(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 February 2003 (27.02.2003)

PCT

(10) International Publication Number
WO 03/017031 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number: PCT/US02/24993

(22) International Filing Date: 8 August 2002 (08.08.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/312,998 20 August 2001 (20.08.2001) US

(71) Applicant *(for all designated States except US)*: **REAL USER CORPORATION** [US/US]; P.O. Box 242, 2020 Pennsylvania Avenue, N.W., Washington, DC 20006 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **BARRETT, Paul, D.** [GB/US]; 4417 Chalfont Place, Bethesda, MD 20816 (US). **RYAN, Andrew** [GB/GB]; 1 Grantham Road, Brighton, East Sussex (GB).

(74) Agent: **GARRETT, Arthur, S.**; Finnegan, Henderson, Farabow, Garrett & Dunner, L., L.P., 1300 I Street, NW, Washington, DC 20005-3315 (US).

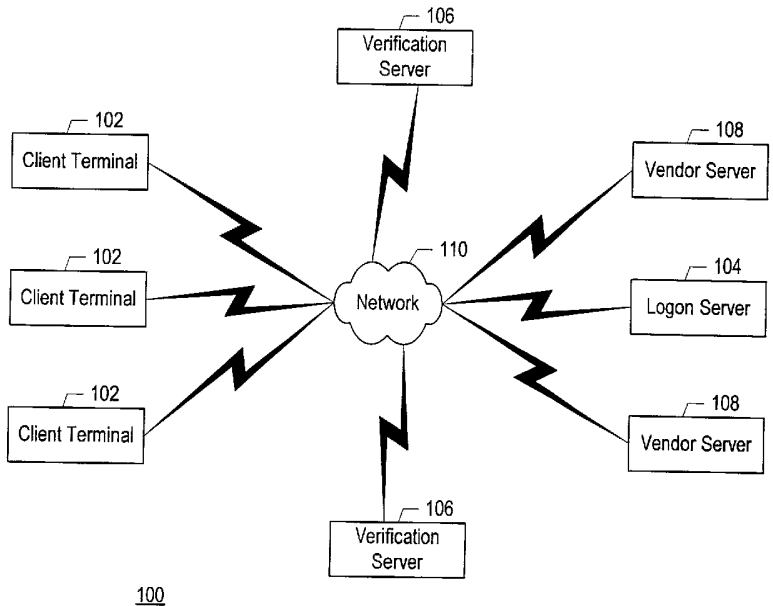
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (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*

[Continued on next page]

(54) Title: SYSTEM, METHOD, AND ARTICLE OF MANUFACTURE FOR PROVIDING SECURITY AND VERIFICATION SERVICES IN AN ONLINE NETWORKS



(57) Abstract: Methods and systems consistent with the present invention provide security and verification services in an online network (e.g., the Internet). In one embodiment, a user may establish an account at a logon server. Then, a verification request that requests verification of user information is received from a requestor. A response is then sent to the requestor by retrieving the requested information from the account on the logon server. Alternatively, a response may also be sent from the verification server. The response may include a digital certificate or a message verifying the user's information.

WO 03/017031 A2

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEM, METHOD, AND ARTICLE OF MANUFACTURE FOR PROVIDING SECURITY AND VERIFICATION SERVICES IN AN ONLINE NETWORK

RELATED APPLICATIONS

[001] This application is related to international patent application no. PCT/IB00/00712, filed April 21, 2000, and U.S. Patent No. 5,608,387, the contents of which are hereby incorporated by reference.

BACKGROUND OF THE INVENTION

Field of the Invention

[002] The present invention relates generally to providing security and verification services in an online network, and more particularly, to a system, method, and article of manufacture for securing and verifying a user's information in an online network. In addition, the present invention relates to a system, method, and article of manufacture for processing a user's purchase request in an online network.

Background Information

[003] In recent years, online networks, such as the Internet, have experienced explosive growth and success due to their ability of providing a user (e.g., a customer) with access to a vast array of resources (e.g., information) and commodities (e.g., products and services) quickly and efficiently. The Internet and more specifically, the World Wide Web ("Web") is a distributed network that includes web servers and web clients. Web servers are software applications that support common protocols, such as Hypertext Transport Protocol (HTTP). Moreover, these web servers make documents, such as documents in hypertext mark up language (HTML), and other resources available to users via web sites. Each web site may include a plurality of web pages and may be identified by a unique address called a Uniform Resource Locator (URL). Web clients include software applications, such as a browser, which a user uses to access a web page, for example.

[004] Most web sites require a user to enter certain information (e.g., name and address) before the user is given access to a resource or before the user is allowed to purchase a commodity. For example, a user's date of birth may be required so that

the web site may prevent a person under a certain age from viewing material of an adult nature or from purchasing certain products, such as tobacco or alcohol. Moreover, a user may be required to transmit financial information (e.g., credit card number) over the Internet to purchase access to a resource or to purchase a commodity.

[005] Once the user provides the required information, most vendors who operate these web sites also want to verify the information supplied by the user to make sure that the information is correct. The vendors, however, may not be able to verify the information quickly and easily. For example, a vendor may need to maintain its own verification means to verify each user's information, a task that may be time consuming and costly. Due to a vendor's inability to verify information, many vendors may prevent certain users from accessing resources or from purchasing commodities and thus, may lose revenues.

[006] Furthermore, a user may be hesitant and may not provide the requested information to a vendor for several reasons. First, a user may be afraid that the information that the user provides to the vendor will be misused because the user may not be able to determine whether a web site is legitimate. Second, a user may wish to remain anonymous either entirely or partially. For example, a user may be willing to provide his or her name and address to the web site, but may not want to give his or her financial information (e.g., credit card number) to the web site. Finally, a user may need to reenter his or her information repeatedly at each web site that the user visits, a task that may be time consuming and inconvenient. As a result, the user may not provide the requested information to the vendor.

[007] Instead of requiring a user to enter information about himself or herself, a web site may obtain such information from a central source, such as a preference server. A preference server may allow a user to store information about the user and may provide the stored information to a web site upon a user's or web site's request. Before providing such information to a web site, a preference server may require a user to enter authentication information (e.g., user name and password) and may prompt the user for confirmation.

[008] Many users, however, do not use such preference servers for various reasons. First, users may not trust such preference servers because users may be afraid that the operators of these preference servers may misuse their information. Second, users may not be satisfied with the security measures taken by such preference servers to protect their information from theft. Finally, users may not be satisfied with the authentication methods used by these preference servers and may be afraid that their authentication information may be compromised by an unauthorized user.

SUMMARY OF A FEW ASPECTS OF THE INVENTION

[009] Methods and systems consistent with the present invention provide security and verification services in an online network (e.g., the Internet). A user may establish an account at a logon server. Then, a request for verification of user information is received from a requestor. A response is then sent to the requestor by retrieving the requested information from the account on the logon server. Alternatively, a response may also be sent from a verification server. The response may include a digital certificate or a message verifying the user's information.

[010] Systems and methods consistent with the present invention may also provide a payment credential to a requestor. A user may establish an account in a database at a logon server. The account may include a payment credential. The payment credential may be encrypted using two keys, one stored in the account and the other on the user's client terminal. After the account has been established, the logon server may receive, from a requestor, a payment credential request. Then, upon request, the payment credential may be sent to a requestor by decrypting it.

[011] Systems and methods consistent with the present invention may also provide user information from a preference server upon request. An account may be established for the user at the logon server and the preference server. The user information may be obtained, encrypted, and stored on the preference server using a key stored in the user's account on the logon server. Then, the encrypted information may be retrieved from the preference server, decrypted, and sent to a requestor upon request.

[012] Systems and methods consistent with the present invention may enable a user to purchase a commodity in an online network. A user may select the commodity provided by a vendor web site. A purchase amount corresponding to the commodity may be sent to a logon server, which may send the purchase amount to a verification server. The verification server may charge the purchase amount to an account corresponding to the user and send to the vendor web site a payment confirmation.

[013] Both the foregoing and the following description are exemplary and explanatory and are intended to provide further explanation of the claimed invention as opposed to limiting it in any manner.

BRIEF DESCRIPTION OF THE DRAWINGS

[014] The accompanying drawings are incorporated in and constitute a part of this specification and, together with the description, explain the principles of the invention. In the drawings,

[015] FIG. 1 is a block diagram of an exemplary system consistent with the present invention;

[016] FIG. 2 is a block diagram of an exemplary client terminal consistent with the present invention;

[017] FIG. 3 is a block diagram of an exemplary logon server consistent with the present invention;

[018] FIG. 4 is a flow diagram of an exemplary method for registering with a logon server of a system consistent with the present invention;

[019] FIG. 5 is a flow diagram of an exemplary method for acquiring a verification using a system consistent with the present invention;

[020] FIG. 6 is a flow diagram of another exemplary method for acquiring a verification using a system consistent with the present invention;

[021] FIGs. 7 and 8 are flow diagrams of exemplary methods of operating a system consistent with the present invention;

[022] FIG. 9 is a flow diagram of an exemplary method for acquiring a payment credential using a system consistent with the present invention;

[023] FIG. 10 is a flow diagram of an exemplary method for using an acquired payment credential using a system consistent with the present invention;

[024] FIG. 11 is a block diagram of another exemplary system consistent with the present invention;

[025] FIG. 12 is a flow diagram of an exemplary method for obtaining information from a preference server using a system consistent with the present invention; and

[026] FIG. 13 is a block diagram of another exemplary system consistent with the present invention.

DETAILED DESCRIPTION

[027] The following detailed description of the invention refers to the accompanying drawings. While the description includes exemplary embodiments, other embodiments are possible, and changes may be made to the embodiments described without departing from the spirit and scope of the invention. The following detailed description does not limit the invention. Instead, the scope of the invention is defined by the appended claims and their equivalents.

[028] Systems, methods, and articles of manufacture consistent with the present invention provide security and verification services in an online network (e.g., the Internet). In accordance with an embodiment, a system may include a client terminal, a logon server, a verification server, and a vendor server. A user, using the client terminal, may register or enroll with the logon server by providing the logon server with a unique set of identification data so that the logon server may subsequently authenticate the user by comparing the identification data provided by the user with the unique set of identification data. The identification data may include, for example, a user name and password.

[029] During registration, the logon server may also request information (e.g., name, address, date of birth) from the user and create an account for the user. The logon server may send a request for verification of this information to a verification server that is being operated by a verification authority (e.g., user's bank). Upon receiving the verification request from the logon server, the verification server may generate and send a response to the logon server. The response may include a

verification or a message indicating that the user's information could not be verified. The verification will depend on the request that was received from the logon server. For example, the verification may include a digital certificate that includes information about the user, a message that includes information about the user, or a response to the request received from the logon server. The logon server may receive the response from the verification server and store it in an account corresponding to the user.

[030] Alternatively, instead of requesting information from the user, the logon server may send a request for information from the verification server, receive the requested information, and store it in the user's account. The information that is received from the verification server may be in the form of a digital certificate.

[031] After the verification or information that is received from the verification server has been stored in the user's account, a user may visit the vendor server and access resources or purchase commodities. If the vendor wants to verify any user information, the vendor server may send a verification request to the logon server. The logon server may in turn send a response to the vendor server. The response may include the digital certificate received from the verification server or a message with the requested information.

[032] Systems, methods, and articles of manufacture consistent with the present invention also process a user's purchase request in an online network. In accordance with an embodiment, once the user has registered with the logon server, as described above, a verification server associated with a verification authority may also be registered with the logon server. Then, when a user desires to purchase access to a resource or a commodity from a vendor's web site, the vendor server may send a purchase request to the logon server, which in turn may send this request to a verification server for processing. The purchase request may include, for example, a purchase amount and the description of the item being purchased. The verification server may process this purchase request, for example, by charging the user's bank account and by sending an approval code to the logon server, which in turn may send it to the vendor server. Since the verification server processes the purchase request, the user's financial information remains anonymous.

[033] In another embodiment, instead of sending the purchase request to the verification server, the logon server may request and receive a payment credential, from the verification server. The payment credential may be a digital certificate or a message including information about a user's financial account (e.g., bank account or a credit card account). The logon server may encrypt the payment credential and store it in the user's account. Then, upon request, the logon server may decrypt the payment credential and provide it to the vendor server. For example, the payment credential may be encrypted using two keys, the first stored in the user's account and the second stored on the user's client terminal in a cookie. The second key may be encrypted with the first key before it is stored on the user's client terminal in a cookie. Then, when a vendor server requests payment, the user may log onto to the logon server, which may in turn decrypt the second key using the first key. Then, the logon server may decrypt the payment credential using the first and second keys and send the payment credential to the vendor server.

[034] Systems, methods, and articles of manufacture consistent with the present invention also secure a user's information that is stored on a central server, such as a preference server. In one embodiment, a system may include a client terminal, a logon server, a preference server, and a vendor server. A user may register with the logon server and the preference server. During registration, the user may provide his or her information to the preference server. Once registered, the user's information on the preference server may be encrypted using a key stored in the user's account on the logon server. Then, when a vendor server requests information from a user, the browser on the user's client terminal may decrypt the encrypted information using the key stored in the user's account and provide the requested information to the vendor server.

[035] Systems, methods, and articles of manufacture consistent with the present invention are not limited to any particular user, vendor, verification authority, resource, or commodity. A user may include, but is not limited to, a customer. A vendor may include, but is not limited to, a merchant, a service provider, a government entity, and a non-profit organization. A verification authority may include, but is not limited to, a bank and a government entity. A resource may

include, but is not limited to, a web site, portion of a web site, and documents or materials located on a web site. A commodity may include, but is not limited to, a product or a service. The commodity may sell for money or may be free.

[036] FIG. 1 is a block diagram of an exemplary system 100 consistent with the present invention. As shown, system 100 may include one or more terminals 102, logon server 104, one or more verification servers 106, and one or more vendor servers 108, which are interconnected by a network 110.

[037] Client terminal 102 may be a computer or a similar device that may receive requests from users, display information to users, and communicate with other computers, such as logon server 104, verification server 106, and vendor server 108. For example, client terminal 102 may include, but is not limited to, a computer, a cellular phone, or a PDA (personal digital assistant). Using client terminal 102, a user may, for example, obtain access to a resource stored on a vendor server 108 and/or purchase a commodity from a vendor server 108. Client terminal 102 may be located, for example, at a user's home or at a location owned or operated by a verification authority (e.g., a bank).

[038] As shown in FIG. 1, systems, methods, and articles of manufacture consistent with the present invention also may include logon server 104. Logon server 104 may be a computer or a similar device that may register users, authenticate users, and store information (e.g., name, address, date of birth) about users in an account corresponding to the user. Each user account may include information about the user and identification data (e.g., user name and password). The information may include verified information and unverified information. Verified information is information that was provided to logon server 104 by verification server 106 or has been verified by logon server 104. Unverified information is information that has not been verified. In one embodiment, a user account may include a digital certificate, such as a X.509 certificate, that has been received from verification server 106 and contains information about a user.

[039] Logon server 104 also may request information about a user from verification server 106, receive the requested information from verification server 106, and store the received information in the user's account. In one embodiment, as

described further in the following description, even if the logon server 104 has not requested information from verification server 106, logon server 104 may receive information from verification server 106 and store the received information in the user's account. In another embodiment, logon server 104 may receive a digital certificate from verification server 106 in response to a request for information about a user.

[040] In addition, logon server 104 may receive requests from vendor servers 108 and process these requests. In one embodiment, logon server 104 may receive a verification request from vendor server 108 requesting the logon server 104 to verify certain information about a user. The logon server 104 may retrieve such information, compare it against the information sent by verification server 106, and send a verification to vendor server 108. In another embodiment, logon server 104 may receive an information request from vendor server 108 requesting certain information about a user, retrieve the requested information, and send the requested information to vendor server 108. In this embodiment, if logon server 104 does not have the requested information, logon server 104 may forward the request to verification server 106, which may in turn provide the requested information to either vendor server 108 or logon server 104 so that the logon server can provide the information to the vendor server 108. In still another embodiment, logon server 104 may send a digital certificate stored in a user's account to vendor server 108 in response to a request for verification of user information.

