

17231 U.S. PTO
092005

PTO/SB/16 (04-04)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c).

Express Mail Label No. EV717834855US

113264 U.S. PTO
60/719273

092005

INVENTOR(S)					
Given Name (first and middle [if any])		Family Name or Surname		Residence (City and either State or Foreign Country)	
Vincent Cedric		Colnot		Milpitas, CA	
Additional inventors are being named on the _____ separately numbered sheets attached hereto					
TITLE OF THE INVENTION (500 characters max)					
Soundpass					
Direct all correspondence to: CORRESPONDENCE ADDRESS					
☒ Customer Number: 24739					
OR					
☐ Firm or Individual Name					
Address					
Address					
City		State		Zip	
Country		Telephone		Fax	
ENCLOSED APPLICATION PARTS (check all that apply)					
☒ Specification Number of Pages 6					
☐ CD(s), Number _____					
☒ Drawing(s) Number of Sheets 13					
☐ Other (specify) _____					
☐ Application Data Sheet. See 37 CFR 1.76					
METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT					
☒ Applicant claims small entity status. See 37 CFR 1.27.					
☒ A check or money order is enclosed to cover the filing fees.					
☒ The Director is hereby authorized to charge filing fees or credit any overpayment to Deposit Account Number: 50-0534					
☐ Payment by credit card. Form PTO-2038 is attached.					
FILING FEE Amount (\$) 100.00					
The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.					
☒ No.					
☐ Yes, the name of the U.S. Government agency and the Government contract number are: _____					

[Page 1 of 2]

Respectfully submitted,

Date 09/20/2005

SIGNATURE

REGISTRATION NO. 35,074

TYPED or PRINTED NAME Donald R. Boys

(if appropriate)
Docket Number: P1987

TELEPHONE 831-726-1457

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

This collection of information is required by 37 CFR 1.51. 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 8 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

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

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

Effective on 12/08/2004.
Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).**FEE TRANSMITTAL**
For FY 2005☒ Applicant claims small entity status. See 37 CFR 1.27**TOTAL AMOUNT OF PAYMENT** (\$) 100.00**Complete if Known**

Application Number	NA
Filing Date	09/20/2005
First Named Inventor	Vincent Cedric Colnol
Examiner Name	NA
Art Unit	NA
Attorney Docket No.	P1987

METHOD OF PAYMENT (check all that apply)☒ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): _____☒ Deposit Account Deposit Account Number: 50-0534 Deposit Account Name: Mark A. Boys

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☐ Charge fee(s) indicated below☐ Charge fee(s) indicated below, except for the filing fee☒ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17☒ Credit any overpayments**WARNING:** Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.**FEE CALCULATION****1. BASIC FILING, SEARCH, AND EXAMINATION FEES**

Application Type	FILING FEES		SEARCH FEES		EXAMINATION FEES		Fees Paid (\$)
	Fee (\$)	Small Entity Fee (\$)	Fee (\$)	Small Entity Fee (\$)	Fee (\$)	Small Entity Fee (\$)	
Utility	300	150	500	250	200	100	0
Design	200	100	100	50	130	65	0
Plant	200	100	300	150	160	80	0
Reissue	300	150	500	250	600	300	0
Provisional	200	100	0	0	0	0	100.00

2. EXCESS CLAIM FEES

Fee Description	Fee (\$)	Small Entity Fee (\$)
Each claim over 20 or, for Reissues, each claim over 20 and more than in the original patent	50	25
Each independent claim over 3 or, for Reissues, each independent claim more than in the original patent	200	100
Multiple dependent claims	360	180

Total Claims	Extra Claims	Fee (\$)	Fee Paid (\$)	Multiple Dependent Claims	Fee (\$)	Fee Paid (\$)
0 - 20 or HP =	0	x 25	= 0			
HP = highest number of total claims paid for, if greater than 20						
Indep. Claims	Extra Claims	Fee (\$)	Fee Paid (\$)			
0 - 3 or HP =	0	x 100	= 0			
HP = highest number of independent claims paid for, if greater than 3						

3. APPLICATION SIZE FEE

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).

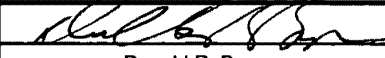
Total Sheets	Extra Sheets	Number of each additional 50 or fraction thereof	Fee (\$)	Fee Paid (\$)
19 - 100 =	0	/ 50 = 0 (round up to a whole number) x	125	= 0

4. OTHER FEE(S)

Non-English Specification, \$130 fee (no small entity discount)

Other: _____

SUBMITTED BY

Signature		Registration No. (Attorney/Agent)	35,074	Telephone	831-726-1457
Name (Print/Type)	Donald R. Boys			Date	09/20/2005

This collection of information is required by 37 CFR 1.136. 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 30 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.

