

(51) International Patent Classification:
H04L 9/32 (2006.01) *G06F 21/00* (2006.01)(21) International Application Number:
PCT/US2010/033194(22) International Filing Date:
30 April 2010 (30.04.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
12/434,442 1 May 2009 (01.05.2009) US(71) Applicant (for all designated States except US):
ANAKAM, INC. [US/US]; 9171 Town Centre Drive,
Suite 460, San Diego, CA 92122 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **WILLIAMS, Jeffrey, B.** [US/US]; 4406 N. 38th Street, Arlington, VA 22207 (US). **CAMAISA, Allan** [US/US]; 9450 La Jolla Farms Road, La Jolla, CA 92037 (US).(74) Agents: **PASTERNAK, Thomas, G.** et al.; Steptoe & Johnson LLP, 1330 Connecticut Avenue, NW, Washington, DC 20036 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— without international search report and to be republished upon receipt of that report (Rule 48.2(g))

(54) Title: OUT OF BAN SYSTEM AND METHOD FOR AUTHENTICATION

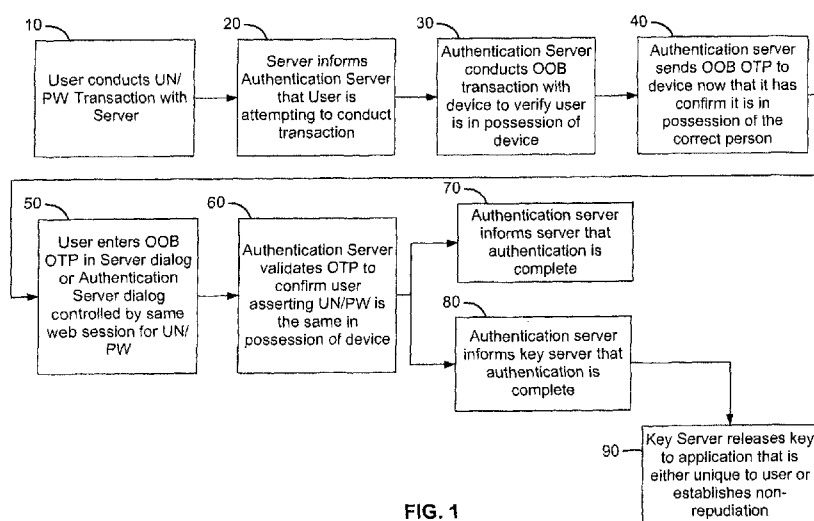


FIG. 1

(57) Abstract: A method and system for out of band authentication for ensuring a user is in possession of a device.

OUT OF BAND SYSTEM AND METHOD FOR AUTHENTICATION RELATED APPLICATIONS

[0001] This application is a continuation-in-part of and claims priority from co-pending U.S. patent application Ser. No. 11/824,694, filed July 2, 2007, which is a continuation-in-part of U.S. patent application Ser. No. 11/257,421, filed October 24, 2005, which is a continuation-in-part of U.S. patent application Ser. No. 11/077,948, filed March 11, 2005, which in turn is a continuation in part of Ser. No. 10/892,584, filed July 15, 2004, all of which are incorporated herein by reference and from all of which is priority claimed.

COPYRIGHT NOTICE

[0002] A portion of the disclosure of this patent document contains material which is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction by anyone of the patent document or the patent disclosure, as it appears in the Patent and Trademark Office patent file or records, but otherwise reserves all copyright rights whatsoever.

BACKGROUND

[0003] The present invention relates generally to methods and systems for authenticating an electronic identity assertion, with a very high confidence that the asserted electronic identity belongs to the person who is asserting it, as opposed to someone who is attempting to pose as another.

[0004] User names and passwords are a ubiquitous way to provide a minimal level of authentication to a computer user seeking to access a system provided to a network of computers such as the World Wide Web (WWW) or to a similar local network. For instance, typical online banking systems require users to log on to a Web server belonging to a financial

institution using a user name and password that have been previously given to the user by the institution. In this way, only a user (hopefully, the true account owner) who possesses both the user name and the password can gain access to that user's account.

[0005] In another example, subscription services and sales are often provided via the WWW. For instance, users can subscribe to Web sites to receive news, music, movies, and the like and to purchase almost anything. To ensure that only users who have paid (or will be subsequently be charged for) the subscription fee and/or services can access the content or purchase the goods or services, a user seeking access is required to log in using a user name and password.