[041] Logon server 104 may be located in a secured area, accessible by authorized personnel only. In the embodiment of FIG. 1, only one logon server 104 is shown. As the size of system 100 grows, however, additional servers may be added. These additional servers may assist with load balancing.

[042] As shown in FIG. 1, systems, methods, and articles of manufacture consistent with the present invention also may include one or more verification servers 106. Verification server 106 may be a computer or a similar device that may verify a user's information and may provide the verified information to logon server 104 and/or vendor server 108. The verified information may be in the form of a digital certificate, such as a X.509 certificate. In addition, verification server 106 may

process purchase requests. For example, if the verification authority is a bank, verification server 106 may receive a purchase request from vendor server 108 or logon server 104 and process this request, for example, by charging the user's account for the amount of the purchase, and then, sending the requesting server an approval code.

[043] Verification server 106 may be owned and/or operated by a verification authority. The number of verification servers 106 may depend on the number of verification authorities and the number of verification authorities may depend on the user information that needs to be verified. Moreover, like logon server 104, verification server 106 may be located in a secured area, accessible by authorized personnel only.

[044] Systems, methods, and articles of manufacture consistent with the present invention also may include one or more vendor servers 108. Vendor server 108 may be a computer or similar device that offers resources and/or commodities to users. Vendor server 108 may offer a user access to these resources only after verifying the user's information, for example, by sending a verification request to logon server 104 or verification server 106 and receiving a response from logon server 104 or verification server 106. In addition, vendor server 108 may receive a purchase request (e.g., request to purchase a commodity that the vendor sells) from a user and send this request to verification server 106 or logon server 104 for processing. In one embodiment, instead of sending the purchase request to verification server 106 or logon server 104, the vendor server 108 may request financial information (e.g., credit card number) from verification server 106 or logon server 104 and upon receiving such information, may process the purchase request, for example, by charging the user's credit card for the amount of the purchase.

[045] Vendor server 108 may be owned and/or operated by a vendor. The number of vendor servers 108 may depend on the number of vendors. Moreover, like logon server 104 and verification server 106, vendor server 108 may be located in a secured area, accessible by authorized personnel only.

[046] Network 110 may be a single or a combination of any type of computer network, such as a Local Area Network (LAN) or a Wide Area Network

(WAN). For example, network 110 may comprise an Ethernet network operating according to the IEEE 802.3 standard. In addition, network 110 may be a combination of public (e.g., Internet) and private networks.

[047] Other system and network configurations will be apparent to those skilled in the art from the foregoing and following description, and thus, are also within the scope of the present invention. For example, verification servers 106 may not be needed in a system where logon server 104 verifies the user information independently.

[048] Moreover, while the components of FIG. 1 are shown as logical devices, one skilled in the art would readily understand that each is associated with a respective physical device. For example, as described in the foregoing description, logon server 104 may be a physical device, such as a computer. Also, it will be known to those skilled in the art that the components of system 100 may use a single or a combination of protocols and technologies to communicate with each other. For example, the components may use HTTP and Transmission Control Protocol/Internet Protocol (TCP/IP) for transport and HTML for presenting information to users. Moreover, depending on the type of components, different protocols and technologies may be used. For example, if the client terminals 102 include cellular telephones, wireless markup language (WML) and wireless application protocol (WAP) also may be used.

[049] FIG. 2 is a block diagram of an exemplary client terminal 102 consistent with the present invention. As shown, client terminal 102 may include browser 202, output device 204, processor 206, memory 208, communications device 210, input device 212, and other software and data storage 214.

[050] Browser 202 may include a conventional software application, such as NETSCAPE NAVIGATOR or INTERNET EXPLORER, for issuing HTTP requests to logon server 104, verification server 106, and vendor server 108. For example, browser 202 may request a specific web page or ask the logon server 104, verification server 106, and vendor server 108 to perform a database query. Browser 202 also may read HTML codes embedded in the web pages received from the various servers to determine how, where, and in what colors and fonts the elements on

the web pages must be displayed. In another embodiment, if cellular phones are used as client terminals 102, a WAP-compatible micro-browser may be used as the browser 202.

[051] Output device 204 may include a device that displays information to users. In addition, client terminal 102 also may include processor 206 and/or memory 208. The processor 206 may control the components of client terminal 102 and assist in processing requests received from other components. The memory 208 may include ROM (Read Only Memory) and/or RAM (Random Access Memory).

[052] Client terminal 102 also may include communications device 210 that may include an interface device for transmitting information from client terminal 102 to network 110 and for receiving information that is addressed to client terminal 102 from network 110. For example, communications device 210 may be a network interface card or a modem. In one embodiment, when sending information, communications device 210 may break the information into packets that are sent across a TCP/IP network 110 to the various servers. In addition, communications device 210 may check for errors in transmission using, for example, cyclical redundancy check ("CRC").

[053] Input device 212 may include a device that is used for receiving input from a user. For example, input device 212 may include a keyboard, a keypad, and/or a pointing device (e.g., a mouse or a trackball). A keypad may comprise a conventional alphanumeric or numeric key entry device. On-site client terminal 102 also may include other software and data storage 214, such as an operating system.

[054] It will be apparent to one skilled in the art that client terminal 102 may include some or all the components shown in FIG. 2. Moreover, it will be apparent to one skilled in the art that client terminal 102 may include additional components not shown in FIG. 2. For example, client terminal 102 may include a printer device to print, for example, information received from the various servers.

[055] FIG. 3 is a block diagram of an exemplary logon server 104 consistent with the present invention. As shown, server 104 may include a communications component 302 and database 304. Communications component 302 may include a combination of software and hardware devices, such as a web server

and a network interface card. Communications component 302 may receive messages from and send messages to client terminals 102 and other servers. Communications component 302 also may decode, decrypt, and error check messages received from client terminals 102 and other servers. It also may encode and encrypt messages to client terminals 102 and other servers.

[056] Communications component 302 may authenticate users using the identification data stored in database 304. For example, if the identification data is a user name and password, communications component 302 may identify a user by comparing the user's user name to the user account and then, authenticating the user by comparing the user's password to the password stored in the user account. In one embodiment, the identification data may include a username along with a unique set of complex images, such as a set of human faces. A system and method for implementing such identification data is disclosed in U.S. Patent No. 5,608,387, which is hereby incorporated by reference. If complex images are used for authentication, then one or more sequences of screen displays may be presented to a user to authenticate their identity through correct image selection. Each screen display may comprise a matrix of images (e.g., a 3x3 matrix) in which one key or true image is displayed with other dummy or decoy images. In order to be authenticated, the user may be required to select the key image over the dummy images from each matrix. This process may be repeated over several screen displays (e.g., four or five screens) so that the user selects all of their unique key images for authentication. Authentication, however, is not limited to username and password authentication or username and complex images authentication. It may include any authentication method known to those skilled in the art. For example, biometric authentication also may be used.

[057] Communications component 302 also may act as an interface between the client terminals 102, verification servers 106, and/or vendor servers 108. For example, communications component 302 may redirect a user's browser from one server to another, for example, after the user has successfully authenticated.

[058] Logon server 104 also may include a database 304. Database 304 may store user accounts, each account including information about the user and

identification data for each user. Database 304 also may store other information, such as web pages.

[059] Although not shown, it will be apparent to one skilled in the art that server 104 may include other components, such as an output device (e.g., monitor), input device (e.g., keyboard and pointing device), network operating system, and a database server. The network operating system may include a conventional network operating system, such as WINDOWS NT SERVER. The network operating system may process requests from client terminals, monitor network hardware and software, coordinate communication in the network, and provide transaction security. The database server may build and maintain database 304. In addition, the database server may retrieve from database 304 user information to respond to requests from verification server 106 or vendor server 108. Furthermore, the database server may be a SQL (Structured Query Language) server.

[060] Moreover, although not shown, the verification server 106 and the vendor server 108 also may include some or all of the components that are included in the logon server 104 shown in FIG. 3.

[061] In accordance with one embodiment of the present invention, a user wishing to use system 100 may establish an account with logon server 104, for example, by registering with server 104. The process of registering will be described now by referring to FIG. 4. In particular, a user may initialize his network connection and browser 202 (step not shown in figure), for example, by connecting to network 110 (e.g., the Internet) via conventional means (e.g., via an Internet service provider). Once connected to network 110, the user may control browser 202 to access logon server 104 (step not shown in figure). Logon server 104 may receive the user access request (step 402) and may process this request, for example, by displaying a welcome web page to user (step 404). A web page of logon server 104 may then prompt the user to enter a user name in order to determine whether the user is registered with logon server 104 (step 406). Alternatively, the user may be prompted to determine if the user is a registered user or persistent client state objects (commonly referred to as "cookies") may be used to determine if the user is a registered user. If the user is not registered and requests to enroll, then logon server

104 may execute a user enrollment procedure to register the user (step 408). As described in the foregoing description, during the enrollment process, the user may be prompted for pertinent user information (e.g., name, address, telephone number, credit card data, etc.) and identification data (e.g., username and password combination). Alternatively, the user information may be obtained from the verification server 106. This process may be used by logon server 104 to set-up a unique account (e.g., file or record) for the user and facilitate future user authentication and access to user information. In addition, this account may facilitate identity management as described in international patent application no. PCT/IB00/00712, filed April 21, 2000, which is hereby incorporated by reference.

[062] After the user has registered with the logon server 104, a prompt may be provided to determine if the user wishes to logon (step 410). If the user decides to logon at a later time or closes the current session, then the process terminates or is suspended until the user again accesses logon server 104 (step 412). If, however, the user requests to log on, then logon server 104 may execute a logon procedure to authenticate the user (step 414). During this phase, the logon server may authenticate the user against his or her unique identification data (e.g., username and password). If the user successfully logs on, then logon server 104 processes requests received from a user, for example, update user information or present web pages of the logon server 104 in response to a user request to access such web pages (step 416). If, however, the user is not able to authenticate, the user may be given another opportunity to logon. After a predetermined number of attempts (e.g., three attempts), the logon server 104 may terminate the logon procedure and/or further block attempts to logon until after a predetermined period and may prompt the user to contact a person associated with logon server 104 (step not shown in the figure).

[063] The information that the user provides during registration with logon server 104 may be unverified information. To verify this information, a user may request a verification from a verification authority. The process of verifying a user's information will be now described by referring to FIGs. 5 and 6.

[064] Although not shown in FIG. 5, a user may connect to network 110 using client terminal 102 and then, request access to logon server 104 using browser

202, for example, by typing in the URL corresponding to logon server 104. Logon server 104 receives this request for access and may display, for example, a welcome web page to the user (step 502). Alternatively, a user may connect to network 110 using client terminal 102 and request access to another server (e.g., vendor server 108). This other server may inform the user of the possibility of obtaining a verification from a verification authority and may prompt the user to select a link that points to logon server 104 if the user wants to obtain such a verification. Once the user selects that link, the user's browser may be redirected to logon server 104 by the other server and logon server 104 may display a welcome web page to the user (step 502).

[065] The logon server 104 may prompt the user to logon (step 504). Although not shown, if the user is already registered and if the user has already authenticated to the logon server 104 during the current browser session, the user may not need to logon. On the other hand, if the user has not registered with the logon server 104, the user may be asked to register and then, logon. Also, if the user has not authenticated during the current browser session, the logon server may prompt the user for identification data (e.g., username and password combination), which the logon server may compare against its database and authenticate the user if they match. To determine whether the user is already registered or if the user has already authenticated during the current session, cookies may be used. In one embodiment, the user may be required to authenticate again even if the user has authenticated during the current browser session to provide increased security. For example, if a predetermined time has elapsed between the user's last logon and current logon, the user may be required to logon again.

[066] Once the user has successfully authenticated, logon server 104 may inform the user that some or all of the information provided by the user has not been verified and then, ask the user whether the user wants to obtain verification from a verification authority (step 506). If the user does not want to obtain verification, then the user is done (step 518). Alternatively, if the user does want to obtain verification, logon server 104 may redirect the user to verification server 106 along with a verification request (step 508). For example, logon server 104 may redirect browser

202 to the web site hosted by verification server 106. The redirection may include, for example, the user's name and the information required by the logon server 104. Redirection methods will be known to those skilled in the art and are within the scope of the present invention. For example, logon server 104 may use an HTTP status 302 code with a location header to redirect the user's browser to verifications server 106. The location header may contain the URL corresponding to verification server 106. The URL may include the web address corresponding to verification server 106 as well as other information (e.g., authentication information).

[067] The request for verification from logon server 104 may include many forms. For example, the logon server 104 may request a digital certification from verification server 106 or request that verification server 106 verify certain information about the user.

[068] Verification server 106 may receive the verification request (not shown in figure) and may request logon information from the user (step 510). The logon information will vary depending on the verification authority and user's location. For example, the logon information may be a username and password that the verification authority mailed to a user at the user's home address if the user is at home and is using client terminal 102 located at his home. On the other hand, if the user is at a location owned or operated by the verification authority (e.g., a bank), the user may show an identification to an employee associated with the verification authority and then, the employee may enter the logon information (e.g., an authorization code) and allow the user to proceed with the verification process. It will be apparent to one skilled in the art that other known methods may be used to authenticate a user and such methods are also within the scope of the present invention. For example, verification server 106 may prompt the user for unique information associated with the user, such as mother's maiden name, and may compare this information against the information provided by the user when the user opened an account with the verification authority.

[069] After the verification server 106 receives the requested information, the verification server 106 compares the information to the information stored in the verification server 106 (step 512). If the information matches, the user is

authenticated (step 512). If, however, the information does not match, the user may be asked to reenter the logon information (not shown in figure). Depending on the verification authority, a user may only be given a predetermined number of attempts to logon and if the user is still unsuccessful in logging on, the user may be asked to contact the verification authority.

[070] Once the user has authenticated, the verification server 106 may send a verification to the logon server 104 by redirecting the user to the logon server 104 (step 514). In one embodiment, the verification that is sent by the verification server may include a message verifying the user's information. In another embodiment, the verification that is sent by the verification server 106 may include a digital certificate, such as a X.509 certificate. The digital certificate may include information about the user that may have been verified by the verification authority. For example, if the verification authority is a bank, the certificate may include a user's name, address, date of birth, social security number, and credit card number.

[071] Although not shown in FIG. 5, in one embodiment, the verification server 106 may display the verification that is being sent to the logon server 104 to the user and request the user's authorization before sending any response to the logon server 104. In this embodiment, the verification will only be sent to the verification server 106 after receiving authorization from the user.

[072] Logon server 104 receives the verification and stores it in the user's account (step 516). The verification acquisition process is now complete (step 518).

[073] In this embodiment, if verifications server 106 cannot authenticate the user or cannot provide a verification, verification server 106 may send a message to logon server 104 indicating that the user could not be authenticated and/or that a verification cannot be provided at this time.

[074] In the above embodiment, logon server 104 requested a verification from the verification server 106. The present invention, however, is not limited to requesting a verification. For example, in another embodiment, if the user only provided limited information, such as user's name and address, during the registration process, the process shown in FIG. 5 could be used to request additional information from the verification server 106, such as all the information that the verification server

106 has about the user. In this embodiment, the verification server 106 may verify the user's information and provide additional information to the logon server 104.