Certificate of Express Mailing

"Express Mail" Mailing Label Number: EV717834855US

Date of Deposit: 09/20/2005

Ref: Case Docket No.: P1987

Application of: Vincent Cedric Colnot

Serial Number: NA

Filing Date: 09/20/2005

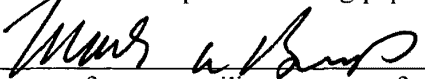
Title of Case: Soundpass

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. Provisional patent application transmittal.
2. Fee Transmittal.
3. Duplicate Fee Transmittal.
4. 6 sheets of specification.
5. 13 sheets of drawings.
6. Check for fees in the amount of \$100.00.
7. Certificate of Express mailing.
8. Postcard listing contents.

Mark A. Boys

(Typed or printed name of person mailing paper or fee)


(Signature of person mailing papers or fee)

SOUNDPASS

The following disclosure in seven pages with thirteen drawing sheets labeled Fig. 1 through Fig. 13 describes, in enabling detail, examples of a system the authors term the SoundPass system, useful for providing very secure identification for transactions over public and private networks. It is to be understood that the descriptions and examples given are exemplary, and do not limit any invention disclosed to just the specifics of any one or limited number of examples.

References to OHVA in this disclosure are to OHVA Inc, in Milpitas, California, a company established to exploit the technology enabled by the SoundPass system.

SoundPass in a preferred embodiment is a secure identifier in a sound format

SoundPass generates a modulated sound containing, in a preferred embodiment, an ID number and session key.

The **ID number** may be fixed and different for every token. Its 16 digits, in an exemplary embodiment, may include data related to the issuer and the token version.

In one embodiment of SoundPass an ID number is first encoded to include an error detection bit, and then encrypted with a proprietary key to ensure exclusive usage of OHVA (proprietary) client software.

The 16 digits in this embodiment are grouped in 2-digit decimal numbers, value range 00-99, and converted into hexadecimal, value range \$00-\$63. This conversion makes the most significant bit of each byte available for storing the error detection bit or parity bit. Then the ID number is encrypted by adding (XOR) the 8-byte applet key chosen by OHVA.

Example

ID number		1 2	3 4	5 6	7 8	9 0	0 1	2 3	4 5
Decimal		12	34	56	78	90	01	23	45
Hexadecimal		\$0C	\$22	\$38	\$4E	\$5A	\$01	\$17	\$2D
Parity bit	+	\$00	\$00	\$80	\$00	\$00	\$80	\$00	\$00
	=	\$0C	\$22	\$B8	\$4E	\$5A	\$81	\$17	\$2D
Applet key	+	\$99	\$AA	\$BB	\$CC	\$DD	\$EE	\$FF	\$55
Encrypted ID	=	\$95	\$88	\$03	\$82	\$87	\$6F	\$E8	\$78

In this example a **session key** is utilized to generate on the PC a hash code of the user password valid only once. In one embodiment a new session key is generated every time the token is activated according to an iterative algorithm: $C_{i+1} = G(N, S, C_i)$.

G: One-way function based on a stream cipher for instance
N: ID number encrypted or not
S: Proprietary secret seed defined by the token issuer
Ci: Current session key

The session key may be an 8-byte number or larger, depending of the token capabilities.

Fig. 1 is a diagram illustrating the encoding and modulation for a Soundpass ID number and session key in a particular embodiment of the invention.

The encrypted ID number and the session key in this example are enclosed into a **transmission protocol** encoding data frames prior to generating a modulated sound signal.

Each frame in this embodiment starts with a flag byte signaling the data type, and ends with a CRC byte which allows the detection of transmission errors.

The frames are encoded in this example using Miller code creating transitions every 1 etu, 1.5 etu, and 2 etu (elementary time unit or bit time) even if the data doesn't change. Any other code could be used, although other codes might create more transitions. The Manchester code for instance creates transitions every 0.5 etu and 1 etu.

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

The encoded bit flow in this example is finally modulated using a modulation, FSK for instance, generating an audible sound compatible with PC sound card capabilities. The modulation frequency may be in the range of 0 Hz to 20 kHz, and preferably in the range of 300 Hz to 3 kHz compatible with telephone networks (wired and mobile).