[0006] In either case, it is possible that a password can be stolen and information and products/services/money intended only for the rightful owner of the password can consequently fall into the hands of a password thief.

[0007] And the problem is getting worse. As was recently noted in the Wall Street Journal (Feb. 2, 2009, "The Menace in the Machines: Cyber-Scams On The Uptick In Downturn"),

"The bear economy is creating a bull market for cyber-crooks. Avivah Litan, vice president with Internet-technology research company Gartner Inc, said clients are telling her that cyber-assaults on many banks have doubled in the past six months in the U.S. and other parts of the world, including the U.K., Canada, Mexico and Brazil. Though most are thwarted by computer-security defenses, such as spam filters and fraud-detection systems that still leaves potentially millions of victims.

'They are all experiencing a lot more attacks, and a lot more ATM fraud' aimed at depositors' accounts, Ms. Litan said.

More than 800 complaints have been logged by the National White Collar Crime Center in Richmond, VA., so far this year from checking-account customers in the U.S. about mysterious, unauthorized transactions of \$10 to \$40 that appear on monthly statements. Craig Butterworth, a spokesman for the center, a federally funded group that assists police agencies, said investigators suspect a data breach or 'phishing' campaign, where deceptive emails and text messages are used to acquire personal information, such as Social Security numbers, user names and passwords.

The FBI's Internet Crime Complaint Center confirms an increase in cyber-attacks. In its most recent Internet Crime Report, the FBI said it received 207,000

complaints about crimes perpetrated over the Internet in 2007, the latest year for which data is available, amounting to nearly \$240 million a year earlier.”

[0008] To ameliorate this problem and minimize the risk of this threat, some institutions have shifted to the implementation of single token, multi-factor authentication solutions using multi-factor cryptographic tokens or multi-factor one-time password devices. Such solutions, which are well known in the art, have heretofore depended upon the costly and cumbersome-distribution of a card or a token to the end users. In the multi-factor cryptographic token and multi-factor one-time password solutions, these deployments face additional challenges because the proper implementation requires a cryptographic key release from the device based upon the use of a password associated with that device. Such devices are costly, and implementations are time consuming and logistically cumbersome to deploy and manage especially for large-scale heterogeneous user-bases. NIST Special Publication 800-63-1, Electronic Authentication Guideline, December 8, 2008, provides technical guidelines for implementing various electronic authentication methods and systems and is incorporated by reference.

BRIEF SUMMARY OF THE INVENTION

[0009] Systems and methods for using out-of-band authentication to confirm the asserted electronic identity of an individual and control the release of a cryptographic key are disclosed herein. When confirming to a very high level of confidence that the asserted electronic identity is that of registered to the individual, these confirm that a person conducting a transaction is who she claims she is by confirming first, something she knows, using a username and password (or username only) as a shared knowledge token, and; confirming second, something she has, the item registered to him; and third, confirming the fact that she has control over that item. Once each of these confirmations is established, a cryptographic key may be released by the out-of-band authentication

process. The cryptographic key released will either be specific to the individual or will be specific to the system that actually releases the key. If the system releases a key that is not specific to the individual, the association with the individual who authenticated the release of the key, thereby establishing non-repudiation of the key, shall be provided by association of the specific transmission of the system key with the unique authentication transaction through auditable logging. The cryptographic key released by the out-of-band authentication may be either symmetric or asymmetric, that is, one key may be used to generate a message authentication code and to verify the code, or two related keys, a public key and a private key, may be used for signature generation and signature verification, respectfully.

[0010] The methods and systems disclosed herein can be used for any sensitive online transaction in which strong assurance of the asserted and the actual electronic identity of the end-user is required. This includes, but is not limited to, electronic government, healthcare, banking, and commercial transactions performed on a network infrastructure including the WWW. The details of the present invention, both as to its structure and operation, can best be understood in reference to the accompanying drawings, in which like reference numerals refer to like parts, and in which:

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] Figure 1 shows the overall general process flow for carrying out embodiments of the method of the present invention.

[0012] Figure 2 shows a first embodiment of a system of the present invention along with a method according to the present invention being carried out; and

[0013] Figure 3 shows a second embodiment of a system of the present invention along with a method being carried out.

