



- (51) **International Patent Classification:**
H04W 8/20 (2009.01) H04W 4/12 (2009.01)
- (21) **International Application Number:**
PCT/US20 12/069870
- (22) **International Filing Date:**
14 December 2012 (14.12.2012)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
61/570,680 14 December 2011 (14.12.2011) US
- (71) **Applicant:** VISA INTERNATIONAL SERVICE ASSOCIATION [US/US]; P.O. Box 8999, M1-12SE, San Francisco, California 94128 (US).
- (72) **Inventor:** CARLSON, Mark; 153 Miramontes Avenue, Half Moon Bay, California 94109 (US).
- (74) **Agents:** JOHNS, Athena C. et al; Kilpatrick Townsend & Stockton LLP, Two Embarcadero Center, 8th Floor, San Francisco, CA 94111 (US).
- (81) **Designated States** (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) **Designated States** (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK,

[Continued on nextpage]

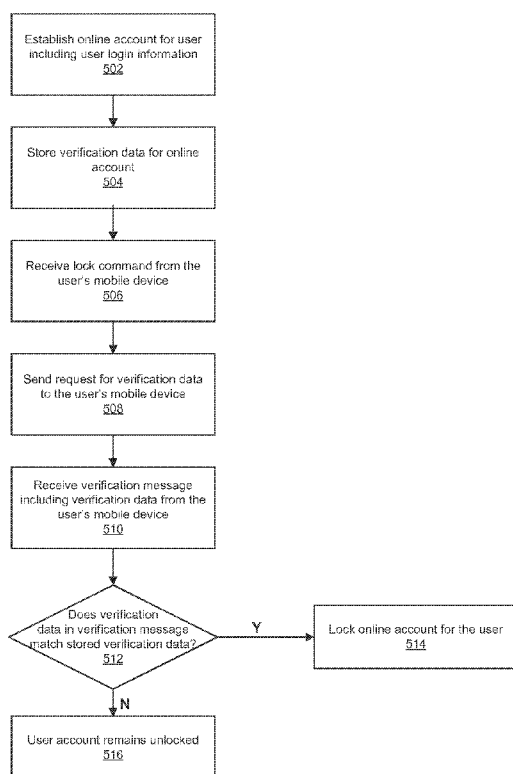
(54) **Title:** ONLINE ACCOUNT ACCESS CONTROL BY MOBILE DEVICE

FIG. 5

(57) **Abstract:** Systems and methods for controlling access to an online account are described. An access control message including an action to be performed on an online account can be sent from a mobile device to a server. A user verification query message can be sent to the mobile device. A user verification response message can be received from the mobile device. The user verification response message can include verification information that is different from login information for the online account. The user verification response message can be verified by comparing the verification information to stored information. If the user verification response message is successfully verified, the action indicated in the access control message can be performed on the online account.

EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU,
LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK,
SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ,
GW, ML, MR, NE, SN, TD, TG).

— before the expiration of the time limit for amending the
claims and to be republished in the event of receipt of
amendments (Rule 48.2(h))

Published:

— with international search report (Art. 21(3))

ONLINE ACCOUNT ACCESS CONTROL BY MOBILE DEVICE

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] The present application is a PCT application of and claims priority to U.S. Provisional Application No. 61/570,680, filed on December 14, 2011 (Attorney Docket No.: 79900-822787), the entire contents of which are herein incorporated by reference for all purposes.

BACKGROUND

[0002] Online accounts for e-mail, social networks, financial account management, and online shopping are increasingly ubiquitous. When an online account is established, a customer typically provides login information such as a username and password combination that is used by the customer to gain access to the account.

[0003] An online account may be compromised, allowing an unauthorized user to gain access to the account. For example, if an unauthorized user discovers the login information for an account, the unauthorized user may enter the login information to access the account. The unauthorized user may use the account to engage in activity that is damaging to the customer who holds the online account. For example, the unauthorized user may send e-mail from an customer's e-mail account to the customer's e-mail contacts. If an unauthorized user gains access to an enrollee's social network account, the unauthorized user may post unwanted content to the social network account. Unauthorized access to an online account associated with a financial account can be particularly dangerous as the unauthorized user may make unauthorized purchases using the financial account.

[0004] When an unauthorized user gains access to the login information for accessing an account, it may be difficult for the customer to regain control of the account. The customer may be required to make a call to the online account provider or visit a physical location of the online account provider to access the account again. These requirements may inconvenience the customer, particularly if the customer is left without access to the account for an extended period of time while taking steps to regain control of the account.

[0005] Embodiments of the invention solve these and other problems.

BRIEF SUMMARY

[0006] Techniques are described for controlling access to an online account with a mobile device. An online account user can send a message, such as an SMS message, indicating an action to take on the account.

[0007] One embodiment is directed to a method for controlling access to an online account. An access control message can be received from a mobile device. The access control message can include an action to be performed on an online account. The online account may be accessible using login information. A user verification query message can be sent to the mobile device. A user verification response message can be received from the mobile device. The user verification response message can include verification information that is different from the login information for the online account. The user verification response message can be verified by comparing the verification information to stored information. If the user verification response message is successfully verified, the action indicated in the access control message can be performed.

[0008] Another embodiment is directed to a mobile device. The mobile device can include a processor and a computer readable medium coupled to the processor. The computer readable medium may include code executable the processor. The code may be operative to send an access control message to a server. The access control message can include an action to be performed on an online account. The online account can be accessed using login information. A user verification query message can be received from the server. The mobile device can send a user verification response message to the server. The user verification response message may include verification information that is different from the login information for the online account. If the user verification response message is verified by the server, the action indicated in the access control message may be performed on the online account.

[0009] A further embodiment is directed to a system for controlling access to an online account. The system can include a processor and a computer readable medium coupled to the processor. The computer readable medium can include code

executable the processor. The code may be operative to receive an access control message from a mobile device. The access control message can include an action to be performed on an online account. The online account can be accessed using login information. A user verification query message may be sent to the mobile device. A user verification response message may be received from the mobile device. The user verification response message can include verification information that is different from the login information for the online account. The user verification response message can be verified by comparing the verification information to the stored information. If the user verification response message is verified, the action indicted in the access control message can be performed on the online account.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] FIG. 1 is an illustrative block diagram of a system for controlling access to an online account.

[0011] FIG. 2 shows an illustrative flow chart for unlocking and locking an online account.

[0012] FIG. 3 shows an illustrative flow chart for using an access control message to lock and unlock a device.

[0013] FIG. 4 shows an illustrative message exchange including a request for a user verification response message.