[075] Several modifications to the verification acquisition process shown in FIG. 5 will be apparent to one skilled in the art from the foregoing and following description. Such modifications also are within the scope of the present invention. For example, in one embodiment, the verification server 106 may send a verification or information about a user to the logon server 104 even if the logon server does not request such information from the verification server 106. In this embodiment, the verification may include some or all the user information that the verification authority has for a particular user. This embodiment will be further described by referring to FIG. 6.

[076] Although not shown in FIG. 6, a user may connect to network 110 using client terminal 102 and then, request access to the verification server 106 using browser 202, for example, by typing in the URL corresponding to the verification server 106. Verification server 106 receives this access request and may display, for example, a welcome web page to the user (step 602). Alternatively, a user may connect to network 110 using client terminal 102 and request access to another server (e.g., vendor server 108). This other server may inform the user of the possibility of obtaining a verification from a verification authority and may prompt the user to select a link that points to verification server 106 if the user wants to obtain such a verification. Once the user selects that link, the user's browser may be redirected to verification server 106 by the other server. Verification server 106 may in turn display a welcome web page to the user (step 602).

[077] The verification server 106 may then prompt the user to logon (step 604). Steps 604 and 606 are similar to steps 510 and 512 shown in FIG. 5 and thus, will not be further described. After the user has authenticated, the verification server 106 may ask the user whether the user would like to send a verification to the logon server 104 (step 608). If the user does not want to send a verification to the logon server 104, then the process is complete (step 618).

[078] If, however, the user does want to send a verification to the logon server, the verification server 106 may send a verification by redirecting the user's

browser to the logon server 104 (step 610). Step 610 is similar to step 514 and will not be described further. The logon server 104 may prompt the user to logon (step 612). This authentication step (step 612) is similar to step 504 shown in FIG. 5 and will not be described further.

[079] After the user has authenticated, the logon server 104 stores the verification in the user account (step 614). Once the verification has been stored, the logon server 104 redirects browser 202 to the verification server 106 (step 616) and the process is complete (step 618).

[080] As described in the foregoing description, the verification may include a message from the verification server 106. Moreover, in this embodiment, if the user is not registered with the logon server 104, the verification server 106 may provide all the required user information to logon server 104 so that the user does not have to provide this information to the logon server 104. In another embodiment, the verification that is sent by the verification server 106 may include a digital certificate, such as a X.509 certificate. The digital certificate may include information about the user that may have been verified by the verification authority.

[081] Furthermore, although not shown in FIG. 6, the verification server 106 may display the information that is being sent to the logon server 104 to the user and request the user's authorization before sending the information to the logon server 104. In this embodiment, the information will only be sent to the verification server 106 after receiving authorization from the user.

[082] Once the information has been verified and stored in the logon server 104, the logon server 104 may provide this information or a verification to vendor servers 108 upon request. The process of providing information or a verification to vendor servers 108 will be described now by referring to FIG. 7.

[083] Although not shown in FIG. 7, a user may connect to network 110 using client terminal 102 and then, request access to vendor server 108 using browser 202, for example, by typing in the URL corresponding to the vendor server 108. Vendor server 108 receives this access request and may display, for example, a welcome web page to the user (step 702). The user may send a request to access a resource (e.g., a document) that the user wants to access or send a purchase request

for a commodity that the user wants to purchase from the web page (step not shown in figure). The resource access request or purchase request may be generated, for example, by clicking on a region of the web page that is displayed to the user. The process of selecting resources and commodities will be known to those skilled in the art and is also within the scope of the present invention.

[084] Vendor server 108 may receive and process this request (step 704). During processing, the vendor server 108 may prompt the user for certain information, such as name, address, and credit card number. The user may provide the requested information to the vendor server 108. In addition, the vendor server 108 may prompt the user for verification of this information (step 706). If the vendor server 108 does not require verification, then, the process is complete (steps 706 and 718) and the user may be given access to the resource or the purchase request may be processed, for example, by charging the user's credit card account.

[085] If, however, the vendor server 108 requires verification, then, the vendor server 108 may, for example, redirect the user to the logon server 104 with a request for verification of the user information from the logon server 104 (step 708). The request for verification may take many different forms. For example, in one embodiment, vendor server 108 may request logon server 104 for a verification that includes a digital certificate. In another embodiment, the request may include the information provided by the user to the vendor server 108 and may request the logon server 104 to verify this information against the information stored in the logon server 104. In still another embodiment, the request may be in the form of a question, such as "Is John Smith over the age of 21," so that at least some of the user's information remains anonymous (in this case, the user's date of birth).

[086] The logon server 104 may prompt the user to logon (step 710). This authentication step is similar to step 504 and will not be described further. Once the user has successfully authenticated, the logon server 104 may process the request received from the vendor server 108 and may prompt the user for confirmation before sending a response to the vendor server 108 (step 712).

[087] Depending on the request from vendor server 108, logon server 104 may send an appropriate response. For example, if vendor server 108 requested logon

server 104 for a verification that includes a digital certificate, logon server 104 may retrieve the digital certificate stored in the user's account from database 304 and send it to vendor server 108. On the other hand, if vendor server 108 requested verification of certain user information, logon server 104 may compare the information provided by vendor server 108 against the information stored in the database 304. The response may include either a verification or a response indicating that the information does not match. In this case, the verification may take many different forms, including a message generated by the logon server 104. For example, the message may say: "According to Verification Authority X, John Smith's full name is John R. Smith and his address is 555 Smith Street, Smithsville, VA 55555" if the vendor server only wanted verification of the user's name and address.

[088] If the user does not want to send a verification to the vendor server 108 (step 712), the logon server 104 may send a response to the vendor server 108 indicating, for example, that the user does not want to send a verification. On the other hand, if the user confirms, the logon server 104 may redirect the browser 202 to the vendor server 108 along with a response, which may include a verification or a response indicating that the information does not match.

[089] The vendor server 108 may receive the response from the logon server and depending on the response, may process the user's request (step 716), and may complete the process (step 718). For example, if the response is a verification, the vendor server 108 gives the user access to the resource or completes the purchase request, for example, by charging the user's credit card account for the amount of the purchase. If, however, the response indicates that the information does not match, the vendor server 108 may, for example, decline the user's request, may request further information from the user, or may request the user to mail in payment before giving the user access to the selected resource or sending the selected commodity to the user.

[090] In the foregoing description, the vendor server 108 requested a verification from the logon server 104. The present invention, however, is not limited to requesting a verification. For example, in another embodiment, if the user only provided limited information, such as user's name and address, during the registration process, the process shown in FIG. 7 could be used to request additional information

from the logon server 104, such as the user's credit card number. In this embodiment, the logon server 104 may verify the user's information and provide additional information to the vendor server 108. In still another embodiment, the vendor server 108 may receive all required information from the logon server 104 instead of prompting the user for such information and then verifying it with the logon server 104.

[091] In another embodiment of the present invention, the verification server 106 may verify the information for a vendor server 108. In this embodiment, the verification server 106 also may process purchase requests for vendors. This embodiment will be further described by reference to FIG. 8.

[092] Although not shown in FIG. 8, a user may connect to network 110 using client terminal 102 and then request access to vendor server 108 using browser 202, for example, by typing in the URL corresponding to the vendor server 108. Vendor server 108 may receive this access request and may display, for example, a welcome web page to the user (step 802 similar to step 702). The user may send a request to access a resource (e.g., a document) that the user wants to access or send a purchase request for a commodity that the user wants to purchase from the web page (step not shown in figure). The resource access request or purchase request may be generated, for example, by clicking on a region of the web page displayed to the user. The process of selecting resources and commodities will be known to those skilled in the art and is also within the scope of the present invention.

[093] Vendor server 108 receives the request and processes this request (step 804 similar to step 704). During processing, the vendor server 108 may prompt the user for certain information, such as name, address, and credit card number. The user may provide the requested information to the vendor server 108. In addition, the vendor server 108 may prompt the user for verification of this information (step 806 similar to step 706). If the vendor server 108 does not require verification, then, the process is complete and the user may be given access to the resource or the purchase request may be processed, for example, by charging the user's credit card account (steps 806 and 834).

[094] If, however, the vendor server 108 requires verification, then, the vendor server 108 may prompt the user to select a verification entity. If the vendor server 108 already has established a relationship with certain verification authorities, then the vendor server 108 may provide the user with a list and prompt the user to select one. On the other hand, if the vendor server 108 has not established a relationship with a verification authority, the vendor server 108 may prompt the user to select the logon server 104. If the vendor server 108 has established a relationship with a verification authority and the logon server 104, the vendor server 108 may list both the verification authority and the logon server 104. Once the user selects a verification entity, the vendor server 108 may send a verification request to the selected entity (step 810) by, for example, redirecting the user's browser 202 to the server corresponding to the selected entity and requesting verification.

[095] As described in the foregoing description, the request for verification may take many different forms. For example, in one embodiment, the request may include the information provided by the user to the vendor server 108 and may request the verification entity to verify this information against the verification entity's information. In another embodiment, the request may be in the form of a question, such as "Is John Smith over the age of 21," so that at least some of the user's information remains anonymous (in this case, the user's date of birth).

[096] If the user selected a verification authority as the verification entity, the verification request is sent to the verification server 106 corresponding to the verification authority (step 810). Verification server 106 receives the verification request (not shown in figure) and requests logon information from the user unless the user has already registered the verification server 106 with logon server 108 (step 812).

[097] As described in the foregoing description, the logon information will vary depending on the verification authority and user's location. For example, the logon information may be a username and password that the verification authority mailed to a user at the user's home address if the user is at home and is using client terminal 102 located at his home. On the other hand, if the user is at the verification authority's location (e.g., a bank), the user may show an identification to an employee

associated with the verification authority and then, the employee may enter the logon information (e.g., an authorization code) and allow the user to proceed with the verification process. It will be apparent to one skilled in the art that other known methods may be used to authenticate a user and such methods are also within the scope of the present invention. For example, verification server 106 may prompt the user for unique information associated with the user, such as mother's maiden name, and may compare this information against the information provided by the user when the user opened an account with the verification authority.

[098] After the verification server 106 receives the requested information, the verification server 106 may compare the information to the information stored in the verification server 106 (step 812). If the information matches, the user may be authenticated (step 812). If, however, the information does not match, the user may be asked to reenter the logon information (not shown in figure). Depending on the verification authority, a user may only be given a predetermined number of attempts to logon and if the user is still unsuccessful in logging on, the user may be asked to contact the verification authority.

[099] If, however, the user has registered the verification server 106 with the logon server 108, then, the user does not need to logon, and instead, the verification server 106 may redirect the user's browser 202 to the logon server 108 for authentication (step 814). To determine whether the user has registered the verification server 106 with the logon server 108, cookies may be used, for example. Registering the verification server 106 allows the logon server 104 to perform authentication and identity management for verification server 106. Registering includes assigning a unique user tag to a user for each verification authority. The user tag may be, for example, a user's social security number, which may be used by the verification authority to associate a user with his or her account. The user tag may be assigned either by the logon server 104 or by the verification server 106. This identity management process is described in detail in related international application no. PCT/IB00/00712, filed April 21, 2000 with respect to a vendor; however, the process may also be used with other entities, such as the verification authority of the present application.

[0100] Upon receiving an authentication request, the logon server 104 authenticates the user (step 816). This authentication step is similar to step 504 shown in FIG. 5 and will not be described further. Once authenticated, the logon server 104 may redirect the user's browser 202 to the verification server 106 with a user tag corresponding to that verification server 106 (step 818). Authenticating to logon server 104 may provide additional assurance of the user's identity to vendor server 108 and verification server 106.

[0101] Upon redirection from the logon server 104 (step 818), verification server 106 may process the request received from the vendor server 108 and may prompt the user for confirmation before sending a response to the vendor server 108 (steps 836 similar to step 712). In one embodiment, the response may include a digital certificate that includes the information about the user. In another embodiment, if the request for verification requested verification of certain user information, the verification server 106 may compare the information provided by the vendor server against the information stored in the verification server (step 836 similar to step 712). The response may include either a verification or a response indicating that the information does not match. The verification may take many different forms. For example, the verification may be a message that states: "According to Verification Authority X, John Smith's full name is John R. Smith and his address is 555 Smith Street, Smithsville, VA 55555" if the vendor server 108 only wanted verification of the user's name and address."

[0102] If the user does not want to send a verification to the vendor server 108, the verification server 106 may send a response to the vendor server 108 indicating, for example, that the user does not want to send a verification.

[0103] On the other hand, if the user confirms, the verification server 106 may redirect the browser 202 to the vendor server 108 along with a response (step 838). The vendor server 108 may receive the response from the verification server 106 and depending on the response, processes the user's request (step 832). For example, if the response is a verification, the vendor server 108 gives the user access to the resource or completes the purchase request, for example, by charging the user's credit card account for the amount of the purchase. If, however, the response

indicates that the information does not match, the vendor server 108 may, for example, decline the user's request, may request further information from the user, or may request the user to mail in payment before giving the user access to a resource or sending the selected commodity to the user.

[0104] If the user selected the logon server 104 as the verification entity (step 808), the verification request is sent to the logon server 104 (step 810) by redirecting the user's browser 202 to the logon server 104. Upon redirection, the logon server 104 prompts the user to authenticate (step 820). This authentication step is similar to step 504 shown in FIG. 5 and will not be described further.

[0105] After the user has successfully authenticated, the logon server 104 may either process the verification request like the embodiment shown in FIG. 7 (step not shown in figure) or may prompt the user to select a verification authority (step 822), for example, if the logon server 104 does not have the requested information. In this embodiment, it will be assumed that the logon server 104 does not have the requested information and thus, prompts the user to select a verification authority. The logon server 104 may next receive the user selection (step 824) and may retrieve the user tag corresponding to the verification authority selected by the user (step not shown in figure).

[0106] The logon server 104 may then redirect the user's browser 202 to the verification server 106 corresponding to the selected verification authority along with the retrieved user tag and verification request (step 826).

[0107] Upon redirection from the logon server (step 826), the verification server 106 may process the request received from the vendor server 108 and may prompt the user for confirmation before sending a response to the logon server 104 (step 828 similar to step 712). If the user does not want to send a verification to the logon server 104, the verification server 106 may send a response to the logon server 104 indicating, for example, that the user does not want to send a verification, which may in turn be sent by the logon server 104 to the vendor server 108.

[0108] On the other hand, if the user confirms, the verification server 106 may redirect the browser 202 to the logon server 104 and send a response to the logon server 104 (step 828). The logon server 104 may in turn send the response to the

vendor server 108 (step 830). The vendor server 108 receives the response from the logon server 104 and depending on the response, processes the user's request (steps 830 and 832). Once the vendor server 108 receives a response and processes the user's request, the process is complete as shown in FIG. 8 (step 834).

[0109] Like the embodiment shown in FIG. 7, this embodiment is not limited to requesting a verification. For example, in another embodiment, the vendor server 108 may request information about the user (e.g., credit card information). In this embodiment, the verification entity may verify the user's information and provide additional information to the vendor server 108. In still another embodiment, the vendor server 108 may receive all required information from the verification entity instead of prompting the user for such information and then verifying it with the verification entity.

[0110] Moreover, in another embodiment, the vendor server 108 could send a purchase request to the verification entity. In this embodiment, the purchase request may include, for example, the amount of the purchase and a description of the commodity or resource being purchased. The verification entity (e.g., a bank) could process the purchase request, for example, by charging the user's account for the amount of the purchase, and by sending an approval code to the vendor server 108. In this embodiment, the user's account information is never given to the vendor server 108 or the logon server 104.

[0111] It will be apparent to one skilled in the art that a user's account may have several verifications. For example, a user's account may have two verifications, one from the user's financial institution verifying the user's account details with that institution and one from a government institution verifying the user's identity (e.g., name, social security information, etc.).