DETAILED DESCRIPTION OF THE DRAWINGS AND THE PRESENTLY PREFERRED EMBODIMENTS

[0014] Referring first to Figure 1, the general overall process flow for carrying out the methods disclosed herein and using the systems disclosed herein is shown and described. It is to be understood that this description can be implemented in various systems and with various insignificant modifications but still within the scope of the present invention. The steps of the general method will be described in more detail in conjunction with the description of various embodiments of the system of the present invention that follow.

[0015] Turning to system flow diagram, At 10, according to the general method of the present invention, a first user conducts a user name/password transaction with a network server as a means of establishing his identity electronically. Next, at 20, the network server informs an authentication server (both which may be a single system or device) that a user is attempting to conduct a transaction. Next, at 30, the authentication server conducts an out-of-band (OOB) transaction with the user's device to verify that the user is in possession of the device. Next, at 40, the authentication server sends an OOB one-time passcode (OTP) to the device that it has confirmed that is in the possession of the correct person. Next, at 50, the user enters the OOB OTP into the server dialogue or the authentication service dialogue, as applicable, which is controlled by the same Web session as the user name/password transaction. Next, at 60, the authentication server validates the OTP to confirm the user asserting the user name/password is the same as the person in possession of the device. Next, two things can happen. Either the authentication server informs the server that authentication process is complete (70), or the authentication server informs the key server that the authorization is complete (80). Finally, at 90, the key server releases a key to the application that is either unique to the user or that establishes non-repudiation.

[0016] A first embodiment of the system disclosed herein as shown in Figure 2, and the system generally is designed to carry out the general process disclosed in Figure 1. System 110 comprises a network that makes use of the method of the present invention. Any other suitable network or system may be used however, as well as the WWW. User 112 makes use of computers 116 (only a single computer is shown for clarity), each of which can have a processor and disk and/or solid state program storage for storing software embodying logic, as is well known. Any suitable personal computer, personal digital assistant (PDA), cellular phone, or the like may also be used. Also, each user computer 116 may include one or more input devices such as keyboards, mice, voice recognition devices, etc. as well as one or more output devices such as monitors, printers, other computers, etc., again as is well known

[0017] As is further shown in Figure Two, user computer 116 communicates with server 130 over the WWW 120, a private wide-area network, an internal enterprise network infrastructure, or other equivalent network or combination thereof. Server 130 has a processor and disk and/or solid state storage for storing software embodying logic including all or part of the logic discussed further below necessary for carrying out the present invention, and can be a server of any suitable type for this application. Server 130 may be attached to a plurality of independent servers or can carry out certain functions by itself. All functions may totally be provided on a single physical server. In the embodiment shown, Authentication & Key Server 131 accesses Customer Information Database Server 134 that contains the log in and registration information for various users. It is understood that the database may be pre-populated with user information on existing customers who elect to start up a service utilizing the systems and methods of the present invention. Authentication & Key Server 131 may also access Information Database 136 to supply users with desired information, e.g., bank account records, subscription content, etc. The databases may be implemented in a single data

structure if desired, and are databases of any suitable type kept on any suitable hardware, including on the Application & Key Server 131 itself. There also may be a support key server 132 and an application server 133.

[0018] When a user submits his username and password (115) to the Web site or application hosted on server 130, the username and password are validated by the Server 130. If valid, the Authentication Server 131 receives the username, or a unique reference thereto, from the Server 130. Next, at least two potential processes may occur, but any other suitable method or variation of this method may also occur.

[0019] The first embodiment contemplates a Server-based validation of device possession process, as is further shown in Fig. 2. According to this process, Authentication Server 131 sends an out-of-band Authentication Notification Message (ANM) 140 via short message service (SMS) or other suitable channel to a pre-registered SMS capable device 150 (such as a cell phone, pager, satellite phone, or land-mobile radio) or interactive voice response (IVR) call to a pre-registered voice device 160 (such as a cell phone, home phone, or office phone). This ANM informs the user that a transaction is being conducted and prompts him to enter a secret personal knowledge Token 170 (different from the password entered previously) (e.g. a memorized number or phrase), confirming that he has possession of the device (150 or 160). That personal knowledge token is returned to the Authentication and Key Server 131 as a response using the same channel from which the prompt to enter in was received (e.g. SMS reply, voice response, dual-tone multi frequency (DTMF) entry). Upon receipt of the Token 170 by the Authentication & Key Server 131, if properly validated, a one-time-passcode (OTP) 180 is distributed by the Authentication and Key Server 131 to the user via the pre-registered device (150 or 160) that was just previously validated in their possession. This OTP is then entered by the User to complete the transaction.

