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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 July 2005 (07.07.2005)

PCT

(10) International Publication Number
WO 2005/062155 A1

(51) International Patent Classification[7]: G06F 1/00, H04L 29/06, 29/12

(21) International Application Number: PCT/US2004/037461

(22) International Filing Date: 10 November 2004 (10.11.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/530,599 17 December 2003 (17.12.2003) US
10/890,786 13 July 2004 (13.07.2004) US

(71) Applicant *(for all designated States except US)*: **ORACLE INTERNATIONAL CORPORATION** [US/US]; 500 Oracle Parkway, Redwood Shores, CA 94065 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **MAES, Stephane, H.** [BE/US]; 1093 Nez Perce Court, Fremont, CA 94539 (US).

(74) Agents: **HAAPALA, Melissa** et al.; Townsend and Townsend and Crew LLP, Two Embarcadero Center, Eighth Floor, San Francisco, CA 94111-3834 (US).

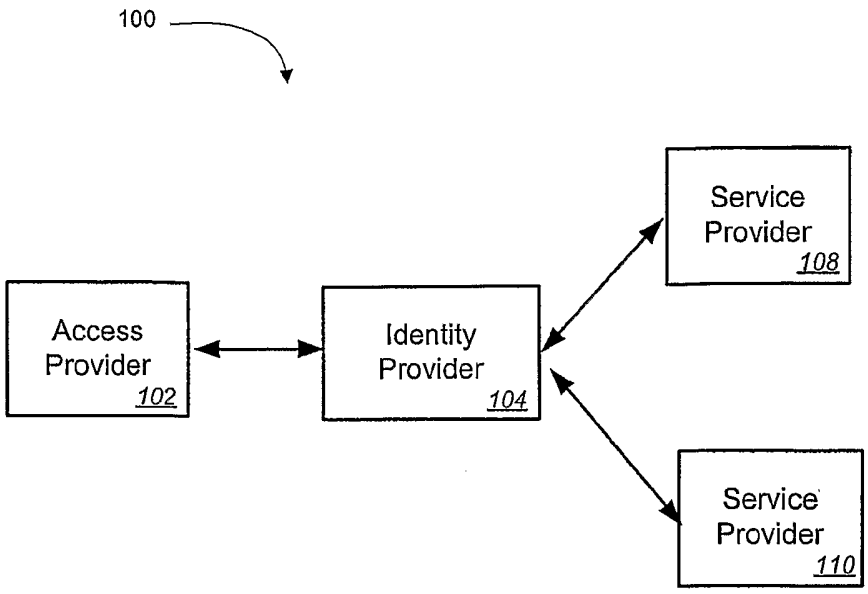
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR,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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) **Title:** METHOD AND APPARATUS FOR PERSONALIZATION AND IDENTITY MANAGEMENT



(57) **Abstract:** Methods and systems are disclosed for personalization and identity management. In one embodiment, the method comprises receiving, from an access provider, a message for a service provider, the message associated with a first identifier of a user of the access provider. A second identifier is obtained, the first identifier is disassociated from the message, and the second identifier is associated with the message. The message associated with the second identifier is then sent to the service provider.

WO 2005/062155 A1

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.

METHOD AND APPARATUS FOR PERSONALIZATION AND IDENTITY MANAGEMENT

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] This application claims the benefit of U.S. Provisional Application No. 60/530,599 entitled "Method and Apparatus for Personalization and Identity Management", filed December 17th 2003, which is incorporated herein by reference.

BACKGROUND OF THE INVENTION

[0002] The present invention generally relates to identity management in e-business. More specifically, the present invention relates to identity management, authentication, user preference and profiles that may be accessed from different locations and different devices, such as in the mobile space.

[0003] Various techniques have been used to manage user identities. Typically, to gain access to a network application or server, a user provides the application or server provider with identity information that identifies the user. The user is then given an login identifier that may be used to access the application or server. In some instances, the application/server may also create a user profile which stores preferences of the user. The application provider may send a cookie or authentication token to the application (e.g., web browser) or device (e.g., user's machine) that the user is using to access the application. Thus, information, such as login identification, user preferences, transaction history, etc., may be saved for the next time the user accesses the network application. However, the user's personalization information (user preferences, transaction history, etc.) cannot be shared across different providers. Additionally, the user identification is known to the service provider.

[0004] Other existing technologies allow a user to use one login identifier to access multiple applications. One example of this technology is a Single-Sign-On (SSO), such as Oracle Single Sign-On Offerings. The SSO is valid for one session between applications that have the particular SSO "hard coded" in the program code. As the SSO is valid for only the single session, personalization of the applications is not provided by the SSO. Furthermore, the user identity is known to all of the applications.

[0005] Another existing approach includes use of a centralized identity management across different service providers, such as Microsoft® Passport technology. The service provider must include program code in the application that allows the identity/authentication provider to authenticate the user. The customer must then use the single identity/authentication provider to logon to the services. This may increase the risk of privacy issues and violations. Furthermore, service providers then become tied to the identity/authentication provider. This may be perceived as an unacceptable monopoly risk to some service providers, especially telecommunication, mobile network operators (MNOs) and banking providers.

[0006] Federated identity management is another approach that may provide for distributed single sign-on across providers. One such federation is the Liberty Alliance Project (http://www.projectliberty.org). An overview maybe found at: http://www.projectliberty.org/specs/liberty-architecture-overview-v1.0.pdf. Federated identity management allows the authentication of a user by a member of the federation to serve as the authentication for other members of the federation. However, there is no mechanism provided that allows for masking of the user identity or for sharing of user preferences or other user personalization information across providers.

BRIEF SUMMARY OF THE INVENTION

[0007] Methods and systems are disclosed for personalization and identity management. In one embodiment, the method comprises receiving a message for a service provider from an access provider, such as a mobile network operator or wireless network provider. The message is associated with a first identifier of a user of the access provider. A second identifier is obtained. The first identifier is disassociated from the message and the second identifier is associated with the message. The message associated with the second identifier is then sent to the service provider. In some embodiments, an indication that the second identifier has been authenticated may also be sent to the service provider.