[0014] FIG. 5 shows an illustrative flow chart for access control of an online account including verification.

[0015] FIG. 6 shows an illustrative block diagram of a computer system.

DETAILED DESCRIPTION

[0016] Systems and methods are described for controlling access to an online account. The online account can include login information used for accessing the account. If a user wishes to disable or enable the ability for the online account to be accessed with the login information, the user may send an access control message

to a server. For example, the user may use a mobile device such as a cellular phone to send a message such as an SMS to the server. The access control message may include a command, such as "lock" or "unlock." The access control message may be received by a server capable of controlling the online account.

[0017] The mobile device may subsequently receive a user verification query message. For example, the server may send a user verification query message to the mobile device. The user verification query message may include a request for the user to enter verification information, such as the last four numbers of a social security number or other personal information.

[0018] The user may send a user verification response message from the mobile device in response to the user verification query message. The user verification response message may include verification information responsive to a query in the user verification query message.

[0019] When the user verification response message is received from the mobile device, the verification information may be compared to stored verification information. For example, the server may receive the user verification response message and compare verification information from the message to verification information stored in the server in association with the online account. If the received verification information matches the stored verification information, the server may perform the action specified in the access control message. For example, if the access control message included a "lock" command, the server may lock the online account. Locking the online account may render the online account inaccessible. For example, it may not be possible to login to the online account using the login information associated with the online account while the online account is locked. If the user subsequently sends an access control message including an "unlock" command, the online account may be unlocked. For example, when the online account is unlocked, it may be possible to login to the online account using the login information.

[0020] Terms used to describe embodiments herein can be understood with reference to the descriptions provided below:

[0021] An "online account" can be any account that can be used via a connection to a network such as the Internet. Examples of online accounts include e-mail, instant message, voice communication, social network accounts, customer accounts

associated with one or more merchants, media accounts (associated with applications for managing stored media, receiving streamed media and/or downloading media, etc.), game accounts, and accounts associated with various other services such as money transfer services. In some embodiments, an online account can provide tools related to a financial account, such as a bank account, credit card account, debit card account, loan management account, bill payment management account, etc.

[0022] When an online account is created, a user may be prompted to provide login information. "Login information" may include a password and an identifier such as a username, e-mail address, or other user identification. The login information may be selected by or assigned to the user. When login information is correctly entered in an interface for an online account, access to the online account may be granted.

[0023] "Verification information" can be information used to verify that an authorized user is taking action with respect to an online account. In some embodiments, verification information is information associated with a mobile device. For example, verification information can include identifying information for a device, such as a Mobile Subscriber Integrated Services Digital Network (MSISDN) number or other telephone number associated with the device, International Mobile Subscriber Identity (IMSI) number, International Mobile Station Equipment Identity (IMEI) number, media access control (MAC) address, internet protocol (IP) address, or other device identification. In some embodiments, verification information includes personal information, such as the last four numbers of a user's social security number, a mother's maiden name, city of birth, etc. A user may be prompted to provide verification information when an account is established, or a user may elect to or be prompted to provide verification information at a later time. Verification information can be entered by the user and stored by a server in association with an online account. In a preferred embodiment, verification information is identifying information for a device other than the device used to create the online account. For example, a user can enter a telephone number associated with the user's cellular phone when the user establishes the online account using a personal computer. Alternatively, verification information about a user may be determined from sources other than user input. In some embodiments, verification information can be acquired from a mobile device during a mobile device registration process. For example, an application executing on a server or on a mobile device may be capable

of determining verification information for a mobile device and transmitting the verification information to a server for storage in association with a user's online account. Verification information can also be a code generated by an online account server, an encrypted message or cryptographic hash generated by a mobile device, or a message generated by a signed application of a mobile device. Other forms of identification and information may be used as verification information.

[0024] A "mobile device" can include any device capable of sending and receiving electronic communications through a network. For example, a mobile device may be a cellular telephone, media player, tablet, laptop computer, or other device. The mobile device may be capable of communicating with a cellular network, local area network, the internet or other network via a wired or wireless connection. Wireless connections may occur via 3G, EDGE, WiFi, or other mobile communication technologies or short range communication technologies such as WiFi, Bluetooth, or other wireless protocols. Typically, a mobile device is configured to be carried by a user.

[0025] A "message" can be information transmitted from the mobile device and received by a server. For example, the message may be a short message service (SMS) communication, an e-mail, an instant message, or a message originated by an application of the mobile device, such as a digitally signed application configured to validate an online account.

[0026] A digital signature may be applied to data to demonstrate the authenticity of the data. For example, an encryption algorithm such as an RSA algorithm may be applied to an application to be installed on mobile device. The digital signature may allow the mobile device to determine that the application to be installed on the mobile device (e.g., the executable file) is authentic and unaltered. In some embodiments, an encryption algorithm may be applied to a message sent by the mobile device. For example, key stored on the mobile device, such as a private key, may be used to sign the message. A key stored on online account server, such as a public key, may be used to allow the server to determine that the message is authentic and unaltered.

[0027] FIG. 1 shows an illustrative block diagram of a system for controlling access to an online account, according to an embodiment. The system 100 can include mobile device 102. Mobile device 102 may be configured to exchange messages

with online account server 104. For example, mobile device 102 may be communicatively coupled to online account server 104 via a network connection.

[0028] Online account server 104 may be a server operated by an online account provider for providing online account functionality to users. Alternatively, online account server 104 may be operated by a partner of the online account provider for providing verification services.

[0029] Online account server 104 may be communicatively coupled to one or more online account databases 106. Login information, verification information, and other data associated with an online account may be stored on one or more online account databases 106. In some embodiments, online account server 104 communicates with another server that is communicatively coupled to one or more online account databases 106. When online account server 104 communicates with online account databases 106 through another server, the other server may be configured to perform an action on an online account.

[0030] Online account server 104 may include validation module 108. Validation module 108 may be a set of instructions stored on data storage element 110 and executed by a processor 112 of online account server 104 for receiving an access control message from a mobile device. Processor 112 may be communicatively coupled to data storage element 110. Validation module 108 may be further configured to send a user verification query message to mobile device 102 and receive a user verification response message from mobile device 102. Validation module may also be configured to verify a user verification response message, for example, by comparing verification information of the verification response message to stored verification information. Verification information may be stored on a data storage element 110 of online account server 104 or on online account database 106. If validation module 108 does not recognize a device, the user can be provided with an alert that the user verification response message was not successfully verified.