[0020] The second embodiment, shown in Fig. Three, is a device-based validation of device possession carried out on the same general system, with slight modifications, and with slightly different steps. In this embodiment, User 112' has a pre-registered SMS or HTML capable device 150' (such as a cell phone or personal digital assistant). This device has data entry (key pad), processing, and storage capability as is well known in the art. Device 150' has an independent Application 200 in its memory, which allows the user to authenticate herself to the device. Application 200 is an application that provides a mechanism to store and update a secret personal knowledge token (e.g. a memorized number or phrase) different from the password entered with the username. This personal knowledge token may be established by the user's enterprise organization or the user herself, such that it can later be used through a challenge and response process to verify that the device is in the possession of the user and not in the hands of another user. Application 200 verifies that the device is in the possession of the person to whom it is registered by the verification of a personal knowledge Token 170, which the User enters into the device to initiate the transaction. Once the User is validated on the device via entry of Token 170, the device 200 sends a secure message 220 to the Authentication and Key Server 131', confirming that User 112' is in possession of the device. Authentication and Key Server 131' then distributes a one-time-passcode (OTP) 180' to the user on the pre-registered device 200 that was just previously validated to be in the proper user's possession.

[0021] Once the user has received the OTP 180 via either method discussed herein, or any suitable variation, she enters the OTP in the web dialog with the Server 130 or 130', thereby confirming that the user who has the device is also the same user who submitted a username and password to the Web site or application on the Server 130 or 130'.

[0022] Authentication and Key Server 131 or 131' then either informs the Server 130 or 130' or the Application Server 133 or 133' directly

through appropriately secured communications protocols that the transaction has been completed satisfactorily or it informs the Key Server 132 or 132' that the authentication transaction has been completed and the key server releases a cryptographic key (either symmetric or asymmetric) to the server 130 or 130' or the application server 133 or 133'. The key released by the key server can either be uniquely representative of the person conducting the authentication (such as PKI) or uniquely representative of the server and the transaction such that it can be non-repudiatively tied back to the user who conducted the authentication transaction.

[0023] While the particular Out of Band System and Method for Authentication as herein shown and described in detail is fully capable of attaining the above-described objects of the invention, it is to be understood that it is the presently preferred embodiment of the present invention and is thus representative of the subject matter which is broadly contemplated by the present invention, that the scope of the present invention fully encompasses other embodiments which may become obvious to those skilled in the art, and that the scope of the present invention is accordingly to be limited by nothing other than the appended claims, in which reference to an element in the singular is not intended to mean "one and only one" unless explicitly so stated, but rather "one or more". It is not necessary for a device or method to address each and every problem sought to be solved by the present invention, for it to be encompassed by the present claims. Furthermore, no element, component, or method step in the present disclosure is intended to be dedicated to the public regardless of whether the element, component, or method step is explicitly recited in the claims. Absent express definitions herein, claim terms are to be given all ordinary and accustomed meanings that are not irreconcilable with the present specification and file history.

[0024] It is therefore intended that the foregoing detailed description be regarded as illustrative rather than limiting, and that it be understood that it

is the following claims, including all equivalents, that are intended to define the spirit and scope of this invention.

CLAIMS

We claim:

1. A method for authentication of a user with a device who is attempting a first transaction comprising the steps of:

Establishing the asserted identity of the user;

Informing an authentication server that the user is attempting to conduct a transaction;

Conducting a second transaction with the user's device and the authentication server to verify that the user is in possession of the device;

Sending an out of band one-time passcode to the device registered to the user;

Entering the one-time passcode into the dialogue;

Validating the one-time passcode; and

Authorizing the first transaction.

2. The method of Claim 1 wherein the device has an application to verify that the user is in possession of the device.
3. The method of Claim 2 wherein the application that verifies the user is in possession of the device is in the authentication server.
4. The method of Claim 1 wherein the transaction is authorized via the release of a symmetric key representative of the individual conducting the transaction.