SoundPass in one embodiment is a two factor authentication solution

Fig. 2 is a diagram illustrating operation of the SoundPass system with an authentication server in an embodiment of the invention.

Something you have: the SoundPass token generating the session key.
Something you know: the user password or PIN code.

The applet downloaded on the PC includes a FSK modem which demodulates and decodes the SoundPass signal. It also comprised encryption means which handle the challenge-response protocol with the server.

The server may be an authentication or payment portal securing online transactions to a group of banks or web merchants.

The SoundPass session key ensures a permanent password encryption; it means that the password is never transmitted over the network in the clear.

Server authentication

In SoundPass the user doesn't enter his username anymore. Instead the server returns the username when it receives the ID number from the token. Only the valid server will return the correct username, thus the user enters his password safely.

User authentication

Fig. 3 is a diagram illustrating User Authentication in an embodiment of a SoundPass system.

In this embodiment the PC generates a hash code based on the session key, challenge, and password. The challenge is a random number generated by the server for each transaction. Access is granted to the user if the hash code is authenticated by the server.

As the session key, the hash code is valid only once.

As the server challenge, the hash code is valid for a short period of time.

In this embodiment the authentication server deduces the session key (Ci) from the previous one (Ci-1) stored in the server database. The server then generates another hash code of the user password stored in the database and compares it to the one received. The authentication is valid if both hash codes are identical, which means the PC and the server have used the same session key and password. If this is the case, the server stores (Ci-1) by (Ci) in the database and (Ci) cannot be reused.

SoundPass in a preferred embodiment is a token with 3 compatible forms

Essentially any device which can play a sound may become a SoundPass token: the modulated sound may be generated, for example, by a specific device like a smartcard, or stored on an existing device (PDA, smart phone) in a sound file format.

Keyjack

Fig. 4 is an electrical/electronic schematic of a SoundPass keyjack in one embodiment of a SoundPass system

The SoundPass signal in one embodiment is generated by a secure chip plugged into a microphone input of a PC. A SoundPass token may be plugged into the headset connector of a mobile device (PDA, smart phone) offering user authentication over a telephone network.

The secure chip in this example comprises a rewritable memory (EEPROM), processing unit or microprocessor, on-chip oscillator, serial interface, and one-wire modem interface. The test interface is a bidirectional interface allowing the token personalization at the end of the manufacturing process.

A resistor (R) adapts the impedance between the chip and microphone input.
A switch (S) activates the modem interface which generates the modulated signal.

The sound card in this embodiment provides a +3V to +5V DC voltage on the microphone input which is sufficient to power (Vcc) the secure chip.

Fig. 5 illustrates two different designs for a Keyjack in an embodiment of a SoundPass system.

Smartcard

Fig. 6 is a diagram illustrating a smartcard (carrying a secure chip) and a reader in an embodiment of the SoundPass system.

In this implementation, a secure chip is embedded in a plastic card; the modem and serial interfaces share the ISO contacts. A specific reader/connector, which may be without any processing means, connects the card chip to the microphone input.

Sound file

In this example the modulated sound, comprising the ID number and session key, is sampled and stored into a sound file using Microsoft wave format (.wav) for instance. The sound file in a preferred embodiment lasts less than a second and in data size is less than 20 kb, compression is not particularly useful as the file is transmitted only once.

The sound file may be generated at the server level and installed on the PC hard disk. Preferably the sound file may be installed on a USB memory key for a better security and portability.

The sound file in one embodiment is updated by the PC applet which includes a FSK modulator generating the modulated signal based on a new session key received from the server.

Alternatively, the sound file is updated by the server every given time (week, month...), this is a static or quasi-static implementation of SoundPass since the same session key is used for several authentications.

Sound generator

Fig. 7 is a diagram showing an embodiment of the SoundPass system with audio provided from a mobile device.

The modulated signal in this embodiment is generated by a sound generator applet installed on the mobile devices (PDA, smart phone). The device speaker transmits the SoundPass signal to the PC acoustically via a microphone plugged into the sound card.

The device may also be wire-connected to the PC microphone input through its speaker or headset output.

Note that the sound file may also be stored and played on mobile devices. This is a static implementation since the session key cannot be updated by the server or an applet.

SoundPass authentication protocol

SoundPass authentication protocol slightly differs depending on the token form.

Keyjack, smartcard

Fig. 8 illustrates how the token generates a new session key after each usage in an embodiment of the SoundPass system.