[0008] In some embodiments, the method may include retrieving personalization information associated with the second identifier and sending a subset of the personalization information to the service provider. By way of example, the personalization information may include user preferences, user device characteristics, user device capabilities, user device settings, user device addresses, and other user personalization information. The method may optionally include a determination that the service provider is authorized to have the

personalization information before the information is sent. Personalization information may have been received from the user, the service provider, and/or derived from user history.

[0009] Alternately, or additionally, the method may also include associating a session to the second identifier and associating the message received from the access provider to the session. The message and one or more additional message(s) received from the access provider, which are associated to the first identifier, may be evaluated for session management information. The session management information may be stored for future retrieval in the event the connection to the service provider is lost and re-established.

[0010] Subsequent to receiving the message from the access provider, a message may be received for the service provider from a second access provider. The message may be associated with a third identifier of the user. The method may then include determining the third identifier is mapped to the first identifier. The third identifier is disassociated from the message and the second identifier is associated with the message. The second message associated with the second identifier is sent to the service provider.

[0011] In an alternate embodiment, the method may comprise receiving a message from a mobile network operator for a service provider. The received message may be associated with a MSISDN of a user. An identifier is obtained and authenticated. The MSISDN is disassociated from the message and the obtained identifier is associated with the message. The message is then sent to the service provider with an indication the identifier has been authenticated. Personalization information indicating preferences of the user is also sent to the service provider.

[0012] In a third embodiment, a system is disclosed. The system comprises an identity component, configured to disassociate a first identifier of a user from a message received from an access provider. The identity provider is also configured to obtain an identifier for a user of an access provider and to associate the second identifier with the message. The system further comprises an authentication component, which is configured to authenticate the second identifier and to associate an indication with the message the second identifier has been authenticated. A communications interface is configured to send the message associated with the second identifier and the indication to the service provider.

[0013] A further understanding of the nature and advantages of the present invention may be realized by reference to the remaining portions of the specification and the drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] Illustrative embodiments in accordance with the invention are illustrated in the drawings in which:

[0015] Fig. 1 illustrates an exemplary embodiment of a system that uses identity management;

[0016] Fig. 2 illustrates an exemplary embodiment of the identity provider of FIG. 1;

[0017] Fig. 3 illustrates a second exemplary embodiment of a system that uses identity management;

[0018] Fig. 4 illustrates a third exemplary embodiment of a system that uses identity management;

[0019] Fig. 5 illustrates a simplified comparison of several currently available mobile network technologies;

[0020] Fig. 6 is a block diagram of a computer system upon which an identity provider may be implemented;

[0021] Fig. 7 is a flow diagram illustrating a method of masking user identification;

[0022] Fig. 8 is a flow diagram illustrating identity management for a user switching access providers.

DETAILED DESCRIPTION OF THE INVENTION

[0023] In the following description, for the purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be apparent, however, to one skilled in the art that the present invention may be practiced without some of these specific details. In other instances, well-known structures and devices are shown in block diagram form.

[0024] Fig. 1 illustrates an exemplary embodiment of a system that may be used to provide identity management to a user. A user may use an access provider 102 to access a network. The network may be a local area network (LAN), a wide area network (WAN), a wireless network, or other type of network. Thus, the access provider 102 may be an Internet Services Provider, a mobile network operator (MNO) or other type of provider to a wireless

communications network, a provider to a wireless network (e.g., General Packet Radio Service (GPRS) network, a WiFi network, 2.5G, EDGE, UMTS, 3G, CDMA, FOMA, etc.). In some embodiments, the user may be accessing the network from a device that is mobile. By way of example, the mobile device may be a laptop, a personal data assistant (PDA), a mobile telephone, or other type of device. In other embodiments, the user device may be relatively stationary, such as a personal computer.

[0025] A user may use the network access provided by access provider 102 to interact with one or more service providers 108, 110. A variety of different types of services may be offered by a service provider 108, 110. For instance, a service provider 108, 110 may provide email services, voice mail services, messaging services (e.g., text messaging, instant messaging, MMS, voice chat, etc.), or application services. By way of example, application services may include a web site that allows the user to purchase goods or services; an application to find the location, presence or availability of somebody; an application to synchronize data with a repository; an application to provision/manage the life cycle of data, applications, or devices; or an application to access a particular domain. It should be appreciated that a wide range of other types of services may also be provided by a service provider 108, 110.

[0026] The user device (not illustrated) has an associated identifier which allows access provider 102 to send messages to it. By way of example, an identifier may be a network interface card (NIC), a mobile identification number (MIN), mobile station ISDN (MSISDN), EMI, SIM information, or USIM information. Messages sent from the user device to service providers 108, 110 via access provider 102 generally have the identifier associated with the message so that the service provider 108, 110 may send messages back to the user. However, in some instances, for privacy, or other reason, the user may not want the service provider to know the identifier. For example, a user of a mobile telephone may not want the service provider 108, 110 to know the user's mobile identification number.

[0027] Identity provider 104 may be used to mask the address of a user from the service providers 108, 110. As will be described in further detail below, the identity provider 104 may obtain a different identifier for the user. Identity provider 104 may disassociate the first identifier from messages sent from the user and in replacement, associate the messages with a second identifier. The messages associated with the second identifier may then be sent to the service provider 108, 110 to which the message was directed. In some instances, identity

provider 104 may also authenticate the second identifier and send an indication along with the message that the second identifier has been authenticated. Service providers 108, 110 route messages back to the user to identity provider 104. Identity provider may then replace the second identifier associated with the messages received from service provider 108, 110 with the first identifier and send the message to access provider 102 for delivery to the user. Thus, the user may conduct transactions with a service provider 108, 110 without providing any identification information, such as the user device address, name, email address, phone number, or other identifying information.

[0028] Fig. 2 illustrates an exemplary embodiment of an identity provider 104. The identity provider 104 includes an identity manager 204. The identity manager 204 may be used to obtain a identifier for a user for the purposes of masking the user identification from a service provider 108, 110. In some instances, a new identifier may be created for the user address. In other instances, the identity manager 204 may determine that an identifier already exists for the user. For example, the identifier used for masking may have already been assigned to another identifier of the user. As another example, the identifier may be assigned to multiple additional identifiers for the same user (e.g., a user using multiple access providers and/or devices), each of which are mapped to the identifier. The same identifier may be used to access multiple service providers 108, 110. Alternately, different identifiers may be obtained for each service provider to mask the identity of the user from the service provider.

