Ki) which is a function of the previous one (Ki-1) emitted by the card such as: Ki=G(Ki-1), G is a one-way function also known by the authentication server.

The session key (Ki) is used by the PC applet to generate a message authentication code (MAC) of the password entered by the user, using the DES algorithm for instance. This first MAC is transmitted to the authentication server along with the card number, allowing the server to retrieve the previous session key (Ki-1) and the password stored in the authentication server database.

The authentication server deduces from (Ki-1) the session key used by the card, and generates a second MAC of the password stored in the database. The authentication is valid only if the first and second MAC are identical, which means the PC and the authentication server have used the same session key (Ki) to generate a MAC of the same password. If this is the case, the authentication server replaces (Ki-1) by (Ki) in the database. The session key (Ki) cannot be reused, even though the session key (Ki) has not been transmitted to the authentication server.").

Colnot does not explicitly teach the following limitations however Bo et al in analogous are does teach the following limitations:

- a software driver configured to perform authentication, the software driver accessible to and executable by the network server application;

- a software applet configured to create a secure data record and for managing transmission and update of the contents of the record; and

(Bo et al., Paragraphs [0242]-[0243], "c) With the agreement of the user, an application of the client 23 is downloaded from the web server 13 as S27 shows. The application is, for example, a Java applet. The user installs the application on the end station as S28 shows. Thus, the application of the client 23 is implemented.

d) With the agreement of the user, the application of the client 23 establishes an SSL connection (an SSL link) with the web server 13 for further transactions as S29 shows.").

(Bo et al., Paragraph [0253], "FIG. 16 shows a method of user authentication and digital audio-visual content encryption key(s) distribution. Each time a registered user wants to enjoy the services from the content provider, the user may be authenticated.").

The driver is the inherent underlying software that makes it possible for a system to operate with its underlying hardware and functions thereof.

- wherein upon a client seeking authorization from the server, the server downloads the software applet

(Bo et al., Paragraphs [0242]-[0243], "c) With the agreement of the user, an application of the client 23 is downloaded from the web server 13 as S27 shows. The application is, for example, a Java applet. The user installs the application on the end station as S28 shows. Thus, the application of the client 23 is implemented.

d) With the agreement of the user, the application of the client 23 establishes an SSL connection (an SSL link) with the web server 13 for further transactions as S29 shows.").

(Bo et al., Paragraph [0253], "FIG. 16 shows a method of user authentication and digital audio-visual content encryption key(s) distribution. Each time a registered user wants to enjoy the services from the content provider, the user may be authenticated.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Colnot in to the method of Bo et al. in order to take advantage of being able to inexpensively add the enhancements of smart card authentication (Colnot, Paragraph [0005]). On in reverse to incorporate the teaching of Bo et al. in to the method of Colnot in order to take advantage of the authentication enhancements provided by Bo et al. (Bo et al., Paragraph [0011]).

Colnot and Bo et al. do not explicitly teach the following limitations however Kocher in analogous are does teach the following limitations:

- the server downloads a timestamp of the request time to the client, the applet executes at the client, retrieves the token from the data storage device, concatenates the token file and the time stamp, hashes the result creating the

secure data record, sends the secure data record to the server, and the server, executing the software driver, compares the secure data record to a similarly hashed result of the time stamp and token value taken from the data repository coupled to the server, authorizing the client with a match.

(Kocher, Column 7, Lines 47-64, "If the sender identification at step 220 is satisfactory, the system proceeds to step 230, where the digital data are cryptographically timestamped using digital timestamp computation apparatus 170. In one preferred embodiment, timestamp computation involves obtaining the date and time from a trusted clock and performing a verifiable cryptographic operation on the digital document data plus the date/time (e.g., combining the hash of the digital data with the date and time, hashing the combination, and digitally signing the result using a private RSA key). As previously described, other techniques, such as the hash tree and catenate timestamping techniques described by Haber et al., may also be used. The apparatus which performs the basic timestamping operation may be, without limitation, the computer which is connected to the modem, or a smart-card or other cryptographic token connected to said computer, or a separate timestamping device or service connected to said computer via a computer network.").

(Kocher, Column 10, Lines 32-46, "If the document was stored in encrypted form, the TTS decrypts the document (if necessary, employing a cryptographic token, networked secure decrypting system, or other decryption mechanism), optionally using a decryption key included with or in the DIV or TTI. The digital timestamp stored with the data is then cryptographically verified as appropriate for the timestamping technique.

For example, a timestamp constructed using an RSA signature may be verified by operating on the timestamp with the public key corresponding to the digital signing key used by the timestamp computation apparatus 170, then verifying that the result corresponds to the cryptographic hash of the combination of the archived digital document data and time indicator. An error is returned if document retrieval or timestamp verification fails.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the trusted time stamping techniques taught by Kocher in to the method of Colnot and Bo et al. as a timestamping would be particularly helpful in enhancing the integrity of a digital key/encryption system as it provides an extra verification layer without adding a disclosure of a key. (RSA Laboratories Frequently Asked Questions About Today's Cryptography version 4.1 Section 7.11 What is digital timestamping?)

As Per Claim 23: The rejection of claim 21 is incorporated and further Colnot, Bo et al. and Kocher do not explicitly teach:

- the data storage device coupled to the client's computer, and storing the token file, is a flash thumb drive

However the examiner is giving official notice the use of flash drives as key sources was well established in the art at the time of invention was made. It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporated the use of flash drives as potential key sources as they provide as highly

expedient manner of having a portable connectable/disconnect-able device easily at the ready.

As Per Claim 26: The rejection of claim 21 is incorporated and further Colnot does not explicitly teach the following limitations however Bo et al in analogous art does teach the following limitations:

- 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

(Bo et al., Paragraph [0152], "In one example, the web server 13 is used to transfer user's personal information from the client 23 to the SRM 5 through a pre-established SSL link. The user's personal information includes user's log-in ID and password. The user account manager 35 in the SRM 5 maintains and manages all the user's personal information.").

(Bo et al., Paragraph [0147], "The encipheror 3 or the encipheror in the encipheror/decipherer module 38 defines a block cipher algorithm, e.g., DES (data encryption standard), AES (advanced encryption standard), or Blowfish. The encipheror 3 or the encipheror in the encipheror/decipherer module 38 also defines the seeds for generating random keys, the preferred key length for the block cipher algorithm that accepts variable length keys, the preferred plaintext block size, e.g., 64 bits, 128 bits, or 256 bits. Otherwise, a default encryption strategy is to be used.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Colnot in to the method of Bo et al. in

order to take advantage of being able to inexpensively add the enhancements of smart card authentication (Colnot, Paragraph [0005]). On in reverse to incorporate the teaching of Bo et al. in to the method of Colnot in order to take advantage of the authentication enhancements provided by Bo et al. (Bo et al., Paragraph [0011]).

As Per Claim 29: The rejection of claim 21 is incorporated and further Colnot does not explicitly teach the following limitations however Bo et al in analogous art does teach the following limitations:

- the software applet is a Java applet and the secure data record token is a Java archive

(Bo et al., Paragraphs [0242]-[0243], "c) With the agreement of the user, an application of the client 23 is downloaded from the web server 13 as S27 shows. The application is, for example, a Java applet. The user installs the application on the end station as S28 shows. Thus, the application of the client 23 is implemented.

d) With the agreement of the user, the application of the client 23 establishes an SSL connection (an SSL link) with the web server 13 for further transactions as S29 shows.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Colnot in to the method of Bo et al. in order to take advantage of being able to inexpensively add the enhancements of smart card authentication (Colnot, Paragraph [0005]). On in reverse to incorporate the

teaching of Bo et al. in to the method of Colnot in order to take advantage of the authentication enhancements provided by Bo et al. (Bo et al., Paragraph [0011]).

As Per Claim 52: Colnot teaches: **A method enabling secure transacting over a network comprising:**

(b) executing the applet at the client, retrieving a token file from a data storage device coupled to the client appliance, the token file comprising an encrypted text string;

(Colnot, Drawings, Figure. 1. "

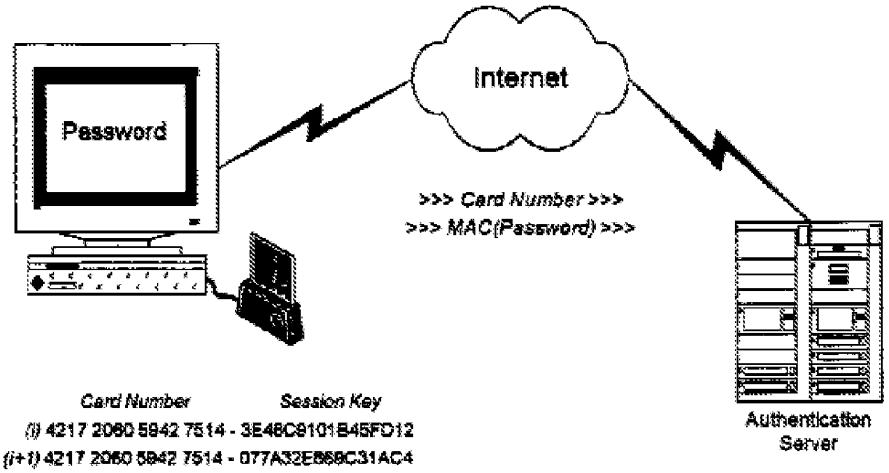


FIG. 1

").

(Colnot, Paragraphs [0011]-[0014], "The method, as detailed in FIG. 1, carries out the user authentication on the Internet. The apparatus comprises a smart card with a modulation output, a card reader plugged into the microphone input, and a PC applet. The user inserts his card in the reader and enters his password on the PC keyboard.

When activated in the card reader, the smart card transmits an identification sequence to the PC in the form of a modulated signal, which is demodulated by the PC applet. The identification sequence comprises an 8-byte card number and an 8-byte random number valid only once. The card number is unique and identifies the card issuer, application version and user account. The random number is a session key (Ki) which is a function of the previous one (Ki-1) emitted by the card such as: Ki=G(Ki-1), G is a one-way function also known by the authentication server.

The session key (Ki) is used by the PC applet to generate a message authentication code (MAC) of the password entered by the user, using the DES algorithm for instance. This first MAC is transmitted to the authentication server along with the card number, allowing the server to retrieve the previous session key (Ki-1) and the password stored in the authentication server database.

The authentication server deduces from (Ki-1) the session key used by the card, and generates a second MAC of the password stored in the database. The authentication is valid only if the first and second MAC are identical, which means the PC and the authentication server have used the same session key (Ki) to generate a MAC of the same password. If this is the case, the authentication server replaces (Ki-1) by (Ki) in the database. The session key (Ki) cannot be reused, even though the session key (Ki) has not been transmitted to the authentication server.").

Colnot does not explicitly teach the following limitations however Bo et al in analogous are does teach the following limitations:

-(a) upon a client seeking authorization from a network server, the server downloading a software applet

(Bo et al., Paragraphs [0242]-[0243], "c) With the agreement of the user, an application of the client 23 is downloaded from the web server 13 as S27 shows. The application is, for example, a Java applet. The user installs the application on the end station as S28 shows. Thus, the application of the client 23 is implemented.

d) With the agreement of the user, the application of the client 23 establishes an SSL connection (an SSL link) with the web server 13 for further transactions as S29 shows.").

(Bo et al., Paragraph [0253], "FIG. 16 shows a method of user authentication and digital audio-visual content encryption key(s) distribution. Each time a registered user wants to enjoy the services from the content provider, the user may be authenticated.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Colnot in to the method of Bo et al. in order to take advantage of being able to inexpensively add the enhancements of smart card authentication (Colnot, Paragraph [0005]). On in reverse to incorporate the teaching of Bo et al. in to the method of Colnot in order to take advantage of the authentication enhancements provided by Bo et al. (Bo et al., Paragraph [0011]).

Colnot and Bo et al. do not explicitly teach the following limitations however Kocher in analogous are does teach the following limitations:

- a timestamp of the request time to a client digital appliance;

(c) concatenating the token file and the timestamp and hashing the result, creating a secure data record;

(d) sending the secure data record to the server;

(e) comparing the secure data record to a similarly hashed result of the time stamp and token value taken from a data repository coupled to the server; and

(f) authorizing the client with a match.

(Kocher, Column 7, Lines 47-64, "If the sender identification at step 220 is satisfactory, the system proceeds to step 230, where the digital data are cryptographically timestamped using digital timestamp computation apparatus 170. In one preferred embodiment, timestamp computation involves obtaining the date and time from a trusted clock and performing a verifiable cryptographic operation on the digital document data plus the date/time (e.g., combining the hash of the digital data with the date and time, hashing the combination, and digitally signing the result using a private RSA key). As previously described, other techniques, such as the hash tree and catenate timestamping techniques described by Haber et al., may also be used. The apparatus which performs the basic timestamping operation may be, without limitation, the computer which is connected to the modem, or a smart-card or other cryptographic token connected to said computer, or a separate timestamping device or service connected to said computer via a computer network.").

(Kocher, Column 10, Lines 32-46, "If the document was stored in encrypted form, the TTS decrypts the document (if necessary, employing a cryptographic token, networked secure decrypting system, or other decryption mechanism), optionally using

a decryption key included with or in the DIV or TTI. The digital timestamp stored with the data is then cryptographically verified as appropriate for the timestamping technique. For example, a timestamp constructed using an RSA signature may be verified by operating on the timestamp with the public key corresponding to the digital signing key used by the timestamp computation apparatus 170, then verifying that the result corresponds to the cryptographic hash of the combination of the archived digital document data and time indicator. An error is returned if document retrieval or timestamp verification fails.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the trusted time stamping techniques taught by Kocher in to the method of Colnot and Bo et al. as a timestamping would be particularly helpful in enhancing the integrity of a digital key/encryption system as it provides an extra verification layer without adding a disclosure of a key. (RSA Laboratories Frequently Asked Questions About Today's Cryptography version 4.1 Section 7.11 What is digital timestamping?)

As Per Claim 53: The rejection of claim 52 is incorporated and further Colnot, Bo et al. and Kocher do not explicitly teach:

- data storage device coupled to the client's appliance, and storing the token file, is a flash thumb drive

However the examiner is giving official notice the use of flash drives as key sources was well established in the art at the time of invention was made. It would have been

obvious to one of ordinary skill in the art at the time of invention was made to incorporated the use of flash drives as potential key sources as they provide as highly expedient manner of having a portable connectable/disconnect-able device easily at the ready.

As Per Claim 54: The rejection of claim 52 is incorporated and further Colnot does not explicitly teach the following limitations however Bo et al in analogous art does teach the following limitations:

- 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

(Bo et al., Paragraph [0152], "In one example, the web server 13 is used to transfer user's personal information from the client 23 to the SRM 5 through a pre-established SSL link. The user's personal information includes user's log-in ID and password. The user account manager 35 in the SRM 5 maintains and manages all the user's personal information.").

(Bo et al., Paragraph [0147], "The encipheror 3 or the encipheror in the encipheror/decipherer module 38 defines a block cipher algorithm, e.g., DES (data encryption standard), AES (advanced encryption standard), or Blowfish. The encipheror 3 or the encipheror in the encipheror/decipherer module 38 also defines the seeds for generating random keys, the preferred key length for the block cipher algorithm that accepts variable length keys, the preferred plaintext block size, e.g., 64 bits, 128 bits, or 256 bits. Otherwise, a default encryption strategy is to be used.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Colnot in to the method of Bo et al. in order to take advantage of being able to inexpensively add the enhancements of smart card authentication (Colnot, Paragraph [0005]). On in reverse to incorporate the teaching of Bo et al. in to the method of Colnot in order to take advantage of the authentication enhancements provided by Bo et al. (Bo et al., Paragraph [0011]).

As Per Claim 55: The rejection of claim 52 is incorporated and further Colnot does not explicitly teach the following limitations however Bo et al in analogous art does teach the following limitations:

- the software applet is a Java applet and the secure data record token is a Java archive

(Bo et al., Paragraphs [0242]-[0243], "c) With the agreement of the user, an application of the client 23 is downloaded from the web server 13 as S27 shows. The application is, for example, a Java applet. The user installs the application on the end station as S28 shows. Thus, the application of the client 23 is implemented.

d) With the agreement of the user, the application of the client 23 establishes an SSL connection (an SSL link) with the web server 13 for further transactions as S29 shows.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Colnot in to the method of Bo et al. in order to take advantage of being able to inexpensively add the enhancements of smart

card authentication (Colnot, Paragraph [0005]). On in reverse to incorporate the teaching of Bo et al. in to the method of Colnot in order to take advantage of the authentication enhancements provided by Bo et al. (Bo et al., Paragraph [0011]).

Conclusion

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BENJAMIN A. KAPLAN whose telephone number is (571)-270-3170. The examiner can normally be reached on 7:30 a.m. - 5:00 p.m. E.S.T..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. 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.

/Benjamin A Kaplan/
Examiner, Art Unit 2434

/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2434

Notice of References Cited	Application/Control No. 11/533,030	Applicant(s)/Patent Under Reexamination COLNOT, VINCENT CEDRIC	
	Examiner BENJAMIN A. KAPLAN	Art Unit 2434	Page 1 of 1

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-			
	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	Author: RSA Laboratories Title: RSA Laboratories' Frequently Asked Questions About Today's Cryptography, Version 4.1 Year: 2000 Publisher: RSA Security Inc.
	V	INSTITUTE FOR MONETARY AND ECONOMIC STUDIES The Security Evaluation of Time Stamping Schemes: The Present Situation and Studies Masashi UNE Discussion Paper No. 2001-E-18 December 2001
	W	
	X	

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

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11533030	COLNOT, VINCENT CEDRIC
	Examiner	Art Unit
	BENJAMIN A KAPLAN	2434

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

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

CLAIM		DATE								
Final	Original	08/28/2009	05/22/2010	11/18/2010						
	1	✓	-	-						
	2	✓	-	-						
	3	✓	-	-						
	4	✓	-	-						
	5	✓	-	-						
	6	✓	-	-						
	7	✓	-	-						
	8	✓	-	-						
	9	✓	-	-						
	10	✓	-	-						
	11	✓	-	-						
	12	✓	-	-						
	13	✓	-	-						
	14	✓	-	-						
	15	✓	-	-						
	16	✓	-	-						
	17	✓	-	-						
	18	✓	-	-						
	19	✓	-	-						
	20	✓	-	-						
	21		✓	✓						
	22		✓	-						
	23		✓	✓						
	24		✓	-						
	25		✓	-						
	26		✓	✓						
	27		✓	-						
	28		✓	-						
	29		✓	✓						
	30		✓	-						
	31		✓	-						
	32		✓	-						
	33		✓	-						
	34		✓	-						
	35		✓	-						
	36		✓	-						

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11533030	COLNOT, VINCENT CEDRIC
	Examiner	Art Unit
	BENJAMIN A KAPLAN	2434

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

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

CLAIM		DATE								
Final	Original	08/28/2009	05/22/2010	11/18/2010						
	37		✓	-						
	38		✓	-						
	39		✓	-						
	40		✓	-						
	41		✓	-						
	42		✓	-						
	43		✓	-						
	44		✓	-						
	45		✓	-						
	46		✓	-						
	47		✓	-						
	48		✓	-						
	49		✓	-						
	50		✓	-						
	51		✓	-						
	52			✓						
	53			✓						
	54			✓						
	55			✓						

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	1	11/533,030.app.	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/18 13:57
S2	296	(("20010037461") or ("20010042124") or ("20020031225") or ("20020099940") or ("20020099942") or ("20020191765") or ("20030009676") or ("20030009692") or ("20030033545") or ("20030056096") or ("20030065919") or ("20030100371") or ("20030126457") or ("20030169713") or ("20030177354") or ("20030233450") or ("20030233583") or ("20040054794") or ("20040127279") or ("20040133789") or ("20040218897") or ("20050010777") or ("20050021613") or ("20050233811") or ("20060006230") or ("20060059265") or ("20060112213") or ("20060155601") or ("20060161775") or ("20060205394") or ("20060272023") or ("20060288407") or ("20070022469") or ("20070067833") or ("20070098175") or ("20070130334") or ("20070190975") or ("20070232355") or ("20070282909") or ("20080177998") or ("20090125717") or ("20090150977") or ("20090198996") or	US-PGPUB; USPAT; USOCR	OR	OFF	2009/08/27 18:23

("4295155") or
("4386233") or
("4423287") or
("4755940") or
("4783798") or
("4888801") or
("4890323") or
("4897875") or
("4905766") or
("4910773") or
("4956862") or
("4997288") or
("5008936") or
("5016277") or
("5022076") or
("5202921") or
("5204961") or
("5210794") or
("5210795") or
("5226079") or
("5237614") or
("5239294") or
("5241594") or
("5261002") or
("5272754") or
("5276735") or
("5311596") or
("5313521") or
("5347387") or
("5349643") or
("5353353") or
("5369705") or
("5371794") or
("5410602") or
("5412726") or
("5425130") or
("5444780") or
("5454000") or
("5469507") or
("5479341") or
("5481613") or
("5485196") or
("5491752") or
("5499297") or
("5500897") or
("5502766") or
("5535276") or
("5557686") or
("5587809") or
("5588060") or
("5590196") or
("5590199") or
("5590200") or
("5592555") or

		("5598459") or ("5602915") or ("5602918") or ("5604663") or ("5604803") or ("5619657") or ("5623601") or ("5633933") or ("5633934") or ("5638448") or ("5643086") or ("5655077") or ("5657390") or ("5666412") or ("5668877") or ("5671279") or ("5673318") or ("5675651") or ("5684950") or ("5687235") or ("5689566") or ("5692400") or ("5699513") or ("5719941") or ("5721779") or ("5724168") or ("5724423") or ("5729594") or ("5732137") or ("5734718") or ("5742756") or ("5745574") or ("5745576") or ("5748736") or ("5754659") or ("5757913") or ("5757918") or ("5764890") or ("5768378") or ("5778065") or ("5778071") or ("5778313")).PN. or (("5781550") or ("5781724") or ("5784463") or ("5787172") or ("5790669") or ("5796833") or ("5799082") or ("5802178") or ("5802497") or ("5805712") or ("5805803") or ("5809117") or					

("5812664") or
("5812669") or
("5812764") or
("5812955") or
("5818936") or
("5822431") or
("5825300") or
("5825877") or
("5825890") or
("5828832") or
("5832209") or
("5832228") or
("5841120") or
("5841864") or
("5850442") or
("5850445") or
("5864665") or
("5870473") or
("5870475") or
("5870544") or
("5872915") or
("5875296") or
("5875394") or
("5875395") or
("5883956") or
("5887063") or
("5887250") or
("5889861") or
("5892829") or
("5892838") or
("5892902") or
("5894552") or
("5903721") or
("5907620") or
("5909491") or
("5913175") or
("5918228") or
("5922074") or
("5923756") or
("5926624") or
("5930362") or
("5931947") or
("5947571") or
("5953422") or
("5963644") or
("5963915") or
("5966441") or
("5967466") or
("5970144") or
("5974144") or
("5978475") or
("5978918") or
("5983350") or
("5995624") or

("5996077") or
("6002767") or
("6009524") or
("6012144") or
("6012632") or
("6017004") or
("6021497") or
("6023764") or
("6026167") or
("6026293") or
("6032150") or
("6032260") or
("6038551") or
("6038892") or
("6044155") or
("6044468") or
("6047072") or
("6047325") or
("6047572") or
("6049878") or
("6052785") or
("6055236") or
("6055636") or
("6061346") or
("6061448") or
("6061448") or
("6061449") or
("6061790") or
("6061796") or
("6061796") or
("6061799") or
("6061799") or
("6065120") or
("6067620") or
("6075860") or
("6081900") or
("6088451") or
("6098056") or
("6119233") or
("6141752") or
("6144848") or
("6148405") or
("6151590") or
("6158007") or
("6178089") or
("6185612") or
("6192474") or
("6198824") or
("6199113") or
("6202081") or
("6216231") or
("6216231") or
("6230266") or
("6233608") or

		("6233687") or ("6233688") or ("6247129") or ("6249867") or ("6249873") or ("6263313") or ("6272633") or ("6282653") or ("6301667") or ("6314468") or ("6345256") or ("6374402") or ("6389403") or ("6389538") or ("6418421") or ("6438600") or ("6449367") or ("6453416") or ("6463537") or ("6678826") or ("6732105") or ("6763370") or ("6907530") or ("6912653") or ("6945870") or ("6973566") or ("7017188") or ("7028182") or ("7073055") or ("7100054")).PN. or (("7103770") or ("7152160") or ("7171467") or ("7184999") or ("7188179") or ("7231025") or ("7287271") or ("7496950") or ("7502928") or ("7509119") or ("7533735")).PN.				
S3	300	(("20010034716") or ("20020014054") or ("20020017079") or ("20020020752") or ("20020032746") or ("20020036114") or ("20020052797") or ("20020073036") or ("20020077992") or ("20020091646") or ("20020103857") or ("20020116274") or ("20020141576") or	US-PGPUB; USPAT; USOCR	OR	OFF	2009/08/27 18:24

("20020157019") or
("20020178364") or
("20020191790") or
("20030014669") or
("20030018916") or
("20030023578") or
("20030028491") or
("20030046586") or
("20030046587") or
("20030046889") or
("20030055733") or
("20030056054") or
("20030056092") or
("20030061173") or
("20030061275") or
("20030061387") or
("20030061506") or
("20030065919") or
("20030081783") or
("20030088426") or
("20030097592") or
("20030100372") or
("20030111266") or
("20030115455") or
("20030126192") or
("20030126483") or
("20030163423") or
("20030163723") or
("20030177348") or
("20030177354") or
("20030182574") or
("20030188003") or
("20030188156") or
("20030188165") or
("20030191932") or
("20030208689") or
("20030221118") or
("20030226014") or
("20030226022") or
("20030229802") or
("20030233550") or
("20030236997") or
("20040002381") or
("20040020164") or
("20040065501") or
("20040068648") or
("20040068726") or
("20040073151") or
("20040083184") or
("20040083375") or
("20040088252") or
("20040089482") or
("20040095083") or
("20040098740") or

		("20040103165") or ("20040111578") or ("20040114182") or ("20040117623") or ("20040117627") or ("20040117635") or ("20040117661") or ("20040121787") or ("20040128517") or ("20040139019") or ("20040158635") or ("20040167465") or ("20040168081") or ("20040182126") or ("20040192303") or ("20040221168") or ("20040224769") or ("20040224771") or ("20040228063") or ("20040230809") or ("20040231594") or ("20040243853") or ("20050002328") or ("20050028487") or ("20050030151") or ("20050031136") or ("20050033980") or ("20050044404") or ("20050050342") or ("20050051448") or ("20050054445") or ("20050055588") or ("20050055815") or ("20050061878") or ("20050081063") or ("20050085931") or ("20050086509") or ("20050091364") or ("20050091527") or ("20050097350") or ("20050102535") or ("20050105736") or ("20050111380") or ("20050114687") or ("20050116026") or ("20050121339") or ("20050132031") or ("20050138356") or ("20050138423") or ("20050144493") or ("20050145695")).PN. or (("20050159203") or ("20050160417") or ("20050172132") or					

		("20050182938") or ("20050185647") or ("20050188251") or ("20050188731") or ("20050198461") or ("20050209006") or ("20050209842") or ("20050213768") or ("20050223220") or ("20050226175") or ("20050240685") or ("20050240712") or ("20050251685") or ("20050251852") or ("20050256806") or ("20050257245") or ("20050268336") or ("20060004964") or ("20060005072") or ("20060015947") or ("20060019657") or ("20060025147") or ("20060026573") or ("20060036693") or ("20060039305") or ("20060039306") or ("20060039321") or ("20060039339") or ("20060039340") or ("20060039360") or ("20060039562") or ("20060039563") or ("20060041750") or ("20060041761") or ("20060042882") or ("20060047784") or ("20060050887") or ("20060056630") or ("20060059543") or ("20060074983") or ("20060085370") or ("20060087192") or ("20060095377") or ("20060111165") or ("20060111794") or ("20060136742") or ("20060143700") or ("20060155589") or ("20060156019") or ("20060156399") or ("20060179308") or ("20060184524") or ("20060189382") or ("20060193474") or					

		("20060197403") or ("20060200660") or ("20060270346") or ("20070041110") or ("20070067833") or ("20070294085") or ("20080098872") or ("20080161951") or ("20080188182") or ("20080228865") or ("20080240468") or ("3683325") or ("4526115") or ("5051564") or ("5282247") or ("5406039") or ("5493767") or ("5656799") or ("5657388") or ("5695183") or ("5749253") or ("5825752") or ("6022009") or ("6038590") or ("6105042") or ("6118732") or ("6178550") or ("6209095") or ("6226697") or ("6233620") or ("6254366") or ("6282653") or ("6298336") or ("6328149") or ("6339827") or ("6382516") or ("6389541") or ("6393569") or ("6442532") or ("6502746") or ("6507908") or ("6520285") or ("6615194") or ("6620047") or ("6671810") or ("6701304") or ("6710893") or ("6722466") or ("6748532") or ("6769068") or ("6789147") or ("6823452") or ("6836795") or ("6845905") or					

		("6901251") or ("6915437") or ("6916247") or ("6920557") or ("6928707") or ("6934848") or ("6945458") or ("6957343") or ("6961759") or ("6970918") or ("6976164") or ("6976172") or ("6996841") or ("7013387") or ("7020476") or ("7024377") or ("7063615") or ("7069442") or ("7084734") or ("7085933") or ("7089587")).PN. or (("7095150") or ("7101296") or ("7103529") or ("7135968") or ("7137016") or ("7143280") or ("7146640") or ("7149821") or ("7152245") or ("7154628") or ("7155615") or ("7159242") or ("7185365") or ("7197644") or ("7207481") or ("7219480") or ("7228566") or ("7237717") or ("7245726") or ("7266703") or ("7290287") or ("7313679") or ("7333717") or ("7336789") or ("7343411") or ("7346929") or ("7350230") or ("7371952") or ("7383193") or ("7401230") or ("7418504") or ("7424610") or ("7428754") or					