[0031] Data storage element 110 can store additional modules having instructions that can be executed by the processor to perform various functions for an online account system. It will be recognized that these modules could be alternatively stored and executed on a server communicatively coupled to online account server 104 and/or online account database 106.

[0032] For example, data storage element 110 can store an enrollment module 120. Enrollment module 120 can provide a user with a form having fields in which the user can input information such as username, password, contact information and other information pertinent to a particular online account. The form may be displayed on mobile device 102 or another device communicatively coupled to online account server 104. In some embodiments, enrollment module 120 can be configured to register mobile device 102. For example, enrollment module 120 may request that a user input identifying information for a mobile device, such as a phone number associated with the mobile device. Enrollment module 120 may alternatively obtain identifying information from the mobile device without requiring user input, for example, by interacting with one or more applications executed by mobile device 102 to obtain information such as a MSISDN number and/or IMSI. The identifying information may be used as verification information.

[0033] In a further example, data storage element 110 can store online account access module 122. Online account access module 122 can provide logic for granting and denying access to an online account. For example, if an access control message has been received by online account server 104 from mobile device 102 and the access control message indicates that access to the online account should be disabled (a "locked" state), online account access module 122 may prevent the account from being accessed even when login information for the online account is correctly entered. Similarly, if an access control message is received indicating that access to the online account should be disabled (an "unlocked" state), online account access module 122 may allow access to the online account when login information is correctly entered. In some embodiments, the online account access module executes an action indicated by an access control message only after a user verification response message has been received from mobile device 102 and verification information in the user verification response message has been verified.

[0034] In other embodiments, the online account access module 122 can include a verification code generation module. The verification code generation module can generate a verification code each time an access control message is received from mobile device 102. A user verification query message including the generated code can be sent from online account server 104 to mobile device 102. The online account access module may execute an action indicated by an access control message only if a user verification response message sent from mobile device 102

to online account server 104 includes the generated code, as verified by validation module 108. In further embodiments, the user can provide the code in addition to login information on an attempt to access the online account if the account was previously locked, deactivated, suspended, etc.

[0035] In some embodiments, an application 114 is stored on a data storage element 116 of mobile device 112 and is executed by a controller 118 communicatively coupled to data storage element 116. For added security, application 114 may be a digitally signed application.

[0036] Data storage elements 110 and 116 may be computer readable media such as a memory or hard drive. A computer readable medium can include a fixed disk or a system memory, disk drives, optical storage devices, solid-state storage device such as a random access memory ("RAM") and/or a read-only memory ("ROM"), which can be programmable, flash-updateable and/or the like. The computer-readable medium of 110 (optionally, in combination with database 106 and other data storage devices) can provide remote, local, fixed, and/or removable storage devices plus storage media for temporarily and/or more permanently containing, storing, transmitting, and retrieving computer-readable information.

[0037] Online account server 104 may also comprise software elements, including an operating system and/or other code, such as an application program (which may be a client application, Web browser, mid-tier application, RDBMS, etc.). It will be appreciated that alternate embodiments of online account server 104 may be used in system 100. For example, elements shown as software might be implemented in hardware.

[0038] A user may wish to use an online account access control feature to maintain an online account in a "locked" state and to "unlock" an account only when the user is actively using the online account. An implementation of this use of online account access control is illustrated with reference to FIG. 2.

[0039] FIG. 2 shows an exemplary use of system 100 to unlock and lock an online account in accordance with an embodiment. At operation 200, an online account can be established for a user. The online account may have associated login information. At operation 202, an access control message can be received by online account server 104 from mobile device 102. The access control message may include an action to be performed on an online account, such as an "unlock" action

enabling access to the online account. For example, the message may be an SMS including the word "unlock." Online access module 122 of online account module 104 may enable access to an online account associated with mobile device 102 in response to receiving the access control message, as indicated at operation 204. For example, online access module 122 may search stored data, such as data stored at data storage element 110 or online account database 106, for an online account associated with the identifying information of mobile device 102 (such as a phone number of mobile device 102). When access to the online account is enabled, the user may login to the account using login information associated with the online account such as username and password. The user may login to the account from mobile device 102 or from another device. In some embodiments, the account is unlocked for a pre-established period of time. Alternatively, a user may send a subsequent command to lock the account.

[0040] At operation 206, an access control message including a "lock" action may be received by online account server 104 from mobile device 102. The lock action may indicate that the user wishes to disable access to the online account. At operation 208, online access module 122 of online account module 104 may disable access to an online account associated with mobile device 102. For example, online access module 122 may search stored data for an online account associated with the identifying information of mobile device 102. When access to the online account is disabled, no user will be able to access the online account using the login information.

[0041] It will be recognized that the access control messages to "unlock" and "lock" the online account as described with reference to FIG. 2 could be sent in reverse order, i.e., the online account could be locked for a period of time and subsequently unlocked. In some embodiments, when access to the online account is disabled ("locked"), the user may login to the account using login information associated with the online account, but no updates to the online account may be made. In other embodiments, when access to the online account is disabled, an online account that is viewable by other users (e.g., a social networking account) is no longer visible to other users. It will be recognized that an account may be enabled and/or disabled in various ways in response to receiving an access control message.

[0042] In some embodiments, an access control message can be used to change a functionality of a device. For example, it may be desirable to lock a device, such as

a wireless router, for a period of time when a user does not wish for the device to be used (e.g., a parent may wish to curtail usage of the internet by a child during a particular period of time).

[0043] FIG. 3 shows an illustrative use of an access control message to lock and unlock a device. At operation 302, mobile device 102 can send an access control message to a device such as a wireless router. The access control message can include an action to be performed on the wireless router. For example, the action could be a "lock" action that prevents the wireless router from transmitting information. At operation 304, the wireless router can disable transmissions in response to the received access control message. The wireless router may determine whether identifying information (e.g., a phone number) for the mobile device 102 from which the access control message was received matches identifying information stored in a memory of the wireless router. In some embodiments, the device can be locked for a pre-established period of time. Alternatively, a user can transmit an unlock command when the user is ready for the device to be re-enabled. At operation 306, mobile device 102 can send an access control message to the device including an "unlock" action to be performed on the wireless router. At operation 308, in response to receiving the access control message, the wireless router can re-enable transmissions. It will be recognized that the access control messages to "lock" and "unlock" the device as described with reference to FIG. 3 could be sent in reverse order, i.e., the device could be unlocked for a period of time and subsequently locked.