[0029] The identity manager 204 may then pass the identifier used for masking to an authentication manager 206 to authenticate the identifier. This may be done based on credentials received from access provider. Credentials may include tokens, cookies digital certificates, SIM authentication, or other types of tokens. In some instances, challenge responses may be sent to the user device to authenticate the user. After the identifier has been authenticated, the authentication manager 206 may then notify the identity manager 204 the identifier has been authenticated. Identity manager 206 may then transmit messages associated with the identifier, with an indicator the identifier has been authenticated.

[0030] In one embodiment, identity manager 204 may receive messages from access provider 102, mask the user identity, and send the messages with the masked identification to service provider 110. Identity manager 204 may also be used to route messages received from service provider 108, 110 to the user by replacing the masked identifier associated with

the messages with the user's identity for the access provider. Thus, when the masked identifier is mapped to multiple user identities for one or more access providers, the identity manager 204 may keep track of the current identifier to use to send messages.

[0031] In other embodiments, messages may be sent to an intermediary such as session/personalization manager 202, which may use identity manager 204 to obtain a masked identification for the user. Thus, identity provider 104 may optionally include session/personalization manager 202 or other type of intermediary to receive messages from access provider 102, obtain an masked identifier from identity manager 102, replace the access provider's identification of the user with the masked identifier, and send the message to the service provider 108, 110. As previously described, identity manager 102 may authenticate the masked identifier; thus, the session/personalization manager 202 (or other type of intermediary) may also send indications with the message(s) that the identifier used for masking has been authenticated. Session/personalization manager 202 or other type of intermediary may also be used to re-route messages received from service provider 108, 110 to the user by replacing the identifier with the access provider's identification of the user.

[0032] Session/personalization manager 202 may also be used to share user personalization information across multiple service providers 108, 110 and/or to perform session management in the event a user switches to a different access provider or uses a different device to access the service provider 108. A detailed description of how session management may be performed when a user roams (switches access provider) or uses a second device to access a service provider may be found in Application Serial No. XX/XXXX,XXX (Atty. Docket No. 021756-000900US), entitled "ROAMING ACROSS DIFFERENT ACCESS MECHANISMS AND NETWORK TECHNOLOGIES", the details of which are hereby incorporated by reference.

[0033] The identifier assigned to the user may be associated to a session for service provider 108, 110. Messages from the user to the service provider 108, 110 received over a predetermined period of time (the user session with the service provider) may then be associated to the session. Session manager 202 may evaluate the messages for session management information. The session management information may include data representing a state of the interaction between the user and the service provider, user preferences within a state or session , and/or other types of session information. As will be described in more detail below, session management information may be used to support

different types of roaming by the user (e.g., suspend and resume, connect/intermittently disconnected/disconnect, and multi-device roaming). Session/personalization manager 202 may use data storage 208 to store the session management information.

[0034] Additionally, session/personalization manager 202 may manage user personalization information. Session/personalization manager 202 may retrieve personalization information associated with the identifier from data storage 208. A subset of the personalization information may be sent to service provider 108, 110. In some instances, the subset may include all of the personalization information, while in other instances, only personalization information applicable to the service provider 108, 110 or for which the service provider 108, 110 is authorized to have, may be sent. In embodiments in which different identifiers for each service provider 108, 110 are provided to mask the user's identity, the personalization information may be mapped to all of the identifiers so that personalization information may be shared across multiple service providers 108, 110. Alternately, a subset of generic personalization information may be mapped to each of the multiple identifiers, while application-specific personalization information may only be mapped to the identifier for the service provider 108, 110 of the specific application.

[0035] Personalization information may include a variety of different types of information. For instance, personalization information may include generic user preferences, preferences or other personalization information related to applications, such as payment information or preferences (e.g., M-commerce, e-Wallet, or other information specifying the user preferences and accounts used to make payments), application settings, account information, contact/address book information, or other types of application specific information. Personalization information may also include information related to devices, such as device settings, unified messaging (UM) priority list on where/how to be contacted, or privacy rules). Other examples of personalization information include user credentials, user subscriptions to services including preferences and privacy settings, user devices (e.g., device characteristics / capabilities, device settings, device addresses, etc.), network / access mechanisms characteristics (e.g., multi-channel, multimodal, voice, etc.), and other types of information storing preferences or other information about the user. The user personalization information may be explicitly set or provided by the user. Alternately or additionally, session/personalization manager 202 may derive preferences or personalization information from messages sent between user and service providers 108, 110. In embodiments in which the session/personalization manager 202 derives personalization management, Platform for

Privacy Preferences (P3P) may be used for some applications to determine the type of information that is being transmitted by the messages.

[0036] Session/personalization manager 202 may send personalization information to a service provider 108, 110 at the time the user initiates a session with the service provider or at other times, such as during an on-going session, that preference information may be used to establish a context related to the user. The personalization information may also or alternately be sent in response to receiving a request form the service provider 108, 110. For example, the session/personalization manager 202 may have previously received one or more cookies associated with the identifier from a service provider 108, 110. Instead of forwarding the cookies to the user device, the session/personalization manager 202 may store the cookies in data storage 208. When the service provider requests the cookie(s), session/personalization manager 202 may retrieve the cookie(s) from data storage 208 and send the cookie(s) to the service provider 108, 110. Thus, session/personalization manger 202 may serve as a cookie proxy for the service provider. Other types of personalization information may also be sent at the service provider's 108, 110 request.