The token in this example generates a new session key after each usage:

In this example only half of the hash code (H_c) is transmitted to the server as the client response (L_c).

If $L'_c = L_c$, it means the client and server are using the same session key and password, therefore the server authenticates the user: he has the token, he knows the password.

If the authentication is valid, the application updates the user account with the current session key (C_i), which is then not reusable.

Sound file

Fig. 9 illustrates how the PC applet updates the sound file with the session key transmitted by the server in an embodiment of the SoundPass system.

The new session key (C_{i+1}) is encrypted with the current session key (C_i) prior to be transmitted (J_c) to the PC applet.

Sound generator

Fig. 10 illustrates how the sound applet generates a new session key after each usage in an embodiment of the SoundPass system.

This implementation duplicates the PIN code prior to encryption. The server decrypts the encryption code (E_c) with the session key and compares the result with the PIN code stored in the database.

SoundPass is a secure online payment solution

In this implementation, the banks deploy smart cards (cash, debit or credit) with the OHVA secure chip.

For security reasons, the ID number is different from the embossed card number. However, it includes the card issuer identifier and allows the merchant to route the transaction, along with the dynamic CVV, using the existing bank protocol.

Fig. 11 illustrates details re: the dynamic CVV hash code in an embodiment of the SoundPass system.

The dynamic CVV (Lc) is a 3-digit hash code which authenticates the transaction. It is based on the session key, the transaction data, and the user password or PIN code. The hash code is valid only once, for a given transaction.

If $L'c = Lc$, it means the client and server are using the same session key and password, therefore it authenticates the user: the user has the token, he or she knows the PIN code. In addition, the server can guarantee that the transactions data has not been corrupted.

Activation

Fig. 12 illustrates how SoundPass may be automatically activated by an activation protocol on a server in an embodiment of the SoundPass system.

The activation protocol automatically activates SoundPass on the server.

The user accesses his account with his username and password. The first time he is using SoundPass the ID number and session key are transmitted to the server and stored in the database after authentication. The session key is encrypted (Ic) with the password prior to transmission to the server.

Without token

In case the user forgets or cannot use his token, the authentication protocol is performed using the password has the session key. Fig. 13 illustrates how this is done in an embodiment of the SoundPass system.

This implementation is less secure as the session key (password) is fixed, but still ensures the permanent encryption of the password. Preferably, this authentication provides a limited access to the user account.