[0044] A user may be concerned about the potential for an access control message appearing to originate from the user's mobile device to be sent from an unauthorized user. For example, an unauthorized user may be able to generate a message including identifying information from the user's mobile device although the message from the unauthorized user is actually generated by a different device. To provide added security, the online account server 104 may send a message to the user's mobile device prompting mobile device 102 to provide a response message. In this way, even if an access control message is generated from an unauthorized device, a prompt for additional security information sent to an authorized device can be used to ensure that no action will be taken based on an access control message generated from an unauthorized device.

[0045] FIG. 4 shows an illustrative message exchange including a request for a user verification response message, in accordance with an embodiment. Mobile device 102 can send an access control message 400 to online account server 104. The access control message 400 can be an SMS, instant message, e-mail, message generated by an application (such as a signed application) of mobile device 102, or other message. The access control message 400 can include an action to be performed on an online account. For example, the action can be one or more of: preventing a user from accessing the online account with login information for the online account, enabling a user to access the online account using login information for the online account, disabling editing of information associated with the online account, enabling editing of information associated with the online account, disabling transmitting e-mail from the account, enabling transmitting e-mail from the account, disabling public access to the online account (e.g., a social networking account), enabling public access to the online account, and so on. In some embodiments, a text command, such as "lock" or "unlock" can be included in an SMS sent to a phone number for routing to an online account server. In other embodiments, a user may select a command from a user interface of an application and the application may generate a message (e.g., an SMS or other message format) including information representative of the command.

[0046] When online account server 104 receives access control message 400, online account server 104 can generate user verification query message 402 and send user verification query message 402 to mobile device 102. User verification query message 402 may be an SMS, e-mail, instant message or other message receivable by mobile device 102. User verification query message 402 may include a request for the user to provide verification information, such as personal information known to the user (e.g., last four digits of the user's social security number, mother's maiden name, user's place of birth, etc.) In some embodiments, user verification query message 402 may include a code generated by online account server 104. In various embodiments, the user verification query message 402 is a message receivable by a verification application (e.g., signed application 114) of mobile device 102 that is configured to determine identifying information about mobile device 102 (e.g., MSISDN and/or IMSI).

[0047] When mobile device 102 receives user verification query message 402, mobile device 102 may send a user verification response message 404 to online

server 104. For example, if user verification query message 402 requests verification information, the user may enter the verification information into a message such as an SMS, or enter input into an application interface of an application configured to send a message. The message is sent as user verification response message 404 to online server 104. If user verification query message 402 requests that the user respond with a code included in user verification query message, the user can enter the code in a message such as an SMS and send the message to online server 104. In some embodiments, a verification application of mobile device 102 may send a user verification response message to online account server 104 automatically (i.e., without requiring user input). The user verification response message 404 may include a cryptographic hash value, such as a hash of identifying information of mobile device 102 and additional information such as a current date and/or time. When online account server 104 receives user verification response message 404, validation module 108 may compare information in the user verification response message 404 to verification information stored in data storage 110 (and/or verification information stored in online account database 106 or on another server associated with the online account). For example, validation module may search for validation information stored in association with identifying information of mobile device 102, such as the phone number of mobile device 102. If the user verification response message 404 can be verified, e.g., based on a match between received verification information and stored verification information, one or more actions indicated in access control message 400 may be taken.

[0048] FIG. 5 shows an illustrative use of system 100 for online account access control including verification, according to an embodiment. At operation 502, an online account can be established for a user. The online account may have associated login information, such as a user name and password usable by a user to access the online account. At operation 504, verification information can be stored in association with the online account. For example, a user may be prompted to provide verification information when creating an online account or subsequent to creating an online account, or a user may wish to establish verification functionality after an online account has been created. Verification information is typically information that is different from the login information. Verification information can include one or more of identifying information for mobile device 102, personal information known by the user, etc. In some embodiments, verification information is

generated by online account server 104 when an access control message is received by the online account server. In a further embodiment, verification information can be generated by mobile device 102 when a user verification query message is received by the mobile device.

[0049] At operation 506, an access control message can be received by online account server 104 from mobile device 102. The access control message may include an action to be performed on an online account, such as a "lock" action for disabling access to the online account. For example, the message may be an SMS including the word "lock."

[0050] At operation 508, online account server 104 may send a user verification query message to mobile device 102. The query message may be an SMS asking the user to provide verification information. At operation 510, online account server 104 may receive a user verification response message from mobile device 102. The user verification response message may be an SMS including verification information entered by the user.

[0051] At decision diamond 512, validation module 108 of online account module 104 may determine whether verification information in the user verification response message is valid. For example, validation module 108 may determine whether the received verification information matches verification information stored in data storage 110 of online account server 104, in online account database 106, or in another storage location. If the verification information in the user verification response message is determined to be valid, online account access module 122 of online account server 104 may perform the action indicated in the access control message. For example, if the action is a "lock" action, online account access module 122 may lock the online account, as indicated at operation 514. If the verification information in the user verification response message is not determined to be valid, the online account may remain unlocked, as indicated at operation 516.

[0052] In some embodiments, verification is performed by determining if a user currently has an active status in an application or an online account other than the online account for which an access control message is sent. For example, online account server 104 may receive an access control message for an e-mail account from a user of mobile device 102 and online account server 104 may be able to determine if the user currently has an active status in an instant messaging account.

If online account server 104 determines that the user has an active status in the instant messaging account, online account server 104 may execute the action indicated in the access control message. In other examples, online account server 104 may validate the access control message by determining whether a user has an active status in an application other than the online account, such as an e-mail account, social network account, validation application, or other account or application. Online account server 104 may determine an active status via communications with mobile device 102, via an application executing on online account server 104, or via communication with another server with which the application or account is associated.

[0053] Referring now to FIG. 6, an exemplary computer system according to one embodiment is illustrated. The system may be used to implement any of the computer systems described above (e.g., online account server, online account database, mobile device, etc.). The subsystems shown in FIG. 6 are interconnected via a system bus 602. Additional subsystems such as a printer 604, keyboard 606, fixed disk 608 (or other memory comprising computer readable media), monitor 610, which is coupled to display adapter 612, and others are shown. Peripherals and input/output (I/O) devices, which couple to I/O controller 614 (which can be a processor or other suitable controller), can be connected to the computer system by any number of means known in the art, such as serial port 616. For example, serial port 616 or external interface 618 can be used to connect the computer apparatus to a wide area network such as the Internet, a mouse input device, or a scanner. The interconnection via system bus allows the central processor 620 to communicate with each subsystem and to control the execution of instructions from system memory 622 or the fixed disk 608, as well as the exchange of information between subsystems. The system memory 622 and/or the fixed disk 608 may embody a computer readable medium.