[0037] A variety of techniques may be used to ensure that the service provider 108, 110 only receives authorized personalization information. For example, a service provider may have access to personalization information indicating application settings, such as background color, but not have any access to identity information. Before sending personalization information, the session/personalization manager 202 may therefore determine whether the service provider 108, 110 is authorized to have the personalization information. Session/personalization manager 202 may request authorization from the user before sending information (e.g., via a "pop-up" message), or may consult rules (either default or set by the user) to determine what types of information may be sent. In some embodiments, service providers 108, 110 may have access to data storage 208, but the information may be filtered so that only authorized information may be viewed, retrieved, or modified by service provider 108, 110. Other mechanisms may also be used to prevent unauthorized accessing or sending of personalization information.

[0038] It should be appreciated that in alternate embodiments, the identity provider 104 may be different than that depicted in Fig. 2. For instance, identity provider 104 may not include an authentication manager 206 and may instead use an authentication manager provided by a third party. As another example, session/personalization manager 202 may be

separate components or may only provide either session or personalization management, but not both. As a third example, a different data storage may be used to store personalization information than the data storage used to store session management information. Other alternations are also contemplated.

[0039] One example embodiment in which a user may use identity provider 104 to mask identities is for interactions with a payment provider. The user may login to a merchant site using an identity manager, such as described with Fig. 1, to mask identity. After the user selects the items for purchase and is ready to pay, the merchant may send the user's masked identity to a payment provider. The merchant may also send other personalization, preference, or profile information. The payment provider may then use a protocol such as 3-Domain Secure protocol to obtain authentication for the user. In some embodiments, the identity manager may be used to authenticate the user. Thus, the payment provider may only know that the user has been authenticated and may not know the user identity, payment authorization, or account information. If needed, the payment provider may interact with the user through identity manager for confirmation or other information needed to authorize the transaction. Upon completion, payment provider may request that identity manager bill the account setup by the service provider. The identity provider 104 may then send the user a bill for the payment amount or may send the bill information to the access provider 102 for combination with the access provider bill. Alternately, the payment provider may send a bill notification to the user using identity manager (e.g., sending an email).

[0040] Fig. 3 illustrates an exemplary system 300 that may be used to support identification masking for a user when the user switches access providers. The user may switch from an access provider 302 to a second access provider 304 in a variety of circumstances. For instance, the user may be using a mobile device (e.g., mobile telephone) which roams to a different network. As another example, the user may switch from one type of access provider (e.g., from a General Packet Radio Service (GPRS) access provider) to a second type of access provider (e.g., a WiFi provider). The user may also switch access providers when switching from a first device to a second device that uses a different access provider to access a network. The user may also switch between access providers on various other occasions, such as when switching from one WiFi network to another or switching from WiFi to 3G or GPRS. Sometimes, when the user switches to a different access provider, the identity of the user for the different access providers may stay the same. By way of example, when roaming from one MNO network to a second MNO network, the user's identification (e.g., the

MSISDN number) remains the same. In other instances, the user may change identities, such as when switching devices or switching to a different type of access provider.

[0041] FIG. 3 illustrates an embodiment in which both access providers 302, 304 use the same identity provider 306 to provide identity management. After the user has switched access providers 302, 304, the identity manager 306 receives one or more message(s) for service provider 310 from the second access provider. If the user identity for the second access provider has not changed from the identity for the first access provider, the identity manager 306 may continue to disassociate the access providers' identification of the user from messages sent from the user to the service provider 310 and associate the masked identifier mapped to the access provider's identification of the user (which was obtained when messages were received from access provider 302) with the messages. Messages sent from service provider 310 to the identifier are routed to the user via the second access provider 304 using the access provider's identification of the user.

[0042] In many instances, the user's identity will change when switching from the first access provider 302 to the second address provider 304. In some embodiments, the access providers 302, 304 may be members of a federation in which the access providers 302, 304 have agreed that authentication for user identity for one member (access provider 302) will serve as authentication for an identity maintained by a different member (access provider 304). Thus, identity provider 104 (e.g., in an identity manager 204 component) may maintain a mapping of the identifiers a user has with various access providers 302, 304. As the identity provider 104 maintains this information, the access providers 302, 304 may not know the identities the user has with other access providers. The user may also provide some of the mappings to identity provider 306.

[0043] After receiving a message associated with a third identifier of a user (the identifier used by a second access provider) via the second access provider 304, the identity provider 306 determines the third identifier is mapped to the first identifier associated with messages received from the first access provider 302. The identity provider 306 then disassociates the third identifier from the message and associates the second message with the masked identifier which was mapped to the first identifier. The message associated with the masked identifier is then sent to service provider 310.

[0044] In some embodiments, the user may switch devices, but use the same access provider. In those embodiments, the messages associated with the third identifier may have

been sent from the same access provider. The identity provider 306 may use mappings to determine the masked identifier associated with the first identifier should also be used to mask the identity of the third identifier. Additionally, as was previously described, in some embodiments, identity provider 306 may also provide session and/or personalization management. When the user switched access providers 302, 304 (or switched to a different address), the connection to service provider 310 may have been terminated. After the connection has been re-established by the second access provider, the identity provider 306 may determine the masked identifier is associated with a session with the service provider. The identity provider 306 may then send (or otherwise make available) session management information to the service provider 310. Thus, the user may resume interactions with the service provider 310 at the same, or close to the same, state as when the connection was terminated.

[0045] Fig. 4 illustrates a second exemplary embodiment of a system 400 that may be used to support identification masking for a user when the user switches access providers. In this embodiment, the access providers 402, 404 use different identity providers 406, 408. The access providers 402, 404 may have a federation agreement that allows identity providers 406, 408 to have access to mapping information which associates the identities a user has with various access providers 302, 304. The system includes a data storage 410 which is reachable by both access providers 402, 404. The data storage 410 may be used to store mappings between the user's identities with various access providers to one or more masked identifiers used for interacting with service providers.

[0046] After identity provider 406 has obtained a masked identifier for a first identifier associated with access provider 402, the identity provider 406 may store the mapping from the first identifier to the masked identifier in data storage 410. Thus, when the second identity provider 408 receives a message from access provider 404 associated with the third identifier (used by the second access provider), it may first consult the data storage 410 to determine if a masked identifier has been assigned to the third identifier. In some embodiments, the data storage 410 may also map different identities that the user has with different access providers 402, 404. In these embodiments, a search for a masked identifier associated with the third identifier may return the masked identifier assigned to the first identifier (used by the first access provider). Alternately, access provider 404 may search data storage using all the different identities associated with the third identifier of the user. The access provider 404 may then use the same masked identifier mapped to the first

identifier to mask the third identification of the user from transactions with the service provider 412.