		("7441153") or ("7452278") or ("7455590") or ("7458075") or ("7469341") or ("7469368") or ("7496097") or ("7502475") or ("7506170") or ("7509487") or ("7516331") or ("7530103") or ("7539651") or ("7540516") or ("7549922") or ("7574509") or ("7577258")).PN.				
S4	283	S2 @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:25
S5	285	S3 @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:25
S6	3	S4 S5	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:25
S7	29905	server client authentication @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:52
S8	21050	server client authentication key @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:52
S9	14617	server client authentication key secure @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:52
S10	4843	server client authentication key secure java @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:53
S11	2219	server client authentication key secure java applet @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:53
S12	604	server client authentication key secure java applet archive @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:53
S13	322	server client authentication key secure java applet archive sound card @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:53

S14	322	server client authentication key secure java applet archive sound card network @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:54
S15	283	server client authentication key secure java applet archive sound card network password @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:54
S16	279	server client authentication key secure java applet archive sound card network password session @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:54
S17	30	server client authentication key secure java applet archive sound card network password session seed @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:54
S18	0	server client authentication key secure java applet archive (sound adj source) @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 19:15
S19	1	server client authentication key secure java applet archive (sound same password) @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 19:17
S20	1	10/696,650.app.	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 19:26
S21	244	server client authentication key secure java applet archive (smart adj card) @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 18:48
S22	244	server client authentication key secure java applet archive (smart adj card) network @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 18:48
S23	234	server client authentication key secure java applet archive (smart adj card) network password @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 18:48

S24	225	server client authentication key secure java applet archive (smart adj card) network password session @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 18:49
S25	27	server client authentication key secure java applet archive (smart adj card) network password session seed @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 18:49
S26	1546	(726/2).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2009/08/28 20:32
S27	694	(726/9).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2009/08/28 20:32
S28	2232	(726/26).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2009/08/28 20:32
S29	1545	(726/27).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2009/08/28 20:32
S30	1033	S26 @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 20:32
S31	453	S27 @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 20:32
S32	1688	S28 @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 20:32
S33	1050	S29 @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 20:32
S34	1	S30 S31 S32 S33	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 20:33
S35	3732	S30 or S31 or S32 or S33	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 20:33
S36	1446	key source flash thumb drive @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/05/21 17:21
S37	0	(key adj source) (flash adj thumb adj drive) @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/05/21 17:21

S38	0	(key adj source) (thumb adj drive) @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/05/21 17:21
S39	3	(key adj source) (flash adj drive) @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/05/21 17:21
S40	128	(key) same (flash adj drive) @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/05/21 17:23
S41	6623	(726/2,9,26,27).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2010/05/22 19:21
S42	4273	S41 @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/05/22 19:21
S43	538	S42 @pd>"20090824"	US-PGPUB; USPAT; USOCR	AND	ON	2010/05/22 19:21
S44	15	(key) same (flash adj drive) (time adj stamp) @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/16 17:44
S45	34820	time adj stamp @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/16 17:45
S46	4062	time adj stamp hash @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/16 17:51
S47	954	(time adj stamp) same hash @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/16 17:51
S48	12	(key) same (flash adj drive) (time adj stamp) hash @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/16 17:51
S49	12	S47 S48	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/16 17:52
S50	195	((time adj stamp) same hash) (java or applet) @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/16 17:59
S51	5	((time adj stamp) same hash) (java or applet) concatenate @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/16 18:01
S52	12	(key) same (flash adj drive) (time adj stamp) hash @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/17 18:37

S53	200	Trusted timestamping @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/17 19:43
S54	8	Trusted adj timestamping @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/17 19:43
S55	4062	hash (time adj stamp) hash @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/17 19:48
S56	954	hash same (time adj stamp) hash @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/17 19:48
S57	130	hash near (time adj stamp) hash @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/17 19:48
S58	442	data same hash same (time adj stamp) hash @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/17 19:49
S59	2	data near hash near (time adj stamp) hash @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/17 19:50
S60	1	("7716488").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2010/11/17 19:56
S61	442	data same hash same (time adj stamp) hash @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/18 18:12
S62	129	hash near (time adj stamp) data @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/18 19:41
S63	130	hash near (time adj stamp) @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/18 19:42
S64	2027	hash secure data timestamp @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/18 20:03
S65	894	hash secure data timestamp token @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/18 20:03
S66	3	(hash secure data timestamp token) and @ad<"20050920"	US-PGPUB; USPAT; USOCR	SAME	ON	2010/11/18 20:03
S67	7571	(726/2,9,26,27).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2010/11/18 21:27
S68	4570	S67 @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/18 21:27

S69	297	S68 @pd>"20100518"	US-PGPUB; USPAT; USOCR	AND	ON	2010/11/18 21:27

EAST Search History (Interference)

<This search history is empty>

11/18/2010 9:35:09 PM
C:\Documents and Settings\bkaplan\My Documents\EAST\Workspaces\11533030.wsp

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11533030	COLNOT, VINCENT CEDRIC
	Examiner	Art Unit
	BENJAMIN A KAPLAN	2434

SEARCHED			
Class	Subclass	Date	Examiner
726	2,9,26,27	11/18/2010	BK

SEARCH NOTES		
Search Notes	Date	Examiner
East, Plus Search, Google	11/18/2010	BK

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

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

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

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

Application Number	11/533,030	Filing Date	2006-09-19	Docket Number (if applicable)	P1987	Art Unit	2434
First Named Inventor	Vincent Cedric Colnot			Examiner Name	Benjamin A. Kaplan		

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

SUBMISSION REQUIRED UNDER 37 CFR 1.114

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

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

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

☐ Other _____

☒ Enclosed

☒ Amendment/Reply

☐ Information Disclosure Statement (IDS)

☐ Affidavit(s)/ Declaration(s)

☐ Other _____

MISCELLANEOUS

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

☐ Other _____

FEES

☒ **The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**
The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No 500534

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature

☐ Applicant Signature

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

Signature of Registered U.S. Patent Practitioner			
Signature	/Donald R. Boys/	Date (YYYY-MM-DD)	2010-09-27
Name	Donald R. Boys	Registration Number	35074

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

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

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

PTO/SB/22 (10-08)
Approved for use through 10/31/2008. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARMENT OF COMMERCE
Under the paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless if displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a) **FY 2009** ***(Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).)***	Docket Number (Optional) P1987
Application Number 11/533,030	Filed 09/19/2006
For Vincent Cedric Colnot	
Art Unit 2434	Examiner Benjamin A. Kaplan

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

	Fee	Small Entity Fee	
☑ One month (37 CFR 1.17(a)(1))	$130	$65	$ 65.00
☐ Two months (37 CFR 1.17(a)(2))	$490	$245	$
☐ Three months (37 CFR 1.17(a)(3))	$1110	$555	$
☐ Four months (37 CFR 1.17(a)(4))	$1730	$865	$
☐ Five months (37 CFR 1.17(a)(5))	$2350	$1175	$

☑ Applicant claims small entity status. See 37 CFR 1.27.

☐ A check in the amount of the fee is enclosed.

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

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 50-0534.

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

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest. See 37 CFR 3.71.
Statement under 37 CFR 3.73(b) is enclosed (Form PTO/SB/96).

☑ attorney or agent of record. Registration Number 35,074

☐ attorney or agent under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34 _____

/Donald R. Boys/ — Signature

09/27/2010 — Date

Donald R. Boys — Typed or printed name

831-768-1755 — Telephone Number

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

☐ Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.136(a). 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 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Art Unit: 2434 Examiner: Kaplan, Benjamin A

In Re:	Vincent Cedric Colnot
Case:	P1987
Serial No.:	11/533,030
Filed:	September 19, 2006
Subject:	Methods and Apparatus for Enabling Secure Network-Based Transactions

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Response B

In the Claims

All of the claims standing for examination are reproduced below with appropriate status indication.

1-20. (Canceled)

21. (Currently amended) A system enabling secure transacting over a network comprising:

a network server having an application ~~for~~ storing client information and configured to activate ~~for activating~~ a client for secure transacting in the network, the client connecting to the server through a network-connected digital appliance;

a software driver ~~for performing~~ configured to perform authentication, the software driver accessible to and executable by the network server application;

a software applet ~~for creating~~ configured to create a secure data record and for managing transmission and update of the contents of the record; and

a ~~digital key~~ token comprising an encrypted text string, the token stored on a data storage device ~~enabled to connect~~ coupled to the client's digital appliance, and also in a data repository coupled to the server;

wherein, ~~with the key source connected to the digital appliance, the key is provided to the digital appliance to be provided over the network to the server, to interact with the application for activating the client~~ upon a client seeking authorization from the server, the server downloads the software applet and a timestamp of the request time to the client, the applet executes at the client, retrieves the token from the data storage device, concatenates the token file and the time stamp, hashes the result creating the secure data record, sends the secure data record to the server, and the server, executing the software driver, compares the secure data record to a similarly hashed result of the time stamp and token value taken from the data respository coupled to the server, authorizing the client with a match.

22. (Cancelled)

23. (Currently amended) The system of claim 21 wherein the ~~key source~~ data storage device coupled to the client's computer, and storing the token file, is a flash thumb drive.

24-25. (cancelled)

26. (Currently amended) The system of claim 21, wherein the ~~secure data record~~ token is unique to a client and includes an identification number, a password or personal identification code, a session key, and a ~~secrete~~ secret data seed.

27-28. (Cancelled)

29. (Currently amended) The system of claim 21, wherein the software applet is a Java applet and the token is a Java archive.

30-51. (Cancelled)

52. (New) A method enabling secure transacting over a network comprising:

(a) upon a client seeking authorization from a network server, the server downloading a software applet and a timestamp of the request time to a client digital appliance;

(b) executing the applet at the client, retrieving a token file from a data storage device coupled to the client appliance, the token file comprising an encrypted text string;

(c) concatenating the token file and the timestamp and hashing the result, creating a secure data record;

(d) sending the secure data record to the server;

(e) comparing the secure data record to a similarly hashed result of the time stamp and token value taken from a data repository coupled to the server; and

(f) authorizing the client with a match.

53. (New) The method of claim 52 wherein data storage device coupled to the client's appliance, and storing the token file, is a flash thumb drive.

54. (New) The method of claim 52, wherein 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.

55. (New) The system of claim 52, wherein the software applet is a Java applet and the token is a Java archive.

REMARKS

This response is to the Office Action mailed on 05/28/2010.

From the action:

This is a Final Action in response to communications filed on 01 March 2010. Claims 21-51 are pending in the application. Claims 21-51 are rejected. Claims 1-20 are canceled. Claims 21-51 are new. Rejection of original claims 1-20 are moot in view of their cancelation. 35 U.S.C. § 101 rejections have not been placed on the new claims. In regards to 35 U.S.C. § 112 some issues are still present in the new claims.

Applicant's response:

Acknowledged

From the action:

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

The claims have been stated in a manner where there are not necessarily any specific features being claimed.

In independent claim 21 a system is claimed having:

an application for (some intended purpose),

a software driver for (some intended purpose), and

a software applet for (some intended purpose)

Examiner suggests changing the claim language to read:

an application ~~for storing~~ configured to store ...

a software driver ~~for performing~~ configured to perform ...

a software applet ~~for creating~~ configured to create ...

Also the concluding wherein clause in claim 21 is cut off from the rest of the claim. (See MPEP 2111.04 "Adapted to," "Adapted for," "Wherein," and "Whereby" Clauses [R-3] - 2100 Patentability) Its premise is based on "the key source" which has not been declared yet else ware in the claim. For the sake of examination it is believed that "the key source" is referring to the "key device" and has been examined as such however the connecting language will need to be clarified for consistency.

Claims 22-34 are rejected under 35 USC § 112 as being dependent on claim 21.

Applicant's response:

Applicant has amended claim 21 extensively and believes the problem is corrected in the amendment.

From the action:

Claims 35-36, 37-40 rejected under 35 U.S.C. 102(b) as being anticipated by United States Patent Application Publication No.: US 20040093496 A1 (Colnot).

As Per Claim 35: Colnot teaches: **A sound-producing device for generating a network-transmittable sound frame having embedded therein an identification number and a session key usable to authenticate a client, the device comprising:**

- a semiconductor chip supporting a modem;

(Colnot, Paragraph [0123], "The DRM-system's elements described above with respect to FIG. 1 can include so-called general-purpose computers, workstations, or personal computers, as well as network connectable information-processing devices, for instance, digital home electric appliances, portable terminals, PDAs, or cellular phones.").

Network connectable devices are supporting modems of one sort or another.

- a plug-in interface for enabling coupling with a host digital appliance;

- and a housing of a size and shape to support hand-held operation.

(Colnot, Paragraph [0006], "The above object has been achieved by a smart card transmitting an identification sequence to a PC by means of a card reader plugged into the microphone input of the PC sound card. The reader is actually a simple and inexpensive connector without processing means. The smart card remains compliant with the ISO 7816 standards and can be used in the existing card readers.").

As Per Claim 36: The rejection of claim 35 is incorporated and further Colnot teaches:

- the network is the Internet network

(Colnot, Abstract, "A method and apparatus to secure online transactions on the Internet comprising 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.").

As Per Claim 38: The rejection of claim 35 is incorporated and further Colnot teaches:

- the plug-in interface is a tip/ring/sleeve interface for plugging into a microphone jack on the host digital appliance used to secure authentication

(Colnot, Paragraph [0011], "The method, as detailed in FIG. 1, carries out the user authentication on the Internet. The apparatus comprises a smart card with a modulation output, a card reader plugged into the microphone input, and a PC applet. The user inserts his card in the reader and enters his password on the PC keyboard.").

As Per Claim 39: The rejection of claim 38 is incorporated and further Colnot teaches:

- the sound-producing device derives power from a soundcard residing on the digital appliance used to secure authentication

(Colnot, Paragraph [0019], "The PC sound cards provides a +3V to +5V DC voltage on the microphone input which is sufficient to power (Vbb) the smart card. The resistor R1 adapts the level of the modulated signal to the microphone input. When

pressed, the switch 81 pulls down the reset input (Rst) activating the modulation output (Mod).").

As Per Claim 40: The rejection of claim 35 is incorporated and further Colnot teaches:

- a switch for activating the modem to generate the sound

(Colnot, Paragraph [0019], "The PC sound cards provides a +3V to +5V DC voltage on the microphone input which is sufficient to power (Vbb) the smart card. The resistor R1 adapts the level of the modulated signal to the microphone input. When pressed, the switch S1 pulls down the reset input (Rst) activating the modulation output (Mod).").

Applicant's response:

Applicant has cancelled claims 30-51 rendering these rejections moot.

From the action:

Claim(s) 21-34 & 41-51 is/are rejected under 35 U.S.C. 103(a) as being unpatentable over United States Patent Application Publication No.: US 20040093496 A1 (Colnot) in view of United States Patent Application Publication No.: US 2005/0262573 A1 (Bo et al.).

As Per Claim 21: Colnot teaches: **A system enabling secure transacting over a network comprising:**

- a network server having an application for storing client information and for activating a client for secure transacting in the network, the client connecting to the server through a network-connected digital appliance;

(Colnot, Paragraphs [0011]-[0014], "The method, as detailed in FIG. 1, carries out the user authentication on the Internet. The apparatus comprises a smart card with a modulation output, a card reader plugged into the microphone input, and a PC applet. The user inserts his card in the reader and enters his password on the PC keyboard.

When activated in the card reader, the smart card transmits an identification sequence to the PC in the form of a modulated signal, which is demodulated by the PC applet. The identification sequence comprises an 8-byte card number and an 8-byte random number valid only once. The card number is unique and identifies the card issuer, application version and user account. The random number is a session key (Ki) which is a function of the previous one (Ki-1) emitted by the card such as: Ki=G(Ki-1), G is a one-way function also known by the authentication server.

The session key (Ki) is used by the PC applet to generate a message authentication code (MAC) of the password entered by the user, using the DES algorithm for instance. This first MAC is transmitted to the authentication server along with the card number, allowing the server to retrieve the previous session key (Ki-1) and the password stored in the authentication server database.

The authentication server deduces from (Ki-1) the session key used by the card, and generates a second MAC of the password stored in the database. The authentication is valid only if the first and second MAC are identical, which means the PC and the authentication server have used the same session key (Ki) to generate a MAC of the same password. If this is the case, the authentication server replaces (Ki-1) by (Ki) in the database. The session key (Ki) cannot be reused, even though the session key (Ki) has not been transmitted to the authentication server.").

- a digital key stored on a key device enabled to connect to the client's digital appliance;

- wherein, with the key source connected to the digital appliance, the key is provided to the digital appliance to be provided over the network to the server, to interact with the application for activating the client.

(Colnot, Paragraphs [0011]-[0014], "The method, as detailed in FIG. 1, carries out the user authentication on the Internet. The apparatus comprises a smart card with a modulation output, a card reader plugged into the microphone input, and a PC applet. The user inserts his card in the reader and enters his password on the PC keyboard.

When activated in the card reader, the smart card transmits an identification sequence to the PC in the form of a modulated signal, which is demodulated by the PC applet. The identification sequence comprises an 8-byte card number and an 8-byte random number valid only once. The card number is unique and identifies the card issuer, application version and user account. The random number is a session key (Ki) which is a function of the previous one (Ki-1) emitted by the card such as: Ki=G(Ki-1), G is a one-way function also known by the authentication server.

The session key (Ki) is used by the PC applet to generate a message authentication code (MAC) of the password entered by the user, using the DES algorithm for instance. This first MAC is transmitted to the authentication server along with the card number, allowing the server to retrieve the previous session key (Ki-1) and the password stored in the authentication server database.

The authentication server deduces from (Ki-1) the session key used by the card, and generates a second MAC of the password stored in the database. The authentication is valid only if the first and second MAC are identical, which means the PC and the authentication server have used the same session key (Ki) to generate a MAC of the same password. If this is the case, the authentication server replaces (Ki-1) by (Ki) in the database. The session key (Ki) cannot be reused, even though the session key (Ki) has not been transmitted to the authentication server.").

Colnot does not explicitly teach the following limitations however B0 et al in analogous are does teach the following limitations:

- a software driver for performing authentication, the software driver accessible to the network server application;

- a software applet for creating a secure data record and for managing transmission and update of the contents of the record; and

(Bo et al., Paragraphs [0242]-[0243], "c) With the agreement of the user, an application of the client 23 is downloaded from the web server 13 as S27 shows. The

application is, for example, a Java applet. The user installs the application on the end station as S28 shows. Thus, the application of the client 23 is implemented.

d) With the agreement of the user, the application of the client 23 establishes an SSL connection (an SSL link) with the web server 13 for further transactions as S29 shows.").

(Bo et al., Paragraph [0253], "FIG. 16 shows a method of user authentication and digital audio-visual content encryption key(s) distribution. Each time a registered user wants to enjoy the services from the content provider, the user may be authenticated.").

The driver is the inherent underlying software that makes it possible for a system to operate with its underlying hardware and functions thereof.

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Colnot in to the method of Bo et al. in order to take advantage of being able to inexpensively add the enhancements of smart card authentication (Colnot, Paragraph [0005]). On in reverse to incorporate the teaching of 80 et al. in to the method of Colnot in order to take advantage of the authentication enhancements provided by Bo et al. (Bo et al., Paragraph [0011]).

As Per Claim 22: The rejection of claim 21 is incorporated and further Colnot teaches:

- the key is one of a character string, a modulated audio file, a modulated light source, an infra-red signal, or a vibratory signal

(Colnot, Paragraph [0012], "When activated in the card reader, the smart card transmits an identification sequence to the PC in the form of a modulated signal, which is demodulated by the PC applet. The identification sequence comprises an 8-byte card number and an 8-byte random number valid only once. The card number is unique and identifies the card issuer, application version and user account. The random number is a session key (Ki) which is a function of the previous one (Ki-1) emitted by the card such as: Ki=G(Ki-1), G is a one-way function also known by the authentication server.").

As Per Claim 23: The rejection of claim 21 is incorporated and further Colnot and Bo et al do not explicitly teach:

- the key source is a flash thumb drive

However the examiner is giving official notice the use of flash drives as key sources was well established in the art at the time of invention was made. It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporated the use of flash drives as potential key sources as they provide as highly expedient manner of having a portable connectable/disconnect-able device easily at the ready.

As Per Claim 24: The rejection of claim 21 is incorporated and further Col not teaches:

- the connection to the client's digital appliance is one of a USB port, a microphone jack, an infrared sensor, or a an audio microphone

(Colnot, Paragraph [0011], "The method, as detailed in FIG. 1, carries out the user authentication on the Internet. The apparatus comprises a smart card with a modulation output, a card reader plugged into the microphone input, and a PC applet. The user inserts his card in the reader and enters his password on the PC keyboard.").

As Per Claim 25: The rejection of claim 21 is incorporated and further Colnot teaches:

- the network is the Internet network

(Colnot, Abstract, "A method and apparatus to secure online transactions on the Internet comprising 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.").

As Per Claim 26: The rejection of claim 21 is incorporated and further Colnot does not explicitly teach the following limitations however Bo et al in analogous art does teach the following limitations:

- the secure data record is unique to a client and includes an identification number, a password or personal identification code, a session key, and a secrete data seed

(Bo et al., Paragraph [0152], "In one example, the web server 13 is used to transfer user's personal information from the client 23 to the SRM 5 through a pre-established SSL link. The user's personal information includes user's log-in ID and password. The user account manager 35 in the SRM 5 maintains and manages all the user's personal information.").

(Bo et al., Paragraph [0147], "The encipheror 3 or the encipheror in the encipheror/decipherer module 38 defines a block cipher algorithm, e.g., DES (data encryption standard), AES (advanced encryption standard), or Blowfish. The encipheror 3 or the encipheror in the encipheror/decipherer module 38 also defines the seeds for generating random keys, the preferred key length for the block cipher algorithm that accepts variable length keys, the preferred plaintext block size, e.g., 64 bits, 128 bits, or 256 bits. Otherwise, a default encryption strategy is to be used.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Colnot in to the method of Bo et al. in order to take advantage of being able to inexpensively add the enhancements of smart card authentication (Colnot, Paragraph [0005]). On in reverse to incorporate the teaching of Bo et al. in to the method of Colnot in order to take advantage of the authentication enhancements provided by Bo et al. (Bo et al., Paragraph [0011]).

As Per Claim 27: The rejection of claim 21 is incorporated and further Colnot does not explicitly teach the following limitations however Bo et al in analogous art does teach the following limitations:

- the software driver resides in the same machine as the network server application

(Bo et al., Paragraphs [0242]-[0243], "c) With the agreement of the user, an application of the client 23 is downloaded from the web server 13 as 827 shows. The application is, for example, a Java applet. The user installs the application on the end station as S28 shows. Thus, the application of the client 23 is implemented.

d) With the agreement of the user, the application of the client 23 establishes an SSL connection (an SSL link) with the web server 13 for further transactions as 829 shows.").

(Bo et al., Paragraph [0253], "FIG. 16 shows a method of user authentication and digital audio-visual content encryption key(s) distribution. Each time a registered user wants to enjoy the services from the content provider, the user may be authenticated.").

The driver is the inherent underlying software that makes it possible for a system to operate with its underlying hardware and functions thereof.

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Colnot in to the method of Bo et al. in order to take advantage of being able to inexpensively add the enhancements of smart card authentication (Colnot, Paragraph [0005]). On in reverse to incorporate the teaching of Bo et al. in to the method of Colnot in order to take advantage of the authentication enhancements provided by Bo et al. (Bo et al., Paragraph [0011]).

As Per Claim 28: The rejection of claim 21 is incorporated and further Colnot does not explicitly teach the following limitations however Bo et al in analogous art does teach the following limitations:

- the software driver resides in a machine remote to but accessible from the machine hosting the network server application

(Bo et al., Paragraphs [0242]-[0243], "c) With the agreement of the user, an application of the client 23 is downloaded from the web server 13 as S27 shows. The application is, for example, a Java applet. The user installs the application on the end station as S28 shows. Thus, the application of the client 23 is implemented.

d) With the agreement of the user, the application of the client 23 establishes an SSL connection (an SSL link) with the web server 13 for further transactions as S29 shows.").

(Bo et al., Paragraph [0253], "FIG. 16 shows a method of user authentication and digital audio-visual content encryption key(s) distribution. Each time a registered user wants to enjoy the services from the content provider, the user may be authenticated.").

The driver is the inherent underlying software that makes it possible for a system to operate with its underlying hardware and functions thereof.

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Col not in to the method of 80 et al. in order to take advantage of being able to inexpensively add the enhancements of smart card authentication (Colnot, Paragraph [0005]). On in reverse to incorporate the teaching of Bo et al. in to the method of Colnot in order to take advantage of the authentication enhancements provided by Bo et al. (Bo et al., Paragraph [0011]).

As Per Claim 29: The rejection of claim 21 is incorporated and further Colnot does not explicitly teach the following limitations however Bo et al in analogous art does teach the following limitations:

- the software applet is a Java applet and the secure data record is a Java archive

(Bo et al., Paragraphs [0242]-[0243], "c) With the agreement of the user, an application of the client 23 is downloaded from the web server 13 as S27 shows. The application is, for example, a Java applet. The user installs the application on the end station as S28 shows. Thus, the application of the client 23 is implemented.

d) With the agreement of the user, the application of the client 23 establishes an SSL connection (an SSL link) with the web server 13 for further transactions as S29 shows.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Colnot in to the method of Bo et al. in order to take advantage of being able to inexpensively add the enhancements of smart card authentication (Colnot, Paragraph [0005]). On in reverse to incorporate the teaching of Bo et al. in to the method of Colnot in order to take advantage of the authentication enhancements provided by Bo et al. (Bo et al., Paragraph [0011]).

As Per Claim 30: The rejection of claim 21 is incorporated and further Colnot teaches:

- the key source comprises a semiconductor chip supporting a modem

(Colnot, Paragraph [0123], "The DRM-system's elements described above with respect to FIG. 1 can include so-called general-purpose computers, workstations, or personal computers, as well as network connectable information-processing devices, for instance, digital home electric appliances, portable terminals, PDAs, or cellular phones.").

As Per Claim 31: The rejection of claim 30 is incorporated and further Colnot teaches:

- the semiconductor chip is a part of the key source external to the digital appliance system used to secure authentication

(Colnot, Paragraph [0011], "The method, as detailed in FIG. 1, carries out the user authentication on the Internet. The apparatus comprises a smart card with a modulation output, a card reader plugged into the microphone input, and a PC applet. The user inserts his card in the reader and enters his password on the PC keyboard.").

As Per Claim 32: The rejection of claim 30 is incorporated and further Colnot teaches:

- the semiconductor chip derives power from a sound card of the digital appliance used to secure authentication

(Colnot, Abstract, "A method and apparatus to secure online transactions on the Internet comprising 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.").

(Colnot, Paragraph [0019], "The PC sound cards provides a +3V to +5V DC voltage on the microphone input which is sufficient to power (Vbb) the smart card. The resistor R1 adapts the level of the modulated signal to the microphone input. When pressed, the switch 81 pulls down the reset input (Rst) activating the modulation output (Mod).").

As Per Claim 33: The rejection of claim 21 is incorporated and further Colnot teaches:

- the key is a sound file stored on a machine peripheral to the digital appliance used to secure authentication

(Colnot, Paragraph [0123], "The DRM-system's elements described above with respect to FIG. 1 can include so-called general-purpose computers, workstations, or personal computers, as well as network connectable information-processing devices, for instance, digital home electric appliances, portable terminals, PDAs, or cellular phones.").

As Per Claim 34: The rejection of claim 33 is incorporated and further Colnot teaches:

- the peripheral machine is one of a cellular telephone, a personal digital assistant, or a hand held music player

(Colnot, Paragraph [0123], "The DRM-system's elements described above with respect to FIG. 1 can include so-called general-purpose computers, workstations, or personal computers, as well as network connectable information-processing devices, for instance, digital home electric appliances, portable terminals, PDAs, or cellular phones.").

As Per Claims 41-51: Claims 41-51 are a restatement of the system of claims 21-26 & 30-34 as a method and are rejected under substantially the same reasoning.

Claim(s) 37 is/are rejected under 35 U.S.C. 103(a) as being unpatentable over United States Patent Application Publication No.: US 20040093496 A1 (Colnot).

As Per Claim 37: The rejection of claim 35 is incorporated and further Colnot does not explicitly teach:

- the modem is a frequency-shift keying modem

However the examiner is giving official notice that the frequency-shift keying modem is a very well established modem standard and it would have been obvious to one of

ordinary skill in the art at the time of invention was made to incorporate the use of the standard variations of hardware already well known and prevalent at the time of invention was made.

Applicant's response:

The applicant has amended and narrowed claim 21 extensively, while reciting the same subject matter. Claim 21 now recites:

21. (Currently amended) A system enabling secure transacting over a network comprising:

a network server having an application ~~for~~ storing client information and configured to activate a client for secure transacting in the network, the client connecting to the server through a network-connected digital appliance;

a software driver configured to perform authentication, the software driver accessible to and executable by the network server application;

a software applet configured to create a secure data record and for managing transmission and update of the contents of the record; and

a token comprising an encrypted text string, the token stored on a data storage device coupled to the client's digital appliance, and also in a data repository coupled to the server;

wherein, upon a client seeking authorization from the server, the server downloads the software applet and a timestamp of the request time to the client, the applet executes at the client, retrieves the token from the data storage device, concatenates the token file and the time stamp, hashes the result creating the secure data record, sends the secure data record to the server, and the server, executing the software driver, compares the secure data record to a similarly hashed result of the time stamp and token value taken from the data repository coupled to the server, authorizing the client with a match.

The applicant has cancelled all claims reciting a sound token and any claims depended from such claims, and has recited the token as a token file comprising an encrypted text string. Although in some embodiments (examples) described in the specification it is emphasized that the token is a modulated signal, such as a sound, the specification states clearly on page 27 The token "…could also be a character string coded in a fashion to provide the necessary input."