5. The method of Claim 4 wherein the key is representative of the server on which the transaction was conducted, and can be tied to the unique user through non-repudiatory log and audit capabilities.
6. The method of Claim 1 wherein the transaction is authorized via the release of an asymmetric key representative of the individual conducting the transaction.
7. The method of Claim 6 wherein the key is representative of the server on which the transaction was conducted, and can be tied to the unique user through non-repudiatory log and audit capabilities.
8. The method of claim 1 wherein the out of band passcode is distributed to the end-user's pre-registered device via SMS (text messaging).
9. The method of claim 1 wherein the out of band passcode is distributed to the end-user's pre-registered device via voice.
10. The method of claim 1 wherein the out of band passcode is retrieved by the end-user through the use of their pre-registered voice signature and voice biometrics.
11. A method for authentication of a user with a device who is attempting a transaction comprising the steps of:
 - Establishing the asserted identity of the user;
 - Sending an out of band one-time passcode to the device registered to the user;
 - Validating the one-time passcode; and
 - Authorizing the transaction.

12. The method of Claim 11 wherein the device has an application to verify that the user is in possession of the device.

13. The method of Claim 12 wherein the application that verifies the user is in possession of the device is in the authentication server.

14. The method of Claim 11 wherein the transaction is authorized via the release of a symmetric key representative of the individual conducting the transaction.

15. The method of Claim 14 wherein the key is representative of the server on which the transaction was conducted, and can be tied to the unique user through non-repudiatory log and audit capabilities.

16. The method of Claim 11 wherein the transaction is authorized via the release of an asymmetric key representative of the individual conducting the transaction.

17. The method of Claim 16 wherein the key is representative of the server on which the transaction was conducted, and can be tied to the unique user through non-repudiatory log and audit capabilities.

18. A method for authentication of a user with a device who is attempting a first transaction comprising the steps of:

Establishing the asserted identity of the user;

Conducting a second transaction with the user's device and the authentication server to verify that the user is in possession of the device;

Sending an out of band one-time passcode to the device registered to the user; and

Entering the one-time passcode into the dialogue to authorize the transaction.

19. The method of Claim 18 wherein the device has an application to verify that the user is in possession of the device.
20. The method of Claim 19 wherein the application that verifies the user is in possession of the device is in the authentication server.
21. The method of Claim 18 wherein the transaction is authorized via the release of a symmetric key representative of the individual conducting the transaction.
22. The method of Claim 21 wherein the key is representative of the server on which the transaction was conducted, and can be tied to the unique user through non-repudiatory log and audit capabilities.
23. The method of Claim 18 wherein the transaction is authorized via the release of an asymmetric key representative of the individual conducting the transaction.
24. The method of Claim 23 wherein the key is representative of the server on which the transaction was conducted, and can be tied to the unique user through non-repudiatory log and audit capabilities.