[0047] In addition to the mappings which map the masked identifiers assigned by identity providers 406, 408 to identities a user has with one or more access providers 402, 404, data storage 410 or a different data storage may also store session or personalization information mapped to the identifier. Thus, identity provider 408 may send the session and personalization information to service provider 412 as needed or requested. Alternately, identity providers 406, 408 may not have direct access to the session/personalization information stored by the other identity provider. In these embodiments, the second identity provider 408 may request that the first identity provider 406 send the session and personalization information to the second identity provider 408 or to the service provider 412.

[0048] Fig. 5 illustrates exemplary wireless networks with may be accessed by a user via an access provider. Wireless network technologies include wireless wide area network (WWAN), wireless local area network (WLAN) and wireless personal area network (WPAN) technologies. WWAN technologies typically include cellular and related technologies such as GSM, GPRS, CDPD, CDMA, TDMA, WCDMA, etc. WWAN networks are high power, long range networks that typically have an access range on the order of several kilometers on up. WLAN technologies, on the other hand, are medium power, medium range networks that have an access range on the order of tens of meters while WPAN networks are low power, short range networks that typically have an access range of about 10 meters or less. Examples of WLAN technologies include the IEEE 802.11(a), (b), (e) and (g) technologies and examples of WPAN technologies include Bluetooth, HomeRF, IrDA and IEEE 802.15 technologies. It should be appreciated that networks, other than wireless networks, may be made accessible to a user via an access provider.

[0049] Figure 6 illustrates one embodiment of a computer system 600 upon which a identity provider (or components of an identity provider) may be implemented. The computer system 600 is shown comprising hardware elements that may be electrically coupled via a bus 655. The hardware elements may include one or more central processing units (CPUs) 605; one or more input devices 610 (e.g., a mouse, a keyboard, etc.); and one or more output devices 615 (e.g., a display device, a printer, etc.). The computer system 600 may also include one or more storage device 620. By way of example, storage device(s) 620 may be 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.

[0050] The computer system 600 may additionally include a computer-readable storage media reader 625; a communications system 630 (e.g., a modem, a network card (wireless or wired), an infra-red communication device, etc.); and working memory 640, which may include RAM and ROM devices as described above. In some embodiments, the computer system 600 may also include a processing acceleration unit 635 , which can include a DSP, a special-purpose processor and/or the like

[0051] The computer-readable storage media reader 625 can further be connected to a computer-readable storage medium, together (and, optionally, in combination with storage device(s) 620) comprehensively representing remote, local, fixed, and/or removable storage devices plus storage media for temporarily and/or more permanently containing computer-readable information. The communications system 630 may permit data to be exchanged with a network and/or any other computer.

[0052] The computer system 600 may also comprise software elements, shown as being currently located within a working memory 640, including an operating system 645 and/or other code 650, such as an application program. The application programs may implement an identity provider, components of the identity provider, and/or the methods of the invention. It should be appreciate that alternate embodiments of a computer system 600 may have numerous variations from that described above. For example, customized hardware might also be used and/or particular elements might be implemented in hardware, software (including portable software, such as applets), or both. Further, connection to other computing devices such as network input/output devices may be employed.

[0053] Fig. 7 illustrates an exemplary method that may be used to mask user identification. The method may begin by receiving 702 a message for a service provider. The message is associated with a first user identifier and may be received from an access provider which provides a user device access to a network. A second identifier, which will be used to mask the user identity, is obtained 704. The second identifier may be obtained 704 by an identity provider (e.g., an identity manager 204 component). The second identifier may have been previously obtained and mapped to the first identifier or a third identifier mapped to the first identifier, which is also associated with the user. Alternately, a new identifier may be created and used for the second identifier.

[0054] The first identifier associated with the message is disassociated 706 from the message and the obtained second identifier is associated 708 with the message in its place. Thus, the second identifier may be used to route messages back to an identity provider, which will replace the second identifier with the first identifier and send to the access provider for forwarding to the user. After the second identifier has been associated with the message, the message is sent 710 to the service provider.

[0055] In some embodiments, session and/or personalization information may also be retrieved 712. The session information may have been session information for a session associated with the obtained second identifier. The session information may be sent 714 to the service provider so that the user may resume interactions with the session provider in the previous state indicated by the session information. Personalization information may also be sent 714 to the service provider which specifies user preferences, device capabilities, and other user personalization information. Alternately, the service provider may have access to personalization information (or a subset of the personalization information) associated with the identifier.

[0056] Fig. 8 illustrates an exemplary method that may be used to perform identity management when a user switches access providers. Subsequent to the receipt 702 of one or more messages from a first access provider, a message may be received 802 from a second access provider. The message may be associated with the same user identifier that is used by the first access provider. For example, this may occur when the user roams to a different network or switches to a different device which uses a different access provider to access the network. Alternately, the third identifier of the user associated with the message received from the second access provider may different from the first identifier associated with messages received from the first access provider. After the message has been received 802, a determination may be made that the third identifier is mapped to the first identifier associated with messages received 702 from the first access provider.

[0057] The third identifier is disassociated 806 from the message. The masked identifier obtained 704 for the messages associated with the first identifier is associated with the message from the second access provider. The message is then sent 801 to the service provider. Optionally, session and/or personalization information may also be sent 812.

[0058] In the foregoing description, for the purposes of illustration, methods were described in a particular order. It should be appreciated that in alternate embodiments, the

methods may be performed in a different order than that described. Additionally, the methods may include fewer, additional, or different blocks than those described. It should also be appreciated that the methods described above may be performed by hardware components or may be embodied in sequences of machine-executable instructions, which may be used to cause a machine, such as a general-purpose or special-purpose processor or logic circuits programmed with the instructions to perform the methods. These machine-executable instructions may be stored on one or more machine readable mediums, such as CD-ROMs or other type of optical disks, floppy diskettes, ROMs, RAMs, EPROMs, EEPROMs, magnetic or optical cards, flash memory, or other types of machine-readable mediums suitable for storing electronic instructions. Alternatively, the methods may be performed by a combination of hardware and software.