[0112] In addition to obtaining a verification from a verification authority, systems, methods, and articles of manufacture also facilitate in acquiring a payment credential from a verification authority. A payment credential may include information about a user's financial account (e.g., a bank account or a credit card account). The payment credential may be in the form of a digital certificate or a

message. FIG. 9 is a flow diagram of an exemplary method for acquiring a payment credential using a system consistent with the present invention.

[0113] Although not shown in FIG. 9, a user may connect to network 110 using client terminal 102 and then, request access to the verification server 106 using browser 202, for example, by typing in the URL corresponding to the verification server 106. Verification server 106 receives this access request and may display, for example, a welcome web page to the user (step 902).

[0114] Alternatively, a user may connect to network 110 using client terminal 102 and request access to another server (e.g., vendor server 108 or logon server 104). This other server may inform the user of the possibility of obtaining a payment credential from a verification authority and may prompt the user to select a link that points to verification server 106 if the user wants to obtain such a credential. Once the user selects that link, the user's browser may be redirected to verification server 106 by the other server. Verification server 106 may in turn display a welcome web page to the user (step 902).

[0115] The verification server 106 may then prompt the user to logon, receive logon information from the user, and authenticate the user (steps 904 and 906). Steps 904 and 906 are similar to steps 510 and 512 shown in FIG. 5 and thus, will not be further described.

[0116] After the user has authenticated, the verification server 106 may ask the user whether the user would like to send a payment credential to the logon server 104 (step 908). If the user does not want to send a payment credential to the logon server 104, then the process is complete (step 924).

[0117] If, however, the user does want to send a payment credential to logon server 104, the verification server 106 may send a payment credential to logon server 104 by redirecting the user's browser to the logon server 104 (step 910). The logon server 104 may prompt the user to logon (step 912). This authentication step (step 912) is similar to step 504 shown in FIG. 5 and will not be described further.

[0118] After the user has authenticated, the logon server 104 may prompt the user for an account number corresponding to the payment credential (step 914). For example, if the verification authority that issued this payment credential was a credit

card company and the payment credential included information about the credit card, then the account number may be the credit card number associated with the credit card. In one embodiment, instead of the account number, the logon server 104 may assign or prompt the user to select a first key (e.g., a password).

[0119] Next, logon server 104 may encrypt the payment credential received from verification server 106 using the account number or the first key and a second key (step 916). The second key may be assigned by logon server 104 or may be selected by the user, and may include, for example, a random number. The second key may be stored in the user's account and may be only accessed by logon server 104 after the user has successfully authenticated to it. Before encrypting the payment credential, the logon server 104 may verify that the account number provided by the user matches the account number on the payment credential.

[0120] Once the credential has been encrypted, logon server 104 may store the encrypted credential in the user's account in database 304 (step 918). Then, the logon server 104 may encrypt the account number previously provided by the user using a third key, and may set a cookie that includes the encrypted account number on client terminal 102 (step 920). This third key may be the same key that was used to encrypt the payment credential (i.e., the second key) or may be another key stored in the user's account. This third key, like the other keys, may be assigned by logons server 104 or may be selected by the user, and may include a random number. In one embodiment, the logon server 104 may not encrypt the account number that is included in the cookie.

[0121] After setting the cookie, the logon server 104 may redirect user's browser to verification server 106 if the user started this acquisition process at the verification server 106 (step 922). Alternatively, if the user started the acquisition process at the vendor server 108, the user may be redirected to the vendor server 108. Once the user has been redirected, the acquisition process is complete (step 924).

[0122] The user may perform the steps shown in FIG. 9 for each payment credential that the user wants stored on the logon server 104. For example, if the user has two credit card accounts and wants to obtain payment credentials for both

accounts, the user may complete the process shown in FIG. 9 for each credit card account.

[0123] Once the payment credentials have been stored on logon server 104, a user may use client terminal 102 to purchase a commodity or obtain access to a resource using the payment credentials. In one embodiment, the client terminal 102 may be the same client terminal 102 that the user used to acquire the payment credentials. FIG. 10 is a flow diagram of an exemplary method for using an acquired payment credential using a system consistent with the present invention.

[0124] Although not shown in FIG. 10, a user may connect to network 110 using client terminal 102 and then, request access to vendor server 108 using browser 202, for example, by typing in the URL corresponding to the vendor server 108. Vendor server 108 receives this access request and may display, for example, a welcome web page to the user (step 1002). The user may send a request to access a resource (e.g., a document) that the user wants to access or send a purchase request for a commodity that the user wants to purchase from the web page (step not shown in figure). The resource access request or purchase request may be generated, for example, by clicking on a region of the web page that is displayed to the user. The process of selecting resources and commodities will be known to those skilled in the art and is also within the scope of the present invention.

[0125] Vendor server 108 receives the request and processes this request (step 1004). During processing, the vendor server 108 may prompt the user for certain information, such as name, and address. The user may provide the requested information to the vendor server 108. If the user's request does not have an associated cost, vendor server 108 may process the request and the purchase process is complete (step 1020).

[0126] If, however, the user's request has any associated cost (e.g., cost to access a resource or the cost of the commodities that the user wants to purchase), the vendor server 108 may redirect the user's browser to logon server 104 and send a request for a payment credential to logon server 104 (steps 1006 and 1008).

[0127] The logon server 104 may in turn prompt the user to logon (step 1010). This authentication step is similar to step 504 and will not be described

further. Once the user has successfully authenticated, the logon server 104 may prepare a list of available payment credentials and may prompt the user to select one (step 1012).

[0128] To prepare the list of available payment credentials, logon server 104 may use the key (i.e., the third key), which was used to encrypt the account number included in the cookie stored on client terminal 102, to decrypt the account number. Once the account number has been decrypted, logon server 104 may use the account number or the first key and the second key, which were used to encrypt the payment credential, to decrypt the payment credential that is stored in the user's account. This decryption process may be performed for every payment credential that is stored in the user's account.

[0129] If the user is using a different client terminal than the one that was used to acquire the payment credential, then the user may be prompted to enter the account number or the first key so that the payment credential can be decrypted. Once the payment credential has been decrypted, the user may be given the option of setting a cookie with the encrypted account number on the client terminal 102 that the user is currently using.

[0130] From the list of payment credentials, the user may select one payment credential that the user wants to send to vendor server 108 (step not shown in figure). The logon server 104 may receive the user's selection (step 1014) and may send the payment credential to vendor server 108 by redirecting the user's browser to vendor server 108 (step 1016). In one embodiment, instead of sending the payment credential, the logon server 104 may create a message with the required information and send the message to the vendor server 108 by redirecting the user's browser to vendor server 108.

[0131] Vendor server 108 receives the payment credential and processes the user's request (step 1018). The purchase process is now complete (step 1020).

[0132] Although the processes in FIGs. 9 and 10 are shown to apply to payment credentials, one skilled in the art will understand that theses processes may be used to acquire and use other types of information, such as a verification.

[0133] Systems, methods, and articles of manufacture also facilitate in securing a user's information that may be stored on a central server, such as a preference server. FIG. 11 is a block diagram of an exemplary system 1100 that may be used to secure a user's information on a preference server. As shown, system 1100 may include one or more client terminals 102, logon server 104, preference server 1106, and one or more vendor servers 108, which are interconnected by a network 1110.

[0134] Client terminal 1102 may be a computer or a similar device that may receive requests from users, display information to users, and communicate with other computers, such as logon server 1104, preference server 1106, and vendor server 1108.

[0135] Logon server 1104 may be a computer or a similar device that may register users, authenticate users, and store information (e.g., name and address) about users in an account corresponding to the user.

[0136] Preference server 1106 may be a computer or a similar device that may store user information and may provide it to other entities upon request. User information may include information about the preferences of a user, such as preferred airline, preferred hotel, etc. Preference server 1106 may also encrypt the user information stored on it.

[0137] Vendor server 1108 may be a computer or a similar device that may offer resources and/or commodities to users.

[0138] Network 1110 may be a single or a combination of any type of computer network, such as a Local Area Network (LAN) or a Wide Area Network (WAN). For example, network 1110 may comprise an Ethernet network operating according to the IEEE 802.3 standard. In addition, network 1110 may be a combination of public (e.g., Internet) and private networks.

[0139] In one embodiment, client terminal 1102, logon server 1104, and vendor server 1108 may include some or all components of client terminal 102, logon server 104, and vendor server 108, respectively.

[0140] In accordance with an embodiment, a user wishing to use system 1100 may register with logon server 1104, for example, using the registration process

described with reference to FIG. 4. Similarly, a user may register with preference server 1106 by providing information about himself or herself to the preference server 1106.

[0141] In one embodiment, preference server 1106 may prompt the user for information by displaying a form in a browser executing at the user's client terminal. After the user has completed the form and attempts to submit it, for example, by selecting an icon or a button on the form, the browser may encrypt the user information in the form using a key provided by logon server 1104. Once encrypted, the data in the form is submitted to preference server 1106. The browser may use a plug-in or an in-page script to encrypt the information. Instead of an icon or a button within the form, the browser may also include a feature (e.g., a button or a menu item) that the user may select to the encrypt the information before the information is sent to preference server 1106.

[0142] The preference server 1106 may receive the encrypted information and store it, thus allowing the encryption algorithm and the key to remain anonymous from preference server 1106.

[0143] In another embodiment, preference server 1106 and not the browser may encrypt the information before storing it. In this embodiment, preference server 1106 may prompt the user for information, receive the information, and store it. Before storing the information, however, the preference server 1106 may encrypt the information using a key provided by logon server 1104.

[0144] The key used by the browser or preference server 1106 for encryption may be selected by the user or be assigned by logon server 1104, and may be stored in the user's account on the logon server 104. The key may include a random number.

[0145] In addition, during registration, preference server 1106 may provide identification data to user so that the user can use the identification data to log onto to the preference server 1106. This identification data may be stored on client terminal 1102 in a cookie.

[0146] If the user has registered with preference server 1106 before registering with logon server 1104, the user may register with the logon server 1104 and log onto the preference server 1106 using the identification data provided by the

preference server 1106. Then, the logon server may provide preference server 1106 with a key so that the user information stored on the preference sever 1106 can be encrypted. Alternatively, the user may retrieve the data from the preference server 1106 using the browser on user's client terminal, encrypt the data using the browser, as described above, and send it to preference server 1106.

[0147] Once the user has registered with logon server 1104 and preference server 1106 and once the user information stored on preference server 1106 has been encrypted, the user may provide the user information to others (e.g., vendors) using the logon server 1104 and preference server 1106. FIG. 12 is a flow diagram of an exemplary method for obtaining information from a preference server using a system consistent with the present invention.

[0148] Although not shown in FIG. 12, a user may connect to network 1110 using client terminal 1102 and then, request access to vendor server 1108 using a browser on the client terminal 1102, for example, by typing in the URL corresponding to the vendor server 1108. Vendor server 1108 receives this access request and may display, for example, a welcome web page to the user (step 1202). The user may send a request to access a resource (e.g., a document) that the user wants to access or send a purchase request for a commodity that the user wants to purchase from the web page (step not shown in figure). The resource access request or purchase request may be generated, for example, by clicking on a region of the web page that is displayed to the user. The process of selecting resources and commodities will be known to those skilled in the art and is also within the scope of the present invention.

[0149] Vendor server 1108 receives the request and processes this request (step 1204). During processing, the vendor server 1108 may require certain information about the user (e.g., name, address, and preferred airline information). The vendor server 1108 may prompt the user for such information or may request that information from preference server 1106. Alternatively, the vendor server 1108 may request some information from the user and obtain other information from preference server 1106. If the vendor server 1108 does not need any information from preference server 1106, then vendor server 1108 may complete the user's request and the process is complete (steps 1206 and 1226).

[0150] If, on the other hand, the vendor server 1108 does need some information about the user from preference server 1106, the vendor server 1108 may send a request for such information by redirecting the user's browser to preference server 1106 (steps 1206 and 1208).

[0151] In another embodiment, the user's browser on the client terminal 1102 and not the vendor server 1108 may redirect the user's browser to preference sever 1106. For example, when a user receives a request from vendor server 1108 for information, the user may select a feature (e.g., a button or a menu item) on the user's browser, which in turn, may redirect the user's browser to preference server 1106.

[0152] Preference server 1106 may in turn prompt the user for identification data (e.g., username and password) and may authenticate the user upon receiving the requested information (step 1210). Any known authentication methods may be used to authenticate the user to preference server 1106. In one embodiment, the identification data may be provided to preference server 1106 through a cookie stored on client terminal 1102.

[0153] Once the user has been authenticated, preference server 1106 may redirect user's browser to logon server 1104 and may send user's encrypted information to user's browser (step 1212). Logon server 1104 may in turn prompt user for identification data and authenticate the user upon receiving the requested data (step 1214). Step 1214 is similar to step 504 and is not further described.

[0154] After the user has authenticated, logon server 1104 may send the key, which is stored in the user's account and was used to encrypt user's information, to user's browser (step 1216). The user's browser in turn may decrypt the encrypted information using the encryption key (step 1218). The browser may use a plug-in or an in-page script to decrypt the information.

[0155] Once the information has been decrypted, the browser may prompt user to select the information that the user desires to send to vendor server 1108 (step 1220). For example, once decrypted, the information may be inserted into forms displayed in the browser and edited by the user before submitting them to vendor server 1108.

[0156] Once the user confirms, the browser may send the information to vendor server 1108 (step 1222). The vendor server 1108 may in turn receive the information and process the user's request (step 1224). The process of obtaining information from preference server 1106 is now complete (step 1226).

[0157] One skilled in the art will understand that various modifications can be made to the systems and methods disclosed in this application without departing from the scope of the invention. For example, the system shown in FIG. 1 and FIG. 11 may be combined to create a system, such as the system shown in FIG. 13, that provides payment credentials as well as user information to vendors.

[0158] The above-noted features, other aspects, and principles of the present invention may be implemented in various system or network configurations to provide automated and computational tools for providing security and verification services in an online network. Such configurations and applications may be specially constructed for performing the various processes and operations of the invention or they may include a general purpose computer or computing platform selectively activated or reconfigured by program code to provide the necessary functionality. The processes disclosed herein are not inherently related to any particular computer or other apparatus, and may be implemented by a suitable combination of hardware, software, and/or firmware. For example, various general purpose machines may be used with programs written in accordance with teachings of the invention, or it may be more convenient to construct a specialized apparatus or system to perform the required methods and techniques.

[0159] The present invention also relates to computer readable media that include program instruction or program code for performing various computer-implemented operations based on the methods and processes of the invention. The media and program instructions may be those specially designed and constructed for the purposes of the invention, or they may be of the kind well-known and available to those having skill in the computer software arts. The media may take many forms including, but not limited to, non-volatile media, volatile media, and transmission media. Non-volatile media includes, for example, optical or magnetic disks. Volatile media includes, for example, dynamic memory. Transmission media includes, for

example, coaxial cables, copper wire, and fiber optics. Transmission media can also take the form of acoustic or light waves, such as those generated during radio-wave and infra-red data communications. Examples of program instructions include both machine code, such as produced by compiler, and files containing a high level code that can be executed by the computer using an interpreter.

[0160] It will be apparent to those skilled in the art that various modifications and variations can be made in the system and method of the present invention and in construction of this invention without departing from the scope or spirit of the invention. For example, the logon server 104 may verify the information independently and thus, a verification authority may not be needed. In this example, the logon server could send, for example, a representative to the user's home and obtain the information from the user. Another variation could be that the verification authority sends periodic updates to the information stored in the logon server 104.

[0161] Moreover, other embodiments of the invention will be apparent to those skilled in the art from consideration of the specification and practice of the invention disclosed herein. It is intended that the specification and examples be considered as exemplary only, with a true scope and spirit of the invention being indicated by the following claims.