Further, the applicant has recited that the server transmits an applet and a timestamp to the client appliance, where the applet executes, concatenating the timestamp with the token file and hashing the result to produce a secure data record, which is transmitted to the server to be compared with another data record produced by the server from the same token and timestamp, and similarly hashed.

The use of the timestamp is unique in preparing the secure data record, and is not taught anywhere in the one reference Colnot applied by the examiner. The applicant believes claim 21 is thus patentable over the reference Colnot and BO, taken either singly or in combination, and remaining depended claims 23, 26 and 29 are patentable at least as depended from a patentable claim.

The applicant has cancelled the method claims that followed the limitations of the un-amended system claims, and has entered new method claims 52-55 following the limitations of the amended system claims. Method claims 52-55 are thus patentable over Colnot and Bo.

Summary

As all of the claims, as amended and argued above, have been shown to be patentable over the art presented by the Examiner, applicant respectfully requests reconsideration and the case be passed quickly to issue.

If any fees are due beyond fees paid with this amendment, authorization is made to deduct those fees from deposit account 50-0534. If any time extension is needed beyond any extension requested with this amendment, such extension is hereby requested.

Respectfully Submitted
Vincent Cedric Colnot

By */Donald R. Boys/*
Donald R. Boys
Reg. No. 35,074

Central Coast Patent Agency, Inc.
3 Hangar Way, Suite D
Watsonville, CA 95076
(831) 768-1755

Electronic Patent Application Fee Transmittal

Application Number:	11533030
Filing Date:	19-Sep-2006
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

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 1 month with $0 paid	2251	1	65	65

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Request for continued examination	2801	1	405	405
		Total in USD ($)		**470**

Electronic Acknowledgement Receipt

EFS ID:	8503412
Application Number:	11533030
International Application Number:	
Confirmation Number:	3809
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
Receipt Date:	27-SEP-2010
Filing Date:	19-SEP-2006
Time Stamp:	14:22:25
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$470
RAM confirmation Number	598
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	Request for Continued Examination (RCE)	sb0030e_fillRCE.pdf	697266 c18b3acba8041d5be8e17c5f1d08a53c9aa267c1	no	3
Warnings:					
Information:					
2	Extension of Time	Extension.pdf	865043 3dad4448ec97f1ffd34bf150250cbe7a284bd0ae	no	1
Warnings:					
Information:					
3	Amendment Submitted/Entered with Filing of CPA/RCE	P1987oar2.pdf	148192 8e352a5107a84108534515110 1d0e4fd5577a5d1	no	20
Warnings:					
Information:					
4	Fee Worksheet (PTO-875)	fee-info.pdf	32201 343c2cb1f3405a7b9951ee493fb8371aa6eee836	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1742702		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

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

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
11/533,030	09/19/2006	

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)	SMALL ENTITY ☒		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
	09/27/2010	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 8	Minus	** 51	= 0	X $26 =	0	OR	X $ =	
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $110 =	0	OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

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

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

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

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

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

Legal Instrument Examiner:
/Wanda Meredith/

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/533,030	09/19/2006	Vincent Cedric Colnot	P1987	3809

24739 7590 05/28/2010

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

EXAMINER	
KAPLAN, BENJAMIN A	
ART UNIT	PAPER NUMBER
2434	

NOTIFICATION DATE	DELIVERY MODE
05/28/2010	ELECTRONIC

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

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

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

officeactions@CENTRALCOASTPATENT.COM
plambuth@centralcoastpatent.com

Office Action Summary	Application No.	Applicant(s)	
	11/533,030	COLNOT, VINCENT CEDRIC	
	Examiner	Art Unit	
	BENJAMIN A. KAPLAN	2434	

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

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

Status

1)☒ Responsive to communication(s) filed on *01 March 2010*.

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

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

Disposition of Claims

4)☒ Claim(s) *21-51* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *21-51* is/are rejected.

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

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

Application Papers

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

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

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

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

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

Priority under 35 U.S.C. § 119

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

a)☐ All b)☐ Some * c)☐ None of:

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

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

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

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

Attachment(s)

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

DETAILED ACTION

1. This Office Action is responsive to the most recent papers filed on 1 March 2008.

2. Claims 1-20 are canceled.

3. Claims 21-51 are new.

4. Claims 21-51 are rejected.

Response to Arguments and Amendments

5. Rejection of original claims 1-20 are moot in view of their cancelation.

6. 35 U.S.C. § 101 rejections have not bee placed on the new claims.

7. In regards to 35 U.S.C. § 112 some issues are still present in the new claims.

Claim Rejections - 35 USC § 112

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

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

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

The claims have been stated in a manner where there are not necessarily any specific features being claimed.

In independent claim 21 a system is claimed having:

an application for (some intended purpose),

a software driver for (some intended purpose), and

a software applet for (some intended purpose)

Examiner suggests changing the claim language to read:

an application ~~for storing~~ configured to store …

a software driver ~~for performing~~ configured to perform …

a software applet ~~for creating~~ configured to create …

Also the concluding wherein clause in claim 21 is cut off from the rest of the claim. (See MPEP 2111.04 "Adapted to," "Adapted for," "Wherein," and "Whereby" Clauses [R-3] - 2100 Patentability) Its premise is based on “the key source” which has not been declared yet else ware in the claim. For the sake of examination it is believed that “the key source” is referring to the “key device” and has been examined as such however the connecting language will need to be clarified for consistency.

Claims 22-34 are rejected under 35 USC § 112 as being dependent on claim 21.

Claim Rejections - 35 USC § 102

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

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

11. Claims 35-36, 37-40 rejected under 35 U.S.C. 102(b) as being anticipated by United States Patent Application Publication No.: US 20040093496 A1 (Colnot).

As Per Claim 35: Colnot teaches: **A sound-producing device for generating a network-transmittable sound frame having embedded therein an identification number and a session key usable to authenticate a client, the device comprising:**

- a semiconductor chip supporting a modem;

(Colnot, Paragraph [0123], "The DRM-system's elements described above with respect to FIG. 1 can include so-called general-purpose computers, workstations, or personal computers, as well as network connectable information-processing devices, for instance, digital home electric appliances, portable terminals, PDAs, or cellular phones.").

Network connectable devices are supporting modems of one sort or another.

- a plug-in interface for enabling coupling with a host digital appliance;

- and a housing of a size and shape to support hand-held operation.

(Colnot, Paragraph [0006], "The above object has been achieved by a smart card transmitting an identification sequence to a PC by means of a card reader plugged into the microphone input of the PC sound card. The reader is actually a simple and inexpensive connector without processing means. The smart card remains compliant with the ISO 7816 standards and can be used in the existing card readers.").

As Per Claim 36: The rejection of claim 35 is incorporated and further Colnot teaches:

- the network is the Intemet network

(Colnot, Abstract, "A method and apparatus to secure online transactions on the Internet comprising 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.").

As Per Claim 38: The rejection of claim 35 is incorporated and further Colnot teaches:

- the plug-in interface is a tip/ring/sleeve interface for plugging into a microphone jack on the host digital appliance used to secure authentication

(Colnot, Paragraph [0011], "The method, as detailed in FIG. 1, carries out the user authentication on the Internet. The apparatus comprises a smart card with a modulation output, a card reader plugged into the microphone input, and a PC applet. The user inserts his card in the reader and enters his password on the PC keyboard.").

As Per Claim 39: The rejection of claim 38 is incorporated and further Colnot teaches:

- the sound-producing device derives power from a soundcard residing on the digital appliance used to secure authentication

(Colnot, Paragraph [0019], "The PC sound cards provides a +3V to +5V DC voltage on the microphone input which is sufficient to power (Vbb) the smart card. The resistor R1 adapts the level of the modulated signal to the microphone input. When pressed, the switch S1 pulls down the reset input (Rst) activating the modulation output (Mod).").

As Per Claim 40: The rejection of claim 35 is incorporated and further Colnot teaches:

- a switch for activating the modem to generate the sound

(Colnot, Paragraph [0019], "The PC sound cards provides a +3V to +5V DC voltage on the microphone input which is sufficient to power (Vbb) the smart card. The resistor R1 adapts the level of the modulated signal to the microphone input. When pressed, the switch S1 pulls down the reset input (Rst) activating the modulation output (Mod).").

Claim Rejections - 35 USC § 103

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

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. Claim(s) 21-34 & 41-51 is/are rejected under 35 U.S.C. 103(a) as being unpatentable over United States Patent Application Publication No.: US 20040093496 A1 (Colnot) in view of United States Patent Application Publication No.: US 2005/0262573 A1 (Bo et al.).

As Per Claim 21: Colnot teaches: **A system enabling secure transacting over a network comprising:**

- a network server having an application for storing client information and for activating a client for secure transacting in the network, the client connecting to the server through a network-connected digital appliance;

(Colnot, Drawings, Figure. 1. "

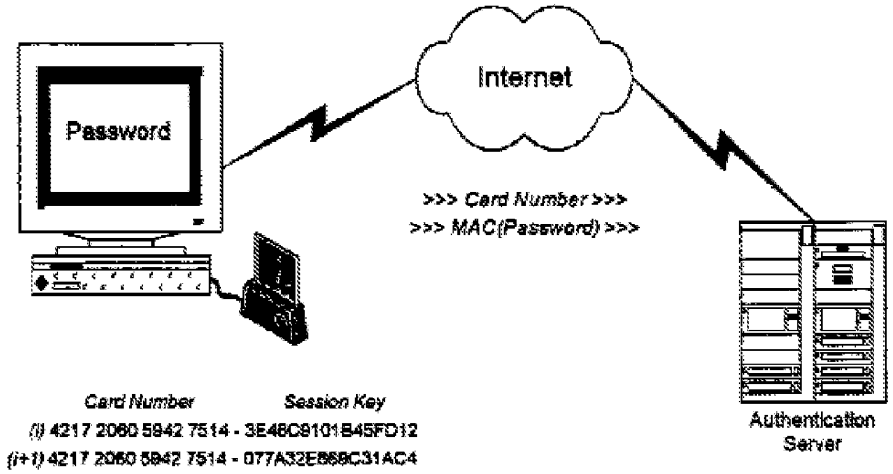


FIG. 1

").

(Colnot, Paragraphs [0011]-[0014], "The method, as detailed in FIG. 1, carries out the user authentication on the Internet. The apparatus comprises a smart card with a modulation output, a card reader plugged into the microphone input, and a PC applet. The user inserts his card in the reader and enters his password on the PC keyboard.

When activated in the card reader, the smart card transmits an identification sequence to the PC in the form of a modulated signal, which is demodulated by the PC applet. The identification sequence comprises an 8-byte card number and an 8-byte random number valid only once. The card number is unique and identifies the card issuer, application version and user account. The random number is a session key (Ki)

which is a function of the previous one (Ki-1) emitted by the card such as: Ki=G(Ki-1), G is a one-way function also known by the authentication server.

The session key (Ki) is used by the PC applet to generate a message authentication code (MAC) of the password entered by the user, using the DES algorithm for instance. This first MAC is transmitted to the authentication server along with the card number, allowing the server to retrieve the previous session key (Ki-1) and the password stored in the authentication server database.

The authentication server deduces from (Ki-1) the session key used by the card, and generates a second MAC of the password stored in the database. The authentication is valid only if the first and second MAC are identical, which means the PC and the authentication server have used the same session key (Ki) to generate a MAC of the same password. If this is the case, the authentication server replaces (Ki-1) by (Ki) in the database. The session key (Ki) cannot be reused, even though the session key (Ki) has not been transmitted to the authentication server.").

- a digital key stored on a key device enabled to connect to the client's digital appliance;

- wherein, with the key source connected to the digital appliance, the key is provided to the digital appliance to be provided over the network to the server, to interact with the application for activating the client.

(Colnot, Paragraphs [0011]-[0014], "The method, as detailed in FIG. 1, carries out the user authentication on the Internet. The apparatus comprises a smart card with

a modulation output, a card reader plugged into the microphone input, and a PC applet. The user inserts his card in the reader and enters his password on the PC keyboard.

When activated in the card reader, the smart card transmits an identification sequence to the PC in the form of a modulated signal, which is demodulated by the PC applet. The identification sequence comprises an 8-byte card number and an 8-byte random number valid only once. The card number is unique and identifies the card issuer, application version and user account. The random number is a session key (Ki) which is a function of the previous one (Ki-1) emitted by the card such as: Ki=G(Ki-1), G is a one-way function also known by the authentication server.

The session key (Ki) is used by the PC applet to generate a message authentication code (MAC) of the password entered by the user, using the DES algorithm for instance. This first MAC is transmitted to the authentication server along with the card number, allowing the server to retrieve the previous session key (Ki-1) and the password stored in the authentication server database.

The authentication server deduces from (Ki-1) the session key used by the card, and generates a second MAC of the password stored in the database. The authentication is valid only if the first and second MAC are identical, which means the PC and the authentication server have used the same session key (Ki) to generate a MAC of the same password. If this is the case, the authentication server replaces (Ki-1) by (Ki) in the database. The session key (Ki) cannot be reused, even though the session key (Ki) has not been transmitted to the authentication server.").

Colnot does not explicitly teach the following limitations however Bo et al in analogous are does teach the following limitations:

- a software driver for performing authentication, the software driver accessible to the network server application;

- a software applet for creating a secure data record and for managing transmission and update of the contents of the record; and

(Bo et al., Paragraphs [0242]-[0243], "c) With the agreement of the user, an application of the client 23 is downloaded from the web server 13 as S27 shows. The application is, for example, a Java applet. The user installs the application on the end station as S28 shows. Thus, the application of the client 23 is implemented.

d) With the agreement of the user, the application of the client 23 establishes an SSL connection (an SSL link) with the web server 13 for further transactions as S29 shows.").

(Bo et al., Paragraph [0253], "FIG. 16 shows a method of user authentication and digital audio-visual content encryption key(s) distribution. Each time a registered user wants to enjoy the services from the content provider, the user may be authenticated.").

The driver is the inherent underlying software that makes it possible for a system to operate with its underlying hardware and functions thereof.

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Colnot in to the method of Bo et al. in order to take advantage of being able to inexpensively add the enhancements of smart card authentication (Colnot, Paragraph [0005]). On in reverse to incorporate the

teaching of Bo et al. in to the method of Colnot in order to take advantage of the authentication enhancements provided by Bo et al. (Bo et al., Paragraph [0011]).

As Per Claim 22: The rejection of claim 21 is incorporated and further Colnot teaches:

- the key is one of a character string, a modulated audio file, a modulated light source, an infra-red signal, or a vibratory signal

(Colnot, Paragraph [0012], "When activated in the card reader, the smart card transmits an identification sequence to the PC in the form of a modulated signal, which is demodulated by the PC applet. The identification sequence comprises an 8-byte card number and an 8-byte random number valid only once. The card number is unique and identifies the card issuer, application version and user account. The random number is a session key (Ki) which is a function of the previous one (Ki-1) emitted by the card such as: Ki=G(Ki-1), G is a one-way function also known by the authentication server.").

As Per Claim 23: The rejection of claim 21 is incorporated and further Colnot and Bo et al do not explicitly teach:

- the key source is a flash thumb drive

However the examiner is giving official notice the use of flash drives as key sources was well established in the art at the time of invention was made. It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporated the use of flash drives as potential key sources as they provide as highly

expedient manner of having a portable connectable/disconnect-able device easily at the ready.

As Per Claim 24: The rejection of claim 21 is incorporated and further Colnot teaches:

- the connection to the client's digital appliance is one of a USB port, a microphone jack, an infrared sensor, or a an audio microphone

(Colnot, Paragraph [0011], "The method, as detailed in FIG. 1, carries out the user authentication on the Internet. The apparatus comprises a smart card with a modulation output, a card reader plugged into the microphone input, and a PC applet. The user inserts his card in the reader and enters his password on the PC keyboard.").

As Per Claim 25: The rejection of claim 21 is incorporated and further Colnot teaches:

- the network is the Internet network

(Colnot, Abstract, "A method and apparatus to secure online transactions on the Internet comprising 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.").

As Per Claim 26: The rejection of claim 21 is incorporated and further Colnot does not explicitly teach the following limitations however Bo et al in analogous art does teach the following limitations:

- the secure data record is unique to a client and includes an identification number, a password or personal identification code, a session key, and a secrete data seed

(Bo et al., Paragraph [0152], "In one example, the web server 13 is used to transfer user's personal information from the client 23 to the SRM 5 through a pre-established SSL link. The user's personal information includes user's log-in ID and password. The user account manager 35 in the SRM 5 maintains and manages all the user's personal information.").

(Bo et al., Paragraph [0147], "The encipheror 3 or the encipheror in the encipheror/decipherer module 38 defines a block cipher algorithm, e.g., DES (data encryption standard), AES (advanced encryption standard), or Blowfish. The encipheror 3 or the encipheror in the encipheror/decipherer module 38 also defines the seeds for generating random keys, the preferred key length for the block cipher algorithm that accepts variable length keys, the preferred plaintext block size, e.g., 64 bits, 128 bits, or 256 bits. Otherwise, a default encryption strategy is to be used.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Colnot in to the method of Bo et al. in order to take advantage of being able to inexpensively add the enhancements of smart card authentication (Colnot, Paragraph [0005]). On in reverse to incorporate the teaching of Bo et al. in to the method of Colnot in order to take advantage of the authentication enhancements provided by Bo et al. (Bo et al., Paragraph [0011]).

As Per Claim 27: The rejection of claim 21 is incorporated and further Colnot does not explicitly teach the following limitations however Bo et al in analogous art does teach the following limitations:

- the software driver resides in the same machine as the network server application

(Bo et al., Paragraphs [0242]-[0243], "c) With the agreement of the user, an application of the client 23 is downloaded from the web server 13 as S27 shows. The application is, for example, a Java applet. The user installs the application on the end station as S28 shows. Thus, the application of the client 23 is implemented.

d) With the agreement of the user, the application of the client 23 establishes an SSL connection (an SSL link) with the web server 13 for further transactions as S29 shows.").

(Bo et al., Paragraph [0253], "FIG. 16 shows a method of user authentication and digital audio-visual content encryption key(s) distribution. Each time a registered user wants to enjoy the services from the content provider, the user may be authenticated.").

The driver is the inherent underlying software that makes it possible for a system to operate with its underlying hardware and functions thereof.

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Colnot in to the method of Bo et al. in order to take advantage of being able to inexpensively add the enhancements of smart card authentication (Colnot, Paragraph [0005]). On in reverse to incorporate the

teaching of Bo et al. in to the method of Colnot in order to take advantage of the authentication enhancements provided by Bo et al. (Bo et al., Paragraph [0011]).

As Per Claim 28: The rejection of claim 21 is incorporated and further Colnot does not explicitly teach the following limitations however Bo et al in analogous art does teach the following limitations:

- the software driver resides in a machine remote to but accessible from the machine hosting the network server application

(Bo et al., Paragraphs [0242]-[0243], "c) With the agreement of the user, an application of the client 23 is downloaded from the web server 13 as S27 shows. The application is, for example, a Java applet. The user installs the application on the end station as S28 shows. Thus, the application of the client 23 is implemented.

d) With the agreement of the user, the application of the client 23 establishes an SSL connection (an SSL link) with the web server 13 for further transactions as S29 shows.").

(Bo et al., Paragraph [0253], "FIG. 16 shows a method of user authentication and digital audio-visual content encryption key(s) distribution. Each time a registered user wants to enjoy the services from the content provider, the user may be authenticated.").

The driver is the inherent underlying software that makes it possible for a system to operate with its underlying hardware and functions thereof.

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Colnot in to the method of Bo et al. in

order to take advantage of being able to inexpensively add the enhancements of smart card authentication (Colnot, Paragraph [0005]). On in reverse to incorporate the teaching of Bo et al. in to the method of Colnot in order to take advantage of the authentication enhancements provided by Bo et al. (Bo et al., Paragraph [0011]).

As Per Claim 29: The rejection of claim 21 is incorporated and further Colnot does not explicitly teach the following limitations however Bo et al in analogous art does teach the following limitations:

- the software applet is a Java applet and the secure data record is a Java archive

(Bo et al., Paragraphs [0242]-[0243], "c) With the agreement of the user, an application of the client 23 is downloaded from the web server 13 as S27 shows. The application is, for example, a Java applet. The user installs the application on the end station as S28 shows. Thus, the application of the client 23 is implemented.

d) With the agreement of the user, the application of the client 23 establishes an SSL connection (an SSL link) with the web server 13 for further transactions as S29 shows.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Colnot in to the method of Bo et al. in order to take advantage of being able to inexpensively add the enhancements of smart card authentication (Colnot, Paragraph [0005]). On in reverse to incorporate the teaching of Bo et al. in to the method of Colnot in order to take advantage of the authentication enhancements provided by Bo et al. (Bo et al., Paragraph [0011]).

As Per Claim 30: The rejection of claim 21 is incorporated and further Colnot teaches:

- the key source comprises a semiconductor chip supporting a modem

(Colnot, Paragraph [0123], "The DRM-system's elements described above with respect to FIG. 1 can include so-called general-purpose computers, workstations, or personal computers, as well as network connectable information-processing devices, for instance, digital home electric appliances, portable terminals, PDAs, or cellular phones.").

As Per Claim 31: The rejection of claim 30 is incorporated and further Colnot teaches:

- the semiconductor chip is a part of the key source external to the digital appliance system used to secure authentication

(Colnot, Paragraph [0011], "The method, as detailed in FIG. 1, carries out the user authentication on the Internet. The apparatus comprises a smart card with a modulation output, a card reader plugged into the microphone input, and a PC applet. The user inserts his card in the reader and enters his password on the PC keyboard.").

As Per Claim 32: The rejection of claim 30 is incorporated and further Colnot teaches:

- the semiconductor chip derives power from a sound card of the digital appliance used to secure authentication

(Colnot, Abstract, "A method and apparatus to secure online transactions on the Internet comprising 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.").

(Colnot, Paragraph [0019], "The PC sound cards provides a +3V to +5V DC voltage on the microphone input which is sufficient to power (Vbb) the smart card. The resistor R1 adapts the level of the modulated signal to the microphone input. When pressed, the switch S1 pulls down the reset input (Rst) activating the modulation output (Mod).").

As Per Claim 33: The rejection of claim 21 is incorporated and further Colnot teaches:

- the key is a sound file stored on a machine peripheral to the digital appliance used to secure authentication

(Colnot, Paragraph [0123], "The DRM-system's elements described above with respect to FIG. 1 can include so-called general-purpose computers, workstations, or personal computers, as well as network connectable information-processing devices, for instance, digital home electric appliances, portable terminals, PDAs, or cellular phones.").

As Per Claim 34: The rejection of claim 33 is incorporated and further Colnot teaches:

- the peripheral machine is one of a cellular telephone, a personal digital assistant, or a hand held music player

(Colnot, Paragraph [0123], "The DRM-system's elements described above with respect to FIG. 1 can include so-called general-purpose computers, workstations, or personal computers, as well as network connectable information-processing devices, for instance, digital home electric appliances, portable terminals, PDAs, or cellular phones.").

As Per Claims 41-51: Claims 41-51 are a restatement of the system of claims 21-26 & 30-34 as a method and are rejected under substantially the same reasoning.

14. Claim(s) 37 is/are rejected under 35 U.S.C. 103(a) as being unpatentable over United States Patent Application Publication No.: US 20040093496 A1 (Colnot).

As Per Claim 37: The rejection of claim 35 is incorporated and further Colnot does not explicitly teach:

- the modem is a frequency-shift keying modem

However the examiner is giving official notice that the frequency-shift keying modem is a very well established modem standard and it would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the use of the standard variations of hardware already well known and prevalent at the time of invention was made.

Conclusion

15. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BENJAMIN A. KAPLAN whose telephone number is (571)-270-3170. The examiner can normally be reached on 7:30 a.m. - 5:00 p.m. E.S.T..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. 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.

/Benjamin A Kaplan/
Examiner, Art Unit 2434
/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2434

Notice of References Cited	Application/Control No. 11/533,030	Applicant(s)/Patent Under Reexamination COLNOT, VINCENT CEDRIC	
	Examiner BENJAMIN A. KAPLAN	Art Unit 2434	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-			
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	FSK MODEM USERS MANUAL REVISION 2.1, June, 1989 COPYRIGHT © 1988 MIILLE APPLIED RESEARCH CO., INC.
	V	
	W	
	X	

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

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11533030	COLNOT, VINCENT CEDRIC
	Examiner	Art Unit
	BENJAMIN A KAPLAN	2434

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

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

CLAIM		DATE								
Final	Original	08/28/2009	05/22/2010							
	1	✓	-							
	2	✓	-							
	3	✓	-							
	4	✓	-							
	5	✓	-							
	6	✓	-							
	7	✓	-							
	8	✓	-							
	9	✓	-							
	10	✓	-							
	11	✓	-							
	12	✓	-							
	13	✓	-							
	14	✓	-							
	15	✓	-							
	16	✓	-							
	17	✓	-							
	18	✓	-							
	19	✓	-							
	20	✓	-							
	21		✓							
	22		✓							
	23		✓							
	24		✓							
	25		✓							
	26		✓							
	27		✓							
	28		✓							
	29		✓							
	30		✓							
	31		✓							
	32		✓							
	33		✓							
	34		✓							
	35		✓							
	36		✓							

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11533030	COLNOT, VINCENT CEDRIC
	Examiner	Art Unit
	BENJAMIN A KAPLAN	2434

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

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

CLAIM		DATE								
Final	Original	08/28/2009	05/22/2010							
	37		✓							
	38		✓							
	39		✓							
	40		✓							
	41		✓							
	42		✓							
	43		✓							
	44		✓							
	45		✓							
	46		✓							
	47		✓							
	48		✓							
	49		✓							
	50		✓							
	51		✓							

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11533030	COLNOT, VINCENT CEDRIC
	Examiner	Art Unit
	BENJAMIN A KAPLAN	2434

SEARCHED			
Class	Subclass	Date	Examiner
726	2,9,26,27	5/22/2010	BK

SEARCH NOTES		
Search Notes	Date	Examiner
East, Plus Search, Google	5/22/2010	BK

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	1	11/533,030.app.	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/18 13:57
S2	296	(("20010037461") or ("20010042124") or ("20020031225") or ("20020099940") or ("20020099942") or ("20020191765") or ("20030009676") or ("20030009692") or ("20030033545") or ("20030056096") or ("20030065919") or ("20030100371") or ("20030126457") or ("20030169713") or ("20030177354") or ("20030233450") or ("20030233583") or ("20040054794") or ("20040127279") or ("20040133789") or ("20040218897") or ("20050010777") or ("20050021613") or ("20050233811") or ("20060006230") or ("20060059265") or ("20060112213") or ("20060155601") or ("20060161775") or ("20060205394") or ("20060272023") or ("20060288407") or ("20070022469") or ("20070067833") or ("20070098175") or ("20070130334") or ("20070190975") or ("20070232355") or ("20070282909") or ("20080177998") or ("20090125717") or ("20090150977") or ("20090198996") or	US-PGPUB; USPAT; USOCR	OR	OFF	2009/08/27 18:23

("4295155") or
("4386233") or
("4423287") or
("4755940") or
("4783798") or
("4888801") or
("4890323") or
("4897875") or
("4905766") or
("4910773") or
("4956862") or
("4997288") or
("5008936") or
("5016277") or
("5022076") or
("5202921") or
("5204961") or
("5210794") or
("5210795") or
("5226079") or
("5237614") or
("5239294") or
("5241594") or
("5261002") or
("5272754") or
("5276735") or
("5311596") or
("5313521") or
("5347387") or
("5349643") or
("5353353") or
("5369705") or
("5371794") or
("5410602") or
("5412726") or
("5425130") or
("5444780") or
("5454000") or
("5469507") or
("5479341") or
("5481613") or
("5485196") or
("5491752") or
("5499297") or
("5500897") or
("5502766") or
("5535276") or
("5557686") or
("5587809") or
("5588060") or
("5590196") or
("5590199") or
("5590200") or
("5592555") or

		("5598459") or ("5602915") or ("5602918") or ("5604663") or ("5604803") or ("5619657") or ("5623601") or ("5633933") or ("5633934") or ("5638448") or ("5643086") or ("5655077") or ("5657390") or ("5666412") or ("5668877") or ("5671279") or ("5673318") or ("5675651") or ("5684950") or ("5687235") or ("5689566") or ("5692400") or ("5699513") or ("5719941") or ("5721779") or ("5724168") or ("5724423") or ("5729594") or ("5732137") or ("5734718") or ("5742756") or ("5745574") or ("5745576") or ("5748736") or ("5754659") or ("5757913") or ("5757918") or ("5764890") or ("5768378") or ("5778065") or ("5778071") or ("5778313")).PN. or (("5781550") or ("5781724") or ("5784463") or ("5787172") or ("5790669") or ("5796833") or ("5799082") or ("5802178") or ("5802497") or ("5805712") or ("5805803") or ("5809117") or					

		("5812664") or					
		("5812669") or					
		("5812764") or					
		("5812955") or					
		("5818936") or					
		("5822431") or					
		("5825300") or					
		("5825877") or					
		("5825890") or					
		("5828832") or					
		("5832209") or					
		("5832228") or					
		("5841120") or					
		("5841864") or					
		("5850442") or					
		("5850445") or					
		("5864665") or					
		("5870473") or					
		("5870475") or					
		("5870544") or					
		("5872915") or					
		("5875296") or					
		("5875394") or					
		("5875395") or					
		("5883956") or					
		("5887063") or					
		("5887250") or					
		("5889861") or					
		("5892829") or					
		("5892838") or					
		("5892902") or					
		("5894552") or					
		("5903721") or					
		("5907620") or					
		("5909491") or					
		("5913175") or					
		("5918228") or					
		("5922074") or					
		("5923756") or					
		("5926624") or					
		("5930362") or					
		("5931947") or					
		("5947571") or					
		("5953422") or					
		("5963644") or					
		("5963915") or					
		("5966441") or					
		("5967466") or					
		("5970144") or					
		("5974144") or					
		("5978475") or					
		("5978918") or					
		("5983350") or					
		("5995624") or					