[0054] It should be understood that the present technology as described above can be implemented in the form of control logic using computer software (stored in a tangible physical medium) in a modular or integrated manner. Based on the disclosure and teachings provided herein, a person of ordinary skill in the art will know and appreciate other ways and/or methods to implement the present technology using hardware and a combination of hardware and software

[0055] Any of the software components or functions described in this application, may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, Java, C++ or Perl using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions, or commands on a computer readable medium, such as a random access memory (RAM), a read only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a CD-ROM. Any such computer readable medium may reside on or within a single computational apparatus, and may be present on or within different computational apparatuses within a system or network.

[0056] The above description is illustrative and is not restrictive. Many variations of the technology will become apparent to those skilled in the art upon review of the disclosure. The scope of the technology should, therefore, be determined not with reference to the above description, but instead should be determined with reference to the pending claims along with their full scope or equivalents.

[0057] One or more features from any embodiment may be combined with one or more features of any other embodiment without departing from the scope of the technology.

[0058] A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

WHAT IS CLAIMED IS:

1 1. A method for controlling access to an online account, the
2 method comprising:
3 receiving an access control message from a mobile device, wherein
4 the access control message includes an action to be performed on an online
5 account, wherein the online account is accessed using login information;
6 sending a user verification query message to the mobile device;
7 receiving a user verification response message from the mobile device,
8 wherein the user verification response message includes verification information that
9 is different from the login information for the online account;
10 verifying the user verification response message, wherein the verifying
11 includes comparing the verification information to stored information; and
12 if the user verification response message is verified, performing the
13 action on an online account, wherein the action is based on the access control
14 message.

1 2. The method of claim 1, further comprising verifying the mobile
2 device, wherein the verifying includes comparing an identifier of the mobile device to
3 a plurality of stored identifiers.

1 3. The method of claim 2, wherein the identifier of the mobile
2 device includes at least one of a Mobile Subscriber Integrated Services Digital
3 Network (MSISDN) number and an International Mobile Subscriber Identity (IMSI).

1 4. The method of claim 1, wherein at least one of the access
2 control message, the user verification query message and the user verification
3 response message is a short message service (SMS) message.

1 5. The method of claim 1, wherein the user verification response
2 message includes a cryptographic hash value.

1 6. The method of claim 1, wherein at least one of the access
2 control message, the user verification query message and the user verification
3 response message is generated by a signed application.

1 7. The method of claim 1, wherein the action is preventing access
2 to the online account using the login information for the online account.

1 8. The method of claim 1, wherein the action is enabling access to
2 the online account using the login information for the online account.

1 9. The method of claim 1, wherein the action is disabling editing of
2 information associated with the online account.

1 10. The method of claim 1, wherein the action is disabling
2 transmitting e-mail from the account.

1 11. The method of claim 1, further comprising:
2 enrolling the online account; and
3 registering the mobile device in association with the online account.

1 12. A mobile device, comprising:
2 a processor; and
3 a computer readable medium coupled to the processor, wherein the
4 computer readable medium includes code executable by the processor, the code
5 operative to:
6 send an access control message to a server, wherein the
7 access control message includes an action to be performed on an online account,
8 wherein the online account is accessed using login information;
9 receive a user verification query message from the server; and
10 send a user verification response message to the server,
11 wherein the user verification response message includes verification
12 information that is different from the login information for the online account;
13 wherein if the user verification response message is verified by the
14 server; the action is performed on the online account.

1 13. The mobile device of claim 12, wherein at least one of the
2 access control message, the user verification query message and the user
3 verification response message is a short message service (SMS) message.

1 14. The mobile device of claim 12, wherein the code is further
2 operative to generate a cryptographic hash value to include in the user verification
3 response message.

4 15. The mobile device of claim 12, wherein at least one of the
5 access control message, the user verification query message and the user
6 verification response message is generated by a signed application.

1 16. A system for controlling access to an online account, the system
2 comprising:

3 a processor; and

4 a computer readable medium coupled to the processor, wherein the
5 computer readable medium includes code executable by the processor, the code
6 operative to:

7 receive an access control message from a mobile device,
8 wherein the access control message includes an action to be performed on an
9 online account, wherein the online account is accessed using login
10 information;

11 send a user verification query message to the mobile device;

12 receive a user verification response message from the mobile
13 device, wherein the user verification response message includes verification
14 information that is different from the login information for the online account;

15 verify the user verification response message, wherein the
16 verifying includes comparing the verification information to stored
17 information; and

18 if the user verification response message is verified, performing
19 the action on an online account, wherein the action is based on the
20 access control message.

1 17. The system of claim 16, wherein the code is further operative to
2 verify the mobile device, wherein the verifying includes comparing an identifier of the
3 mobile device to a plurality of stored identifiers.

1 18. The system of claim 16, wherein the identifier of the mobile
2 device includes at least one of a Mobile Subscriber Integrated Services Digital
3 Network (MSISDN) number and an International Mobile Subscriber Identity (IMSI).

1 19. The system of claim 16, wherein at least one of the access
2 control message, the user verification query message and the user verification
3 response message is a short message service (SMS) message.

1 20. The system of claim 16, wherein the action is preventing access
2 to the online account using the login information for the online account.

1 21. The system of claim 16, wherein the action is enabling access to
2 the online account using the login information for the online account.

1 22. The system of claim 16, wherein the action is disabling editing of
2 information associated with the online account.

1 23. The system of claim 16, wherein the action is disabling
2 transmitting e-mail from the account.