1/3

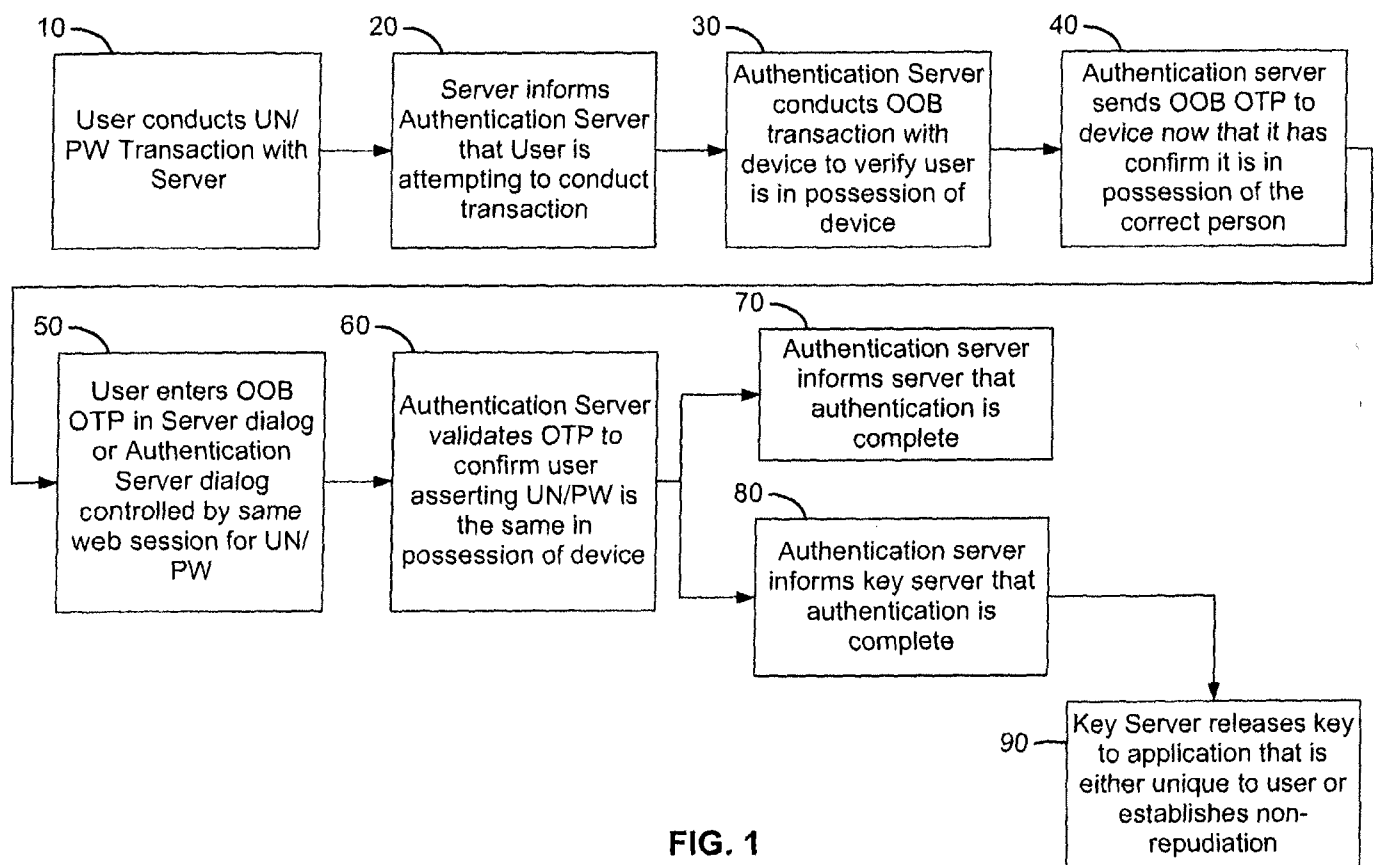


FIG. 1

2/3

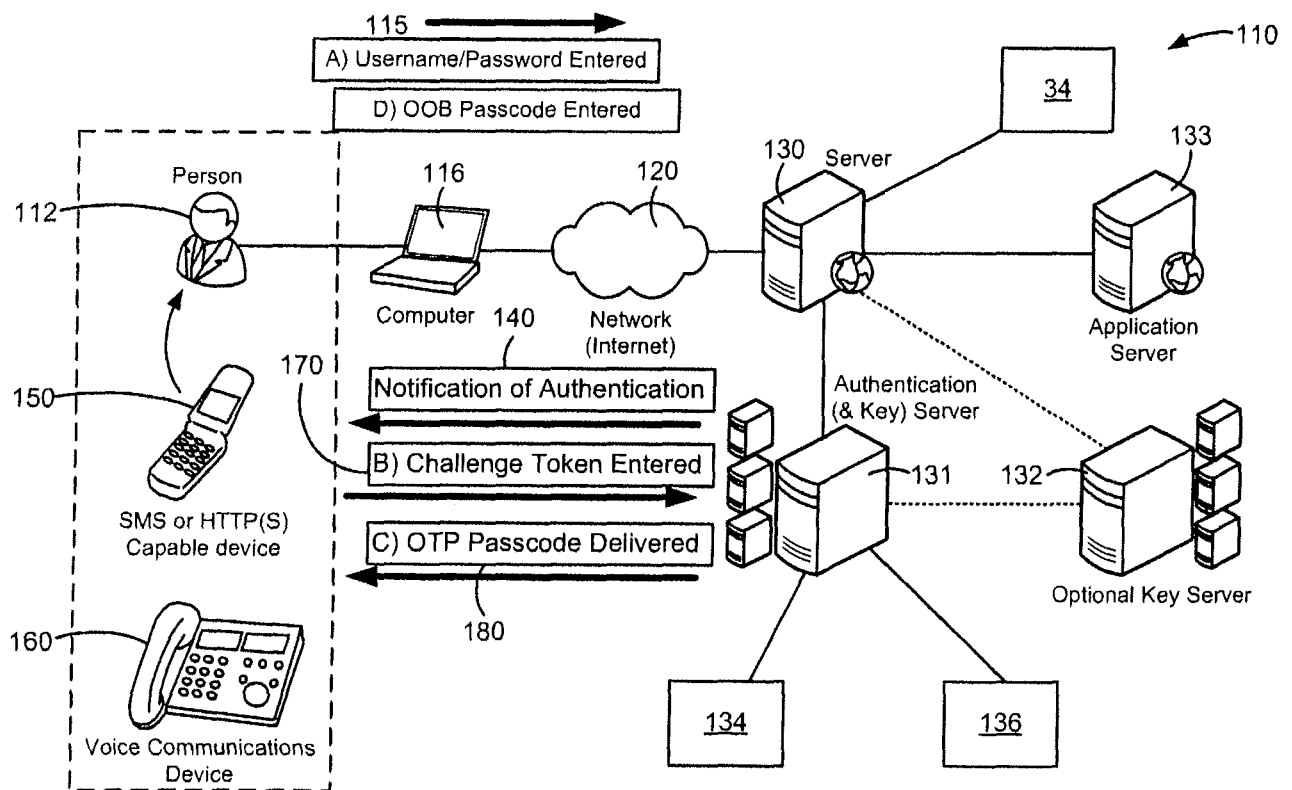