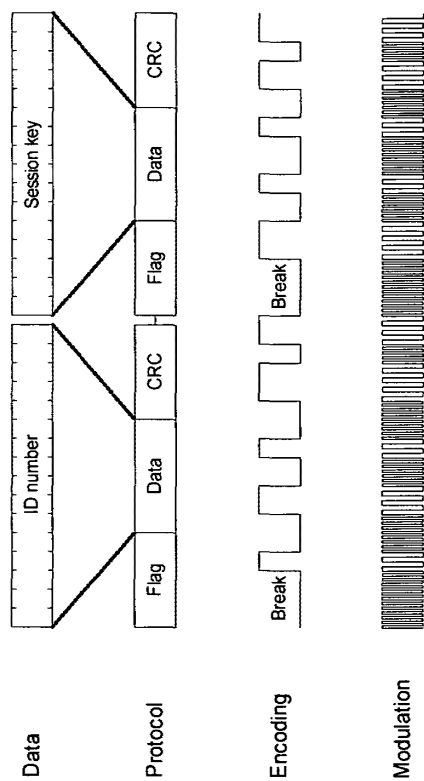


Fig. 1

Best Available Copy

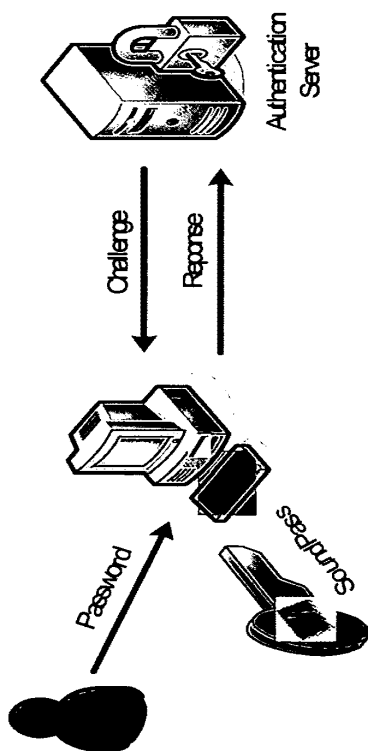


Fig. 2

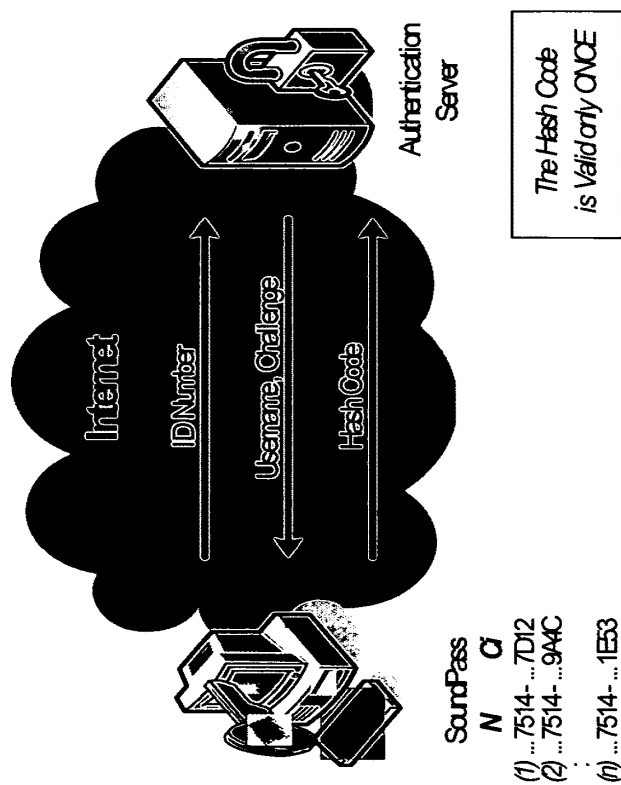


Fig. 3

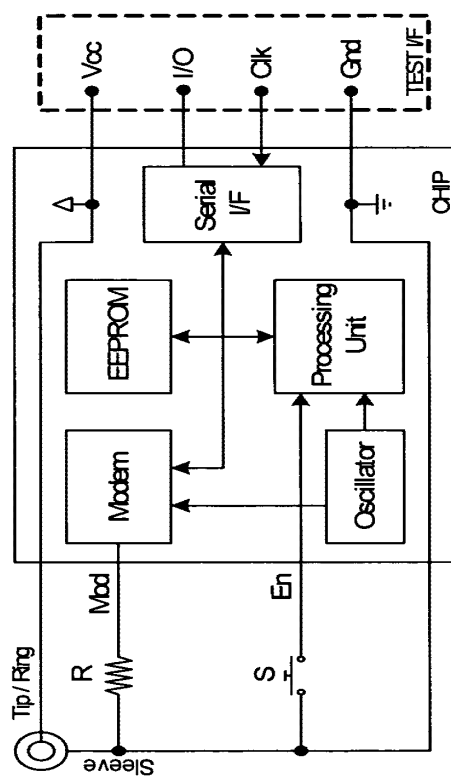


Fig. 4