[0059] While illustrative and presently preferred embodiments of the invention have been described in detail herein, it is to be understood that the inventive concepts may be otherwise variously embodied and employed, and that the appended claims are intended to be construed to include such variations, except as limited by the prior art.

WHAT IS CLAIMED IS:

1. A method comprising:

receiving, from an access provider, a message for a service provider, the message associated with a first identifier of a user of the access provider;

obtaining a second identifier;

disassociating the first identifier from the message;

associating the message with the second identifier; and

sending the message associated with the second identifier to the service provider.

2. The method of claim 1, further comprising:

receiving a second message, associated with the second identifier, from the service provider;

disassociating the second identifier from the second message;

associating the first identifier with the second message;

sending the second message associated with the first identifier to the access provider.

3. The method of claim 1, further comprising:

retrieving personalization information associated with the second identifier;

sending a subset of the personalization information to the service provider.

4. The method of claim 3, wherein sending the personalization information is in response to receiving a request from the service provider to access the portion of the personalization information.

5. The method of claim 4, wherein receiving the request from the service provider comprises receiving a request from the service provider to obtain a cookie, the request associated with the second identifier.

6. The method of claim 3, wherein sending the personalization information comprises receiving authorization from the user to send the personalization information.

7. The method of claim 3, wherein sending the personalization information comprises determining the personalization information may be shared with the service provider.

8. The method of claim 3, wherein the personalization information comprises one or more of user preferences related to the service provider and generic user preferences.

9. The method of claim 3, wherein the personalization information comprises account information.

10. The method of claim 3, wherein the personalization information comprises payment information.

11. The method of claim 3, wherein the personalization information comprises application settings.

12. The method of claim 3, further comprising:

receiving, from the access provider, a second message for a second service provider, the second message associated with the first identifier;

disassociating the first identifier from the second message;

associating the second message with the second identifier;

sending the second message associated with the second identifier to the second service provider; and

sending a second subset of the personalization information to the service provider.

13. The method of claim 3, further comprising:

receiving, from the access provider a second message for a second service provider, the second message associated with the first identifier;

disassociating the first identifier from the second message;

obtaining a third identifier;

associating the second message with the third identifier;

sending the second message associated with the third identifier to the second service provider; and

sending a second subset of the personalization information to the service provider.

14. The method of claim 1, further comprising:

receiving personalization information;

associating the personalization information with the second identifier; and

storing the personalization information associated with the second identifier.

15. The method of claim 14, wherein receiving personalization information comprises receiving personalization information from the user.

16. The method of claim 14, wherein receiving personalization information comprises receiving a cookie from the service provider.

17. The method of claim 14, wherein receiving personalization information comprises receiving one or more of user device characteristics, user device capabilities, user device settings, and user device addresses.

18. The method of claim 14, wherein receiving personalization information comprises receiving at least one user preference.

19. The method of claim 1, further comprising:

associating a session to the second identifier;

associating the message to the session;

evaluating the message for session management information, the session management information including data representing a state of the interaction between the user and the service provider;

receiving one or more additional messages, from the access provider, for the service provider, the one or more additional messages associated with the first identifier;

for each of the additional messages for the service provider, received from the access provider associating the additional messages to the session, and evaluating each of the additional messages for session management information; and

storing the session management information.

20. The method of claim 19, further comprising:

receiving, from a second access provider, a second message for the service provider, the second message associated with a third identifier for the user;

determining the third identifier is mapped to the first identifier;

disassociating the third identifier from the message;

associating the second message with the second identifier; and

sending the second message associated with the second identifier to the service provider.

21. The method of claim 20, further comprising:

determining the second identifier is associated with the session;

retrieving the session management information associated with the session; and

sending the session management information to the service provider.

22. The method of claim 1, further comprising:

receiving, from a second access provider, a second message for the service provider, the second message associated with a third identifier for a user;

determining the third identifier is mapped to the first identifier;

disassociating the third identifier from the message;

associating the second message with the second identifier; and

sending the second message associated with the second identifier to the service provider.

23. The method of claim 22, wherein receiving the message for the service provider comprises receiving the message at a first identity provider, and wherein receiving the second message for the service comprises receiving the second message at a second identity provider, and wherein determining the third identifier is mapped to the first identifier comprises accessing, from the second identity provider, a data storage including user identification mappings mapping user addresses for the first access provider to user addresses for the second access provider.

24. The method of claim 1, wherein obtaining the second identifier comprises determining the first identifier is mapped to the second identifier.

25. The method of claim 1, wherein obtaining the second identifier comprises obtaining a new identification for the user

26. The method of claim 1, further comprising:

authenticating the second identifier; and

wherein sending the message comprises sending the message with an indication the second identifier has been authenticated.

27. The method of claim 1, wherein receiving the message comprises receiving the message from a mobile network operator (MNO).

28. The method of claim 27, wherein first identifier is an MSISDN.

29. The method of claim 1, wherein receiving the message from the access provider comprises receiving the message from a wireless network provider.

30. The method of claim 29, wherein the wireless network provider is one of a provider of General Packet Radio Service (GPRS), WiFi, 2.5G, FOMA, UMTS, CDMA, and EDGE.

31. The method of claim 1, wherein the service provider is a payment provider, the method further comprising:

receiving a request to authorize a payment amount, the request associated with the second identifier;

providing the authorization to the payment provider.

32. The method of claim 31, further comprising transmitting the payment amount to the access provider.

33. A method comprising:

receiving, from a mobile network operator, a message for a service provider, the message associated with a MSISDN of a user;

obtaining an identifier;

authenticating the identifier;

disassociating the MSISDN from the message;

associating the message with the identifier;

sending the message associated with the identifier to the service provider with an indication the identifier has been authenticated; and

sending personalization information indicating preferences of the user to the service provider.