("5996077") or
("6002767") or
("6009524") or
("6012144") or
("6012632") or
("6017004") or
("6021497") or
("6023764") or
("6026167") or
("6026293") or
("6032150") or
("6032260") or
("6038551") or
("6038892") or
("6044155") or
("6044468") or
("6047072") or
("6047325") or
("6047572") or
("6049878") or
("6052785") or
("6055236") or
("6055636") or
("6061346") or
("6061448") or
("6061448") or
("6061449") or
("6061790") or
("6061796") or
("6061796") or
("6061799") or
("6061799") or
("6065120") or
("6067620") or
("6075860") or
("6081900") or
("6088451") or
("6098056") or
("6119233") or
("6141752") or
("6144848") or
("6148405") or
("6151590") or
("6158007") or
("6178089") or
("6185612") or
("6192474") or
("6198824") or
("6199113") or
("6202081") or
("6216231") or
("6216231") or
("6230266") or
("6233608") or

		("6233687") or ("6233688") or ("6247129") or ("6249867") or ("6249873") or ("6263313") or ("6272633") or ("6282653") or ("6301667") or ("6314468") or ("6345256") or ("6374402") or ("6389403") or ("6389538") or ("6418421") or ("6438600") or ("6449367") or ("6453416") or ("6463537") or ("6678826") or ("6732105") or ("6763370") or ("6907530") or ("6912653") or ("6945870") or ("6973566") or ("7017188") or ("7028182") or ("7073055") or ("7100054")).PN. or (("7103770") or ("7152160") or ("7171467") or ("7184999") or ("7188179") or ("7231025") or ("7287271") or ("7496950") or ("7502928") or ("7509119") or ("7533735")).PN.				
S3	300	(("20010034716") or ("20020014054") or ("20020017079") or ("20020020752") or ("20020032746") or ("20020036114") or ("20020052797") or ("20020073036") or ("20020077992") or ("20020091646") or ("20020103857") or ("20020116274") or ("20020141576") or	US-PGPUB; USPAT; USOCR	OR	OFF	2009/08/27 18:24

("20020157019") or
("20020178364") or
("20020191790") or
("20030014669") or
("20030018916") or
("20030023578") or
("20030028491") or
("20030046586") or
("20030046587") or
("20030046889") or
("20030055733") or
("20030056054") or
("20030056092") or
("20030061173") or
("20030061275") or
("20030061387") or
("20030061506") or
("20030065919") or
("20030081783") or
("20030088426") or
("20030097592") or
("20030100372") or
("20030111266") or
("20030115455") or
("20030126192") or
("20030126483") or
("20030163423") or
("20030163723") or
("20030177348") or
("20030177354") or
("20030182574") or
("20030188003") or
("20030188156") or
("20030188165") or
("20030191932") or
("20030208689") or
("20030221118") or
("20030226014") or
("20030226022") or
("20030229802") or
("20030233550") or
("20030236997") or
("20040002381") or
("20040020164") or
("20040065501") or
("20040068648") or
("20040068726") or
("20040073151") or
("20040083184") or
("20040083375") or
("20040088252") or
("20040089482") or
("20040095083") or
("20040098740") or

		("20040103165") or ("20040111578") or ("20040114182") or ("20040117623") or ("20040117627") or ("20040117635") or ("20040117661") or ("20040121787") or ("20040128517") or ("20040139019") or ("20040158635") or ("20040167465") or ("20040168081") or ("20040182126") or ("20040192303") or ("20040221168") or ("20040224769") or ("20040224771") or ("20040228063") or ("20040230809") or ("20040231594") or ("20040243853") or ("20050002328") or ("20050028487") or ("20050030151") or ("20050031136") or ("20050033980") or ("20050044404") or ("20050050342") or ("20050051448") or ("20050054445") or ("20050055588") or ("20050055815") or ("20050061878") or ("20050081063") or ("20050085931") or ("20050086509") or ("20050091364") or ("20050091527") or ("20050097350") or ("20050102535") or ("20050105736") or ("20050111380") or ("20050114687") or ("20050116026") or ("20050121339") or ("20050132031") or ("20050138356") or ("20050138423") or ("20050144493") or ("20050145695")).PN. or (("20050159203") or ("20050160417") or ("20050172132") or					

		("20050182938") or ("20050185647") or ("20050188251") or ("20050188731") or ("20050198461") or ("20050209006") or ("20050209842") or ("20050213768") or ("20050223220") or ("20050226175") or ("20050240685") or ("20050240712") or ("20050251685") or ("20050251852") or ("20050256806") or ("20050257245") or ("20050268336") or ("20060004964") or ("20060005072") or ("20060015947") or ("20060019657") or ("20060025147") or ("20060026573") or ("20060036693") or ("20060039305") or ("20060039306") or ("20060039321") or ("20060039339") or ("20060039340") or ("20060039360") or ("20060039562") or ("20060039563") or ("20060041750") or ("20060041761") or ("20060042882") or ("20060047784") or ("20060050887") or ("20060056630") or ("20060059543") or ("20060074983") or ("20060085370") or ("20060087192") or ("20060095377") or ("20060111165") or ("20060111794") or ("20060136742") or ("20060143700") or ("20060155589") or ("20060156019") or ("20060156399") or ("20060179308") or ("20060184524") or ("20060189382") or ("20060193474") or					

		("20060197403") or ("20060200660") or ("20060270346") or ("20070041110") or ("20070067833") or ("20070294085") or ("20080098872") or ("20080161951") or ("20080188182") or ("20080228865") or ("20080240468") or ("3683325") or ("4526115") or ("5051564") or ("5282247") or ("5406039") or ("5493767") or ("5656799") or ("5657388") or ("5695183") or ("5749253") or ("5825752") or ("6022009") or ("6038590") or ("6105042") or ("6118732") or ("6178550") or ("6209095") or ("6226697") or ("6233620") or ("6254366") or ("6282653") or ("6298336") or ("6328149") or ("6339827") or ("6382516") or ("6389541") or ("6393569") or ("6442532") or ("6502746") or ("6507908") or ("6520285") or ("6615194") or ("6620047") or ("6671810") or ("6701304") or ("6710893") or ("6722466") or ("6748532") or ("6769068") or ("6789147") or ("6823452") or ("6836795") or ("6845905") or					

		("6901251") or ("6915437") or ("6916247") or ("6920557") or ("6928707") or ("6934848") or ("6945458") or ("6957343") or ("6961759") or ("6970918") or ("6976164") or ("6976172") or ("6996841") or ("7013387") or ("7020476") or ("7024377") or ("7063615") or ("7069442") or ("7084734") or ("7085933") or ("7089587")).PN. or (("7095150") or ("7101296") or ("7103529") or ("7135968") or ("7137016") or ("7143280") or ("7146640") or ("7149821") or ("7152245") or ("7154628") or ("7155615") or ("7159242") or ("7185365") or ("7197644") or ("7207481") or ("7219480") or ("7228566") or ("7237717") or ("7245726") or ("7266703") or ("7290287") or ("7313679") or ("7333717") or ("7336789") or ("7343411") or ("7346929") or ("7350230") or ("7371952") or ("7383193") or ("7401230") or ("7418504") or ("7424610") or ("7428754") or					

		("7441153") or ("7452278") or ("7455590") or ("7458075") or ("7469341") or ("7469368") or ("7496097") or ("7502475") or ("7506170") or ("7509487") or ("7516331") or ("7530103") or ("7539651") or ("7540516") or ("7549922") or ("7574509") or ("7577258")).PN.				
S4	283	S2 @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:25
S5	285	S3 @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:25
S6	3	S4 S5	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:25
S7	29905	server client authentication @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:52
S8	21050	server client authentication key @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:52
S9	14617	server client authentication key secure @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:52
S10	4843	server client authentication key secure java @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:53
S11	2219	server client authentication key secure java applet @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:53
S12	604	server client authentication key secure java applet archive @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:53
S13	322	server client authentication key secure java applet archive sound card @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:53

S14	322	server client authentication key secure java applet archive sound card network @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:54
S15	283	server client authentication key secure java applet archive sound card network password @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:54
S16	279	server client authentication key secure java applet archive sound card network password session @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:54
S17	30	server client authentication key secure java applet archive sound card network password session seed @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:54
S18	0	server client authentication key secure java applet archive (sound adj source) @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 19:15
S19	1	server client authentication key secure java applet archive (sound same password) @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 19:17
S20	1	10/696,650.app.	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 19:26
S21	244	server client authentication key secure java applet archive (smart adj card) @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 18:48
S22	244	server client authentication key secure java applet archive (smart adj card) network @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 18:48
S23	234	server client authentication key secure java applet archive (smart adj card) network password @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 18:48

S24	225	server client authentication key secure java applet archive (smart adj card) network password session @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 18:49
S25	27	server client authentication key secure java applet archive (smart adj card) network password session seed @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 18:49
S26	1546	(726/2).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2009/08/28 20:32
S27	694	(726/9).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2009/08/28 20:32
S28	2232	(726/26).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2009/08/28 20:32
S29	1545	(726/27).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2009/08/28 20:32
S30	1033	S26 @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 20:32
S31	453	S27 @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 20:32
S32	1688	S28 @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 20:32
S33	1050	S29 @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 20:32
S34	1	S30 S31 S32 S33	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 20:33
S35	3732	S30 or S31 or S32 or S33	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 20:33
S36	1446	key source flash thumb drive @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/05/21 17:21
S37	0	(key adj source) (flash adj thumb adj drive) @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/05/21 17:21

S38	0	(key adj source) (thumb adj drive) @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/05/21 17:21
S39	3	(key adj source) (flash adj drive) @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/05/21 17:21
S40	128	(key) same (flash adj drive) @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/05/21 17:23
S41	6623	(726/2,9,26,27).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2010/05/22 19:21
S42	4273	S41 @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2010/05/22 19:21
S43	538	S42 @pd>"20090824"	US-PGPUB; USPAT; USOCR	AND	ON	2010/05/22 19:21

EAST Search History (Interference)

< This search history is empty>

5/ 22/ 2010 7:25:10 PM
C:\ Documents and Settings\ bkaplan\ My Documents\ EAST\ Workspaces\ 11533030.wsp

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
Art Unit: 2434 Examiner: Kaplan, Benjamin A.

In Re:	Vincent Cedric Colnot
Case:	P1987
Serial No.:	11/533,030
Filed:	09/19/2006
Subject:	Methods and Apparatus for Enabling Secure Network Transactions

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Response A

In the claims:

All of the claims standing for examination are presented below with appropriate status indication.

1-20. (Canceled)

21. (New) A system enabling secure transacting over a network comprising:

a network server having an application for storing client information and for activating a client for secure transacting in the network, the client connecting to the server through a network-connected digital appliance;

a software driver for performing authentication, the software driver accessible to the network server application;

a software applet for creating a secure data record and for managing transmission and update of the contents of the record; and

a digital key stored on a key device enabled to connect to the client's digital appliance;

wherein, with the key source connected to the digital appliance, the key is provided to the digital appliance to be provided over the network to the server, to interact with the application for activating the client.

22. (New) The system of claim 21 wherein the key is one of a character string, a modulated audio file, a modulated light source, an infra-red signal, or a vibratory signal.

23. (New) The system of claim 21 wherein the key source is a flash thumb drive.

24. (New) The system of claim 21 wherein the connection to the client's digital appliance is one of a USB port, a microphone jack, an infrared sensor, or a an audio microphone.

25. (New) The system of claim 21, wherein the network is the Internet network.

26. (New) The system of claim 21, wherein the secure data record is unique to a client and includes an identification number, a password or personal identification code, a session key, and a secrete data seed.

27. (New) The system of claim 21, wherein the software driver resides in the same machine as the network server application.

28. (New) The system of claim 21, wherein the software driver resides in a machine remote to but accessible from the machine hosting the network server application.

29. (New) The system of claim 21, wherein the software applet is a Java applet and the secure data record is a Java archive.

30. (New) The system of claim 21, wherein the key source comprises a semiconductor chip supporting a modem.

31. (New) The system of claim 30, wherein the semiconductor chip is a part of the key source external to the digital appliance system used to secure authentication.

32. (New) The system of claim 30, wherein the semiconductor chip derives power from a sound card of the digital appliance used to secure authentication.

33. (New) The system of claim 21, wherein the key is a sound file stored on a machine peripheral to the digital appliance used to secure authentication.

34. (New) The system of claim 33, wherein the peripheral machine is one of a cellular telephone, a personal digital assistant, or a hand held music player.

35. (New) A sound-producing device for generating a network-transmittable sound frame having embedded therein an identification number and a session key usable to authenticate a client, the device comprising:

a semiconductor chip supporting a modem;

a plug-in interface for enabling coupling with a host digital appliance; and

a housing of a size and shape to support hand-held operation.

36. (New) The device of claim 35, wherein the network is the Internet network.

37. (New) The device of claim 35, wherein the modem is a frequency-shift keying modem.

38. (New) The device of claim 35, wherein the plug-in interface is a tip/ring/sleeve interface for plugging into a microphone jack on the host digital appliance used to secure authentication.

39. (New) The device of claim 38, wherein the sound-producing device derives power from a soundcard residing on the digital appliance used to secure authentication.

40. (New) The device of claim 35 further comprising a switch for activating the modem to generate the sound.

41. (New) A method for enabling secure transacting over a network comprising:

(a) executing an application on a network server for storing client information and for activating a client for secure transacting in the network;

(b) connecting to the server over the network by the client through a network-connected digital appliance;

(c) providing a digital key to the digital appliance by a key source;

(d) providing the digital key to the server by the digital appliance; and

(e) authenticating the client by the application executing on the network, using the key provided and information regarding the client accessible to the network server.

42. (New) The method of claim 41 wherein the key is one of a character string, a modulated audio file, a modulated light source, an infra-red signal, or a vibratory signal.

43. (New) The method of claim 41 wherein the key source is a flash thumb drive.

44. (New) The method of claim 41 wherein the key source provides the key to the digital appliance through one of a USB port, a microphone jack, an infrared sensor, or a an audio microphone.

45. (New) The method of claim 41, wherein the network is the Internet network.

46. (New) The method of claim 41, wherein the information regarding the client comprises an identification number, a password or personal identification code, a session key, and a secrete data seed.

47. (New) The method of claim 41, wherein the key source comprises a semiconductor chip supporting a modem.

48. (New) The method of claim 47, wherein the semiconductor chip is a part of the key source external to the digital appliance system used to secure authentication.

49. (New) The method of claim 47, wherein the semiconductor chip derives power from a sound card of the digital appliance used to secure authentication.

50. (New) The method of claim 41, wherein the key is a sound file stored on a machine peripheral to the digital appliance used to secure authentication.

51. (New) The method of claim 50, wherein the peripheral machine is one of a cellular telephone, a personal digital assistant, or a hand held music player.

Remarks

The present Response is to the non-final Office Action mailed on 09/02/2009. Claims 1-20 are standing for examination.

Claim Rejections - 35 USC § 112

5. Claims 1-20 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The claims have been stated in a manner where there are not necessarily any specific features being claimed.

In independent claim 1 a system is claimed having:
a network sever application for (some intended purpose),
a software driver for (some intended purpose), and
a software applet for (some intended purpose)

Claims 2-11 are dependent on claim 1 and do not alleviate the deficiency.

Examiner suggests changing the claim language to read:
a network sever application ~~for storing~~ configured to store ...
a software driver ~~for performing~~ configured to perform ...
a software applet ~~for creating~~ configured to create ...

In independent claim 12 the claim language starts "In a system for" placing the claim language at two levels of removal from being limitations. First by placing it as "in a system" which means the system is not the actual invention and secondly it is for and intended use.

Claims 13-17 are dependent on claim 12 and do not alleviate the deficiency.

If what is intended to be claim is a system then the format of "A system for (preamble) said system comprising: (limitations of the system)" would be suggested.

If instead it is features of a device that are intended to be claimed a format such as "A device in a system for (preamble) said device comprising: (limitations of the device)."

In independent claim 18 the claim language states "A method for (an intended purpose)" however their is never established a clear delimitation to the start of the actual limitations of the method normally indicated by the words "said method comprising".

Claims 19-20 are dependent on claim 18 and do not alleviate the deficiency.

Applicant's response:

Applicant herein cancels claims 1-20. New claims 21-51 are herein presented for examination. Applicant believes the new claims, as presented, do not include the deficiencies pointed out in the 112 rejection, above.

Claim Rejections - 35 USC § 101

7. Claim(s) 1-20 are non-statutory because they are neither tied to a specific machine nor do they provide a transformation of material.

In claims independent claim 1-12 the elements: (a network sever application, a software driver, and a software applet) are claimed in the form of free floating software.

In claims 13-20 there are no physical structures present with which to make a judgment that the requirements of 35 USC § 101 have been met. (view the 35 USC § 112 rejections shown previously in this office action.)

Applicant's response:

Applicant herein cancels claims 1-20. New claims 21-51 are herein presented for examination. Applicant believes the new claims, as presented, do not include the deficiencies pointed out in the 101 rejection, above.

Claim Rejections - 35 USC § 102

9. Claim(s) 12-20 is/are rejected under 35 U.S.C. 102(b) as being anticipated by United States Patent Application Publication No.: US 20040093496 A1 (Colnot).

Applicant's response:

Applicant herein cancels claims 1-20 and presents new claims 21-51 for examination. Applicant believes that all of the newly claimed subject matter is not taught in the reference of Colnot. Further, applicant questions whether Colnot is a valid reference in the present rejection. Applicant's effective filing date is established with a provisional filing dated 09/20/2005. The filing date of Colnot is 05/13/2004; less than 1 year.

Claim Rejections - 35 USC § 103

11. Claim(s) 1-11 is/are rejected under 35 U.S.C. 103(a) as being unpatentable over United States Patent Application Publication No.: US 2005/0262573 A1 (Bo et al.) in view of United States Patent Application Publication No.: US 20040093496 A1 (Colnot).

Applicant's response:

Applicant cancels claims 1-20, presenting new claims 21-51. Applicant believes that Bo et al. fails to teach the subject matter contained in the newly presented claims. Further, applicant wishes to note that there is a common inventor in the present case and the references cited by the Examiner, and that the subject matter relied upon in the reference of Colnot is commonly owned and invented by the present inventor. The applicant reserves the right to analyze this probability relative to the applicability of the references at a later time.

Applicant will address the merits of valid rejections against the newly presented claims in the next Office Action issued by the Examiner.

Summary

As all of the claims, as amended and argued above, have been shown to be patentable over the art presented by the Examiner, applicant respectfully requests reconsideration and the case be passed quickly to issue.

If any fees are due beyond fees paid with this amendment, authorization is made to deduct those fees from deposit account 50-0534. If any time extension is needed beyond any extension requested with this amendment, such extension is hereby requested.

Respectfully Submitted,
Vincent Cedric Colnot

By */Donald R. Boys/*
Donald R. Boys
Reg. No. 35,074

Central Coast Patent Agency, Inc.3
Hangar Way, Suite D
Watsonville, CA 95076
831-768-1755

Electronic Patent Application Fee Transmittal

Application Number:	11533030
Filing Date:	19-Sep-2006
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

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Claims in excess of 20	2202	11	26	286
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 3 months with $0 paid	2253	1	555	555
Miscellaneous:				
		Total in USD ($)		**841**

Electronic Acknowledgement Receipt

EFS ID:	7111689
Application Number:	11533030
International Application Number:	
Confirmation Number:	3809
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
Receipt Date:	01-MAR-2010
Filing Date:	19-SEP-2006
Time Stamp:	15:52:47
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$841
RAM confirmation Number	2801
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	Extension of Time	Extension.pdf	845288 fe849fdb1858ca9307f3143591e01b91d5522980	no	1
Warnings:					
Information:					
2	Amendment/Req. Reconsideration-After Non-Final Reject	1987oar1.pdf	88986 9fe716b19a958b6229d6df35b071cb5ec746e83e	no	10
Warnings:					
Information:					
3	Fee Worksheet (PTO-875)	fee-info.pdf	32161 686c82261c3ac06cf880f2a72ba34f8509469d8f	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	966435		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/22 (10-08)
Approved for use through 10/31/2008. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARMENT OF COMMERCE
Under the paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless if displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a) **FY 2009** ***(Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).)***	Docket Number (Optional) P1987
Application Number 11/533,030	Filed 09/19/2006
For Vincent Cedric Colnot	
Art Unit 2434	Examiner Benjamin A. Kaplan

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

		Fee	Small Entity Fee	
☐	One month (37 CFR 1.17(a)(1))	$130	$65	$
☐	Two months (37 CFR 1.17(a)(2))	$490	$245	$
☑	Three months (37 CFR 1.17(a)(3))	$1110	$555	$ 555
☐	Four months (37 CFR 1.17(a)(4))	$1730	$865	$
☐	Five months (37 CFR 1.17(a)(5))	$2350	$1175	$

☑ Applicant claims small entity status. See 37 CFR 1.27.

☐ A check in the amount of the fee is enclosed.

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

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 50-0534.

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

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest. See 37 CFR 3.71.
Statement under 37 CFR 3.73(b) is enclosed (Form PTO/SB/96).

☑ attorney or agent of record. Registration Number 35,074

☐ attorney or agent under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34 _____

/Donald R. Boys/	03/01/2010
Signature	Date
Donald R. Boys	831-768-1755
Typed or printed name	Telephone Number

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

☐ Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.136(a). 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 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

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

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
11/533,030	09/19/2006	

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)	SMALL ENTITY ☒		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
AMENDMENT	03/01/2010	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 31	Minus	** 20	= 11	X $26 =	286	OR	X $ =	
	Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $110 =	0	OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE	286	OR	TOTAL ADD'L FEE	

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

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

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

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

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

Legal Instrument Examiner:
/TONYA MCBRIDE/

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/533,030	09/19/2006	Vincent Cedric Colnot	P1987	3809

24739 7590 09/02/2009

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

EXAMINER	
KAPLAN, BENJAMIN A	
ART UNIT	PAPER NUMBER
2434	

MAIL DATE	DELIVERY MODE
09/02/2009	PAPER

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

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

Office Action Summary	Application No.	Applicant(s)	
	11/533,030	COLNOT, VINCENT CEDRIC	
	Examiner	Art Unit	
	BENJAMIN A. KAPLAN	2434	

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

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

Status

1)☒ Responsive to communication(s) filed on *18 October 2006*.

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

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

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

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

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

Application Papers

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

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

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

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

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

Priority under 35 U.S.C. § 119

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

a)☐ All b)☐ Some * c)☐ None of:

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

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

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

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

Attachment(s)

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

DETAILED ACTION

1. This Office Action is in response to the most recent papers filed on 18 October 2006.

2. Claims 1-20 are pending.

3. Claims 1-20 are rejected.

Claim Rejections - 35 USC § 112

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

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

5. Claims 1-20 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The claims have been stated in a manner where there are not necessarily any specific features being claimed.

In independent claim 1 a system is claimed having:

a network sever application for (some intended purpose),

a software driver for (some intended purpose), and

a software applet for (some intended purpose)

Claims 2-11 are dependent on claim 1 and do not alleviate the deficiency.

Examiner suggests changing the claim language to read:

a network sever application ~~for storing~~ configured to store …

a software driver ~~for performing~~ configured to perform …

a software applet ~~for creating~~ configured to create …

In independent claim 12 the claim language starts “In a system for” placing the claim language at two levels of removal from being limitations. First by placing it as “in a system” which means the system is not the actual invention and secondly it is for and intended use.

Claims 13-17 are dependent on claim 12 and do not alleviate the deficiency.

If what is intended to be claim is a system then the format of "A system for (preamble) said system comprising: (limitations of the system)” would be suggested.

If instead it is features of a device that are intended to be claimed a format such as "A device in a system for (preamble) said device comprising: (limitations of the device).”

In independent claim 18 the claim language states “A method for (an intended purpose)” however their is never established a clear delimitation to the start of the actual limitations of the method normally indicated by the words “said method comprising”.

Claims 19-20 are dependent on claim 18 and do not alleviate the deficiency.

Claim Rejections - 35 USC § 101

6. 35 U.S.C. 101 reads as follows:

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

7. Claim(s) 1-20 are non-statutory because they are neither tied to a specific machine nor do they provide a transformation of material.

In claims independent claim 1-12 the elements: (a network sever application, a software driver, and a software applet) are claimed in the form of free floating software.

In claims 13-20 there are no physical structures present with which to make a judgment that the requirements of 35 USC § 101 have been met. (view the 35 USC § 112 rejections shown previously in this office action.)

Claim Rejections - 35 USC § 102

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

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

9. Claim(s) 12-20 is/are rejected under 35 U.S.C. 102(b) as being anticipated by United States Patent Application Publication No.: US 20040093496 A1 (Colnot).

As Per Claim 12: Colnot teaches: **In a system for enabling secure transacting over a network**,

- a sound-producing device for generating a network transmittable sound frame having embedded therein an identification number and a session key used to authenticate a client, the device comprising: a semiconductor chip supporting a modem; an electrical plug-in interface for enabling coupling with a host machine; and a housing of a size and shape to support hand-held operation

(Colnot, Drawings, Figure. 1. "

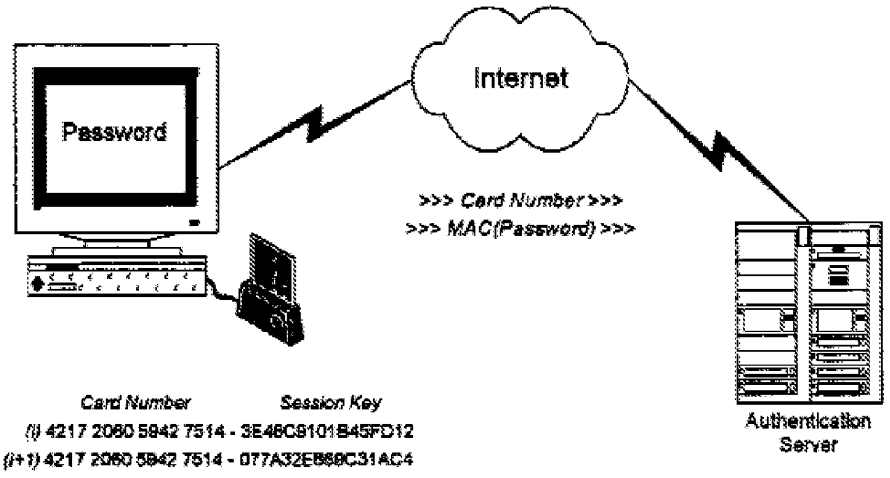


FIG. 1

").

(Colnot, Paragraphs [0011]-[0014], "The method, as detailed in FIG. 1, carries out the user authentication on the Internet. The apparatus comprises a smart card with a modulation output, a card reader plugged into the microphone input, and a PC applet. The user inserts his card in the reader and enters his password on the PC keyboard.

When activated in the card reader, the smart card transmits an identification sequence to the PC in the form of a modulated signal, which is demodulated by the PC applet. The identification sequence comprises an 8-byte card number and an 8-byte random number valid only once. The card number is unique and identifies the card

issuer, application version and user account. The random number is a session key (Ki) which is a function of the previous one (Ki-1) emitted by the card such as: Ki=G(Ki-1), G is a one-way function also known by the authentication server.

The session key (Ki) is used by the PC applet to generate a message authentication code (MAC) of the password entered by the user, using the DES algorithm for instance. This first MAC is transmitted to the authentication server along with the card number, allowing the server to retrieve the previous session key (Ki-1) and the password stored in the authentication server database.

The authentication server deduces from (Ki-1) the session key used by the card, and generates a second MAC of the password stored in the database. The authentication is valid only if the first and second MAC are identical, which means the PC and the authentication server have used the same session key (Ki) to generate a MAC of the same password. If this is the case, the authentication server replaces (Ki-1) by (Ki) in the database. The session key (Ki) cannot be reused, even though the session key (Ki) has not been transmitted to the authentication server.").

As Per Claim 13: The rejection of claim 12 is incorporated and further the internet is a data-packet-network.

As Per Claim 14: The rejection of claim 12 is incorporated and further frequency-shift keying is the basic activity used to form modem communication (along with amplitude modulation and phase modulation)

As Per Claim 15: The rejection of claim 12 is incorporated and further Colnot teaches:

- the electrical plug-in interface is a tip/ring/sleeve interface for plugging into a microphone jack on a host machine used to secure authentication

(Colnot, Paragraph [0011], "The method, as detailed in FIG. 1, carries out the user authentication on the Internet. The apparatus comprises a smart card with a modulation output, a card reader plugged into the microphone input, and a PC applet. The user inserts his card in the reader and enters his password on the PC keyboard.").

As Per Claim 16: The rejection of claim 15 is incorporated and further Colnot teaches:

- the sound-producing device derives power from a soundcard residing on a host machine used to secure authentication

(Colnot, Abstract, "A method and apparatus to secure online transactions on the Internet comprising 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.").

(Colnot, Paragraph [0008], "FIG. 2A is a schematic of the reader powered by the microphone input.").

As Per Claim 17: The rejection of claim 12 is incorporated and further Colnot teaches:

- a switch for activating the modem to generate the sound

(Colnot, Paragraph [0019], "The PC sound cards provides a +3V to +5V DC voltage on the microphone input which is sufficient to power (Vbb) the smart card. The resistor R1 adapts the level of the modulated signal to the microphone input. When pressed, the switch S1 pulls down the reset input (Rst) activating the modulation output (Mod).").