FIG. 2

3/3

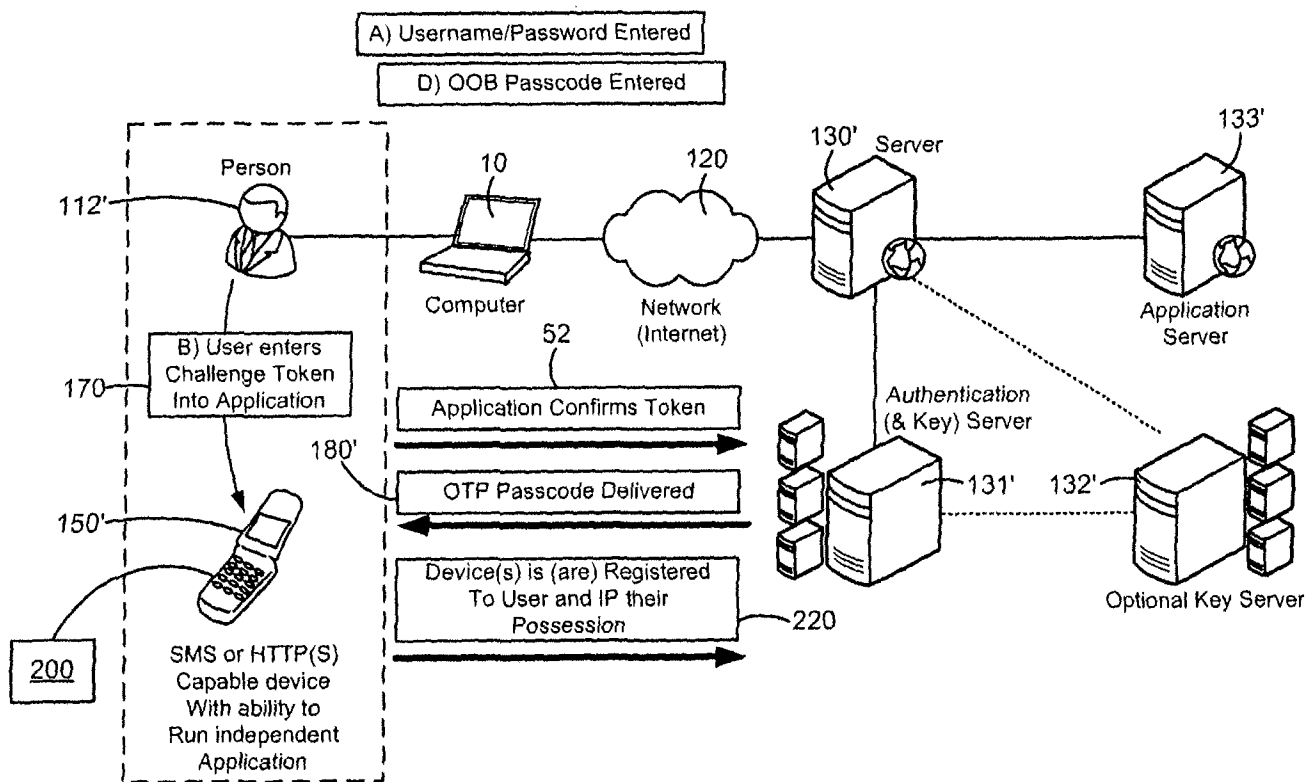


FIG. 3