WHAT IS CLAIMED IS:

1. A method for verifying user information, comprising:

establishing an account in a database for a user;

receiving, from a requestor, a verification request for verification of user information; and

sending, to the requestor, a response to the verification request.

2. The method of claim 1, wherein establishing an account in a database for a user comprises:

requesting, from a verification authority, a verification, the verification including user information;

receiving, from the verification authority, the verification;

storing the verification in the account.

3. The method of claim 2, wherein sending, to the requestor, a response to the verification request comprises sending a response including the verification.

4. The method of claim 2, wherein receiving, from the verification authority, the verification comprises receiving, from the verification authority, a digital certificate, the digital certificate including user information.

5. The method of claim 4, wherein sending, to the requestor, a response to the verification request comprises sending, to the requestor, the digital certificate.

6. The method of claim 2, wherein receiving, from the verification authority, the verification comprises receiving, from the verification authority, a message, the message including user information.

7. The method of claim 6, wherein sending, to the requestor, a response to the verification request comprises sending, to the requestor, the message.

8. The method of claim 1, wherein receiving, from a requestor, a verification request comprises receiving, by a verification authority, the verification request.

9. The method of claim 8, wherein sending, to the requestor, a response to the verification request comprises sending, by the verification authority to the requestor, a digital certificate, the digital certificate including user information.

10. The method of claim 8, wherein sending, to the requestor, a response to the verification request comprises sending, by the verification authority to the requestor, a message, the message including user information.

11. A method for providing a payment credential to a requestor, comprising:

establishing an account in a database for a user;

receiving, from a requestor, a payment credential request for a user; and

sending, to the requestor, a response to the payment credential request.

12. The method of claim 11, wherein establishing an account in a database for a user comprises:

requesting, from a verification authority, a payment credential, the payment credential including financial information for an account corresponding to the user;

receiving, from the verification authority, the payment credential;

storing the payment credential in the account.

13. The method of claim 12, wherein storing the payment credential in the account comprises:

encrypting the payment credential with a first key and a second key, the first key being stored in the account;

storing the encrypted credential in the account.

14. The method of claim 13, further comprising setting a cookie at a client terminal of the user, the cookie including the second key.

15. The method of claim 14, wherein setting a cookie at a client terminal comprises:

encrypting the second key with a third key; and

storing the encrypted second key in the cookie.

16. The method of claim 15, wherein sending, to the requestor, a response to the payment credential request comprises:

decrypting the second key in the cookie with the third key;

decrypting the payment credential using the first key and the second decrypted key; and

sending, to the requestor, the payment credential.

17. A method for providing user information in a system including a logon server, a preference server, and a client terminal, the method comprising:

establishing, at the logon server, a first account for a user;

establishing, at the preference server, a second for the user;

obtaining user information;

encrypting the user information using a key stored in the first account;

storing the encrypted user information in the second account;

receiving, at a browser of the client terminal from a requestor, a request for the user information; and

sending, to the requestor, the requested user information.

18. The method of claim 17, wherein sending, to the requestor, the requested user information comprises:

sending, by the preference server, the encrypted user information to the browser of the client terminal;

sending, by the logon server, the key to the browser;

decrypting, at the browser, the user information using the key; and

sending, by the browser to the requestor, the decrypted user information.

19. The method of claim 18, wherein decrypting, at the browser, the user information using the key comprises decrypting the user information using a browser plug-in or an in-page script.

20. The method of claim 17, wherein encrypting the user information using a key stored in the first account comprises encrypting, by the browser, the user information.

21. The method of claim 20, wherein encrypting, by the browser, the user information comprises encrypting the user information using a browser plug-in or an in-page script.

22. A method for purchasing a commodity in an online network, comprising:

selecting the commodity on a vendor web site by a user;

sending, to a logon server, a purchase amount corresponding to the commodity;

authenticating the user at the logon server;

sending, to a verification server, the purchase amount and an identifier for the user;

charging, at the verification server, the purchase amount to an account corresponding to the user; and

sending, to the vendor web site, a payment confirmation.

23. The method of claim 22, wherein sending, to the vendor web site, a payment conformation comprises:

sending, to the logon server, a payment confirmation; and

sending, by the logon server to the vendor web site, the payment confirmation.

24. A computer-readable medium containing instructions for causing a computer to perform a method for verifying user information, the method comprising:

establishing an account in a database for a user;

receiving, from a requestor, a verification request for verification of user information; and

sending, to the requestor, a response to the verification request.

25. The computer-readable medium of claim 24, wherein establishing an account in a database for a user comprises:

requesting, from a verification authority, a verification, the verification including user information;

receiving, from the verification authority, the verification;

storing the verification in the account.

26. The computer-readable medium of claim 25, wherein sending, to the requestor, a response to the verification request comprises sending a response including the verification.

27. The computer-readable medium of claim 25, wherein receiving, from the verification authority, the verification comprises receiving, from the verification authority, a digital certificate, the digital certificate including user information.

28. The computer-readable medium of claim 27, wherein sending, to the requestor, a response to the verification request comprises sending, to the requestor, the digital certificate.

29. The computer-readable medium of claim 25, wherein receiving, from the verification authority, the verification comprises receiving, from the verification authority, a message, the message including user information.

30. The computer-readable medium of claim 29, wherein sending, to the requestor, a response to the verification request comprises sending, to the requestor, the message.

31. The computer-readable medium of claim 24, wherein receiving, from a requestor, a verification request comprises receiving, by a verification authority, the verification request.

32. The computer-readable medium of claim 31, wherein sending, to the requestor, a response to the verification request comprises sending, by the verification authority to the requestor, a digital certificate, the digital certificate including user information.

33. The computer-readable medium of claim 31, wherein sending, to the requestor, a response to the verification request comprises sending, by the verification authority to the requestor, a message, the message including user information.

34. A computer-readable medium containing instructions for causing a computer to perform a method for providing a payment credential to a requestor, the method comprising:

establishing an account in a database for a user;

receiving, from a requestor, a payment credential request for a user; and

sending, to the requestor, a response to the payment credential request.

35. The computer-readable medium of claim 34, wherein establishing an account in a database for a user comprises:

requesting, from a verification authority, a payment credential, the payment credential including financial information for an account corresponding to the user;

receiving, from the verification authority, the payment credential;

storing the payment credential in the account.

36. The computer-readable medium of claim 35, wherein storing the payment credential in the account comprises:

encrypting the payment credential with a first key and a second key, the first key being stored in the account; and

storing the encrypted credential in the account.

37. The computer-readable medium of claim 36, wherein the method further comprises setting a cookie at a client terminal of the user, the cookie including the second key.

38. The computer-readable medium of claim 37, wherein setting a cookie at a client terminal comprises:

encrypting the second key with a third key; and

storing the encrypted second key in the cookie.

39. The computer-readable medium of claim 38, wherein sending, to the requestor, a response to the payment credential request comprises:

decrypting the second key in the cookie with the third key;

decrypting the payment credential using the first key and the second decrypted key; and

sending, to the requestor, the payment credential.

40. A computer-readable medium containing instructions for causing a computer to perform a method for providing user information in a system including a logon server, a preference server, and a client terminal, the method comprising:

establishing, at the logon server, a first account for a user;

establishing, at the preference server, a second account for the user;

obtaining user information;

encrypting the user information using a key stored in the first account;

storing the encrypted user information in the second account;

receiving, at a browser of the client terminal from a requestor, a request for the user information; and

sending, to the requestor, the requested user information.

41. The computer-readable medium of claim 40, wherein sending, to the requestor, the requested user information comprises:

sending, by the preference server, the encrypted user information to the browser of the client terminal;

sending, by the logon server, the key to the browser;

decrypting, at the browser, the user information using the key; and

sending, by the browser to the requestor, the decrypted user information.

42. The computer-readable medium of claim 41, wherein decrypting, at the browser, the user information using the key comprises decrypting the user information using a browser plug-in or an in-page script.

43. The computer-readable medium of claim 40, wherein encrypting the user information using a key stored in the first account comprises encrypting, by the browser, the user information

44. The computer-readable medium of claim 43, wherein encrypting, by the browser, the user information comprises encrypting the user information using a browser plug-in or an in-page script.

45. A computer-readable medium containing instructions for causing a computer to perform a method for purchasing a commodity in an online network, the method comprising:

selecting the commodity on a vendor web site by a user;

sending, to a logon server, a purchase amount corresponding to the commodity;

authenticating the user at the logon server;

sending, to a verification server, the purchase amount and an identifier for the user;

charging, at the verification server, the purchase amount to an account corresponding to the user; and

sending, to the vendor web site, a payment confirmation.

46. The computer-readable medium of claim 45, wherein sending, to the vendor web site, a payment conformation comprises:

sending, to the logon server, a payment confirmation; and

sending, by the logon server to the vendor web site, the payment confirmation.

47. A system for verifying user information, comprising:

a logon server including at least one user account;

a verification server, connected to the logon server, for verifying user information; and

a vendor server, connected to the logon server and the verification server, for verifying user information.

48. The system of claim 47, wherein the at least one user account includes a verification of the user information received from the verification server.

49. The system of claim 48, wherein the verification comprises one of a digital certificate including user information and a message that includes user information.

50. The system of claim 48, wherein the logon server includes means for sending the verification from the logon server to the vendor server in response to a request for verification of user information.

51. The system of claim 47, wherein the verification server includes means for sending a verification to the vendor server in response to a request for verification of user information.

52. A system for providing a payment credential to a requestor, comprising:

a logon server with at least one user account, the user account including an encrypted payment credential;

a verification server, connected to the logon server, for sending the payment credential to the logon server; and

a vendor server for requesting the payment credential from the logon server.

53. The system of claim 52, further comprising a client terminal with a browser.

54. The system of claim 53, wherein the browser includes means for encrypting the payment credential using a first key and a second key, the first key being stored in the account.

55. The system of claim 54, wherein the second key is encrypted with a third key and stored in a cookie on the client terminal.

56. The system of claim 55, wherein the third key is the same as the second key.

57. The system of claim 55, wherein the first, second, and third keys comprise one of a random number, a unique identifier assigned by the logon server, and a personal identifier selected by a user.

58. The system of claim 54, wherein the first key comprises an account number corresponding to the payment credential.

59. A system for providing user information, comprising:

a logon server with at least one user account, the user account including a key;

a preference server with at least one user account, the user account including user information that has been encrypted using the key; and

a vendor server for requesting the encrypted user information.

60. The system of claim 59, further comprising a client terminal with a browser for encrypting the user information with the key.

61. The system of clam 60, wherein the key comprises a random number, a unique identifier assigned by the logon server, or a personal identifier selected by the user.

62. A system for purchasing a commodity in an online network, comprising:

a logon server with at least one user account, the user account including information about a financial account of a user;

a vendor server for sending a purchase request to the logon server, the purchase request including a purchase amount and being generated in response to a request by the user; and

a verification server, connected to the logon server, for processing the purchase request.

63. The system of claim 62, wherein the verification server includes means for sending a payment confirmation to the vendor server, the payment confirmation including a confirmation that the purchase amount has been changed to the financial account of the user.

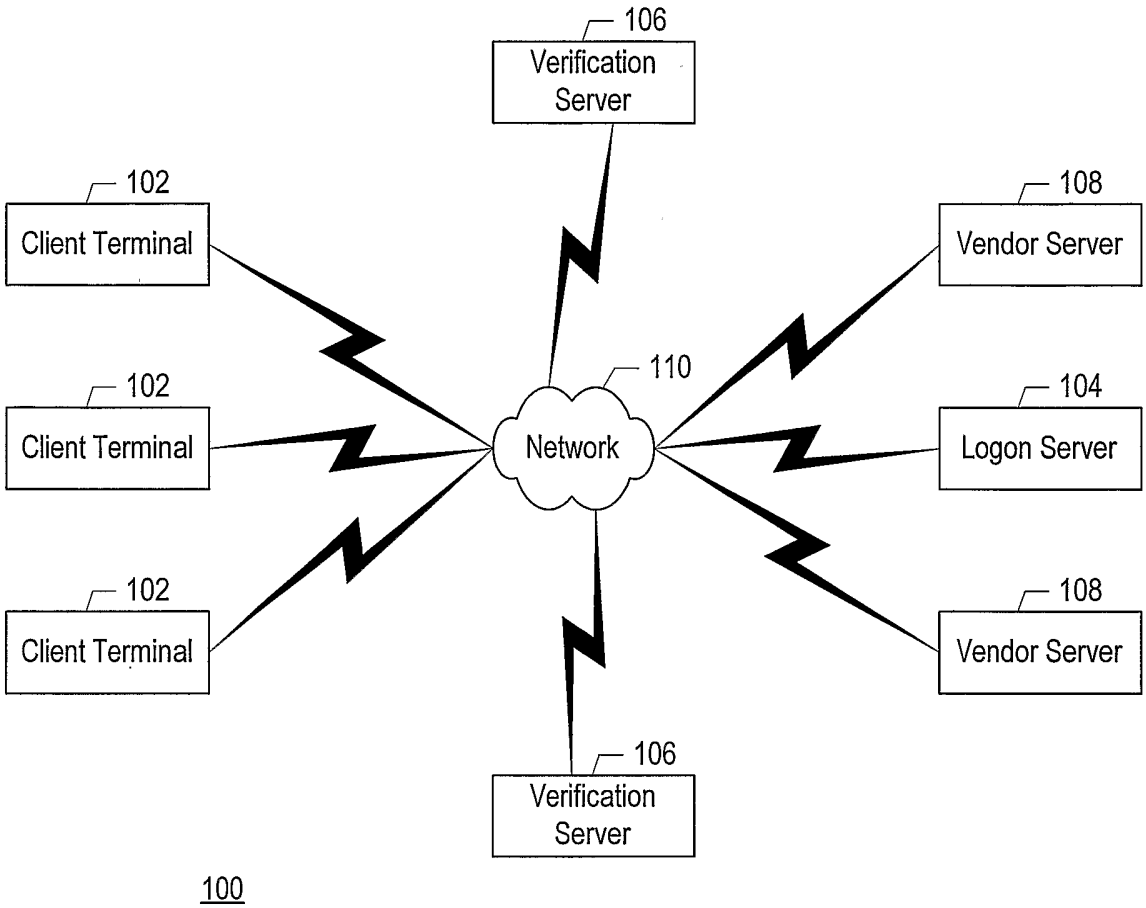

106
Verification Server
102
Client Terminal
108
Vendor Server
110
102
Client Terminal
Network
104
Logon Server
102
Client Terminal
108
Vendor Server
106
Verification Server
100