1/6

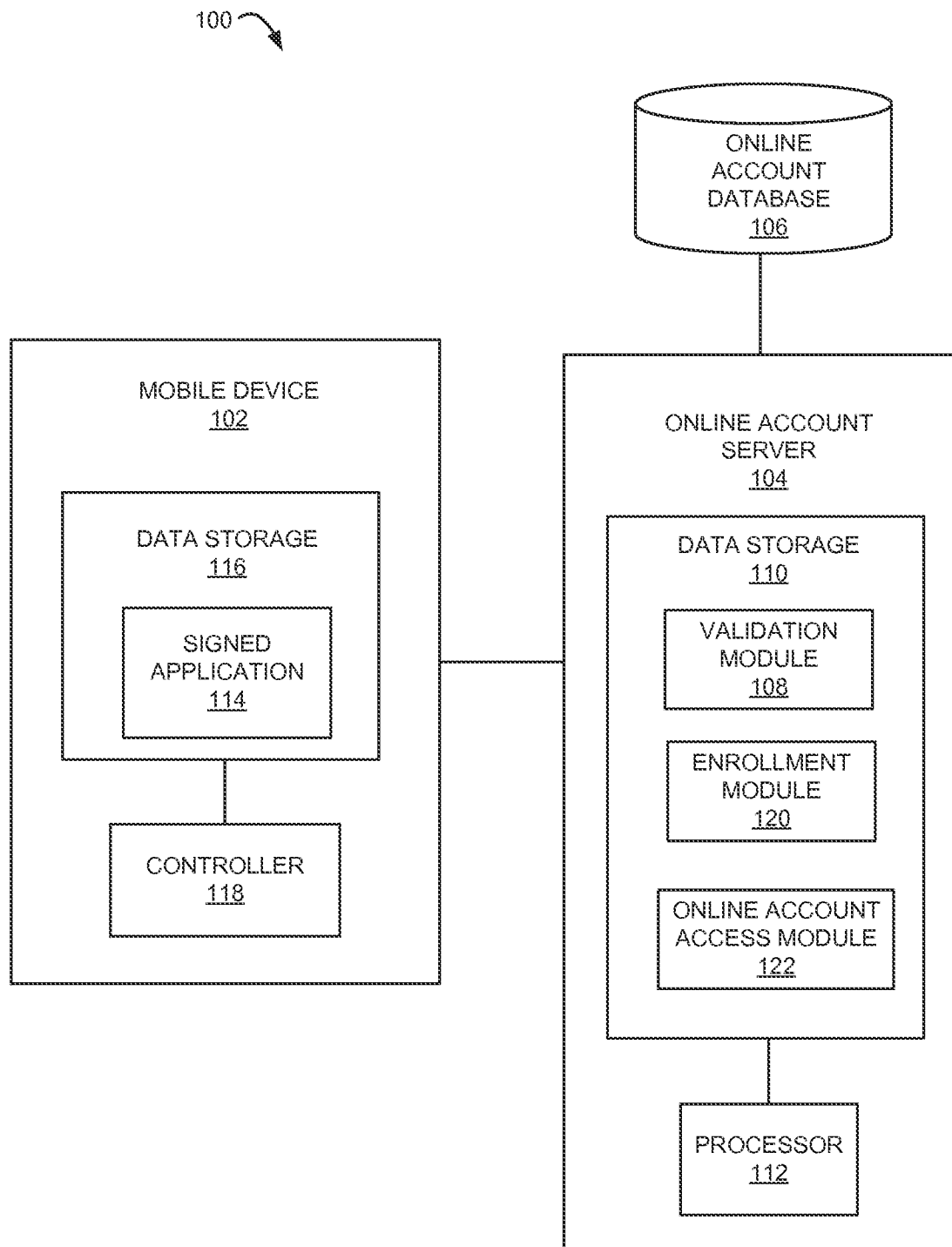
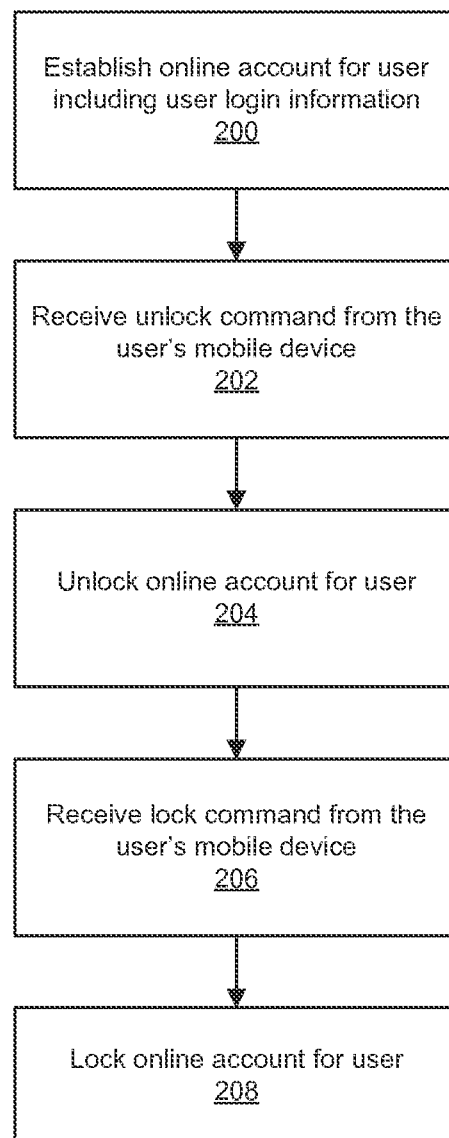
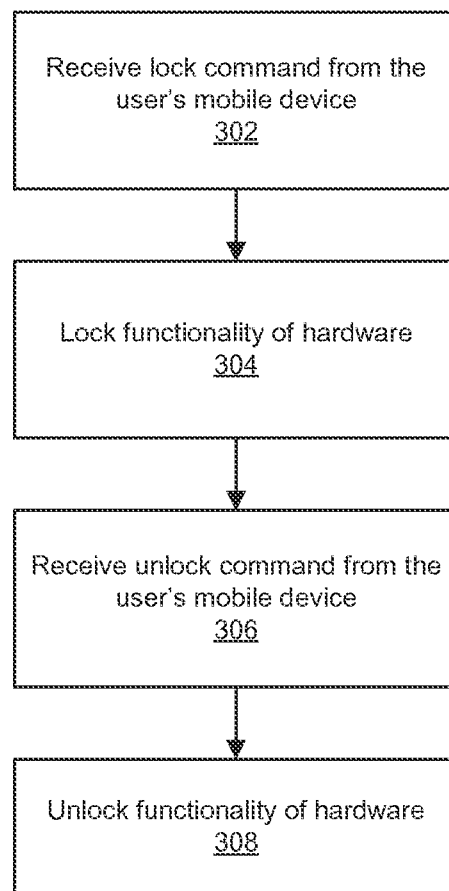