34. A method comprising:

receiving, from a service provider, a message for a user, the message associated with the a first identifier;

determining the first identifier is mapped to a second identifier of the user for an access provider;

disassociating the first identifier from the message;

associating the second identifier with the second message;

sending the second message associated with the first identifier to the access provider.

35. A system comprising:

an identity component, configured to disassociate a first identifier of a user from a message received from an access provider, obtain a second identifier for the user; and to associate the second identifier with the message;

an authentication component, configured to authenticate the second identifier, and to associate an indication with the message the second identifier has been authenticated;

a communications interface to send the message associated with the second identifier and the indication to the service provider.

36. The system of claim 35, wherein the identity manager further comprises:

a personalization manager to track user personalization information and to send at least a subset of the personalization information to the service provider; and

data storage to store the personalization information.

37. The system of claim 35, further comprising:

a session manager to track session management information, the session management information including information indicating a state of the interaction between the user and the service provider; and

a data storage to store the session management information.

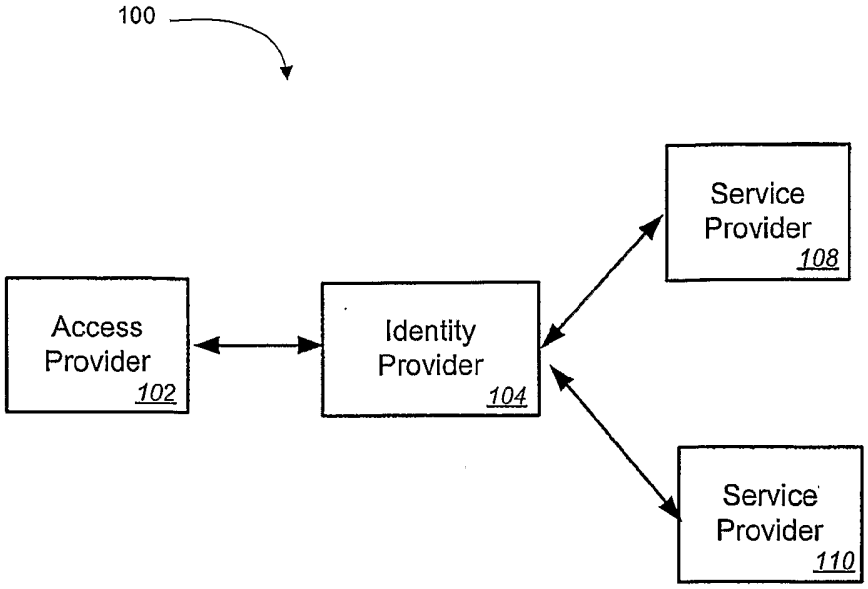

100
Service Provider 108
Access Provider 102
Identity Provider 104
Service Provider 110

Fig. 1

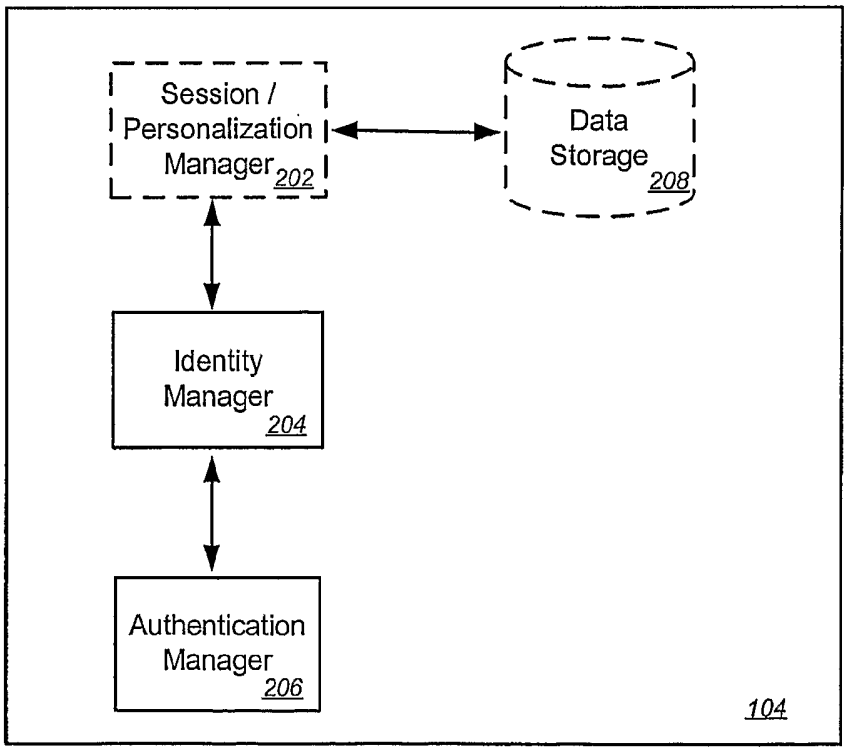

Session / Personalization Manager 202
Data Storage 208
Identity Manager 204
Authentication Manager 206
104