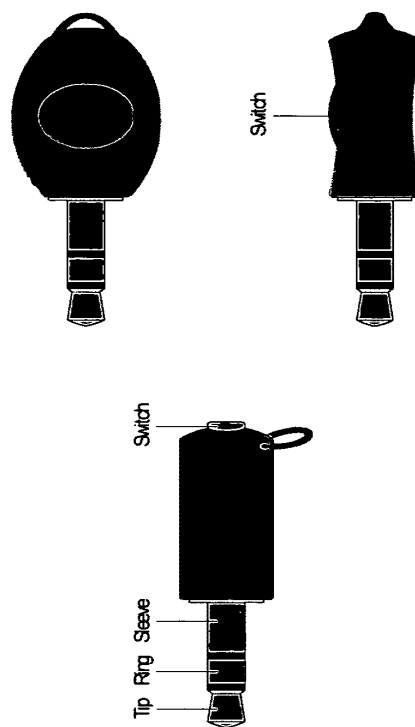


Fig. 5

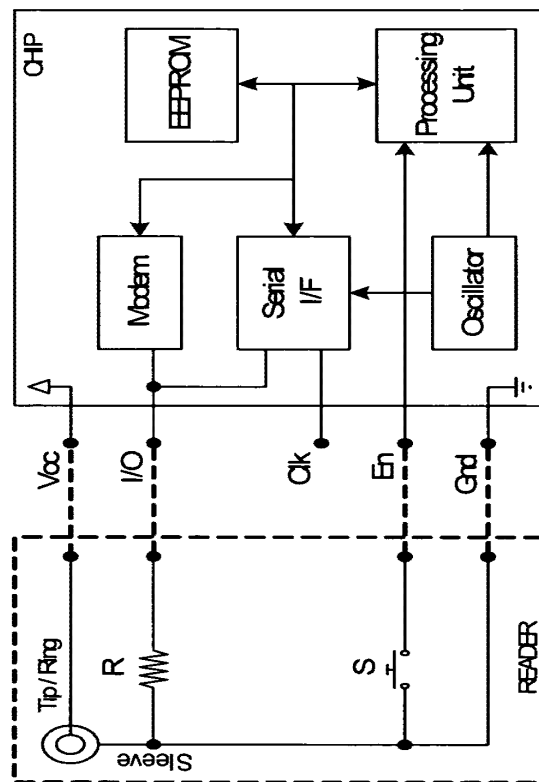


Fig.6

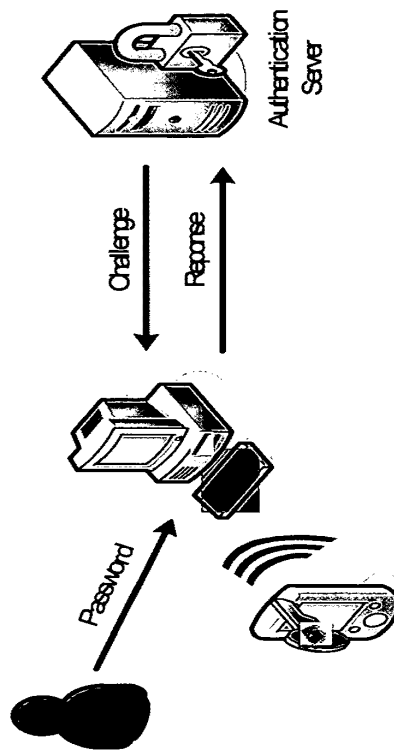


Fig.7

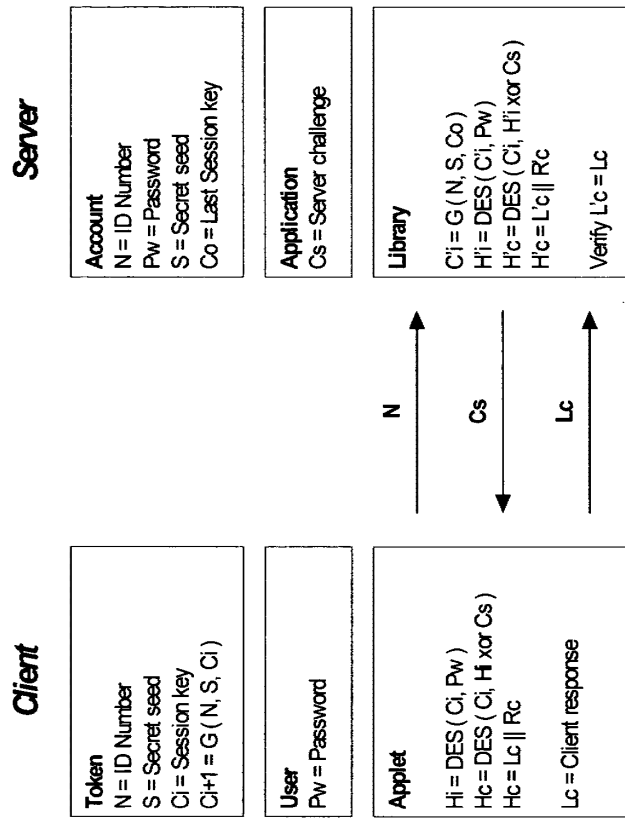


Fig.8

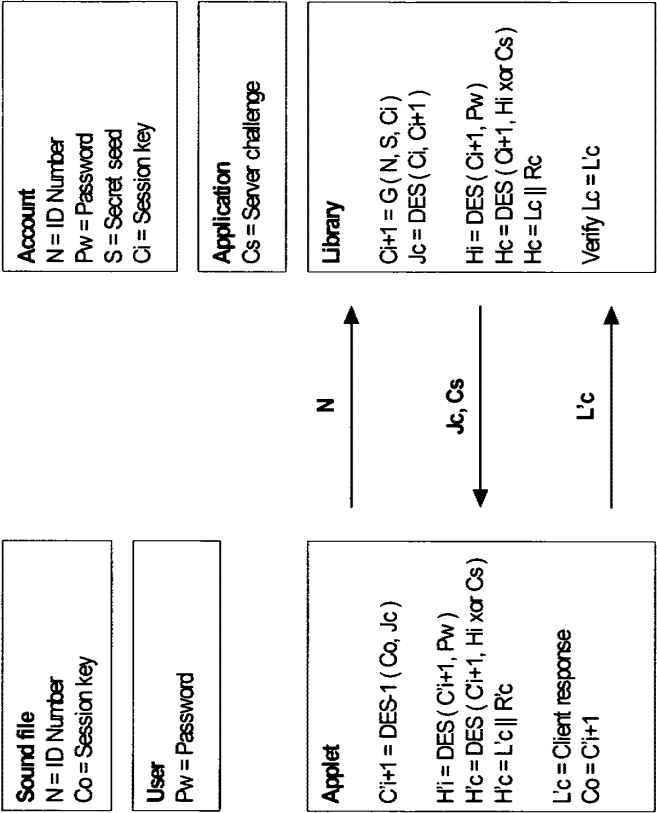