FIG. 1

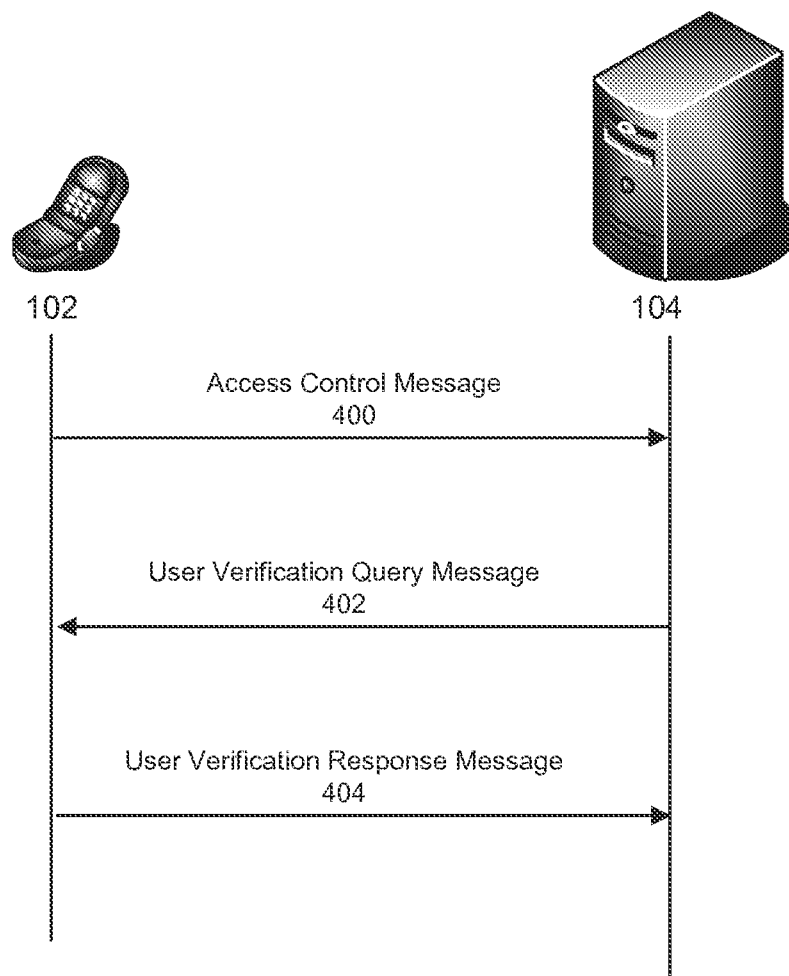
2/6

**FIG. 2**

3/6

**FIG. 3**

4/6

**FIG. 4**

5/6

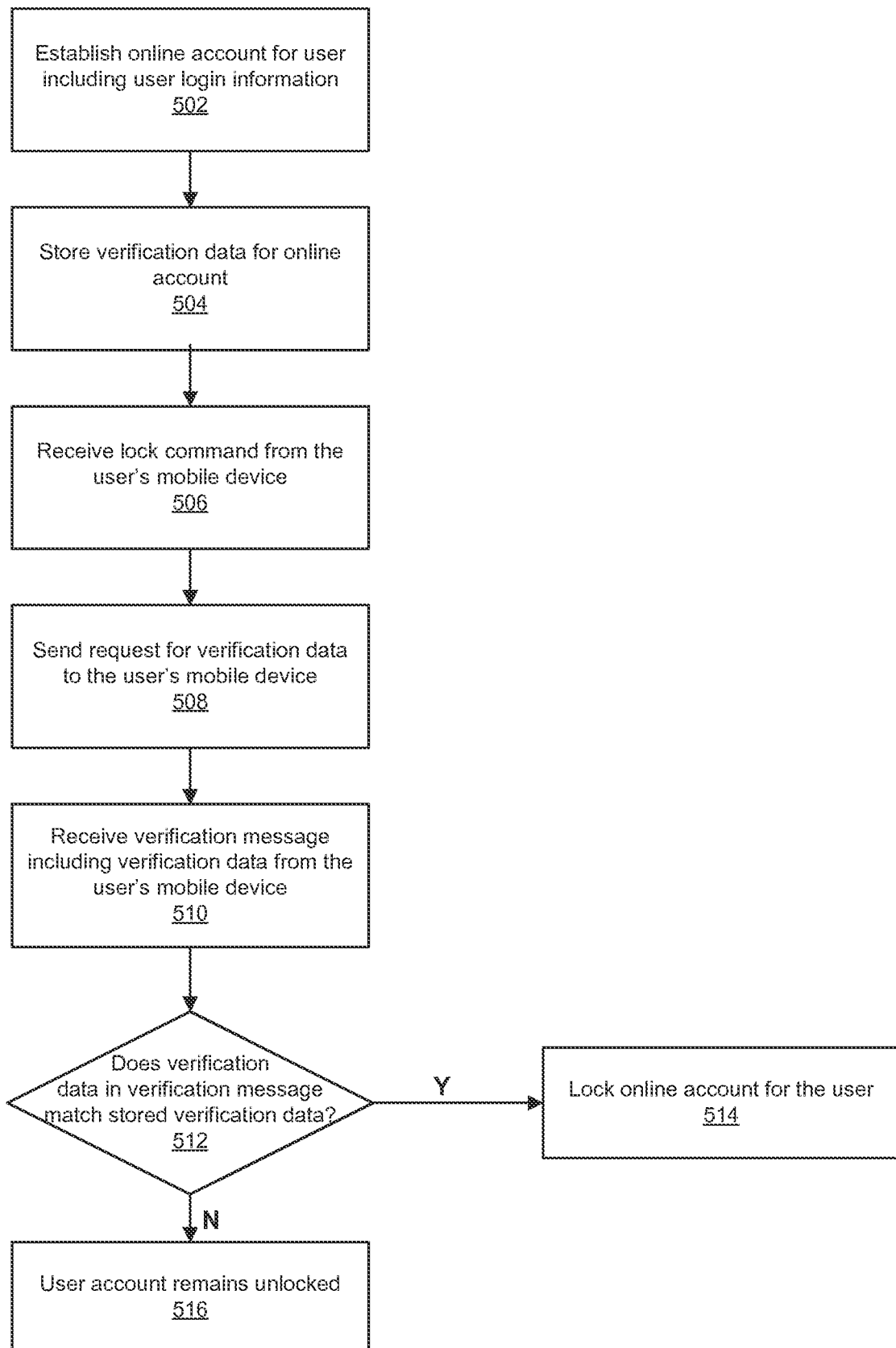


FIG. 5

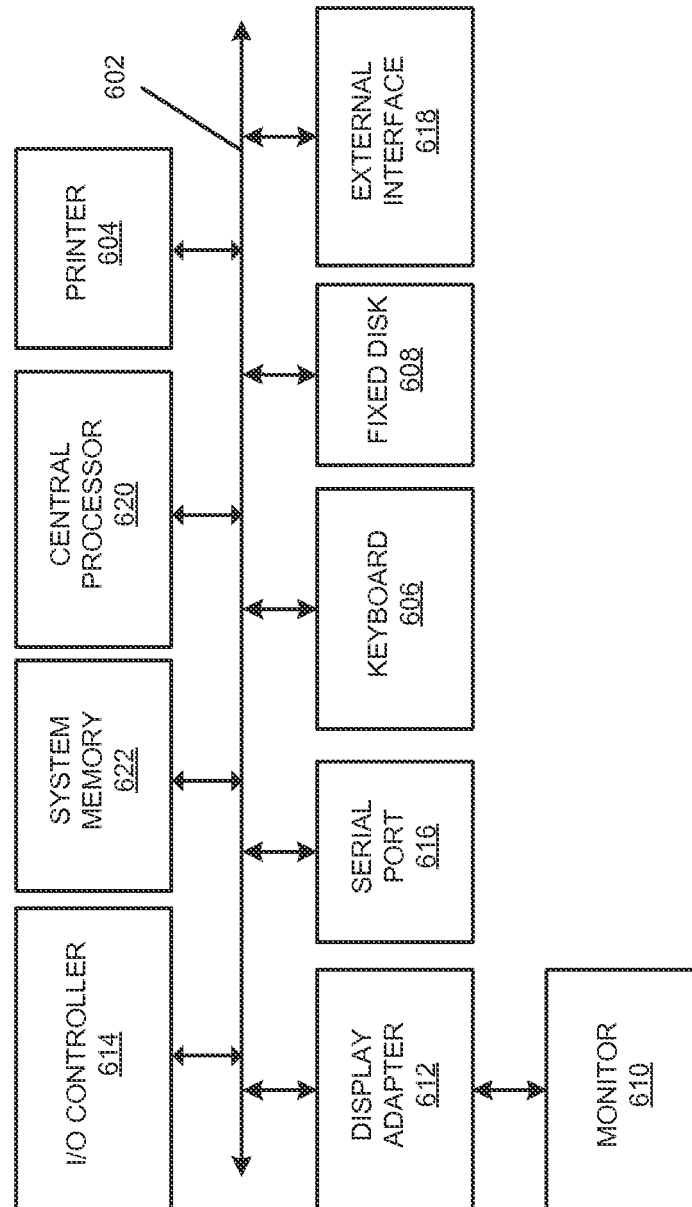


FIG. 6

A. CLASSIFICATION OF SUBJECT MATTER***H04W 8/20(2009.01)i, H04W 4/12(2009.01)i***

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W 8/20; H04W 4/12; G06F 11/30; G06K 5/00; G06F 17/60; H04M 1/00; H04L 9/32; H04L 9/00; G06Q 20/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS(KIPO internal) & keywords: access, message, verify, compare, perform, action, and similar terms.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2010-0057619 Al (WELLER, KEVIN D. et al.) 04 March 2010 See paragraphs [0050]-[0057] , [0163H0187] ; claims 1, 5, 15; and figures 2, 12A, 13.	1-23
Y	US 2002-0129264 Al (ROWLAND, CRAIG H. et al.) 12 September 2002 See paragraphs [0036]-[0067] ; claims 13-14 ; and figures 2, 4.	1-23
A	US 2006-0015743 Al (CAMAISA, ALLAN et al.) 19 January 2006 See paragraphs [0026]-[0034] ; claims 1-4 ; and figures 2-3 .	1-23
A	US 2005-0263588 Al (BABI, RENE PIERRE et al.) 01 December 2005 See paragraphs [0053]-[0063] ; claims 1-2 , 7 ; and figure 4.	1-23
A	US 2010-0223145 Al (DRAGT, BRUCE) 02 September 2010 See paragraphs [0107]-[0117] ; claims 1-6 ; and figure 4.	1-23



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

29 April 2013 (29.04.2013)

Date of mailing of the international search report

30 April 2013 (30.04.2013)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
189 Cheongsu-ro, Seo-gu, Daejeon Metropolitan
City, 302-70 1, Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

KIM, Byoung Sung

Telephone No. 82-42-481-8403



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2012/069870

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2010-0057619 A1	04.03.2010	AU 2001-257280 B2	19.04.2007