As Per Claim 18: Colnot teaches: **A method for sending a secure modulated sound pass from a sound-producing device having a semiconductor chip supporting a modem, an electrical plug-in interface for enabling coupling with a host machine, and a housing of a size and shape to support hand-held operation to a software applet for demodulating the sound pass to glean the secure data embedded therein comprising the acts: (a) plugging the device into an audio line-in of a host machine used to secure authentication; and (b) activating the device to generate and input the sound pass.**

(Colnot, Drawings, Figure. 1. "

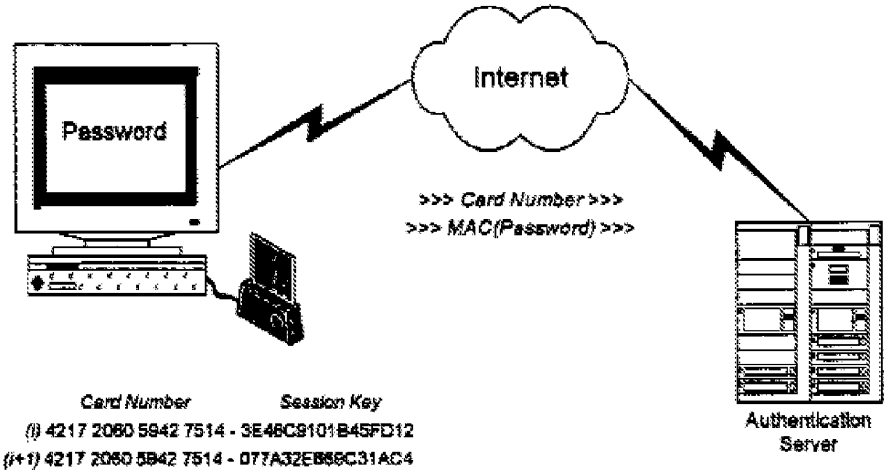


FIG. 1

").

(Colnot, Paragraphs [0011]-[0014], "The method, as detailed in FIG. 1, carries out the user authentication on the Internet. The apparatus comprises a smart card with a modulation output, a card reader plugged into the microphone input, and a PC applet. The user inserts his card in the reader and enters his password on the PC keyboard.

When activated in the card reader, the smart card transmits an identification sequence to the PC in the form of a modulated signal, which is demodulated by the PC applet. The identification sequence comprises an 8-byte card number and an 8-byte random number valid only once. The card number is unique and identifies the card issuer, application version and user account. The random number is a session key (Ki) which is a function of the previous one (Ki-1) emitted by the card such as: Ki=G(Ki-1), G is a one-way function also known by the authentication server.

The session key (Ki) is used by the PC applet to generate a message authentication code (MAC) of the password entered by the user, using the DES algorithm for instance. This first MAC is transmitted to the authentication server along

with the card number, allowing the server to retrieve the previous session key (Ki-1) and the password stored in the authentication server database.

The authentication server deduces from (Ki-1) the session key used by the card, and generates a second MAC of the password stored in the database. The authentication is valid only if the first and second MAC are identical, which means the PC and the authentication server have used the same session key (Ki) to generate a MAC of the same password. If this is the case, the authentication server replaces (Ki-1) by (Ki) in the database. The session key (Ki) cannot be reused, even though the session key (Ki) has not been transmitted to the authentication server.").

As Per Claim 19: The rejection of claim 18 is incorporated and further Colnot teaches:

- in act (a), the audio line-in is one of a microphone input, universal serial bus, or a telephone line port of the host machine

(Colnot, Abstract, "A method and apparatus to secure online transactions on the Internet comprising 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.").

As Per Claim 20: The rejection of claim 18 is incorporated and further Colnot teaches:

- in act (b), activation is caused by manipulating a switch on the device

(Colnot, Paragraph [0019], "The PC sound cards provides a +3V to +5V DC voltage on the microphone input which is sufficient to power (Vbb) the smart card. The resistor R1 adapts the level of the modulated signal to the microphone input. When pressed, the switch S1 pulls down the reset input (Rst) activating the modulation output (Mod).").

Claim Rejections - 35 USC § 103

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

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claim(s) 1-11 is/are rejected under 35 U.S.C. 103(a) as being unpatentable over United States Patent Application Publication No.: US 2005/0262573 A1 (Bo et al.) in view of United States Patent Application Publication No.: US 20040093496 A1 (Colnot).

As Per Claim 1: Bo et al. teaches: **A system for enabling secure transacting over a network comprising:**

- a network sever application for storing client information and activating clients for secure transacting

(Bo et al., Paragraph [0109], “FIG. 1 shows a DRM (digital rights management) system according to a first specific embodiment of this invention. With reference to FIG. 1, the DRM system includes a session resource manager (SRM) 5 coupled via a suitable connection, such as an SSL (secure sockets layer) connection, to a web server 13. In turn, the web server 13 is used to allow a client 23, such as a user's end station, to access the features provided by the SRM 5 via an appropriate web browser 15 and/or an SSL connection. A server agent platform 14 is implemented and provided in the web server 13.”).

- a software driver for performing authentication, the software driver accessible to the network server;

- a software applet for creating a secure data record and for managing transmission and update of the contents of the record;

(Bo et al., Paragraphs [0242]-[0243], “c) With the agreement of the user, an application of the client 23 is downloaded from the web server 13 as S27 shows. The application is, for example, a Java applet. The user installs the application on the end station as S28 shows. Thus, the application of the client 23 is implemented.

d) With the agreement of the user, the application of the client 23 establishes an SSL connection (an SSL link) with the web server 13 for further transactions as S29 shows.”).

(Bo et al., Paragraph [0253], "FIG. 16 shows a method of user authentication and digital audio-visual content encryption key(s) distribution. Each time a registered user wants to enjoy the services from the content provider, the user may be authenticated.").

The driver is the inherent underlying software that makes it possible for a system to operate with its underlying hardware and functions thereof.

Bo et al. does not explicitly teach the following limitation:

- and a sound source in the form of a file or a sound generating device, the sound source being part of or having access to the secure data record.

However Colnot in analogous art does teach the above limitation:

(Colnot, Paragraph [0011], "The method, as detailed in FIG. 1, carries out the user authentication on the Internet. The apparatus comprises a smart card with a modulation output, a card reader plugged into the microphone input, and a PC applet. The user inserts his card in the reader and enters his password on the PC keyboard.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Colnot in to the method of Bo et al. in order to take advantage of being able to inexpensively add the enhancements of smart card authentication (Colnot, Paragraph [0005]).

As Per Claim 2: The rejection of claim 1 is incorporated and further Bo et al. teaches:

- the network is a data-packet-network

(Bo et al., Paragraphs [0028]-[0029], "A fourteenth aspect of this invention provides a digital right management system for managing the presentation of content, comprising a base station, at least one end station, and a communications network for interconnecting the base station and the end station. The base station includes a processor for a1) receiving an access request from an end station via the communications network; a2) generating an agent in response to the access request; a3) transferring the agent to the end station via the communications network, wherein the end station implements the agent and the implemented agent determines end station data indicative of an identity of the end station and transfers the end station data to the base station via the communications network; a4) authenticating the end station in response to the end station data; a5) deciding whether the authentication is successful; and a6) authorizing the end station to perform the presentation of content when the authentication is successful. The end station includes a display; and a processor for b21) generating an access request; b22) transferring the access request to the base station via the communications network; b23) receiving the agent from the base station via the communications network; b24) implementing the agent, wherein the implemented agent determines the end station data and transfers the end station data to the base station via the communications network, and wherein the base station authenticates the end station in response to the end station data and decides whether the authentication is successful; and b25) presenting the content by use of the display when the base station decides that the authentication is successful.

A fifteenth aspect of this invention provides a method of decrypting content for presentation. The content includes one or more data packets each having an encrypted payload. The method comprises the steps of receiving encrypted content; determining the payload in each data packet; decrypting the determined payload using first and second keys; and combining the decrypted payloads of the one or more data packets to form decrypted content.").

As Per Claim 3: The rejection of claim 1 is incorporated and further Bo et al. teaches:

- the secure data record is unique to a client and includes an identification number, a password or personal identification code, a session key, and a secrete data seed

(Bo et al., Paragraph [0152], "In one example, the web server 13 is used to transfer user's personal information from the client 23 to the SRM 5 through a pre-established SSL link. The user's personal information includes user's log-in ID and password. The user account manager 35 in the SRM 5 maintains and manages all the user's personal information.").

(Bo et al., Paragraph [0147], "The encipheror 3 or the encipheror in the encipheror/decipherer module 38 defines a block cipher algorithm, e.g., DES (data encryption standard), AES (advanced encryption standard), or Blowfish. The encipheror 3 or the encipheror in the encipheror/decipherer module 38 also defines the seeds for generating random keys, the preferred key length for the block cipher algorithm that

accepts variable length keys, the preferred plaintext block size, e.g., 64 bits, 128 bits, or 256 bits. Otherwise, a default encryption strategy is to be used.").

As Per Claims 4 and 5: The rejection of claim 1 is incorporated and further:

(Bo et al., Paragraph [0109], "FIG. 1 shows a DRM (digital rights management) system according to a first specific embodiment of this invention. With reference to FIG. 1, the DRM system includes a session resource manager (SRM) 5 coupled via a suitable connection, such as an SSL (secure sockets layer) connection, to a web server 13. In turn, the web server 13 is used to allow a client 23, such as a user's end station, to access the features provided by the SRM 5 via an appropriate web browser 15 and/or an SSL connection. A server agent platform 14 is implemented and provided in the web server 13.").

The driver is the inherent underlying software that makes it possible for a system to operate with its underlying hardware and functions thereof. Drivers are present on both the SRM and the Web server.

As Per Claim 6: The rejection of claim 1 is incorporated and further Bo et al. teaches:

- the software applet is a Java applet and the secure data record is a Java archive

(Bo et al., Paragraphs [0242]-[0243], "c) With the agreement of the user, an application of the client 23 is downloaded from the web server 13 as S27 shows. The

application is, for example, a Java applet. The user installs the application on the end station as S28 shows. Thus, the application of the client 23 is implemented.

d) With the agreement of the user, the application of the client 23 establishes an SSL connection (an SSL link) with the web server 13 for further transactions as S29 shows.").

As Per Claim 7: The rejection of claim 1 is incorporated and further Bo et al. teaches:

- the sound source is a semiconductor chip supporting a modem

(Bo et al., Paragraph [0120], "It will be appreciated by persons skilled in the art that any one or more of the SRM 5, the web server 13, the encipheror 3, and the file/data server 4 may be provided at a centralised base station which can then be coupled to one or more end stations inclusive of the client device 23 via a suitable communications network. Examples of the communications network are the Internet, one or more WANs (wide area networks), and LANs (local area networks).").

The modem is the specific card or device that caries out the communications on the network to which the other various devisees and components of the method are attached.

As Per Claim 8: The rejection of claim 7 is incorporated and further Bo et al. does not explicitly teach the following limitation:

- the semiconductor chip is external to a client system used to secure authentication

However Colnot in analogous art does teach the above limitation:

(Colnot, Paragraph [0011], "The method, as detailed in FIG. 1, carries out the user authentication on the Internet. The apparatus comprises a smart card with a modulation output, a card reader plugged into the microphone input, and a PC applet. The user inserts his card in the reader and enters his password on the PC keyboard.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Colnot in to the method of Bo et al. in order to take advantage of being able to inexpensively add the enhancements of smart card authentication (Colnot, Paragraph [0005]).

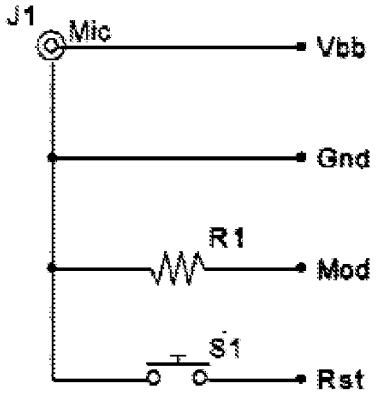
As Per Claim 9: The rejection of claim 8 is incorporated and further Bo et al. does not explicitly teach the following limitation:

- the semiconductor chip derives power from a sound card of the system used to secure authentication

(Colnot, Paragraph [0008], "FIG. 2A is a schematic of the reader powered by the microphone input.").

(Colnot, Drawings, Figure. 2A. "

FIG. 2A



").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Colnot in to the method of Bo et al. in order to take advantage of being able to inexpensively add the enhancements of smart card authentication (Colnot, Paragraph [0005]).

As Per Claim 10 and 11: The rejection of claim 1 is incorporated and further Bo et al. teaches:

- the sound source is a sound file stored on a machine peripheral to the machine used to secure authentication

- the peripheral machine is one of a cellular telephone, a personal digital assistant, or a hand held music player

(Colnot, Paragraph [0123], "The DRM-system's elements described above with respect to FIG. 1 can include so-called general-purpose computers, workstations, or personal computers, as well as network connectable information-processing devices, for

instance, digital home electric appliances, portable terminals, PDAs, or cellular phones.").

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BENJAMIN A. KAPLAN whose telephone number is (571)-270-3170. The examiner can normally be reached on 7:30 a.m. - 5:00 p.m. E.S.T..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. 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.

/Benjamin A Kaplan/

Examiner, Art Unit 2434

/Farid Homayounmehr/
AU: 2439

Notice of References Cited	Application/Control No. 11/533,030	Applicant(s)/Patent Under Reexamination COLNOT, VINCENT CEDRIC	
	Examiner BENJAMIN A. KAPLAN	Art Unit 2434	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,282,653 B1	08-2001	Berstis et al.	726/26
*	B	US-2003/0065919 A1	04-2003	Albert et al.	713/168
*	C	US-2003/0177354 A1	09-2003	CARTER, GEORGE E.	713/164
*	D	US-2004/0093496 A1	05-2004	Colnot, Vincent Cedric	713/168
*	E	US-2004/0107356 A1	06-2004	Shamoon et al.	713/193
*	F	US-2005/0262573 A1	11-2005	Bo et al.	726/027
*	G	US-7,233,948 B1	06-2007	Shamoon et al.	707/9
*	H	US-7,359,883 B2	04-2008	Namba et al.	705/59
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

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

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

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11533030	COLNOT, VINCENT CEDRIC
	Examiner	Art Unit
	BENJAMIN A KAPLAN	2434

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

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

CLAIM		DATE								
Final	Original	08/28/2009								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11533030	COLNOT, VINCENT CEDRIC
	Examiner	Art Unit
	BENJAMIN A KAPLAN	2434

SEARCHED			
Class	Subclass	Date	Examiner
726	2,9,26,27	8/28/2009	BK

SEARCH NOTES		
Search Notes	Date	Examiner
East, Plus Search, Google	8/28/2009	BK

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	1	11/533,030.app.	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/18 13:57
S2	296	(("20010037461") or ("20010042124") or ("20020031225") or ("20020099940") or ("20020099942") or ("20020191765") or ("20030009676") or ("20030009692") or ("20030033545") or ("20030056096") or ("20030065919") or ("20030100371") or ("20030126457") or ("20030169713") or ("20030177354") or ("20030233450") or ("20030233583") or ("20040054794") or ("20040127279") or ("20040133789") or ("20040218897") or ("20050010777") or ("20050021613") or ("20050233811") or ("20060006230") or ("20060059265") or ("20060112213") or ("20060155601") or ("20060161775") or ("20060205394") or ("20060272023") or ("20060288407") or ("20070022469") or ("20070067833") or ("20070098175") or ("20070130334") or ("20070190975") or ("20070232355") or ("20070282909") or ("20080177998") or ("20090125717") or ("20090150977") or ("20090198996") or	US-PGPUB; USPAT; USOCR	OR	OFF	2009/08/27 18:23

("4295155") or
("4386233") or
("4423287") or
("4755940") or
("4783798") or
("4888801") or
("4890323") or
("4897875") or
("4905766") or
("4910773") or
("4956862") or
("4997288") or
("5008936") or
("5016277") or
("5022076") or
("5202921") or
("5204961") or
("5210794") or
("5210795") or
("5226079") or
("5237614") or
("5239294") or
("5241594") or
("5261002") or
("5272754") or
("5276735") or
("5311596") or
("5313521") or
("5347387") or
("5349643") or
("5353353") or
("5369705") or
("5371794") or
("5410602") or
("5412726") or
("5425130") or
("5444780") or
("5454000") or
("5469507") or
("5479341") or
("5481613") or
("5485196") or
("5491752") or
("5499297") or
("5500897") or
("5502766") or
("5535276") or
("5557686") or
("5587809") or
("5588060") or
("5590196") or
("5590199") or
("5590200") or
("5592555") or

		("5598459") or ("5602915") or ("5602918") or ("5604663") or ("5604803") or ("5619657") or ("5623601") or ("5633933") or ("5633934") or ("5638448") or ("5643086") or ("5655077") or ("5657390") or ("5666412") or ("5668877") or ("5671279") or ("5673318") or ("5675651") or ("5684950") or ("5687235") or ("5689566") or ("5692400") or ("5699513") or ("5719941") or ("5721779") or ("5724168") or ("5724423") or ("5729594") or ("5732137") or ("5734718") or ("5742756") or ("5745574") or ("5745576") or ("5748736") or ("5754659") or ("5757913") or ("5757918") or ("5764890") or ("5768378") or ("5778065") or ("5778071") or ("5778313")).PN. or (("5781550") or ("5781724") or ("5784463") or ("5787172") or ("5790669") or ("5796833") or ("5799082") or ("5802178") or ("5802497") or ("5805712") or ("5805803") or ("5809117") or					

("5812664") or
("5812669") or
("5812764") or
("5812955") or
("5818936") or
("5822431") or
("5825300") or
("5825877") or
("5825890") or
("5828832") or
("5832209") or
("5832228") or
("5841120") or
("5841864") or
("5850442") or
("5850445") or
("5864665") or
("5870473") or
("5870475") or
("5870544") or
("5872915") or
("5875296") or
("5875394") or
("5875395") or
("5883956") or
("5887063") or
("5887250") or
("5889861") or
("5892829") or
("5892838") or
("5892902") or
("5894552") or
("5903721") or
("5907620") or
("5909491") or
("5913175") or
("5918228") or
("5922074") or
("5923756") or
("5926624") or
("5930362") or
("5931947") or
("5947571") or
("5953422") or
("5963644") or
("5963915") or
("5966441") or
("5967466") or
("5970144") or
("5974144") or
("5978475") or
("5978918") or
("5983350") or
("5995624") or

("5996077") or
("6002767") or
("6009524") or
("6012144") or
("6012632") or
("6017004") or
("6021497") or
("6023764") or
("6026167") or
("6026293") or
("6032150") or
("6032260") or
("6038551") or
("6038892") or
("6044155") or
("6044468") or
("6047072") or
("6047325") or
("6047572") or
("6049878") or
("6052785") or
("6055236") or
("6055636") or
("6061346") or
("6061448") or
("6061448") or
("6061449") or
("6061790") or
("6061796") or
("6061796") or
("6061799") or
("6061799") or
("6065120") or
("6067620") or
("6075860") or
("6081900") or
("6088451") or
("6098056") or
("6119233") or
("6141752") or
("6144848") or
("6148405") or
("6151590") or
("6158007") or
("6178089") or
("6185612") or
("6192474") or
("6198824") or
("6199113") or
("6202081") or
("6216231") or
("6216231") or
("6230266") or
("6233608") or

		("6233687") or ("6233688") or ("6247129") or ("6249867") or ("6249873") or ("6263313") or ("6272633") or ("6282653") or ("6301667") or ("6314468") or ("6345256") or ("6374402") or ("6389403") or ("6389538") or ("6418421") or ("6438600") or ("6449367") or ("6453416") or ("6463537") or ("6678826") or ("6732105") or ("6763370") or ("6907530") or ("6912653") or ("6945870") or ("6973566") or ("7017188") or ("7028182") or ("7073055") or ("7100054")).PN. or (("7103770") or ("7152160") or ("7171467") or ("7184999") or ("7188179") or ("7231025") or ("7287271") or ("7496950") or ("7502928") or ("7509119") or ("7533735")).PN.				
S3	300	(("20010034716") or ("20020014054") or ("20020017079") or ("20020020752") or ("20020032746") or ("20020036114") or ("20020052797") or ("20020073036") or ("20020077992") or ("20020091646") or ("20020103857") or ("20020116274") or ("20020141576") or	US-PGPUB; USPAT; USOCR	OR	OFF	2009/08/27 18:24

("20020157019") or
("20020178364") or
("20020191790") or
("20030014669") or
("20030018916") or
("20030023578") or
("20030028491") or
("20030046586") or
("20030046587") or
("20030046889") or
("20030055733") or
("20030056054") or
("20030056092") or
("20030061173") or
("20030061275") or
("20030061387") or
("20030061506") or
("20030065919") or
("20030081783") or
("20030088426") or
("20030097592") or
("20030100372") or
("20030111266") or
("20030115455") or
("20030126192") or
("20030126483") or
("20030163423") or
("20030163723") or
("20030177348") or
("20030177354") or
("20030182574") or
("20030188003") or
("20030188156") or
("20030188165") or
("20030191932") or
("20030208689") or
("20030221118") or
("20030226014") or
("20030226022") or
("20030229802") or
("20030233550") or
("20030236997") or
("20040002381") or
("20040020164") or
("20040065501") or
("20040068648") or
("20040068726") or
("20040073151") or
("20040083184") or
("20040083375") or
("20040088252") or
("20040089482") or
("20040095083") or
("20040098740") or

		("20040103165") or ("20040111578") or ("20040114182") or ("20040117623") or ("20040117627") or ("20040117635") or ("20040117661") or ("20040121787") or ("20040128517") or ("20040139019") or ("20040158635") or ("20040167465") or ("20040168081") or ("20040182126") or ("20040192303") or ("20040221168") or ("20040224769") or ("20040224771") or ("20040228063") or ("20040230809") or ("20040231594") or ("20040243853") or ("20050002328") or ("20050028487") or ("20050030151") or ("20050031136") or ("20050033980") or ("20050044404") or ("20050050342") or ("20050051448") or ("20050054445") or ("20050055588") or ("20050055815") or ("20050061878") or ("20050081063") or ("20050085931") or ("20050086509") or ("20050091364") or ("20050091527") or ("20050097350") or ("20050102535") or ("20050105736") or ("20050111380") or ("20050114687") or ("20050116026") or ("20050121339") or ("20050132031") or ("20050138356") or ("20050138423") or ("20050144493") or ("20050145695")).PN. or (("20050159203") or ("20050160417") or ("20050172132") or					

		("20050182938") or ("20050185647") or ("20050188251") or ("20050188731") or ("20050198461") or ("20050209006") or ("20050209842") or ("20050213768") or ("20050223220") or ("20050226175") or ("20050240685") or ("20050240712") or ("20050251685") or ("20050251852") or ("20050256806") or ("20050257245") or ("20050268336") or ("20060004964") or ("20060005072") or ("20060015947") or ("20060019657") or ("20060025147") or ("20060026573") or ("20060036693") or ("20060039305") or ("20060039306") or ("20060039321") or ("20060039339") or ("20060039340") or ("20060039360") or ("20060039562") or ("20060039563") or ("20060041750") or ("20060041761") or ("20060042882") or ("20060047784") or ("20060050887") or ("20060056630") or ("20060059543") or ("20060074983") or ("20060085370") or ("20060087192") or ("20060095377") or ("20060111165") or ("20060111794") or ("20060136742") or ("20060143700") or ("20060155589") or ("20060156019") or ("20060156399") or ("20060179308") or ("20060184524") or ("20060189382") or ("20060193474") or					

		("20060197403") or ("20060200660") or ("20060270346") or ("20070041110") or ("20070067833") or ("20070294085") or ("20080098872") or ("20080161951") or ("20080188182") or ("20080228865") or ("20080240468") or ("3683325") or ("4526115") or ("5051564") or ("5282247") or ("5406039") or ("5493767") or ("5656799") or ("5657388") or ("5695183") or ("5749253") or ("5825752") or ("6022009") or ("6038590") or ("6105042") or ("6118732") or ("6178550") or ("6209095") or ("6226697") or ("6233620") or ("6254366") or ("6282653") or ("6298336") or ("6328149") or ("6339827") or ("6382516") or ("6389541") or ("6393569") or ("6442532") or ("6502746") or ("6507908") or ("6520285") or ("6615194") or ("6620047") or ("6671810") or ("6701304") or ("6710893") or ("6722466") or ("6748532") or ("6769068") or ("6789147") or ("6823452") or ("6836795") or ("6845905") or					

		("6901251") or ("6915437") or ("6916247") or ("6920557") or ("6928707") or ("6934848") or ("6945458") or ("6957343") or ("6961759") or ("6970918") or ("6976164") or ("6976172") or ("6996841") or ("7013387") or ("7020476") or ("7024377") or ("7063615") or ("7069442") or ("7084734") or ("7085933") or ("7089587")).PN. or (("7095150") or ("7101296") or ("7103529") or ("7135968") or ("7137016") or ("7143280") or ("7146640") or ("7149821") or ("7152245") or ("7154628") or ("7155615") or ("7159242") or ("7185365") or ("7197644") or ("7207481") or ("7219480") or ("7228566") or ("7237717") or ("7245726") or ("7266703") or ("7290287") or ("7313679") or ("7333717") or ("7336789") or ("7343411") or ("7346929") or ("7350230") or ("7371952") or ("7383193") or ("7401230") or ("7418504") or ("7424610") or ("7428754") or					

		("7441153") or ("7452278") or ("7455590") or ("7458075") or ("7469341") or ("7469368") or ("7496097") or ("7502475") or ("7506170") or ("7509487") or ("7516331") or ("7530103") or ("7539651") or ("7540516") or ("7549922") or ("7574509") or ("7577258")).PN.				
S4	283	S2 @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:25
S5	285	S3 @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:25
S6	3	S4 S5	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:25
S7	29905	server client authentication @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:52
S8	21050	server client authentication key @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:52
S9	14617	server client authentication key secure @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:52
S10	4843	server client authentication key secure java @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:53
S11	2219	server client authentication key secure java applet @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:53
S12	604	server client authentication key secure java applet archive @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:53
S13	322	server client authentication key secure java applet archive sound card @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:53

S14	322	server client authentication key secure java applet archive sound card network @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:54
S15	283	server client authentication key secure java applet archive sound card network password @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:54
S16	279	server client authentication key secure java applet archive sound card network password session @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:54
S17	30	server client authentication key secure java applet archive sound card network password session seed @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 18:54
S18	0	server client authentication key secure java applet archive (sound adj source) @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 19:15
S19	1	server client authentication key secure java applet archive (sound same password) @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 19:17
S20	1	10/696,650.app.	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/27 19:26
S21	244	server client authentication key secure java applet archive (smart adj card) @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 18:48
S22	244	server client authentication key secure java applet archive (smart adj card) network @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 18:48
S23	234	server client authentication key secure java applet archive (smart adj card) network password @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 18:48

S24	225	server client authentication key secure java applet archive (smart adj card) network password session @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 18:49
S25	27	server client authentication key secure java applet archive (smart adj card) network password session seed @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 18:49
S26	1546	(726/2).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2009/08/28 20:32
S27	694	(726/9).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2009/08/28 20:32
S28	2232	(726/26).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2009/08/28 20:32
S29	1545	(726/27).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2009/08/28 20:32
S30	1033	S26 @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 20:32
S31	453	S27 @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 20:32
S32	1688	S28 @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 20:32
S33	1050	S29 @ad<"20050920"	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 20:32
S34	1	S30 S31 S32 S33	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 20:33
S35	3732	S30 or S31 or S32 or S33	US-PGPUB; USPAT; USOCR	AND	ON	2009/08/28 20:33

8/28/2009 9:44:39 PM
C:\Documents and Settings\bkaplan\My Documents\EAST\Workspaces\11533030.wsp

PLUS Search Results for S/N 11533030, Searched Wed Aug 19 08:10:52 EDT 2009

The Patent Linguistics Utility System (PLUS) is a USPTO automated search system for U.S. Patents from 1971 to the present PLUS is a query-by-example search system which produces a list of patents that are most closely related linguistically to the application searched. This search was prepared by the staff of the Scientific and Technical Information Center, SIRA.