FIG. 1

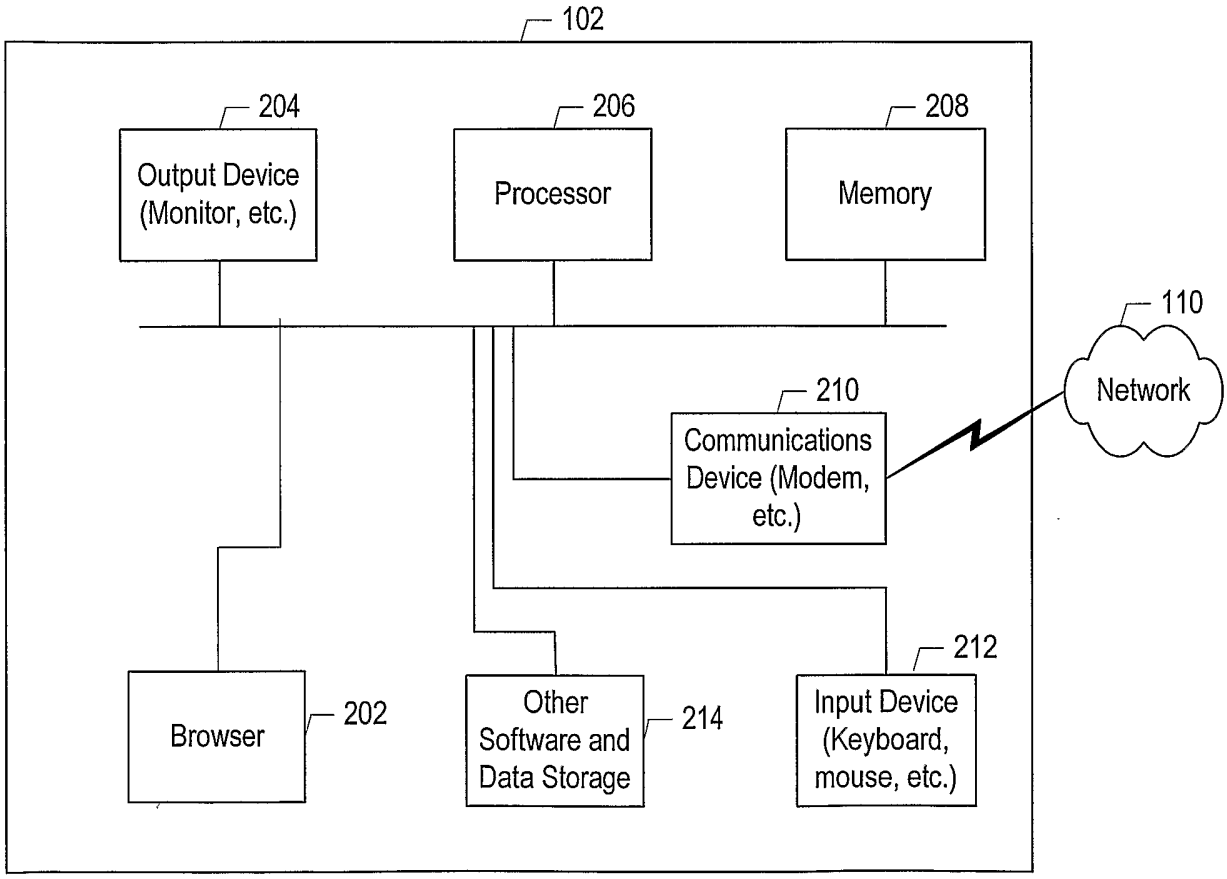

102
204
Output Device (Monitor, etc.)
206
Processor
208
Memory
110
Network
210
Communications Device (Modem, etc.)
212
Input Device (Keyboard, mouse, etc.)
Browser
202
Other Software and Data Storage
214

FIG. 2

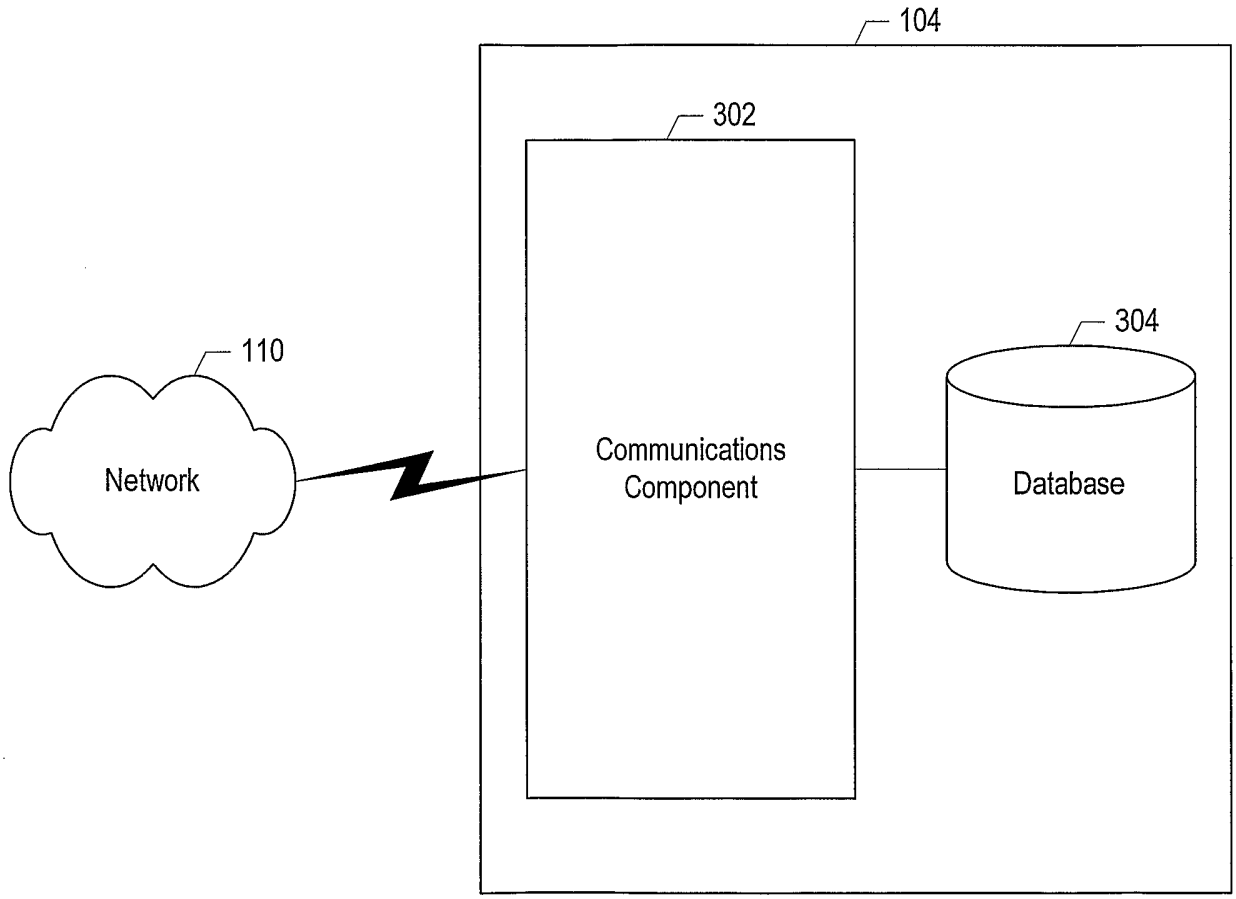

104
302
304
110
Network
Communications Component
Database

FIG. 3

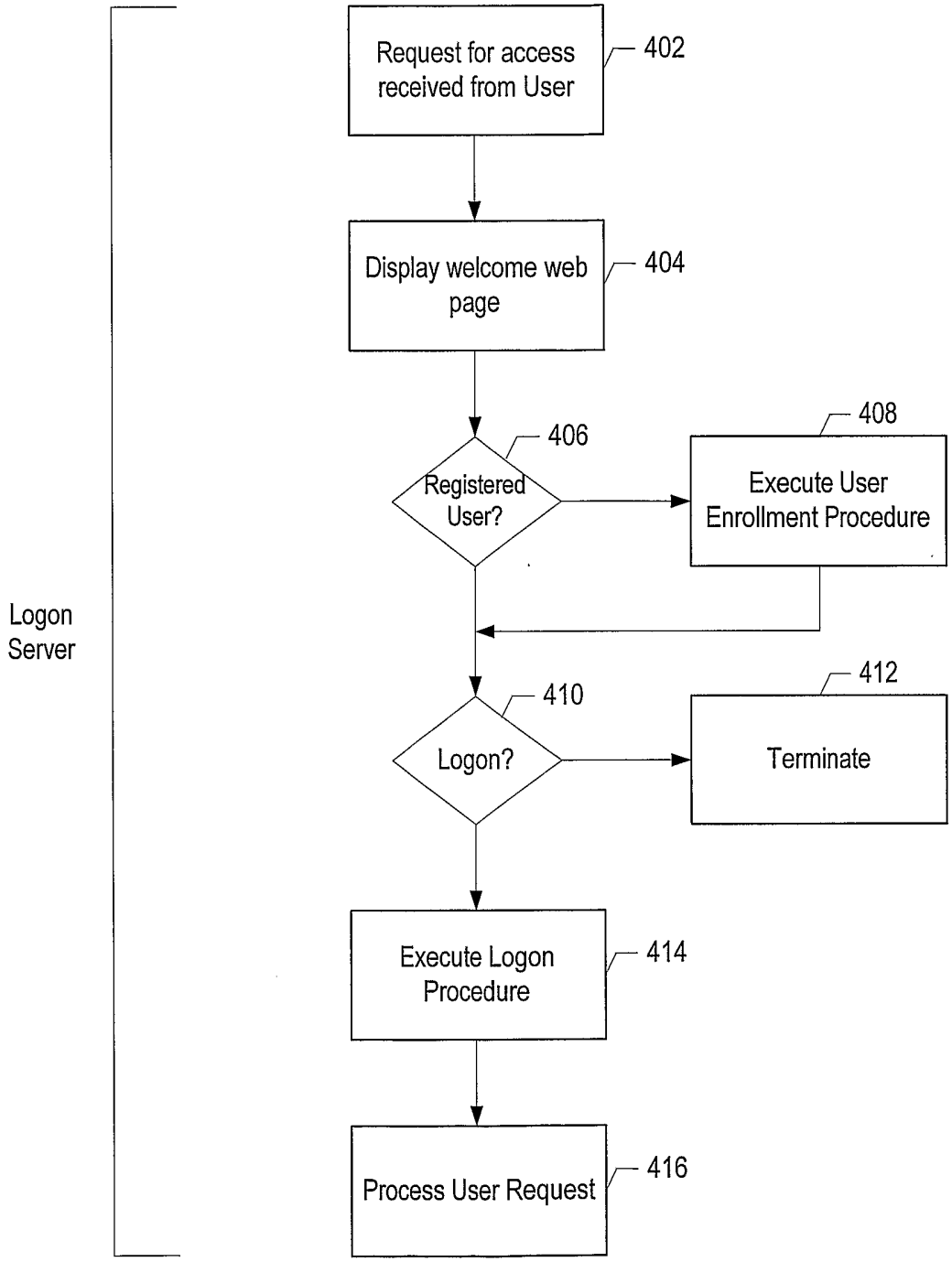

Logon Server
Request for access received from User
402
Display welcome web page
404
406
Registered User?
408
Execute User Enrollment Procedure
410
Logon?
412
Terminate
Execute Logon Procedure
414
Process User Request
416

FIG. 4

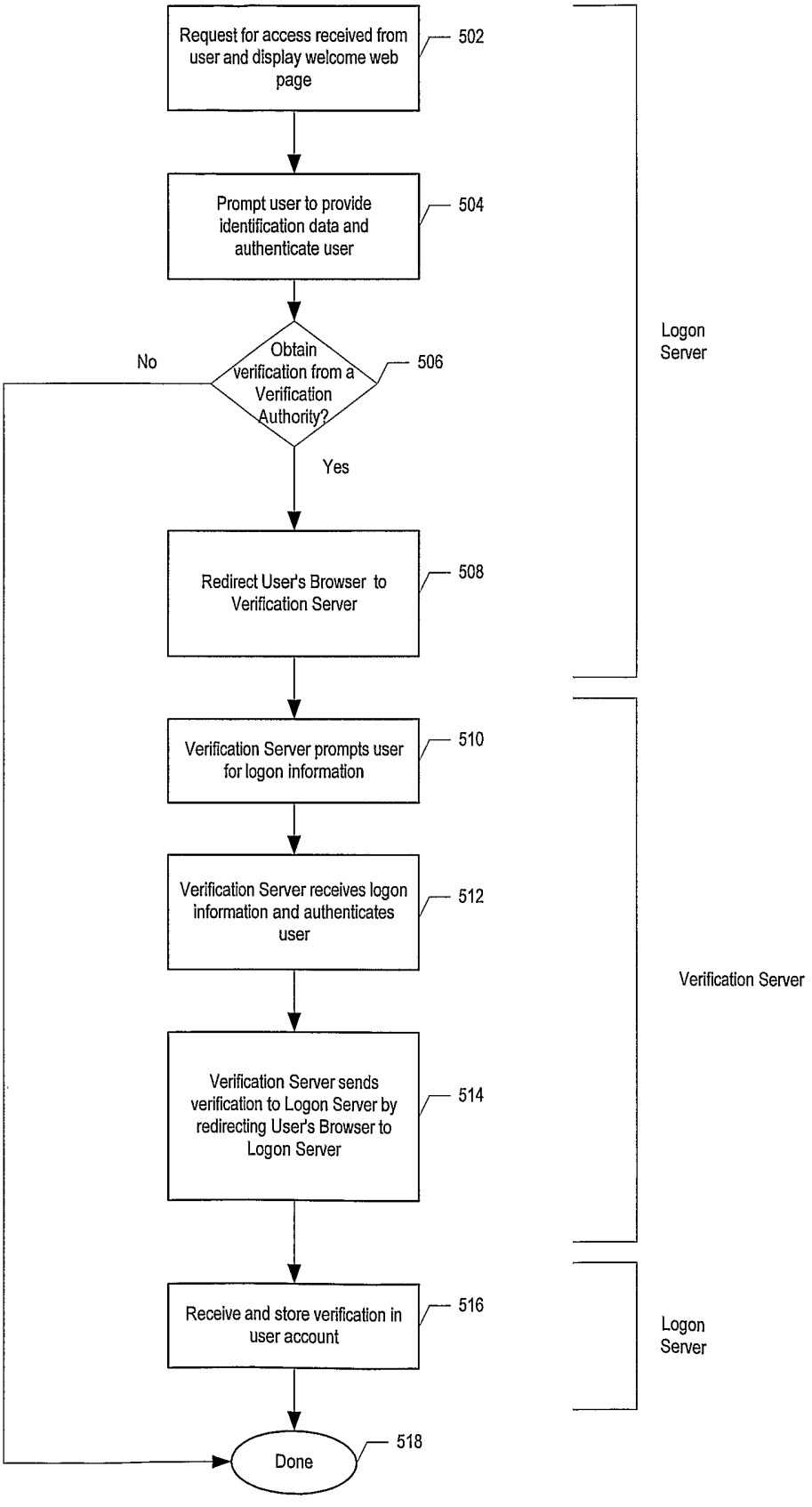

Request for access received from user and display welcome web page
502
Prompt user to provide identification data and authenticate user
504
Obtain verification from a Verification Authority?
506
No
Yes
Redirect User's Browser to Verification Server
508
Verification Server prompts user for logon information
510
Verification Server receives logon information and authenticates user
512
Verification Server sends verification to Logon Server by redirecting User's Browser to Logon Server
514
Receive and store verification in user account
516
Done
518
Logon Server
Verification Server
Logon Server