		AU 2001-257280 C1	19.04.2007
		AU 2001-57280 A1	07.11.2001
		CA 2407653 A1	01.11.2001
		EP 1277180 A2	22.01.2003
		EP 2278538 A1	26.01.2011
		JP 05025875 B2	29.06.2012
		JP 2003-532206 A	28.10.2003
		KR 10-0933387 B1	22.12.2009
		KR 10-1015341 B1	16.02.2011
		KR 10-2009-0116813 A	11.11.2009
		US 2002-0111919 A1	15.08.2002
		US 2002-0194138 A1	19.12.2002
		US 2003-0212642 A1	13.11.2003
		US 2010-0332393 A1	30.12.2010
		US 7827115 B2	02.11.2010
		US 7991701 B2	02.08.2011
		US 8271395 B2	18.09.2012
		WO 01-82246 A2	01.11.2001
US 2002-0129264 A1	12.09.2002	AT 419574 T	15.01.2009
		AU 2002-239889 B2	31.01.2008
		CA 2434674 A1	18.07.2002
		CN 1295904 C	17.01.2007
		CN 1524361 A	25.08.2004
		DE 60230601 D1	12.02.2009
		EP 1381928 A2	21.01.2004
		EP 1381928 A4	15.12.2004
		EP 1381928 B1	31.12.2008
		US 7058968 B2	06.06.2006
		WO 2002-056152 A2	18.07.2002
		WO 2002-056152 A3	06.11.2003
US 2006-0015743 A1	19.01.2006	CA 2759510 A1	04.11.2010
		EP 1766839 A1	28.03.2007
		EP 1766839 B1	06.03.2013
		EP 2425583 A2	07.03.2012
		US 2006-0015742 A1	19.01.2006
		US 2006-0069921 A1	30.03.2006
		US 2007-0266257 A1	15.11.2007
		US 2008-0250477 A1	09.10.2008
		US 2009-0259848 A1	15.10.2009
		US 2010-0100967 A1	22.04.2010
		US 7676834 B2	09.03.2010
		US 8079070 B2	13.12.2011
		US 8219822 B2	10.07.2012
		US 8296562 B2	23.10.2012
		WO 2006-019451 A1	23.02.2006
		WO 2009-006148 A1	08.01.2009

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2012/069870Patent document
cited in search reportPublication
datePatent family
member(s)Publication
date

W0 2009-155177 A1 23. 12. 2009
W0 2010-127263 A2 04. 11. 2010
W0 2010-127263 A3 28. 06. 2012
W0 2010-138910 A1 02. 12. 2010

US 2005-0263588 A1 01. 12. 2005

US 7229006 B2 12. 06. 2007

US 2010-0223145 A1 02. 09. 2010

None