5656799 99
20060270346 99
20070067833 99
20080161951 99
20080228865 99
6722466 82
20040065501 82
20040089482 82
3683325 80
5406039 80
5749253 80
6105042 80
6118732 80
6282653 80
6382516 80
6520285 80
7135968 80
7245726 80
7333717 80
7371952 80
20020020752 80
20020036114 80
20030046889 80
20030177354 80
20040068648 80
20040073151 80
20050031136 80
20050121339 80
20050182938 80
20070041110 80
20070294085 80
20080098872 80
20080188182 80
20080240468 80
4526115 67
5051564 67
5282247 67
5493767 67
5657388 67
5695183 67
5825752 67
6022009 67
6038590 67
6178550 67
6209095 67
6226697 67
6233620 67
6254366 67
6298336 67
6328149 67
6339827 67
6389541 67
6393569 67
6442532 67
6502746 67
6507908 67
6615194 67
6620047 67
6671810 67
6701304 67
6710893 67
6748532 67
6769068 67
6789147 67
6823452 67
6836795 67
6845905 67
6901251 67
6915437 67
6916247 67
6920557 67
6928707 67
6934848 67
6945458 67
6957343 67
6961759 67
6970918 67
6976164 67
6976172 67
6996841 67
7013387 67
7020476 67
7024377 67
7063615 67
7069442 67
7084734 67
7085933 67
7089587 67
7095150 67
7101296 67
7103529 67
7137016 67
7143280 67
7146640 67
7149821 67
7152245 67
7154628 67
7155615 67
7159242 67
7185365 67
7197644 67
7207481 67
7219480 67
7228566 67
7237717 67
7266703 67
7290287 67
7313679 67
7336789 67
7343411 67
7346929 67
7350230 67
7383193 67
7401230 67
7418504 67
7424610 67
7428754 67
7441153 67
7452278 67
7455590 67
7458075 67
7469341 67
7469368 67
7496097 67
7502475 67
7506170 67
7509487 67
7516331 67
7530103 67
7539651 67
7540516 67
7549922 67
7574509 67
7577258 67
20010034716 67
20020014054 67
20020017079 67
20020032746 67
20020052797 67
20020073036 67
20020077992 67
20020091646 67
20020103857 67
20020116274 67
20020141576 67
20020157019 67
20020178364 67

20020191790 67
20030014669 67
20030018916 67
20030023578 67
20030028491 67
20030046586 67
20030046587 67
20030055733 67
20030056054 67
20030056092 67
20030061173 67
20030061275 67
20030061387 67
20030061506 67
20030065919 67
20030081783 67
20030088426 67
20030097592 67
20030100372 67
20030111266 67
20030115455 67
20030126192 67
20030126483 67
20030163423 67
20030163723 67
20030177348 67
20030182574 67
20030188003 67
20030188156 67
20030188165 67
20030191932 67
20030208689 67
20030221118 67
20030226014 67
20030226022 67
20030229802 67
20030233550 67
20030236997 67
20040002381 67
20040020164 67
20040068726 67
20040083184 67
20040083375 67
20040088252 67
20040095083 67
20040098740 67
20040103165 67
20040111578 67
20040114182 67
20040117623 67
20040117627 67
20040117635 67
20040117661 67
20040121787 67
20040128517 67
20040139019 67
20040158635 67
20040167465 67
20040168081 67
20040182126 67
20040192303 67
20040221168 67
20040224769 67
20040224771 67
20040228063 67
20040230809 67
20040231594 67
20040243853 67
20050002328 67
20050028487 67
20050030151 67
20050033980 67
20050044404 67
20050050342 67
20050051448 67
20050054445 67
20050055588 67
20050055815 67
20050061878 67
20050081063 67
20050085931 67
20050086509 67
20050091364 67
20050091527 67
20050097350 67
20050102535 67
20050105736 67
20050111380 67
20050114687 67
20050116026 67
20050132031 67
20050138356 67
20050138423 67
20050144493 67
20050145695 67
20050159203 67
20050160417 67
20050172132 67
20050185647 67
20050188251 67
20050188731 67
20050198461 67
20050209006 67
20050209842 67
20050213768 67
20050223220 67
20050226175 67
20050240685 67
20050240712 67
20050251685 67
20050251852 67
20050256806 67
20050257245 67
20050268336 67
20060004964 67
20060005072 67
20060015947 67
20060019657 67
20060025147 67
20060026573 67
20060036693 67
20060039305 67
20060039306 67
20060039321 67
20060039339 67
20060039340 67
20060039360 67
20060039562 67
20060039563 67
20060041750 67
20060041761 67
20060042882 67
20060047784 67
20060050887 67
20060056630 67
20060059543 67
20060074983 67
20060085370 67
20060087192 67
20060095377 67
20060111165 67
20060111794 67
20060136742 67
20060143700 67
20060155589 67
20060156019 67
20060156399 67
20060179308 67
20060184524 67
20060189382 67
20060193474 67
20060197403 67
20060200660 67

PLUS Search Results for S/N 11533030, Searched Tue Aug 18 14:06:52 EDT 2009

The Patent Linguistics Utility System (PLUS) is a USPTO automated search system for U.S. Patents from 1971 to the present PLUS is a query-by-example search system which produces a list of patents that are most closely related linguistically to the application searched. This search was prepared by the staff of the Scientific and Technical Information Center, SIRA.

20070067833 99
7509119 76
20050010777 76
20070190975 76
5870544 70
6023764 70
5809117 70
6119233 70
20060155601 70
6158007 67
6032150 67
6438600 67
6453416 67
6907530 67
6912653 67
7100054 67
7103770 67
7287271 67
7502928 67
20010037461 67
20010042124 67
20020031225 67
20020099940 67
20020099942 67
20030033545 67
20030169713 67
20060112213 67
20060288407 67
20090125717 67
5311596 67
5272754 67
5675651 67
5778071 67
5832209 67
6075860 67
6233687 67
6233688 67
6301667 67
6314468 67
6374402 67
6463537 67
6678826 67
6732105 67
6763370 67
6973566 67
7017188 67
7073055 67
7152160 67
7171467 67
7184999 67
7188179 67
7496950 67
20030009676 67
20030009692 67
20030056096 67
20030065919 67
20030233450 67
20030233583 67
20040054794 67
20050021613 67
20060006230 67
20060059265 67
20060161775 67
20060272023 67
20070022469 67
20070098175 67
20070130334 67
20070282909 67
20080177998 67
20090150977 67
20090198996 67
7231025 64
7533735 64
20020191765 64
20030126457 64
20040127279 64
20040133789 64
20040218897 64
20070232355 64
5966441 58
4295155 58
4905766 58
4956862 58
5210794 58
5347387 58
5425130 58
5479341 58
5485196 58
5692400 58
5724168 58
5947571 58
6017004 58
6038892 58
6047572 58
6178089 58
6263313 58
6272633 58
6282653 58
6345256 58
6389403 58
6389538 58
6418421 58
6945870 58
7028182 58
20030100371 58
20030177354 58
20050233811 58
20060205394 58
5604663 58
5967466 58
6144848 58
6449367 58
6061346 56
5444780 56
5500897 56
5745576 56
6032260 56
6055236 56
6151590 56
5349643 56
5491752 56
5590200 56
5619657 56
5687235 56
5729594 56
5734718 56
5742756 56
5764890 56
5778065 56
5802178 56
5805803 56
5818936 56
5822431 56
5828832 56
5832228 56
5850445 56
5864665 56
5887063 56
5887250 56
5923756 56
5922074 56
5931947 56
5970144 56
6012144 56
6026293 56
6061448 56
6061448 56

6065120 56
6067620 56
6081900 56
6088451 56
6098056 56
6141752 56
6148405 56
6185612 56
6192474 56
6198824 56
6199113 56
6202081 56
6216231 56
6216231 56
6230266 56
6233608 56
6247129 56
6249867 56
6249873 56
4386233 56
4423287 56
4755940 56
4783798 56
4888801 56
4890323 56
4897875 56
4910773 56
4997288 56
5008936 56
5016277 56
5022076 56
5202921 56
5204961 56
5210795 56
5226079 56
5237614 56
5239294 56
5241594 56
5261002 56
5276735 56
5313521 56
5353353 56
5369705 56
5371794 56
5410602 56
5412726 56
5454000 56
5469507 56
5481613 56
5499297 56
5502766 56
5535276 56
5557686 56
5587809 56
5588060 56
5590196 56
5590199 56
5592555 56
5598459 56
5602918 56
5602915 56
5604803 56
5623601 56
5633933 56
5633934 56
5638448 56
5643086 56
5655077 56
5657390 56
5666412 56
5668877 56
5671279 56
5673318 56
5684950 56
5689566 56
5699513 56
5719941 56
5721779 56
5724423 56
5732137 56
5745574 56
5748736 56
5754659 56
5757913 56
5757918 56
5768378 56
5778313 56
5781724 56
5781550 56
5784463 56
5787172 56
5790669 56
5796833 56
5799082 56
5802497 56
5805712 56
5812955 56
5812764 56
5812669 56
5812664 56
5825890 56
5825877 56
5825300 56
5841120 56
5841864 56
5850442 56
5870475 56
5870473 56
5872915 56
5875395 56
5875394 56
5875296 56
5883956 56
5889861 56
5892829 56
5892838 56
5892902 56
5894552 56
5903721 56
5907620 56
5909491 56
5913175 56
5918228 56
5926624 56
5930362 56
5953422 56
5963915 56
5963644 56
5974144 56
5978918 56
5978475 56
5983350 56
5995624 56
5996077 56
6002767 56
6009524 56
6012632 56
6021497 56
6026167 56
6038551 56
6044155 56
6044468 56
6047325 56
6047072 56
6049878 56
6052785 56
6055636 56
6061449 56
6061790 56
6061796 56
6061799 56
6061796 56
6061799 56

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(c) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/533,030	09/19/2006	Vincent Cedric Colnot	P1987

CONFIRMATION NO. 3809

24739
CENTRAL COAST PATENT AGENCY, INC
3 HANGAR WAY SUITE D
WATSONVILLE, CA95076

Title: Methods and Apparatus for Enabling Secure Network-Based Transactions

Publication No. US-2007-0067833-A1
Publication Date: 03/22/2007

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 703-305-3028.

Pre-Grant Publication Division, 703-605-4283



Certificate of Express Mailing

"Express Mail" Mailing Label Number: **EV980193960US**
Date of Deposit: **10/18/2006**
Ref: Case Docket No.: **P1987**
Application of: **Vincent Cedric Colnot**
Serial Number: **11/533,030**
Filing Date: **09/19/2006**
Title of Case: **Methods and Apparatus for Enabling Secure Network-Based Transactions**

I hereby certify that the attached papers are being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 C.F.R. 1.10 on the date indicated above and addressed to the Commissioner for Patents, Alexandria, VA 22313-1450.

1. Part 2 of the Notice to File Missing Parts.
2. Response to the Notice to File Missing Parts.
3. Signed Declaration and Power of Attorney.
4. Check for fees in the amount of $65.00.
5. Certificate of Express Mailing.
6. Postcard Listing Contents.

Sheri Beasley

(Typed or printed name of person mailing paper or fee)

Sheri Beasley

(Signature of person mailing papers or fee)



In The United States Patent and Trademark Office
Examiner: NA Art Unit: 2131

"Express Mail" Mailing Label Number: EV980193960US
Application of: Vincent Cedric Colnot
Docket: P1987
Serial No.: 11/533,030
Filed: 09/19/2006
Title: Methods and Apparatus for Enabling Secure Network-Based Transactions

Mail Stop Missing Parts
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Dear Sir:

RESPONSE TO NOTICE TO FILE MISSING PARTS OF APPLICATION

A notice to file missing parts of application was mailed in the above-referenced case on **10/06/2006**, indicating that the signature on the Declaration and Power of Attorney is missing. Submitted herewith is Part 2 of the Notice to file missing parts, a signed Declaration and Power of Attorney and a check for fees in the amount of **$65** in compliance with 37 CFR 1.27. Applicant respectfully requests that the signed Declaration and Power of Attorney be matched with the above referenced case file.

Respectfully Submitted,
Vincent Cedric Colnot

By */Donald R. Boys/*
Donald R. Boys
Reg. No. 35,074

Central Coast Patent Agency, Inc.
3 Hangar Way, Suite D
Watsonville, CA 95076
(831) 768-1755

10-20-06

OIPE MAP96 OCT 18 2006 PATENT & TRADEMARK OFFICE

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371 (c) DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NUMBER
11/533,030	09/19/2006	Vincent Cedric Colnot	P1987

CONFIRMATION NO. 3809

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

FORMALITIES LETTER

Date Mailed: 10/06/2006

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items and pay any fees required below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The oath or declaration is unsigned.

The applicant needs to satisfy supplemental fees problems indicated below.

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

- To avoid abandonment, a surcharge (for late submission of filing fee, search fee, examination fee or oath or declaration) as set forth in 37 CFR 1.16(f) of $65 for a small entity in compliance with 37 CFR 1.27, must be submitted with the missing items identified in this letter.

SUMMARY OF FEES DUE:

Total additional fee(s) required for this application is **$65** for a small entity

- **$65** Surcharge.

Replies should be mailed to: Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

10/23/2006 CCHAU1 00000017 11533030 65.00 OP
01 FC:2051

A copy of this notice MUST be returned with the reply.

Office of Initial Patent Examination (571) 272-4000, or 1-800-PTO-9199, or 1-800-972-6382
PART 2 - COPY TO BE RETURNED WITH RESPONSE

OIPE
OCT 18 2006
PATENT & TRADEMARK OFFICE

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

ATTORNEY DOCKET NO. **P1987**

As a below named inventor, I hereby declare that: My residence, post office address and citizenship are as stated below next to my name. I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled: **Method and Apparatus for Enabling Secure Network-Based Transactions**

the specification of which (check one) ☐ is attached hereto.
☒ was filed on: 09/19/2006 as patent application serial number 11/533,030
☐ and was amended on _____
(If applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above. I acknowledge the duty to disclose information which is material to patentability in accordance with Title 37, Code of Federal Regulations sec. 1.56. In the case that the present application is a continuation-in-part application, I further acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations sec. 1.56. which became available between the filing date of the prior application and the filing date of the present application. I hereby claim foreign priority benefits under Title 35, United States Code s119 of any foreign applications for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)

(Number)	(Country)	(Day/Month/Year Filed)
(Number)	(Country)	(Day/Month/Year Filed)

I hereby claim the benefit under Title 35, United States Codes, sec. 119 and sec. 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, sec. 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, sec. 156(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application.

(Application Serial No.): 60/719,273 (Filing Date): 09/20/2005 (Status): pending
(Application Serial No.): _____ (Filing Date): _____ (Status): _____
(Application Serial No.): _____ (Filing Date): _____ (Status): _____
(Application Serial No.): _____ (Filing Date): _____ (Status): _____
(Application Serial No.): _____ (Filing Date): _____ (Status): _____

POWER OF ATTORNEY: As a named inventor, I hereby appoint:

☒ Practitioners at customer number: 24739

OR

☐ Practitioners: Name: Registration number

to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

Please send all correspondence practitioners at:

☒ The practitioners at the customer number indicated above

OR

☐ Customer number:

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

ATTORNEY DOCKET NO. P1987

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

Full name of sole or first inventor: Vincent Cedric Colnot

1st inventor's signature: _____ Dated: 29 Sept 06

Residence: 803 Kevenaire Dr., Milpitas, CA 95035 US Citizenship: France

Post Office Address: Same

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371 (c) DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NUMBER
11/533,030	09/19/2006	Vincent Cedric Colnot	P1987

CONFIRMATION NO. 3809

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

FORMALITIES LETTER

Date Mailed: 10/06/2006

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items and pay any fees required below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The oath or declaration is unsigned.

The applicant needs to satisfy supplemental fees problems indicated below.

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

- To avoid abandonment, a surcharge (for late submission of filing fee, search fee, examination fee or oath or declaration) as set forth in 37 CFR 1.16(f) of $65 for a small entity in compliance with 37 CFR 1.27, must be submitted with the missing items identified in this letter.

SUMMARY OF FEES DUE:

Total additional fee(s) required for this application is **$65** for a small entity

- **$65** Surcharge.

Replies should be mailed to: Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

A copy of this notice MUST be returned with the reply.

Office of Initial Patent Examination (571) 272-4000, or 1-800-PTO-9199, or 1-800-972-6382
PART 3 - OFFICE COPY

METHODS AND APPARATUS FOR ENABLING SECURE NETWORK-BASED TRANSACTIONS

CROSS-REFERENCE TO RELATED APPLICATIONS

The present invention claims priority to a U.S. provisional patent application serial number 60/719,273 filed on 09/20/2005. The referenced application is included herein at least by reference.

BACKGROUND OF THE INVENTION

1. Field of the Invention

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

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 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 EEPROM, a processing unit or a microprocessor, an on-chip oscillator, an IS0 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.

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.

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.

SUMMARY OF THE INVENTION

A system is provided for enabling secure transacting over a network includes a network sever application for storing client information and activating clients for secure transacting, a software driver for performing authentication, the software driver accessible to the network server a software applet for creating a secure data record and for managing transmission and update of the contents of the record, and a sound source in the form of a file or a sound generating device, the sound source being part of or having access to the secure data record.

In one embodiment, the network is a data-packet-network. In a preferred embodiment, the secure data record is unique to a client and includes an identification number, a password or personal identification code, a session key, and a secrete data seed. In one embodiment, the software driver resides in the same machine as the network server application. In another embodiment, the software driver resides in a machine remote to but accessible from the machine hosting the network server application. In one embodiment, the software applet is a Java applet and the secure data record is a Java archive.

In one embodiment, the sound source is a semiconductor chip supporting a modem. In a variation of this embodiment, the semiconductor chip is external to a client system used to secure authentication. In a preferred embodiment, the semiconductor chip derives power from a sound card of the system used to secure authentication.

In another embodiment, the sound source is a sound file stored on a machine peripheral to the machine used to secure authentication. In a variation of this embodiment, the peripheral machine is one of a cellular telephone, a personal digital assistant, or a hand held music player.

According to another aspect of the present invention, in a system for enabling secure transacting over a network, a sound-producing device is provided for generating a network transmittable sound frame having embedded therein an identification number and a session key used to authenticate a client. The device includes a semiconductor chip supporting a modem, an electrical plug-in interface for enabling coupling with a host machine, and a housing of a size and shape to support hand-held operation.

In one embodiment, the network is a data-packet-network. In a preferred embodiment, the modem is a frequency-shift keying modem. In one embodiment, the electrical plug-in interface is a tip/ring/sleeve interface for plugging into a microphone jack on a host machine used to secure authentication. Also in one embodiment, the sound-producing device derives power from a soundcard residing on a host machine used

to secure authentication. In a preferred embodiment, the system further includes a switch for activating the modem to generate the sound.

In still another aspect of the invention, a method is provided for sending a secure modulated sound pass from a sound-producing device having a semiconductor chip supporting a modem, an electrical plug-in interface for enabling coupling with a host machine, and a housing of a size and shape to support hand-held operation to a software applet for demodulating the sound pass to glean the secure data embedded therein. The method includes acts for (a) plugging the device into an audio line-in of a host machine used to secure authentication, and (b) activating the device to generate and input the sound pass. In a preferred aspect, the audio line-in is one of a microphone input, universal serial bus, or a telephone line port of the host machine. Also in a preferred aspect, in act (b), activation is caused by manipulating a switch on the device.

BRIEF DESCRIPTION OF THE DRAWING FIGURES

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.

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.

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.

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.

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.

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.

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 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) 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 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.

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.

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 [Ci+1 = G (N, S, Ci)] 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. Ci= the current session 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 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 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.

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 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.

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.

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 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.

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.

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.

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 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 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.

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 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. 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 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 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 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 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 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 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 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.

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 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 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 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 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.

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 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. 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

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 Ci+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 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 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 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 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 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 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 901and 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 Ci+1 and is derived from a one way function (G) of N, S, and Ci, or Ci+1=G(N,S,Ci). In library 906, the transmission (Jc) is the new session key encrypted with the last session key (Ci) or Jc= DES (Ci, Ci+1).

The server sends Jc and the server challenge (Cs) 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 Hi=DES (Ci+1,PW).

The applet on the client generates a final hash code (H'c) which is an encryption of Hi and the server challenge using the received session key and adding an xor function or H'c=DES(Ci+1,Hi,xor,Cs). The server performs the same hash Hc=DES(Ci+1,Hi,xor,Cs). 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 Co (the last session key used). The last operation occurs after the client is successfully validated. L'c is compared to Lc 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 Ci. The sound applet 1001 generates a new session key expressed as Ci+1, which is = to G(H,S,Ci) 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 (Secrete Seed), and Co (Last Session Key) used by the client.

In this example, user 1003 enters a PIN code (Pc) 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, Pc, S, and Co.

In this implementation the user entered PIN code is duplicated Rc=Pc||Pc. A value Ei is generated and is an encryption of Ci and Rc or Ei=DES(Ci,Rc). Eventually, the PC applet 1005 creates an encryption code (Ec) that is the encryption of Ei and Cs using the session key (Ci) and adding an xor function. Expressed in this example, it is Ec=DES(Ci,Ei,xor,Cs). Ec 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 Ci where Ci 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 secrete seed (S), the last session key used by the client (Co), and the client PIN code (Pc).

Like the smart card or key jack implementation described further above, the token generates the new session key expressed as Ci+1=G(N,S,Ci). The user may enter a PIN code (Pc) and then may perform a series of banking transactions by submitting transaction data B1-Bn. For each transaction, a new hash code (Hc) is generated by applet 1205 on the client PC. The final Hc is a dynamic card verification value (CVV) based on the session key, the transaction data (b1-Bn) for the instant transaction, and the Pc. In this example, Hc=Lc, 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 Hc Lc 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 Bi-Bn 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 secrete 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 Hi= DES(PW,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 ser4vice 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 secrete 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 is act 1408 the token deployment mode is not dynamic, then at act 1410 the applet write 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.

What is claimed is:

1. A system for enabling secure transacting over a network comprising:

a network sever application for storing client information and activating clients for secure transacting;

a software driver for performing authentication, the software driver accessible to the network server;

a software applet for creating a secure data record and for managing transmission and update of the contents of the record; and

a sound source in the form of a file or a sound generating device, the sound source being part of or having access to the secure data record.

2. The system of claim 1, wherein the network is a data-packet-network.

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

4. The system of claim 1, wherein the software driver resides in the same machine as the network server application.

5. The system of claim 1, wherein the software driver resides in a machine remote to but accessible from the machine hosting the network server application.

6. The system of claim 1, wherein the software applet is a Java applet and the secure data record is a Java archive.

7. The system of claim 1, wherein the sound source is a semiconductor chip supporting a modem.

8. The system of claim 7, wherein the semiconductor chip is external to a client system used to secure authentication.

9. The system of claim 8, wherein the semiconductor chip derives power from a sound card of the system used to secure authentication.

10. The system of claim 1, wherein the sound source is a sound file stored on a machine peripheral to the machine used to secure authentication.

11. The system of claim 10, wherein the peripheral machine is one of a cellular telephone, a personal digital assistant, or a hand held music player.

12. In a system for enabling secure transacting over a network, a sound-producing device for generating a network transmittable sound frame having embedded therein an identification number and a session key used to authenticate a client, the device comprising:

a semiconductor chip supporting a modem;

an electrical plug-in interface for enabling coupling with a host machine; and

a housing of a size and shape to support hand-held operation.

13. The system of claim 12, wherein the network is a data-packet-network.

14. The system of claim 12, wherein the modem is a frequency-shift keying modem.

15. The system of claim 12, wherein the electrical plug-in interface is a tip/ring/sleeve interface for plugging into a microphone jack on a host machine used to secure authentication.

16. The system of claim 15, wherein the sound-producing device derives power from a soundcard residing on a host machine used to secure authentication.

17. The system of claim 12 further including a switch for activating the modem to generate the sound.

18. A method for sending a secure modulated sound pass from a sound-producing device having a semiconductor chip supporting a modem, an electrical plug-in interface for enabling coupling with a host machine, and a housing of a size and shape to support hand-held operation to a software applet for demodulating the sound pass to glean the secure data embedded therein comprising the acts:

(a) plugging the device into an audio line-in of a host machine used to secure authentication; and

(b) activating the device to generate and input the sound pass.

19. The method of claim 18, wherein in act (a), the audio line-in is one of a microphone input, universal serial bus, or a telephone line port of the host machine.

20. The method of claim 18, wherein in act (b), activation is caused by manipulating a switch on the device.

ABSTRACT OF THE DISCLOSURE

A system for enabling secure transacting over a network has a network sever application for storing client information and activating clients for secure transacting, a software driver for performing authentication, the software driver accessible to the network server, a software applet for creating a secure data record and for managing transmission and update of the contents of the record, and a sound source in the form of a file or a sound generating device, the sound source being part of or having access to the secure data record.

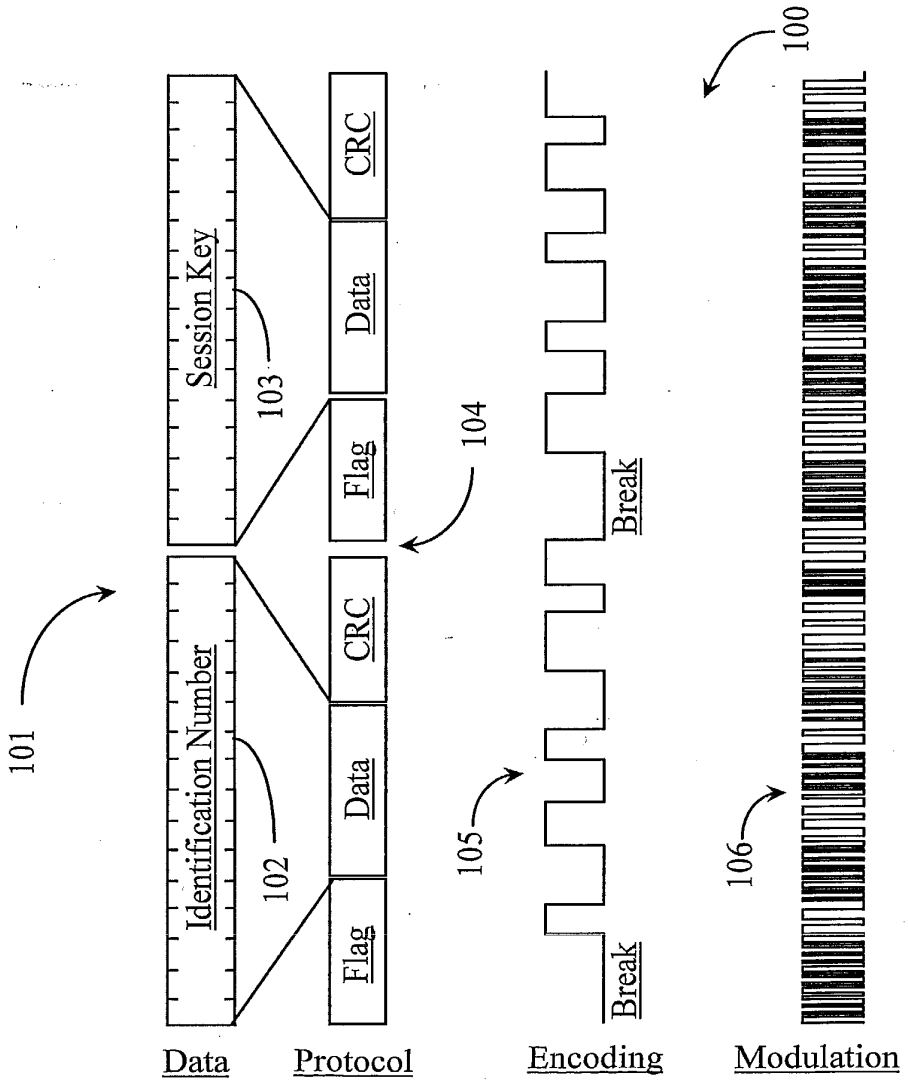

100
101
Identification Number
Session Key
102
103
104
Flag
Data
CRC
Flag
Data
CRC
105
Break
Break
106
Data
Protocol
Encoding
Modulation

Fig. 1

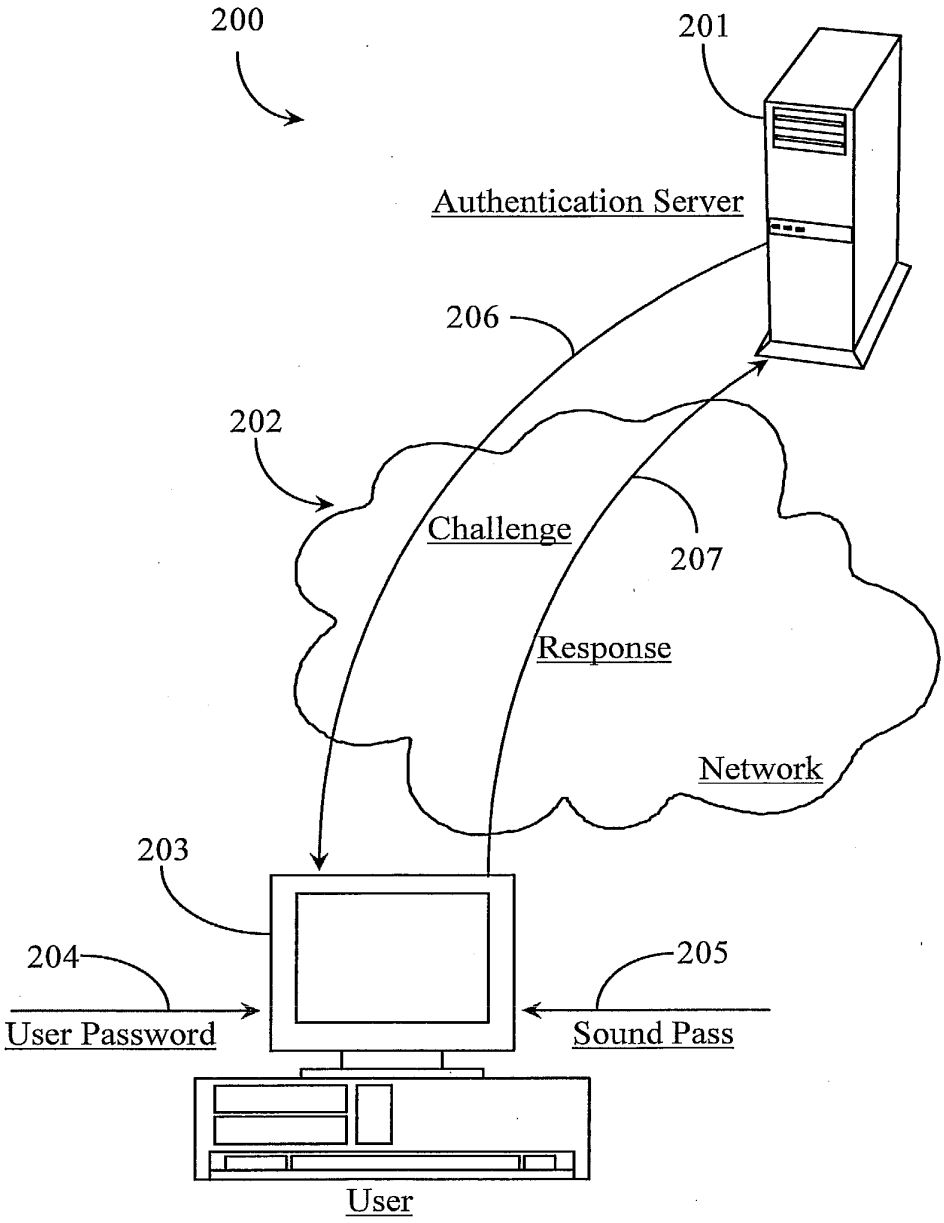

200
201
Authentication Server
206
202
Challenge
207
Response
Network
203
204
205
User Password
Sound Pass
User