FIG. 5

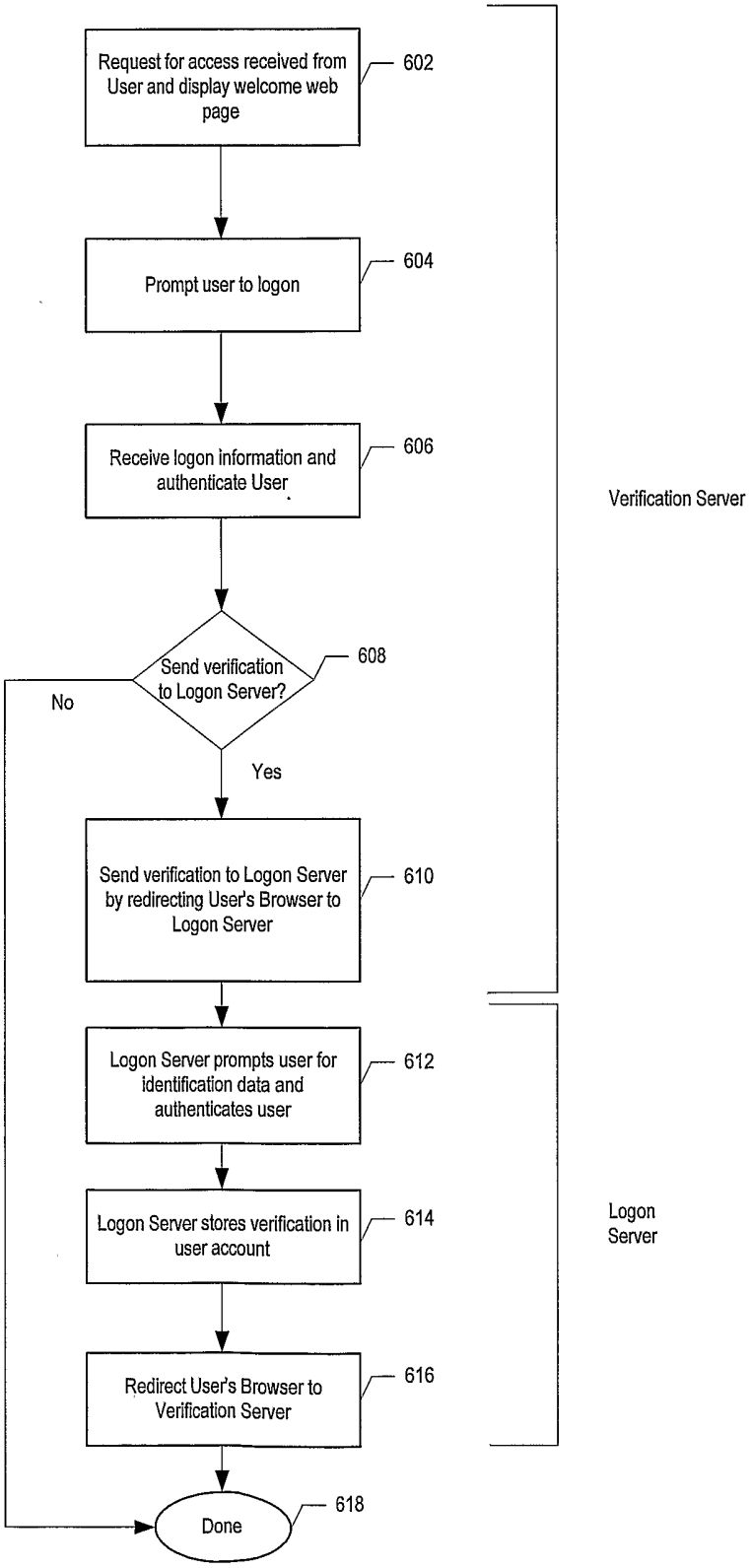

Request for access received from User and display welcome web page
602
Prompt user to logon
604
Receive logon information and authenticate User
606
Verification Server
Send verification to Logon Server?
608
No
Yes
Send verification to Logon Server by redirecting User's Browser to Logon Server
610
Logon Server prompts user for identification data and authenticates user
612
Logon Server stores verification in user account
614
Logon Server
Redirect User's Browser to Verification Server
616
Done
618

FIG. 6

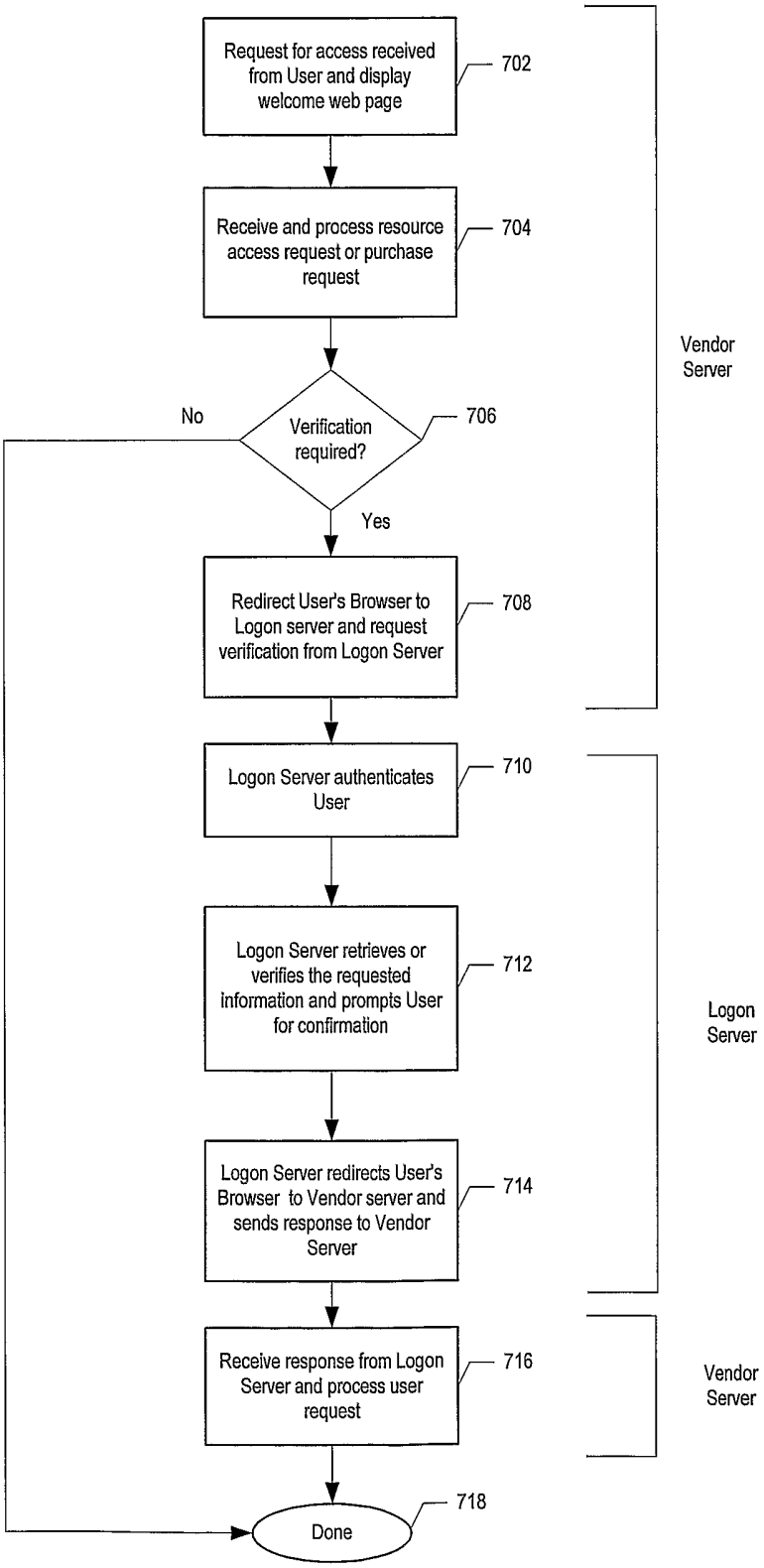

Request for access received from User and display welcome web page
702
Receive and process resource access request or purchase request
704
Verification required?
706
No
Yes
Redirect User's Browser to Logon server and request verification from Logon Server
708
Vendor Server
Logon Server authenticates User
710
Logon Server retrieves or verifies the requested information and prompts User for confirmation
712
Logon Server redirects User's Browser to Vendor server and sends response to Vendor Server
714
Logon Server
Receive response from Logon Server and process user request
716
Vendor Server
Done
718

FIG. 7

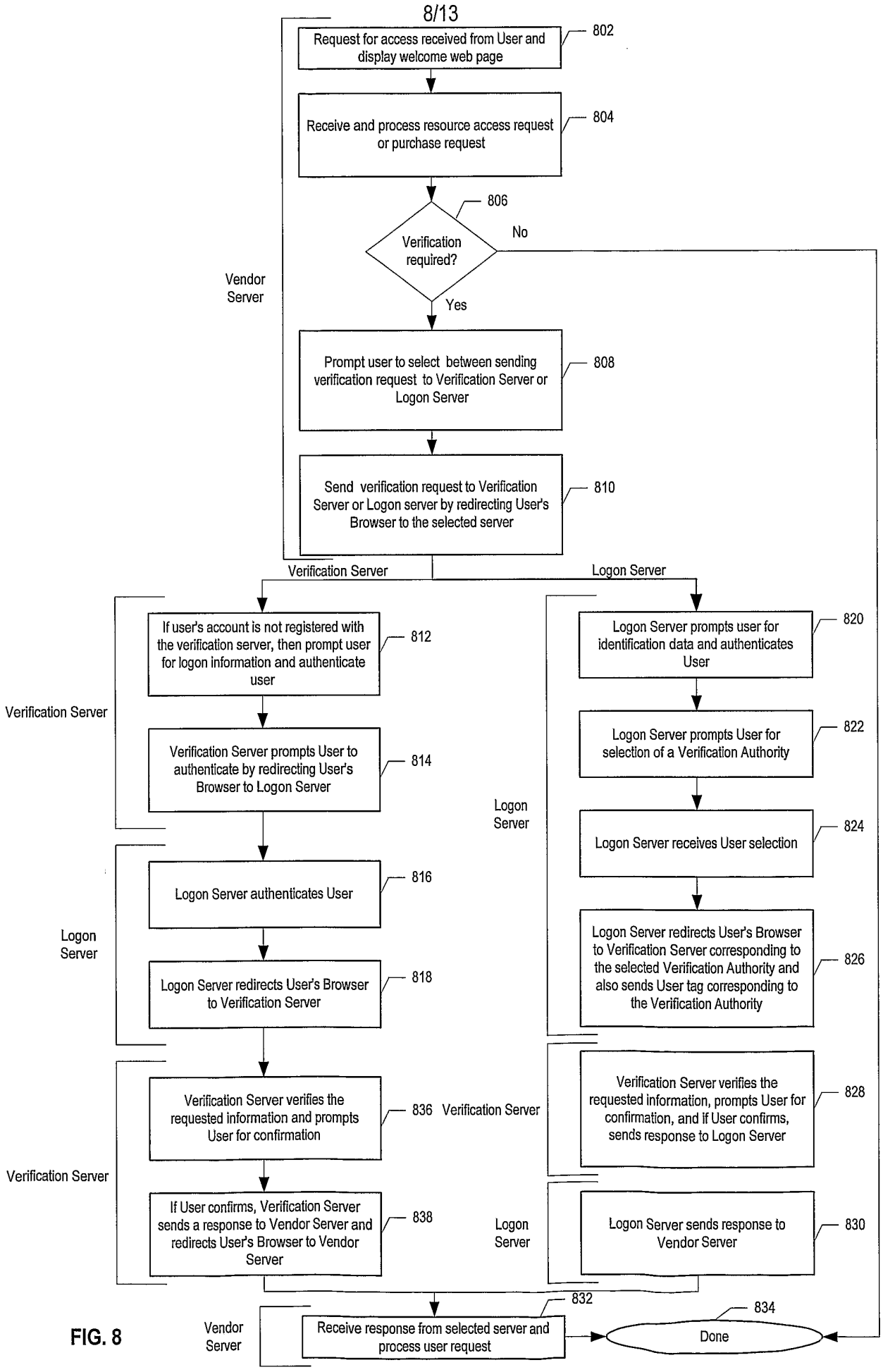

Request for access received from User and display welcome web page
802
Receive and process resource access request or purchase request
804
Verification required?
806
No
Yes
Vendor Server
Prompt user to select between sending verification request to Verification Server or Logon Server
808
Send verification request to Verification Server or Logon server by redirecting User's Browser to the selected server
810
Verification Server
Logon Server
If user's account is not registered with the verification server, then prompt user for logon information and authenticate user
812
Verification Server
Verification Server prompts User to authenticate by redirecting User's Browser to Logon Server
814
Logon Server authenticates User
816
Logon Server
Logon Server redirects User's Browser to Verification Server
818
Verification Server verifies the requested information and prompts User for confirmation
836
Verification Server
If User confirms, Verification Server sends a response to Vendor Server and redirects User's Browser to Vendor Server
838
Verification Server
Logon Server prompts user for identification data and authenticates User
820
Logon Server prompts User for selection of a Verification Authority
822
Logon Server
Logon Server receives User selection
824
Logon Server redirects User's Browser to Verification Server corresponding to the selected Verification Authority and also sends User tag corresponding to the Verification Authority
826
Verification Server verifies the requested information, prompts User for confirmation, and if User confirms, sends response to Logon Server
828
Logon Server
Logon Server sends response to Vendor Server
830
Receive response from selected server and process user request
832
Vendor Server
Done
834

FIG. 8

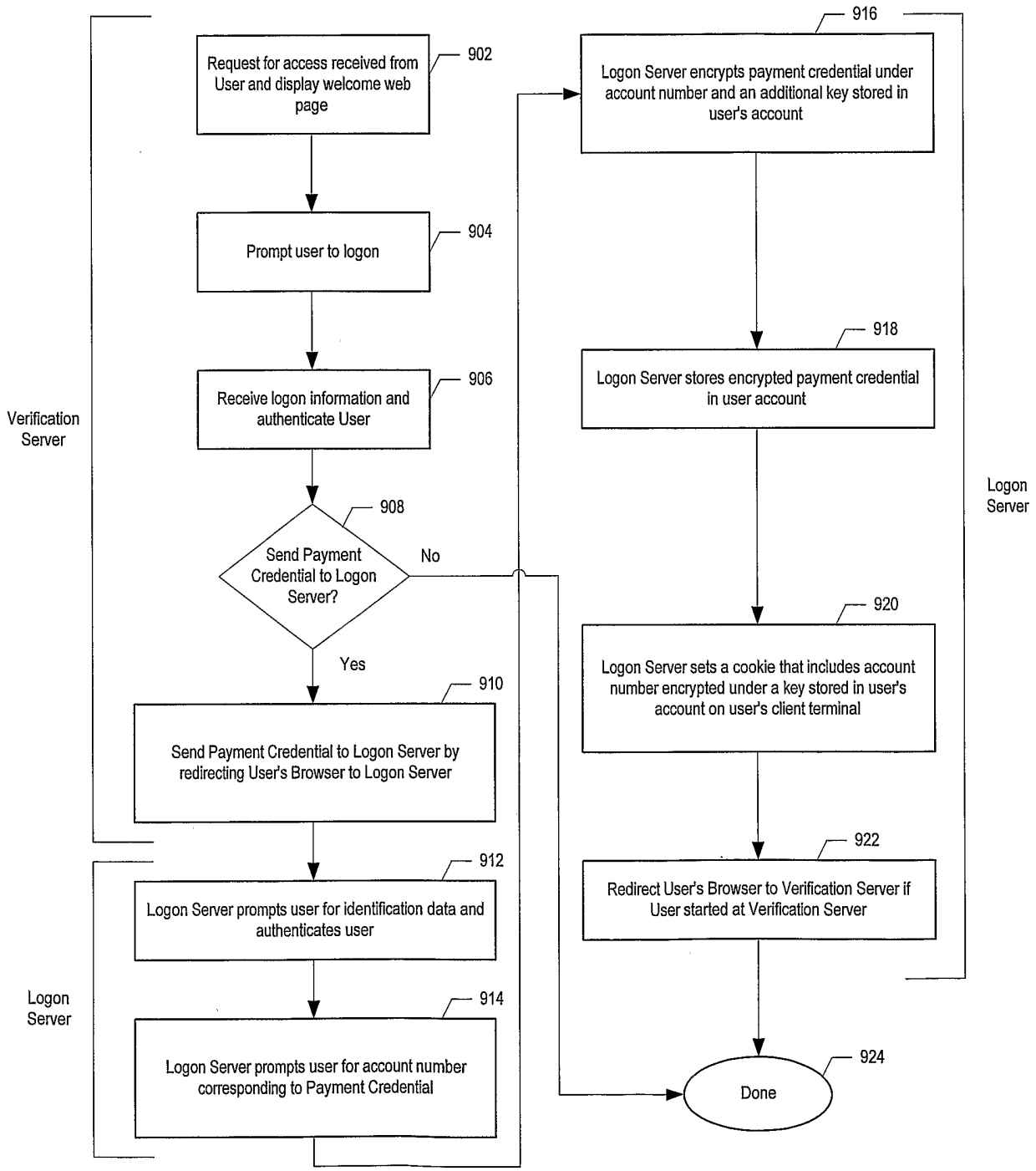

Verification Server
Logon Server
Logon Server
Request for access received from User and display welcome web page
902
Prompt user to logon
904
Receive logon information and authenticate User
906
Send Payment Credential to Logon Server?
908
No
Yes
Send Payment Credential to Logon Server by redirecting User's Browser to Logon Server
910
Logon Server prompts user for identification data and authenticates user
912
Logon Server prompts user for account number corresponding to Payment Credential
914
Logon Server encrypts payment credential under account number and an additional key stored in user's account
916
Logon Server stores encrypted payment credential in user account
918
Logon Server sets a cookie that includes account number encrypted under a key stored in user's account on user's client terminal
920
Redirect User's Browser to Verification Server if User started at Verification Server
922
Done
924