Fig.9

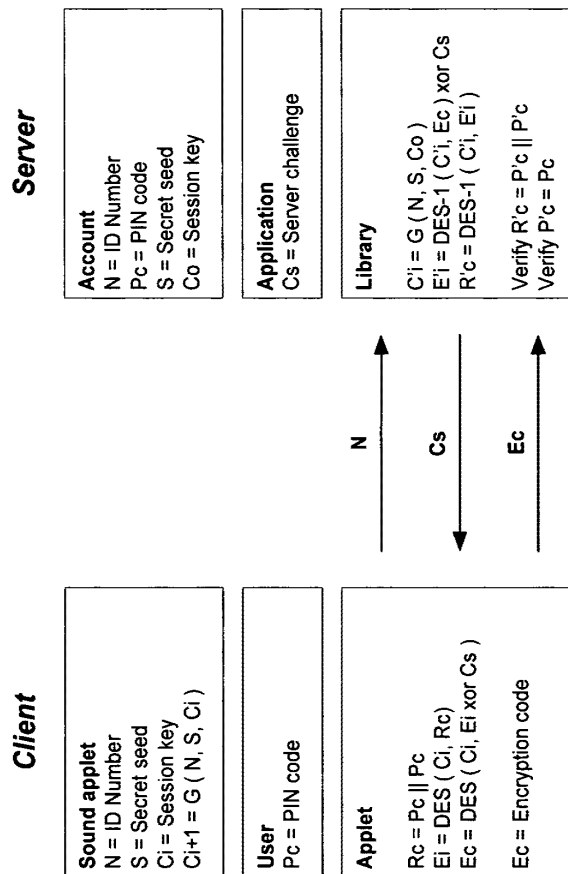


Fig.10

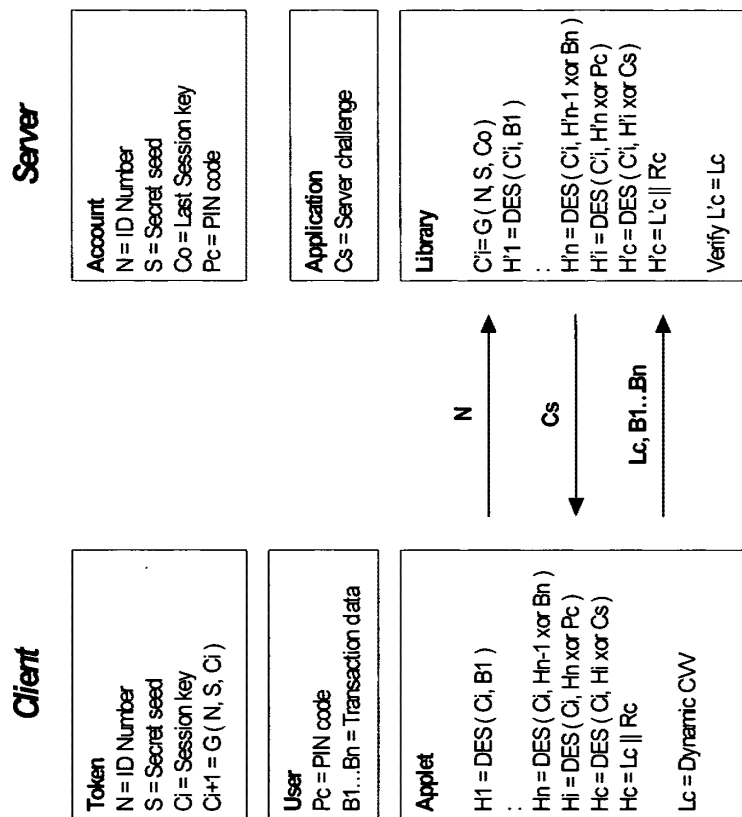


Fig.11

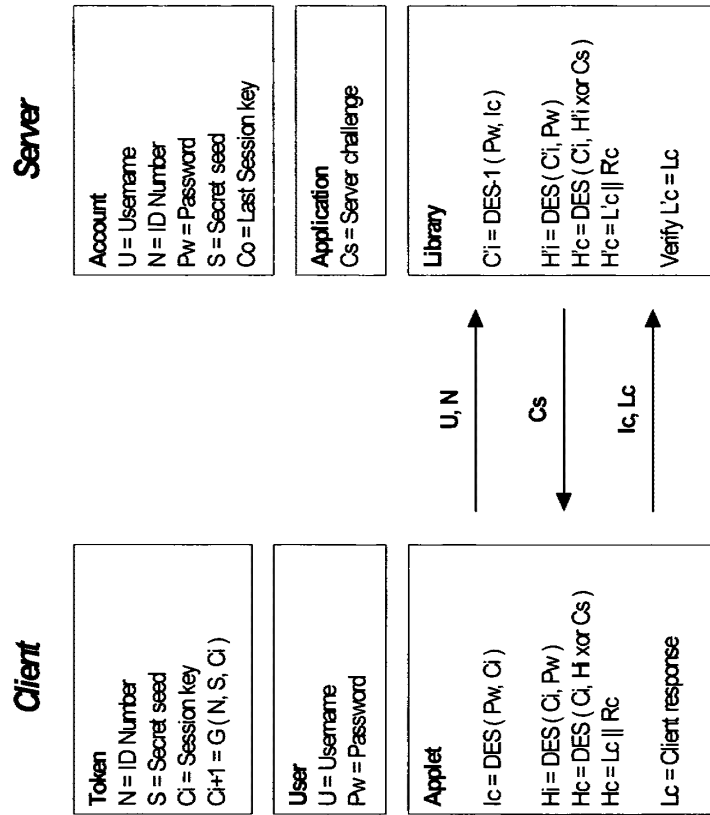


Fig.12

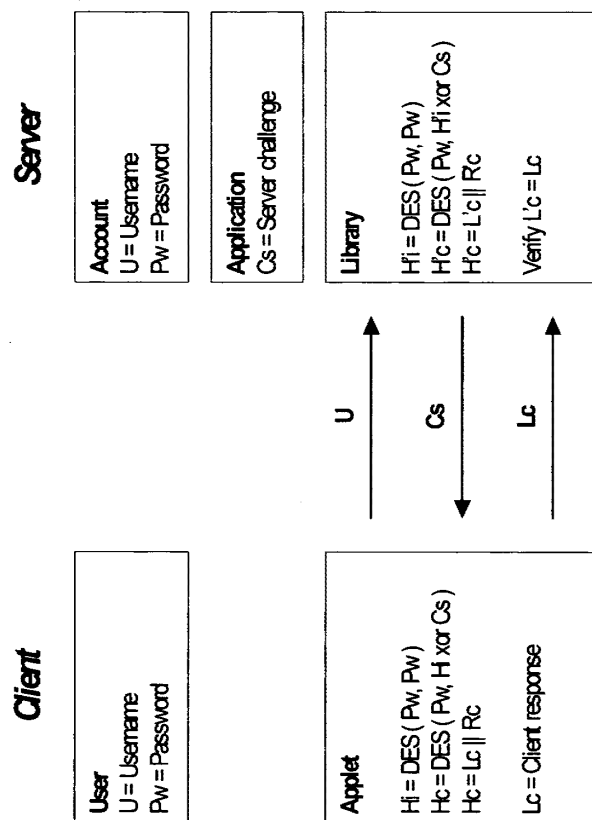


Fig.13

PATENT APPLICATION SERIAL NO _____

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE
FEE RECORD SHEET

09/26/2005 MBERHE 00000054 60719273

01 FC:2005 100.00 OP

PTO-1556
(5/87)

U.S. Government Printing Office: 2002 — 486-257/88033