Fig. 2

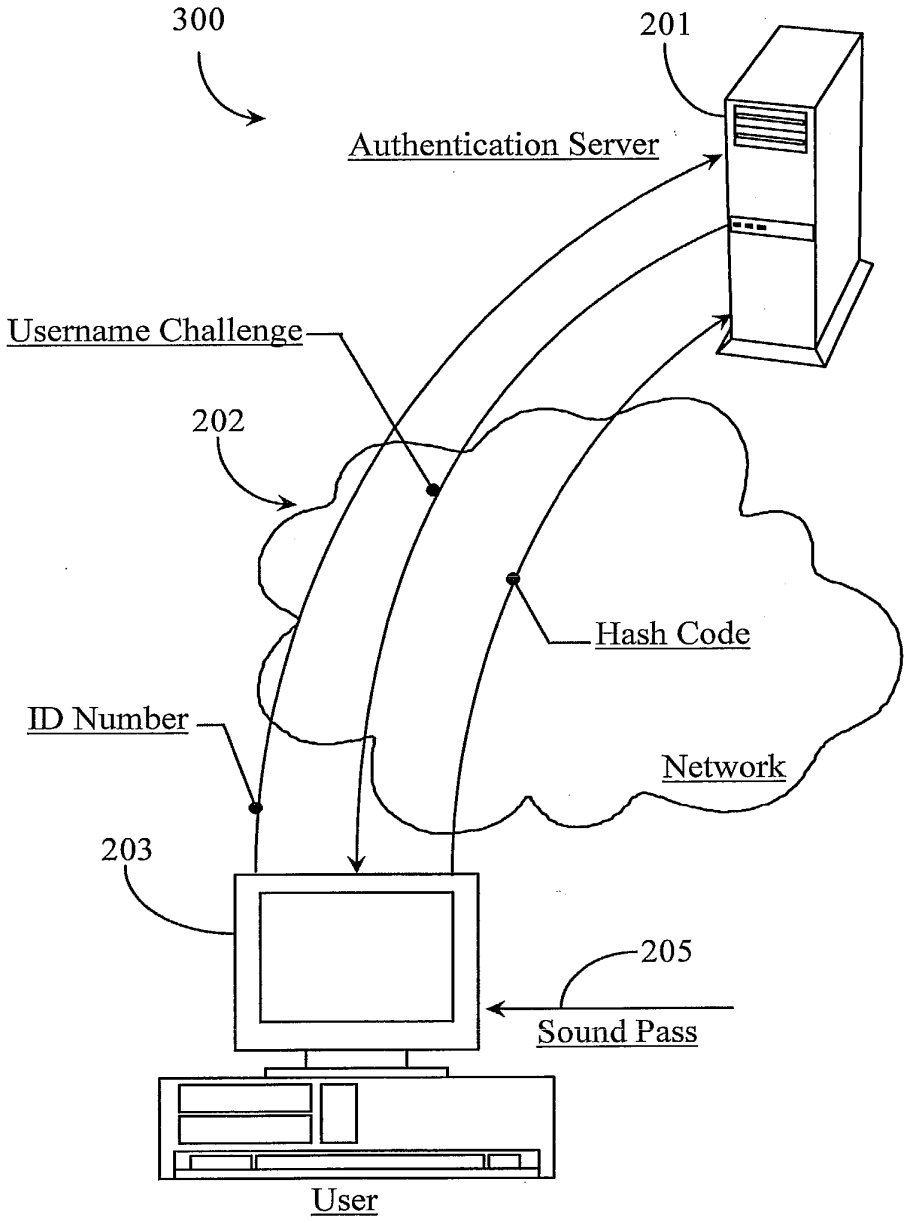

300
201
Authentication Server
Username Challenge
202
Hash Code
ID Number
Network
203
205
Sound Pass
User

Fig. 3

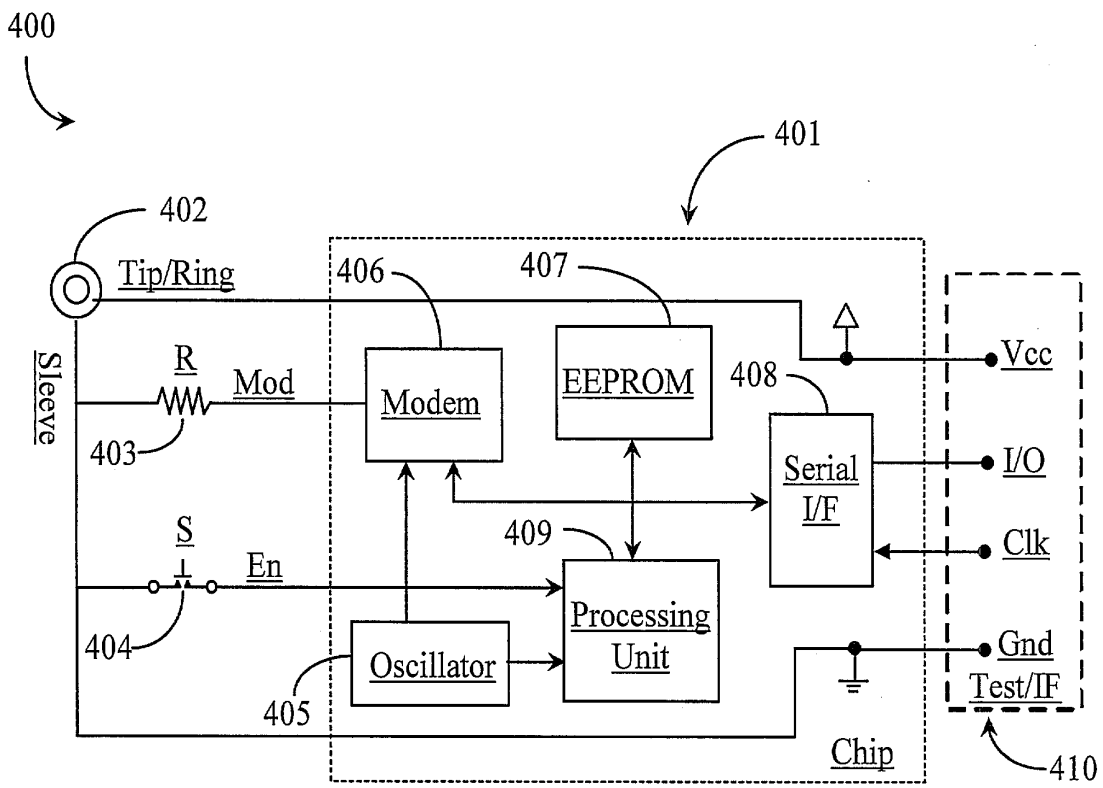

400
401
402
Tip/Ring
406
407
Sleeve
R
Mod
403
Modem
EEPROM
408
Vcc
Serial
I/F
I/O
Clk
S
En
404
409
Processing
Unit
Oscillator
405
Gnd
Test/IF
Chip
410

Fig. 4

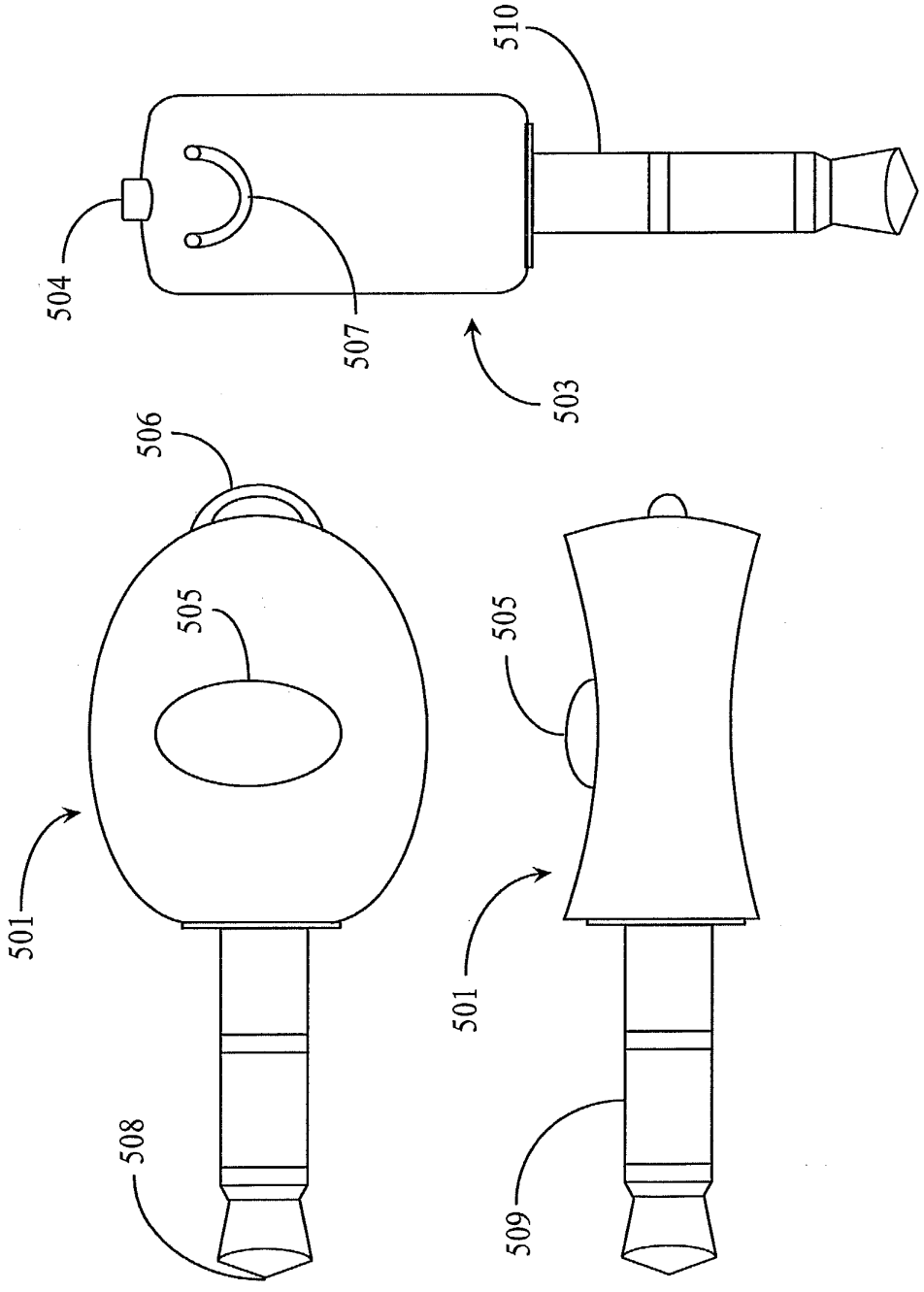


Fig. 5

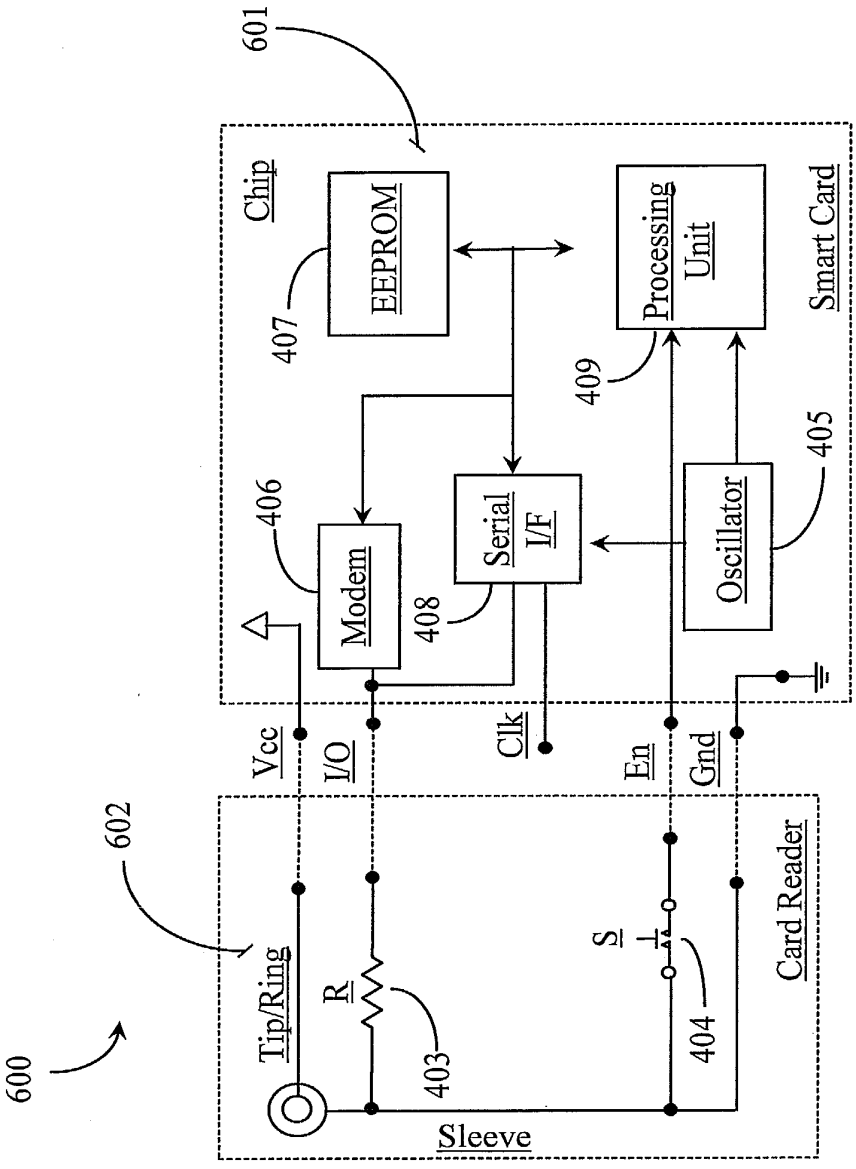

600
602
601
Chip
Smart Card
EEPROM
407
Processing Unit
409
Modem
406
Serial I/F
408
Oscillator
405
Vcc
I/O
Clk
En
Gnd
Tip/Ring
R
403
S
404
Card Reader
Sleeve

Fig.6

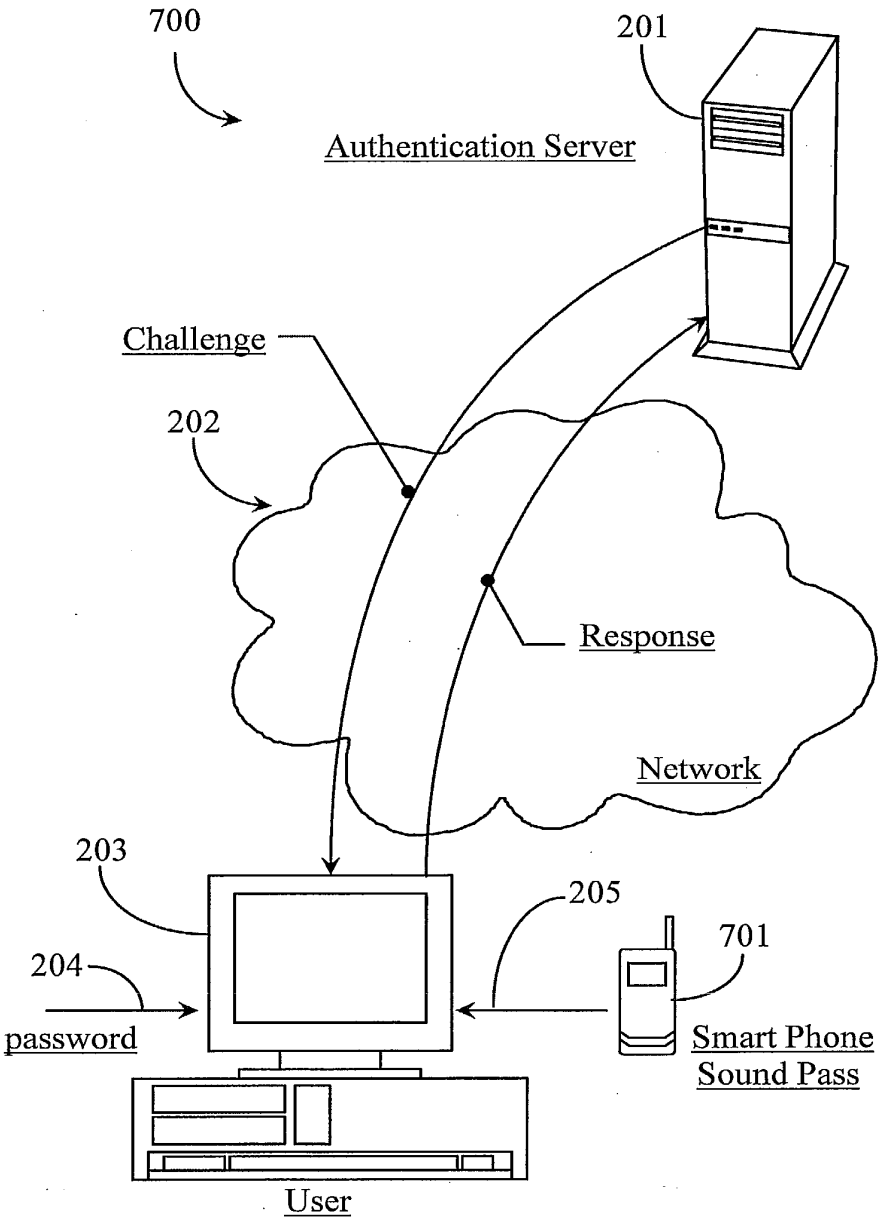

700
201
Authentication Server
Challenge
202
Response
Network
203
205
701
204
password
Smart Phone
Sound Pass
User

Fig. 7

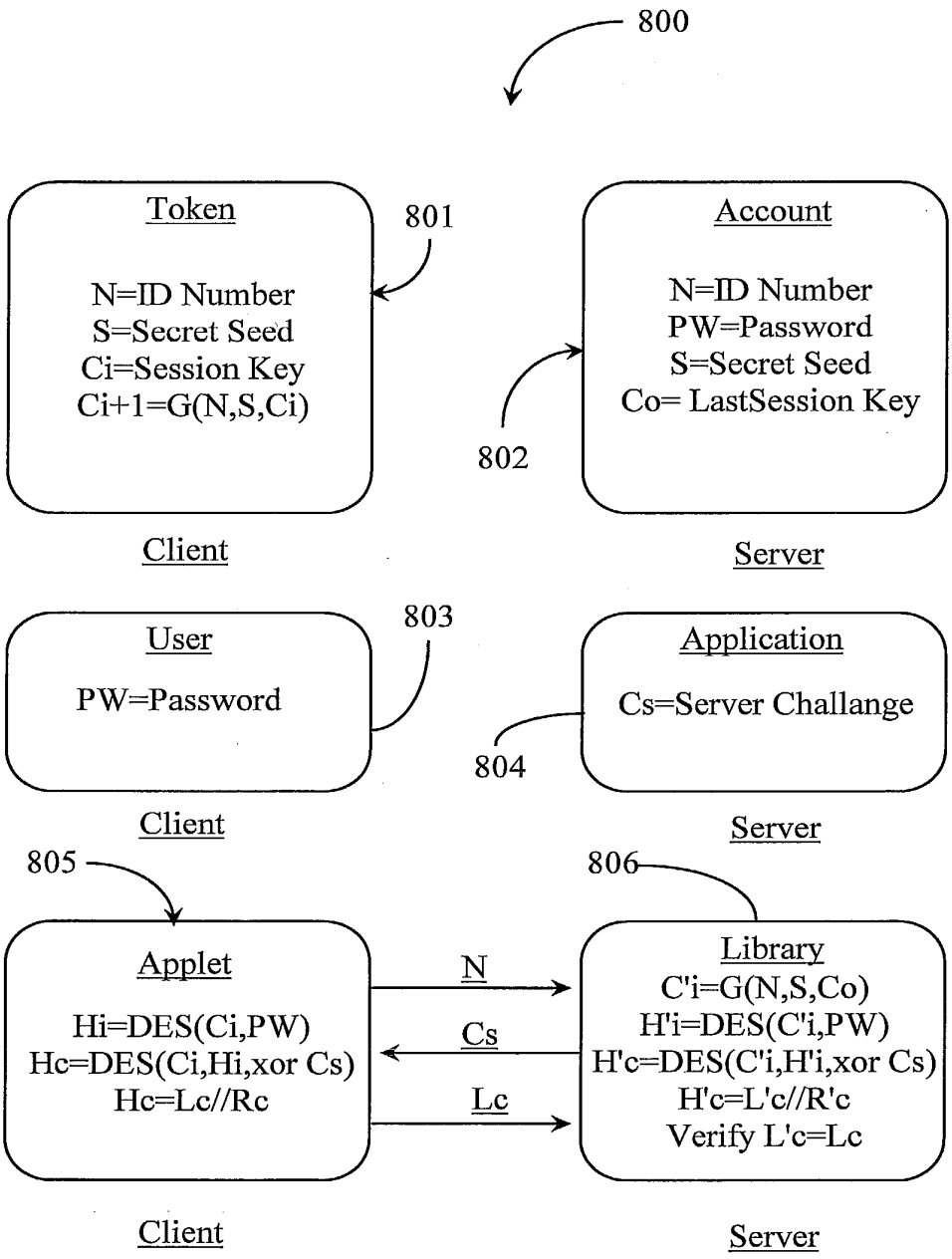

800
Token
N=ID Number
S=Secret Seed
Ci=Session Key
Ci+1=G(N,S,Ci)
801
802
Account
N=ID Number
PW=Password
S=Secret Seed
Co= LastSession Key
Client
Server
User
PW=Password
803
804
Application
Cs=Server Challange
Client
Server
805
806
Applet
Hi=DES(Ci,PW)
Hc=DES(Ci,Hi,xor Cs)
Hc=Lc//Rc
N
Cs
Lc
Library
C'i=G(N,S,Co)
H'i=DES(C'i,PW)
H'c=DES(C'i,H'i,xor Cs)
H'c=L'c//R'c
Verify L'c=Lc
Client
Server

Fig. 8

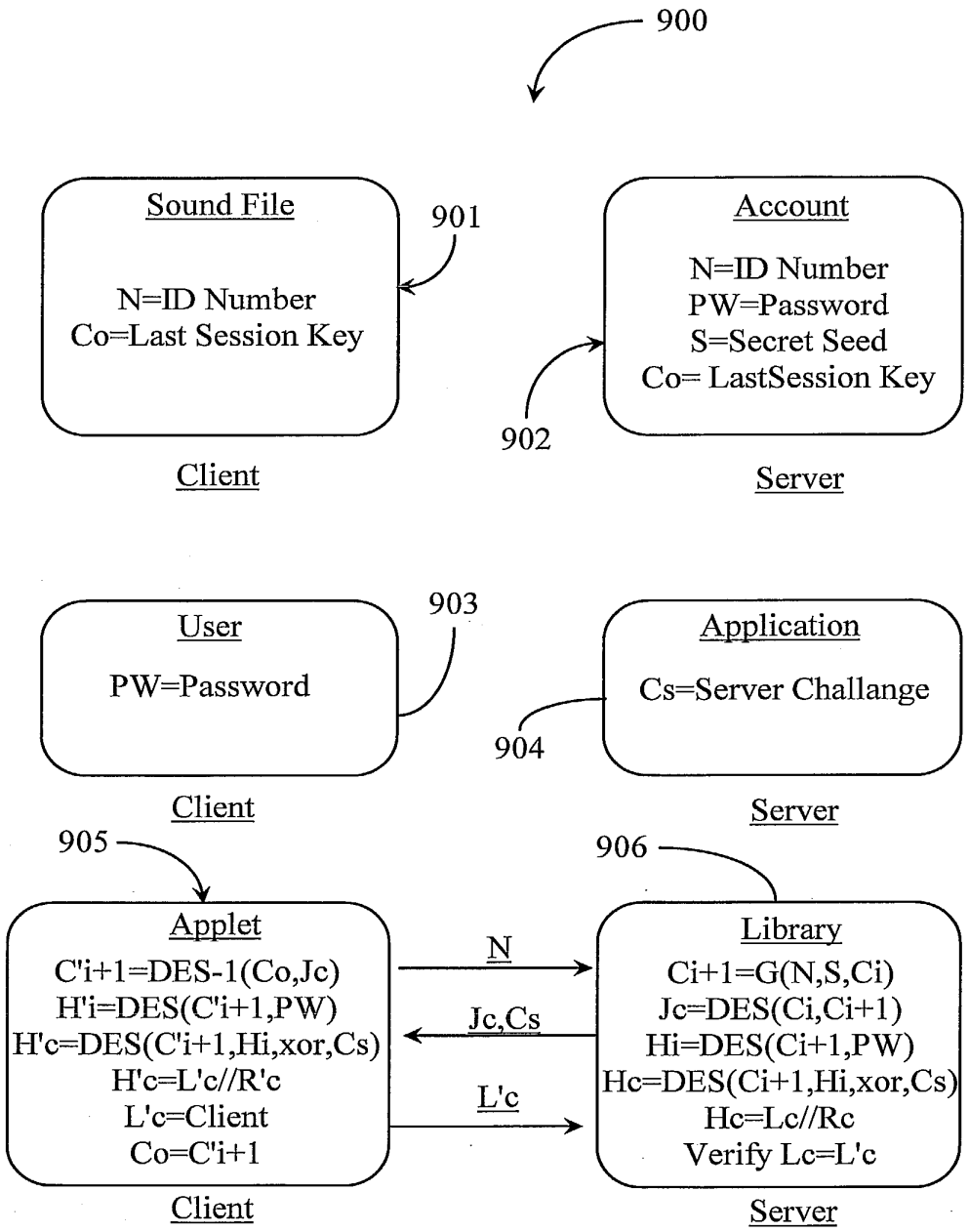

900
Sound File
N=ID Number
Co=Last Session Key
901
Account
N=ID Number
PW=Password
S=Secret Seed
Co= LastSession Key
902
Client
Server
User
PW=Password
903
Application
Cs=Server Challange
904
Client
Server
905
906
Applet
C'i+1=DES-1(Co,Jc)
H'i=DES(C'i+1,PW)
H'c=DES(C'i+1,Hi,xor,Cs)
H'c=L'c//R'c
L'c=Client
Co=C'i+1
N
Jc,Cs
L'c
Library
Ci+1=G(N,S,Ci)
Jc=DES(Ci,Ci+1)
Hi=DES(Ci+1,PW)
Hc=DES(Ci+1,Hi,xor,Cs)
Hc=Lc//Rc
Verify Lc=L'c
Client
Server

Fig. 9

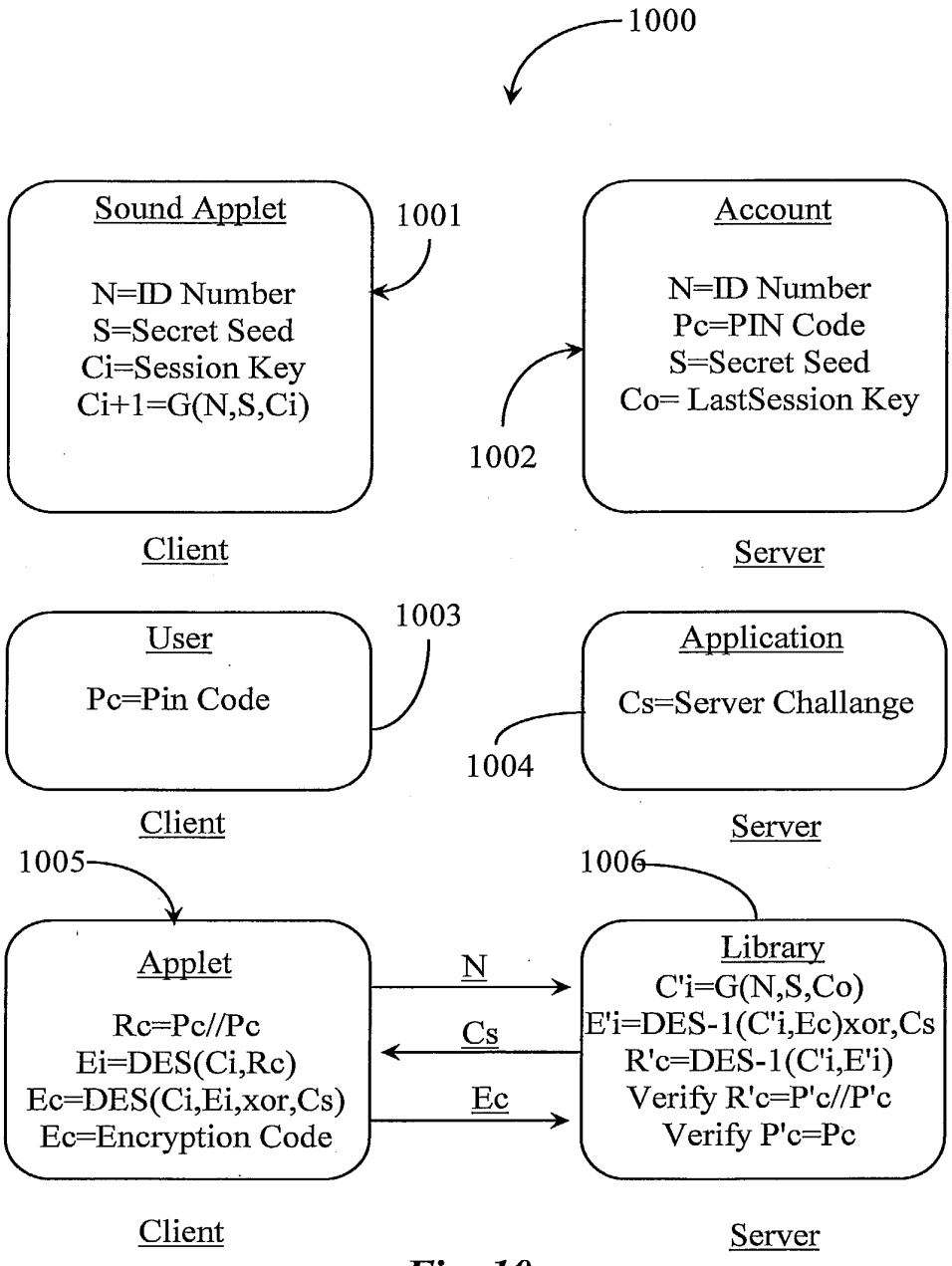

1000
Sound Applet
1001
N=ID Number
S=Secret Seed
Ci=Session Key
Ci+1=G(N,S,Ci)
Client
Account
N=ID Number
Pc=PIN Code
S=Secret Seed
Co= LastSession Key
1002
Server
User
1003
Pc=Pin Code
Client
Application
Cs=Server Challange
1004
Server
1005
1006
Applet
Rc=Pc//Pc
Ei=DES(Ci,Rc)
Ec=DES(Ci,Ei,xor,Cs)
Ec=Encryption Code
N
Cs
Ec
Library
C'i=G(N,S,Co)
E'i=DES-1(C'i,Ec)xor,Cs
R'c=DES-1(C'i,E'i)
Verify R'c=P'c//P'c
Verify P'c=Pc
Client
Server