FIG. 9

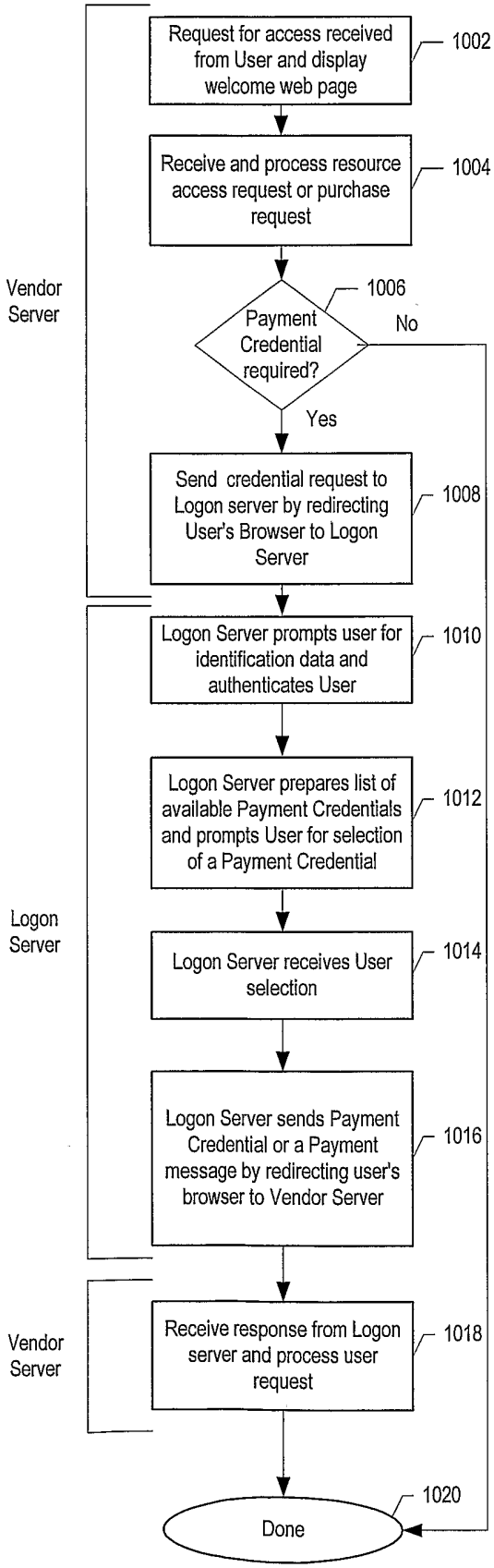

Request for access received from User and display welcome web page
1002
Receive and process resource access request or purchase request
1004
Vendor Server
Payment Credential required?
1006
No
Yes
Send credential request to Logon server by redirecting User's Browser to Logon Server
1008
Logon Server prompts user for identification data and authenticates User
1010
Logon Server prepares list of available Payment Credentials and prompts User for selection of a Payment Credential
1012
Logon Server
Logon Server receives User selection
1014
Logon Server sends Payment Credential or a Payment message by redirecting user's browser to Vendor Server
1016
Vendor Server
Receive response from Logon server and process user request
1018
Done
1020

FIG. 10

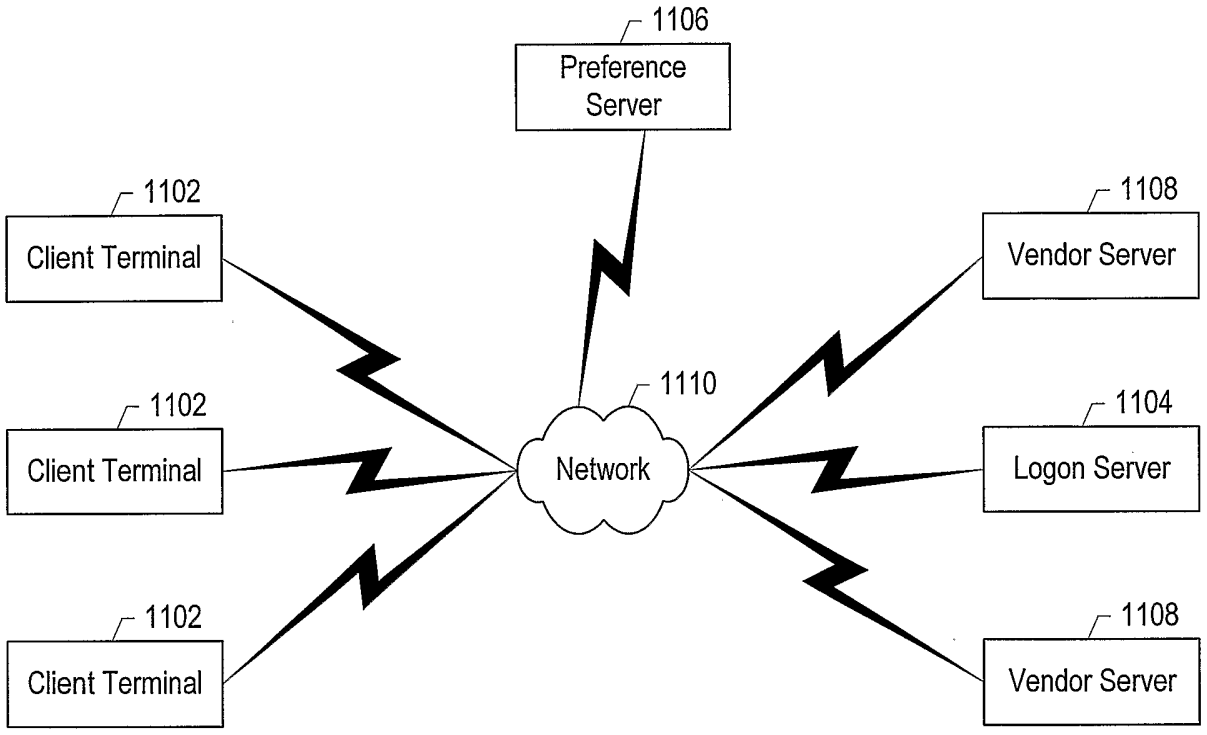

1106
Preference Server
1102
Client Terminal
1102
Client Terminal
1102
Client Terminal
1110
Network
1108
Vendor Server
1104
Logon Server
1108
Vendor Server
1100

FIG. 11

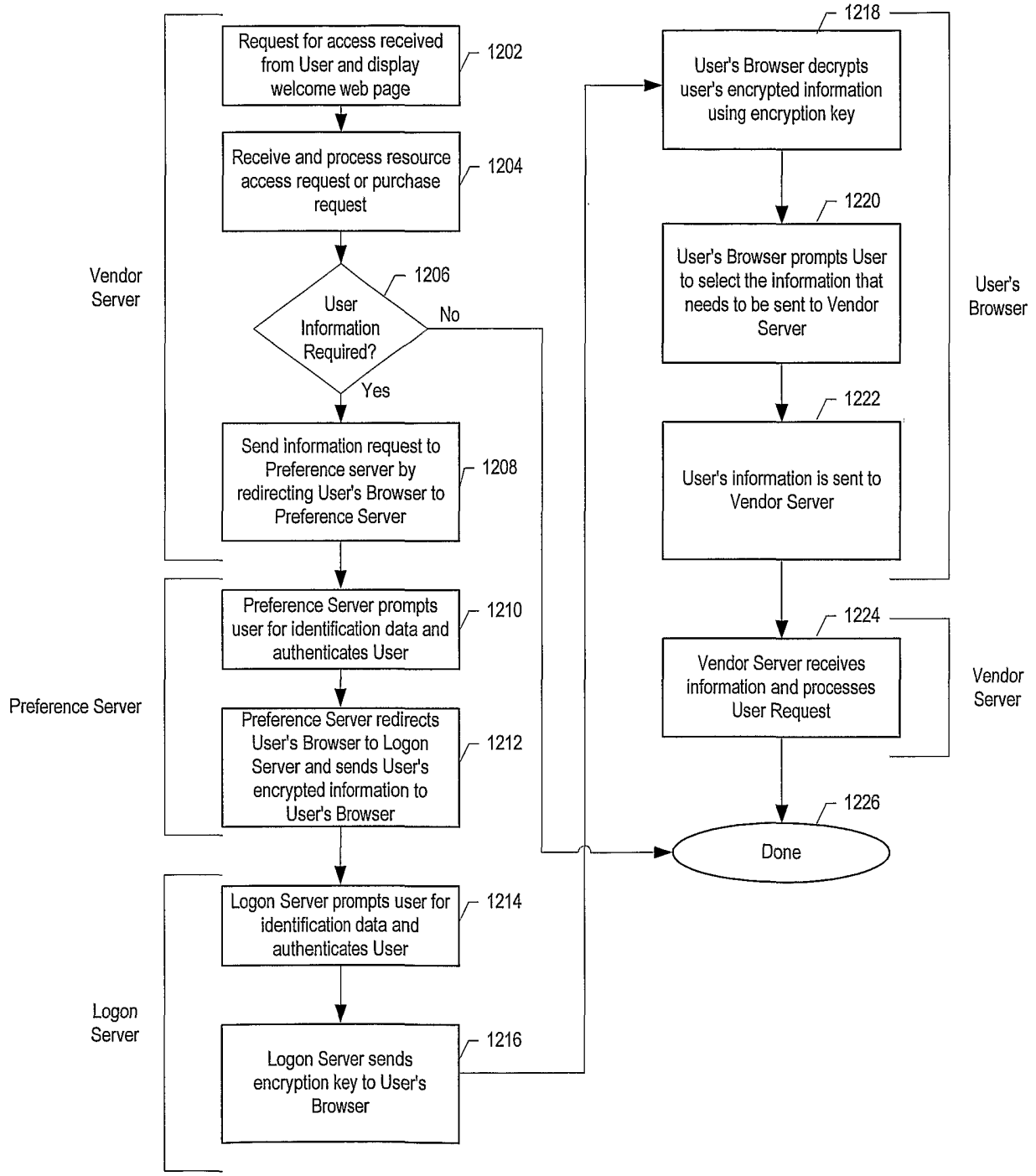

Vendor Server
Request for access received from User and display welcome web page
1202
Receive and process resource access request or purchase request
1204
User Information Required?
1206
No
Yes
Send information request to Preference server by redirecting User's Browser to Preference Server
1208
Preference Server
Preference Server prompts user for identification data and authenticates User
1210
Preference Server redirects User's Browser to Logon Server and sends User's encrypted information to User's Browser
1212
Logon Server
Logon Server prompts user for identification data and authenticates User
1214
Logon Server sends encryption key to User's Browser
1216
User's Browser
User's Browser decrypts user's encrypted information using encryption key
1218
User's Browser prompts User to select the information that needs to be sent to Vendor Server
1220
User's information is sent to Vendor Server
1222
Vendor Server
Vendor Server receives information and processes User Request
1224
Done
1226

FIG. 12

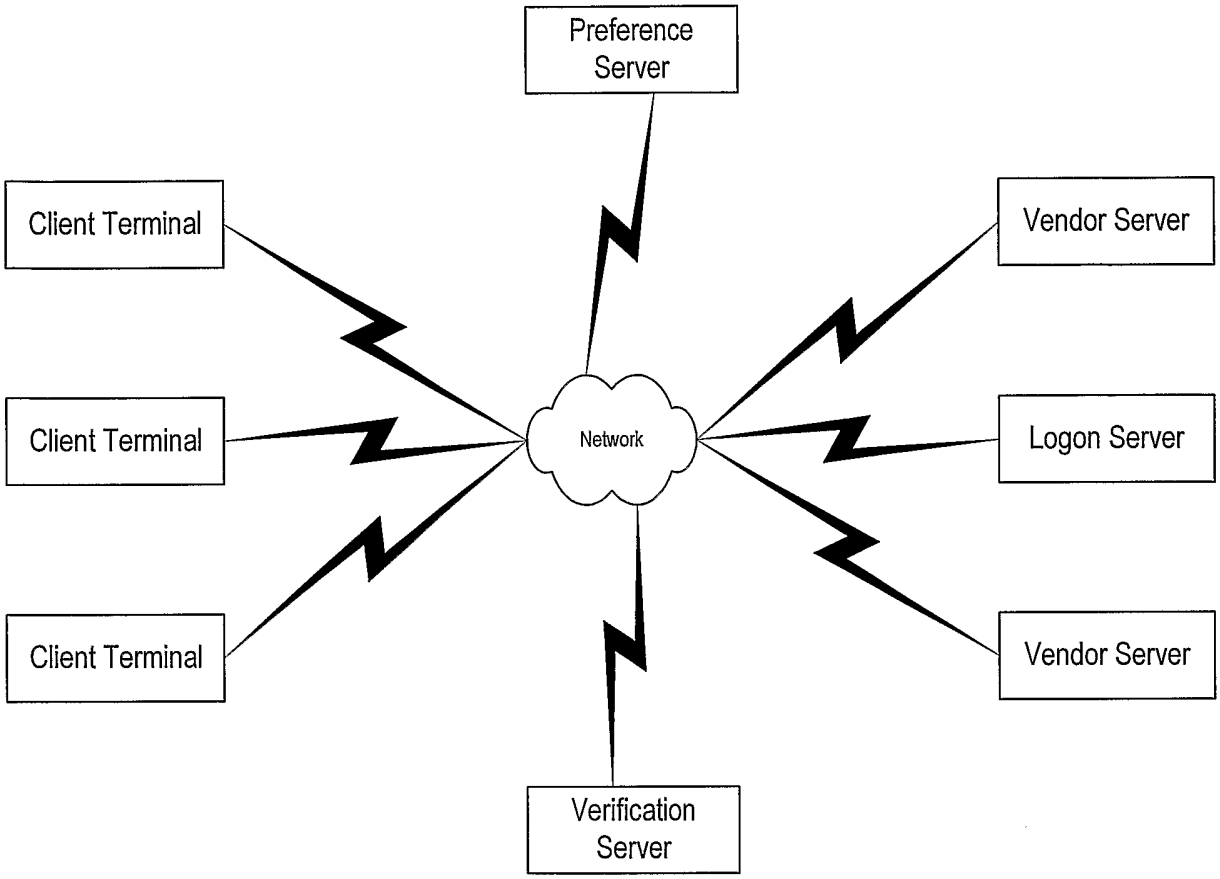

Preference Server
Client Terminal
Client Terminal
Client Terminal
Network
Vendor Server
Logon Server
Vendor Server
Verification Server

FIG. 13