Fig. 10

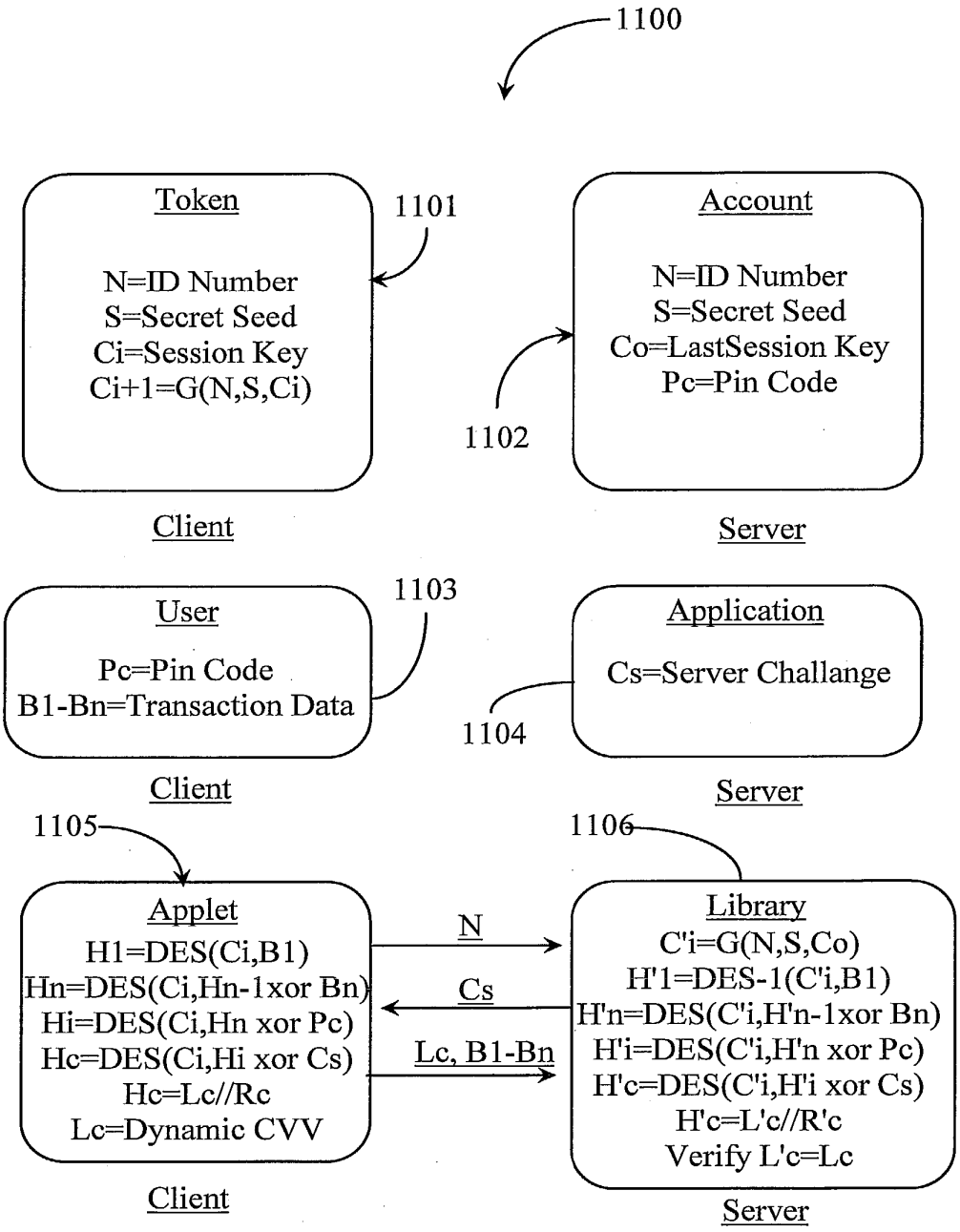

1100
Token
1101
N=ID Number
S=Secret Seed
Ci=Session Key
Ci+1=G(N,S,Ci)
Client
Account
N=ID Number
S=Secret Seed
Co=LastSession Key
Pc=Pin Code
1102
Server
User
1103
Pc=Pin Code
B1-Bn=Transaction Data
Client
Application
Cs=Server Challange
1104
Server
1105
1106
Applet
H1=DES(Ci,B1)
Hn=DES(Ci,Hn-1xor Bn)
Hi=DES(Ci,Hn xor Pc)
Hc=DES(Ci,Hi xor Cs)
Hc=Lc//Rc
Lc=Dynamic CVV
Client
N
Cs
Lc, B1-Bn
Library
C'i=G(N,S,Co)
H'1=DES-1(C'i,B1)
H'n=DES(C'i,H'n-1xor Bn)
H'i=DES(C'i,H'n xor Pc)
H'c=DES(C'i,H'i xor Cs)
H'c=L'c//R'c
Verify L'c=Lc
Server

Fig. 11

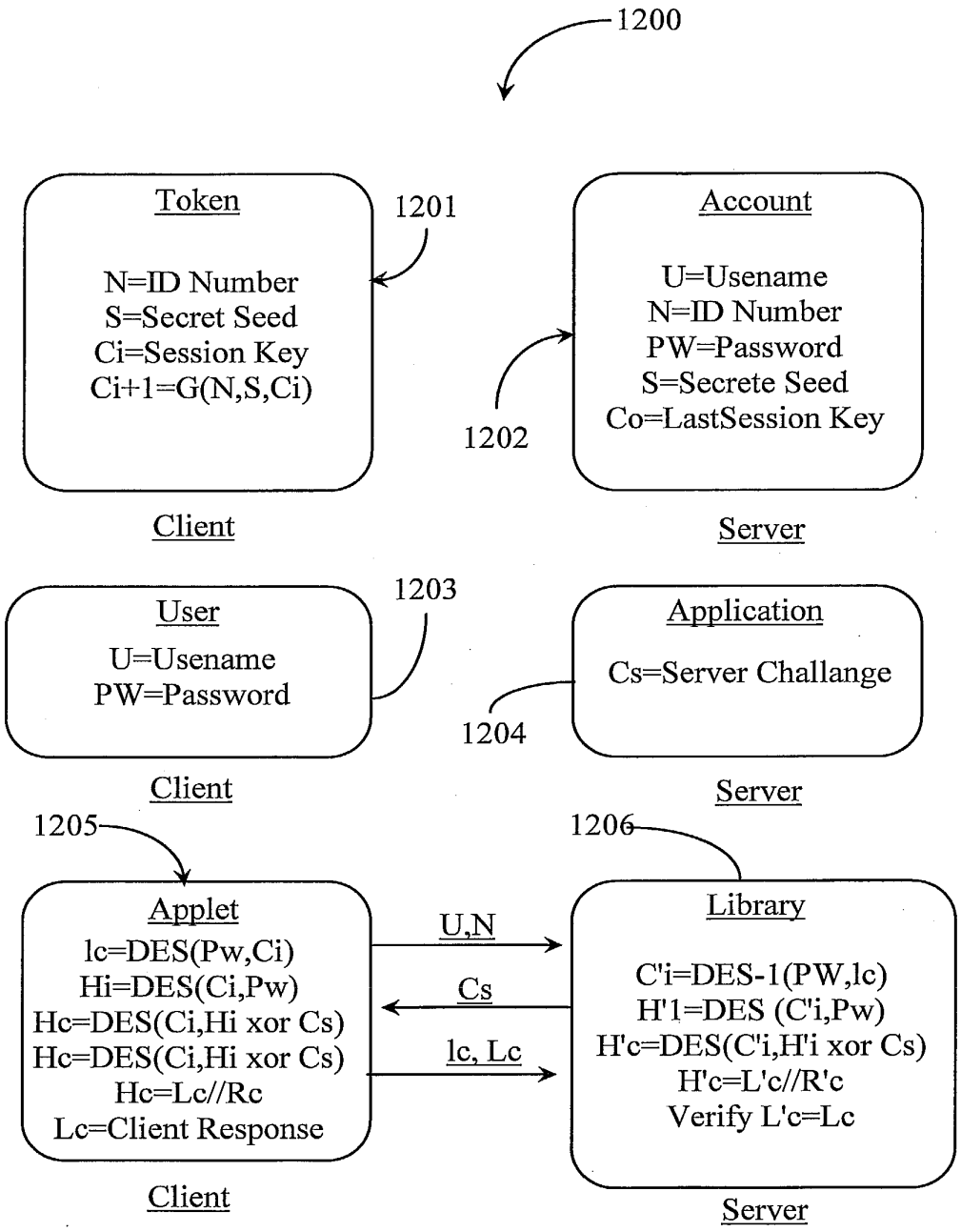

1200
Token
1201
N=ID Number
S=Secret Seed
Ci=Session Key
Ci+1=G(N,S,Ci)
Client
Account
U=Usename
N=ID Number
PW=Password
S=Secrete Seed
Co=LastSession Key
1202
Server
User
1203
U=Usename
PW=Password
Client
Application
Cs=Server Challange
1204
Server
1205
1206
Applet
lc=DES(Pw,Ci)
Hi=DES(Ci,Pw)
Hc=DES(Ci,Hi xor Cs)
Hc=DES(Ci,Hi xor Cs)
Hc=Lc//Rc
Lc=Client Response
Client
U,N
Cs
lc, Lc
Library
C'i=DES-1(PW,lc)
H'1=DES (C'i,Pw)
H'c=DES(C'i,H'i xor Cs)
H'c=L'c//R'c
Verify L'c=Lc
Server

Fig. 12

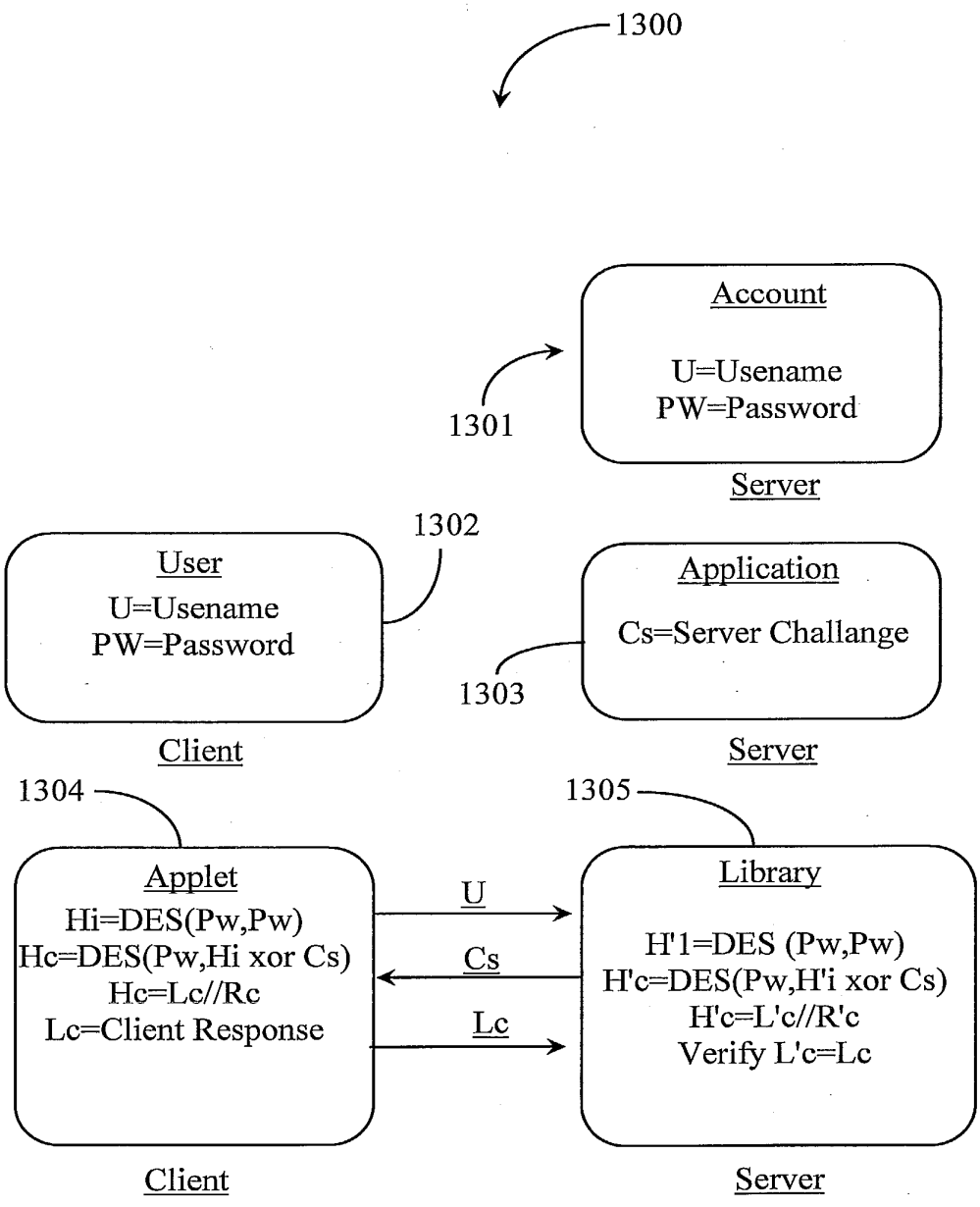

1300
Account
U=Usename
PW=Password
1301
Server
1302
User
U=Usename
PW=Password
Application
Cs=Server Challange
1303
Client
Server
1304
1305
Applet
Hi=DES(Pw,Pw)
Hc=DES(Pw,Hi xor Cs)
Hc=Lc//Rc
Lc=Client Response
U
Cs
Lc
Library
H'1=DES (Pw,Pw)
H'c=DES(Pw,H'i xor Cs)
H'c=L'c//R'c
Verify L'c=Lc
Client
Server

Fig. 13

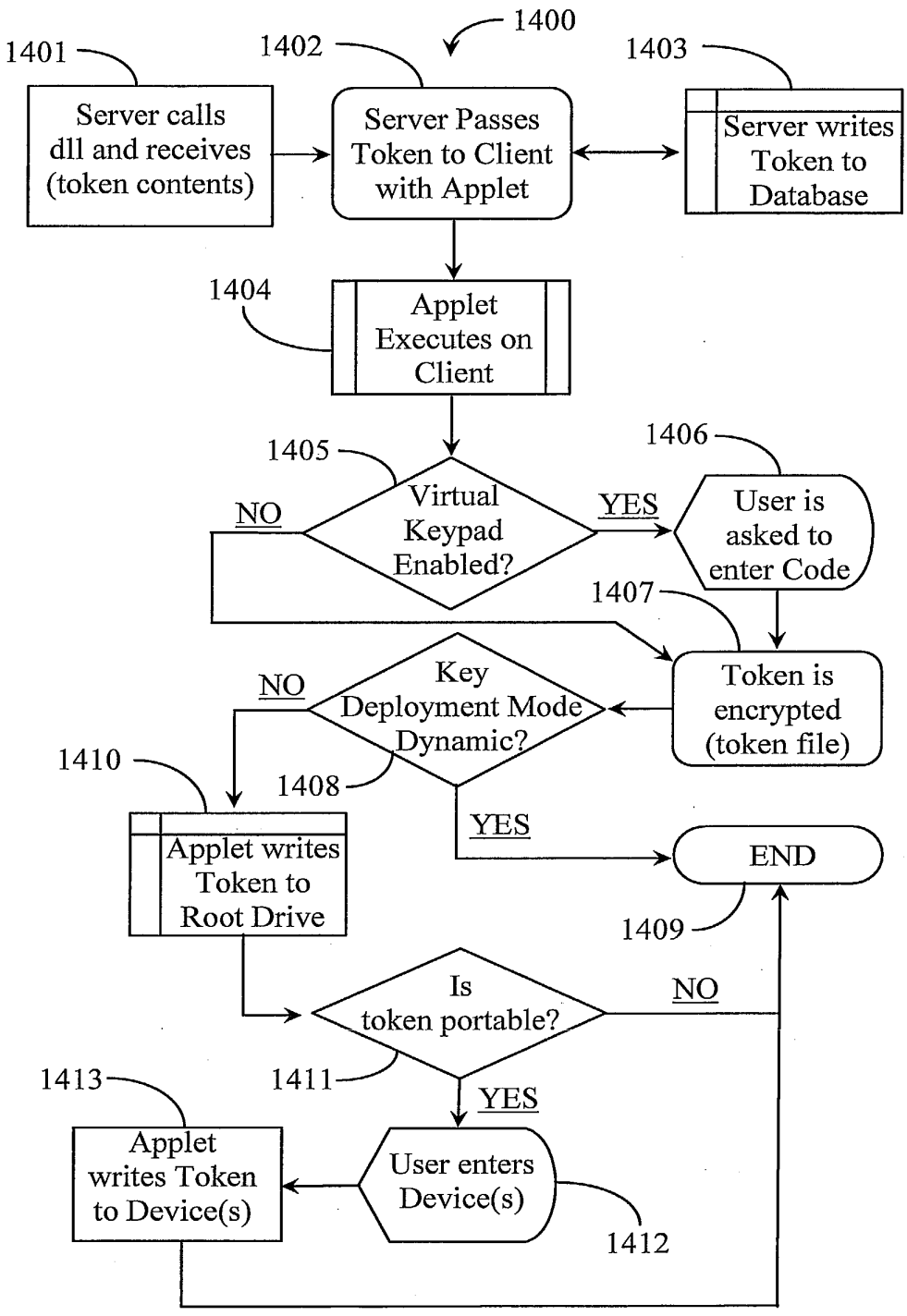

1400
1401
1402
1403
Server calls dll and receives (token contents)
Server Passes Token to Client with Applet
Server writes Token to Database
1404
Applet Executes on Client
1405
1406
Virtual Keypad Enabled?
NO
YES
User is asked to enter Code
1407
Token is encrypted (token file)
Key Deployment Mode Dynamic?
NO
1408
YES
1410
Applet writes Token to Root Drive
END
1409
Is token portable?
NO
1411
YES
1413
Applet writes Token to Device(s)
User enters Device(s)
1412

Fig. 14

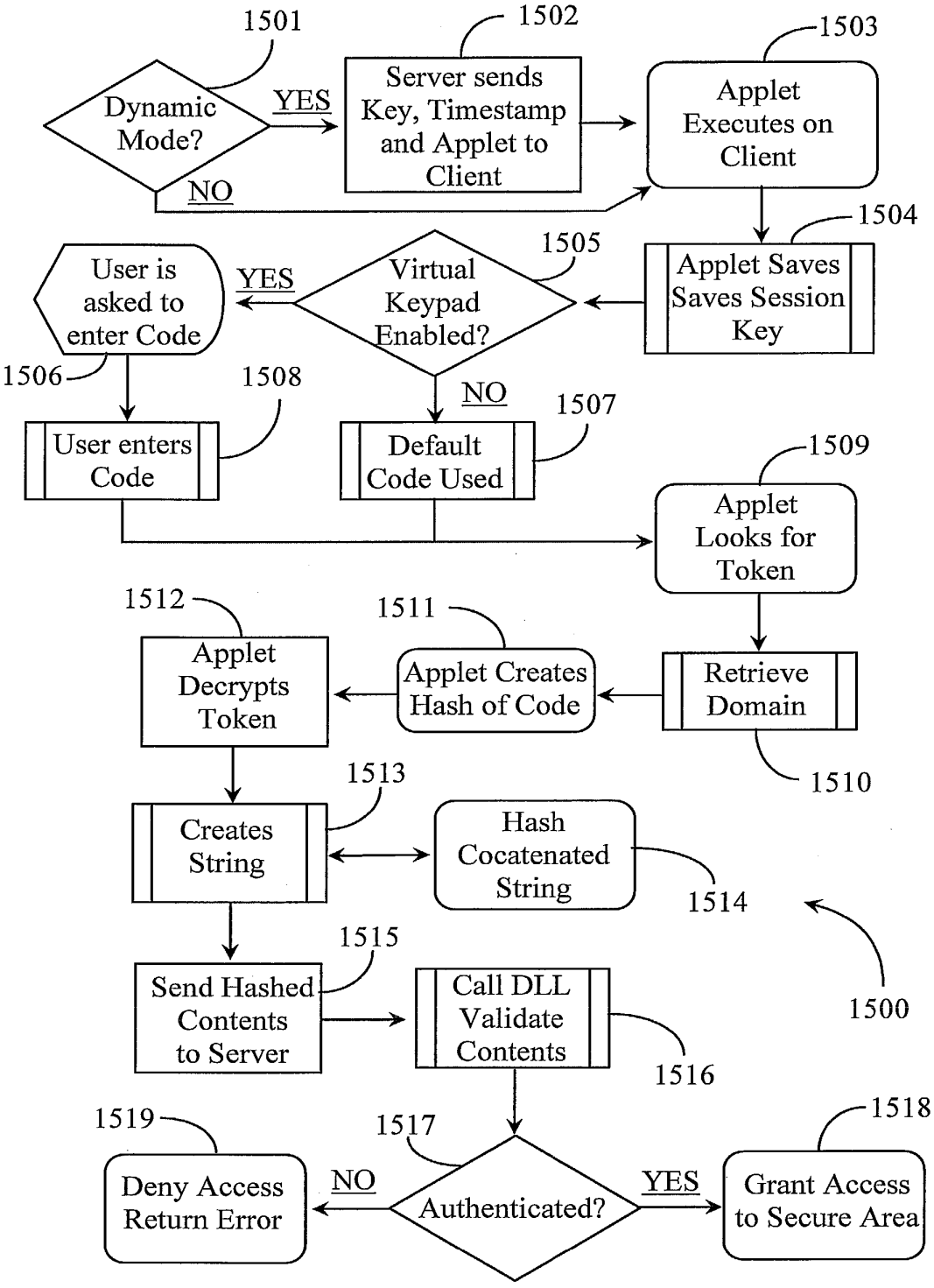

1501
Dynamic Mode?
YES
NO
1502
Server sends Key, Timestamp and Applet to Client
1503
Applet Executes on Client
1504
Applet Saves Saves Session Key
1505
Virtual Keypad Enabled?
YES
User is asked to enter Code
1506
1508
User enters Code
NO
1507
Default Code Used
1509
Applet Looks for Token
1510
Retrieve Domain
1511
Applet Creates Hash of Code
1512
Applet Decrypts Token
1513
Creates String
Hash Cocatenated String
1514
1515
Send Hashed Contents to Server
Call DLL Validate Contents
1516
1500
1517
Authenticated?
NO
YES
1519
Deny Access Return Error
1518
Grant Access to Secure Area

Fig. 15

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

ATTORNEY DOCKET NO. **P1987**

As a below named inventor, I hereby declare that: My residence, post office address and citizenship are as stated below next to my name. I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled: **Methods and Apparatus for Enabling Secure Network-Based Transactions**

the specification of which (check one) ☒ is attached hereto.
☐ was filed on: _____ as patent application serial number _____
☐ and was amended on _____
(If applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above. I acknowledge the duty to disclose information which is material to patentability in accordance with Title 37, Code of Federal Regulations sec. 1.56. In the case that the present application is a continuation-in-part application, I further acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations sec. 1.56. which became available between the filing date of the prior application and the filing date of the present application. I hereby claim foreign priority benefits under Title 35, United States Code s119 of any foreign applications for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)

(Number)	(Country)	(Day/Month/Year Filed)
(Number)	(Country)	(Day/Month/Year Filed)

I hereby claim the benefit under Title 35, United States Codes, sec. 119 and sec. 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, sec. 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, sec. 156(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application.

(Application Serial No.): 60/719,273 (Filing Date): 09/20/2005 (Status): pending
(Application Serial No.): _____ (Filing Date): _____ (Status): _____
(Application Serial No.): _____ (Filing Date): _____ (Status): _____
(Application Serial No.): _____ (Filing Date): _____ (Status): _____
(Application Serial No.): _____ (Filing Date): _____ (Status): _____

POWER OF ATTORNEY: As a named inventor, I hereby appoint:

☒ Practitioners at customer number: 24739

OR

☐ Practitioners: Name: Registration number

to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

Please send all correspondence practitioners at:

☒ The practitioners at the customer number indicated above

OR

☐ Customer number:

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

ATTORNEY DOCKET NO. **P1987**

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

Full name of sole or first inventor: Vincent Cedric Colnot

1st inventor's signature: _____ Dated: _____

Residence: 803 Kevenaire Dr., Milpitas, CA 95035 US Citizenship: France

Post Office Address: Same

PTO/SB/14 (08-05)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	P1987
	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.)

Applicant Information:

Applicant 1 Remove

Applicant Authority ◉ Inventor ○ Legal Representative under 35 U.S.C. 117 ○ Party of Interest under 35 U.S.C. 118

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

Citizenship under 37 CFR 1.41(b) [i] FR

Mailing Address of Applicant:

Address 1	803 Kevenaire Drive
Address 2	

City	Milpitas	State/Province	CA
Postal Code	95035	**Country** [i]	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

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

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	24739		
Email Address	info@centralcoastpatent.com	Add Email	Remove Email
Email Address	rexboys@centralcoastpatent.com	Add Email	Remove Email
Email Address	plambuth@centralcoastpatent.com		Remove Email

PTO/SB/14 (08-05)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

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

Application Information:

Title of the Invention	Methods and Apparatus for Enabling Secure Network-Based Transactions		
Attorney Docket Number	P1987	**Small Entity Status Claimed**	☑
Application Type	Nonprovisional		
Subject Matter	Utility		
Suggested Class (if any)		**Sub Class (if any)**	
Suggested Technology Center (if any)			
Total Number of Drawing Sheets (if any)		**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 been and will not be the subject of an application filed in another country, or under a multilateral agreement, that requires publication at eighteen months after filing.			

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).
Enter either 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	○ US Representative (37 CFR 11.9)
Customer Number	24739		

Domestic Priority Information:

This section allows for the applicant to claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c). 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(a)(2) or CFR 1.78(a)(4), and need not otherwise be made part of the specification.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	non provisional of	60719273	2005-09-20

Additional Domestic Priority Data may be generated within this form by selecting the **Add** button. Add

Foreign Priority Information:

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. 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(a).

PTO/SB/14 (08-05)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

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

			Remove
Application Number	Country [i]	Parent Filing Date (YYYY-MM-DD)	Priority Claimed
			◯ Yes ◉ No
Additional Foreign Priority Data may be generated within this form by selecting the **Add** button.			Add

Assignee Information:

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

Assignee 1 Remove

If the Assignee is an Organization check here. ☐

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

Mailing Address Information:

Address 1			
Address 2			
City		**State/Province**	
Country [i]		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee Data may be generated within this form by selecting the **Add** button. Add

Signature:

A signature of the applicant or representative is required in accordance with 37 CFR 1.33 and 10.18. Please see 37 CFR 1.4(d) for the form of the signature.

Signature	/Donald R. Boys/			Date (YYYY-MM-DD)	2006-09-19
First Name	Donald	Last Name	Boys	Registration Number	35074

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

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	Methods and Apparatus for Enabling Secure Network-Based Transactions
First Named Inventor:	Vincent Cedric Colnot
Filer:	Donald Rex Boys/Sheri Beasley
Attorney Docket Number:	P1987

Filed as Small Entity

Utility Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility filing Fee (Electronic filing)	4011	1	75	75
Utility Search Fee	2111	1	250	250
Utility Examination Fee	2311	1	100	100
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**425**

Electronic Acknowledgement Receipt

EFS ID:	1207916
Application Number:	11533030
Confirmation Number:	3809
Title of Invention:	Methods and Apparatus for Enabling Secure Network-Based Transactions
First Named Inventor:	Vincent Cedric Colnot
Customer Number:	24739
Filer:	Donald Rex Boys/Sheri Beasley
Filer Authorized By:	Donald Rex Boys
Attorney Docket Number:	P1987
Receipt Date:	19-SEP-2006
Filing Date:	
Time Stamp:	13:01:16
Application Type:	Utility
International Application Number:	

Payment information:

Submitted with Payment	yes
Payment was successfully received in RAM	$425
RAM confirmation Number	1130
Deposit Account	500534

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)	Multi Part	Pages

1		1987PA.pdf	125158	yes	31
	Multipart Description				
	Doc Desc		**Start**	**End**	
	Specification		1	27	
	Claims		28	30	
	Abstract		31	31	
Warnings:					
Information:					
2	Drawings	DRAWINGS.pdf	268115	no	15
Warnings:					
Information:					
3	Oath or Declaration filed	POA1987.pdf	94491	no	2
Warnings:					
Information:					
4	Application Data Sheet	US_ADS_Form_SB_14.pdf	1080963	no	4
Warnings:					
Information:					
5	Fee Worksheet (PTO-875)	fee-info.pdf	8374	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1577101		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.