Fig. 2

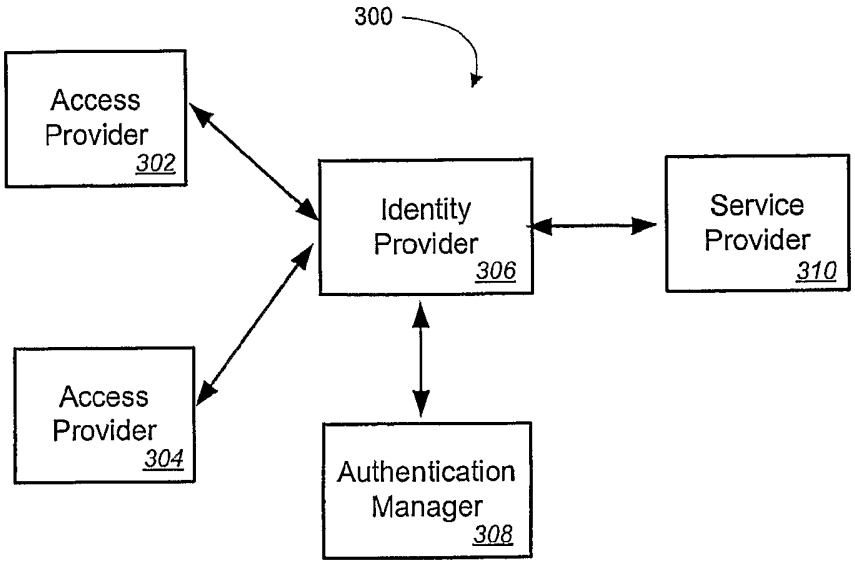

300
Access Provider 302
Identity Provider 306
Service Provider 310
Access Provider 304
Authentication Manager 308

Fig. 3

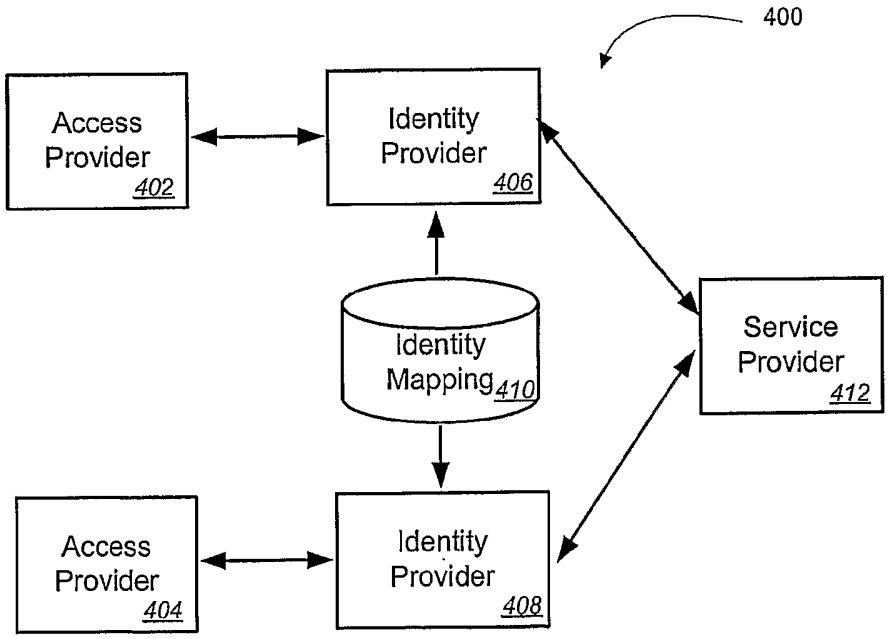

400
Access Provider 402
Identity Provider 406
Service Provider 412
Identity Mapping 410
Access Provider 404
Identity Provider 408

Fig. 4

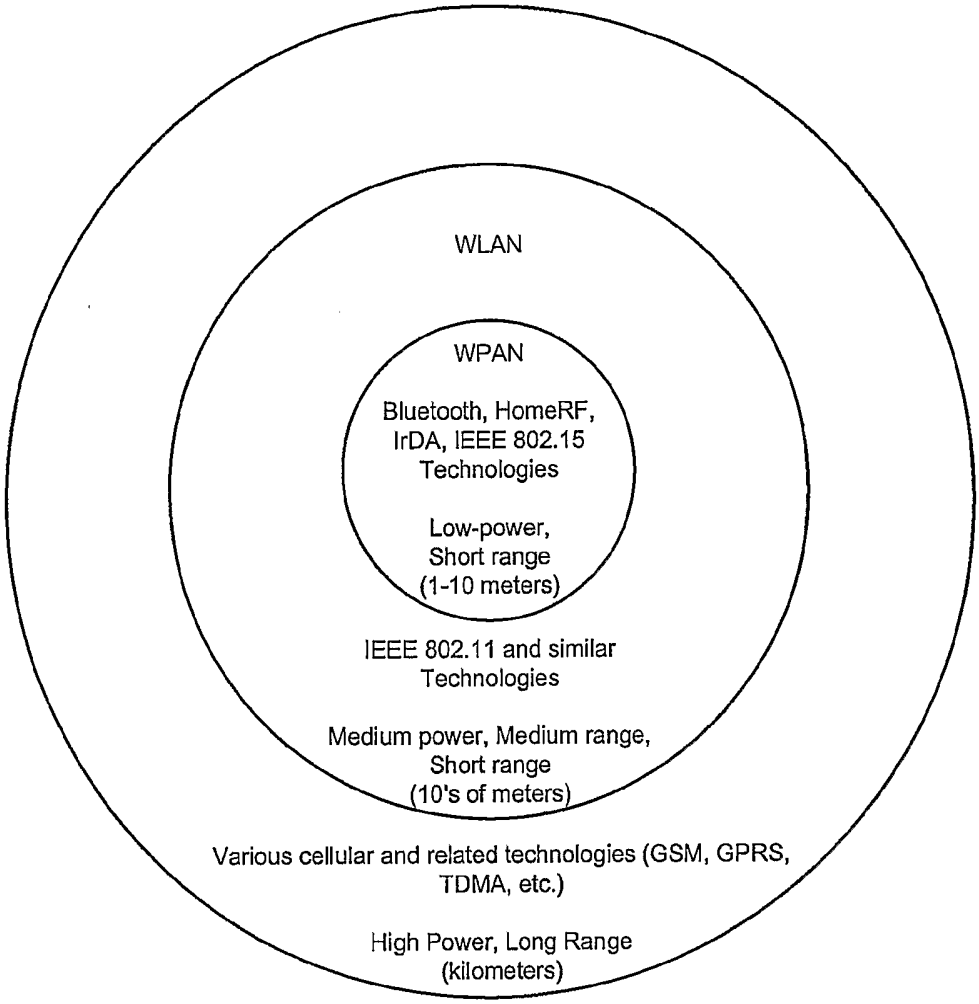

WLAN
WPAN
Bluetooth, HomeRF, IrDA, IEEE 802.15 Technologies
Low-power, Short range (1-10 meters)
IEEE 802.11 and similar Technologies
Medium power, Medium range, Short range (10's of meters)
Various cellular and related technologies (GSM, GPRS, TDMA, etc.)
High Power, Long Range (kilometers)

Fig. 5

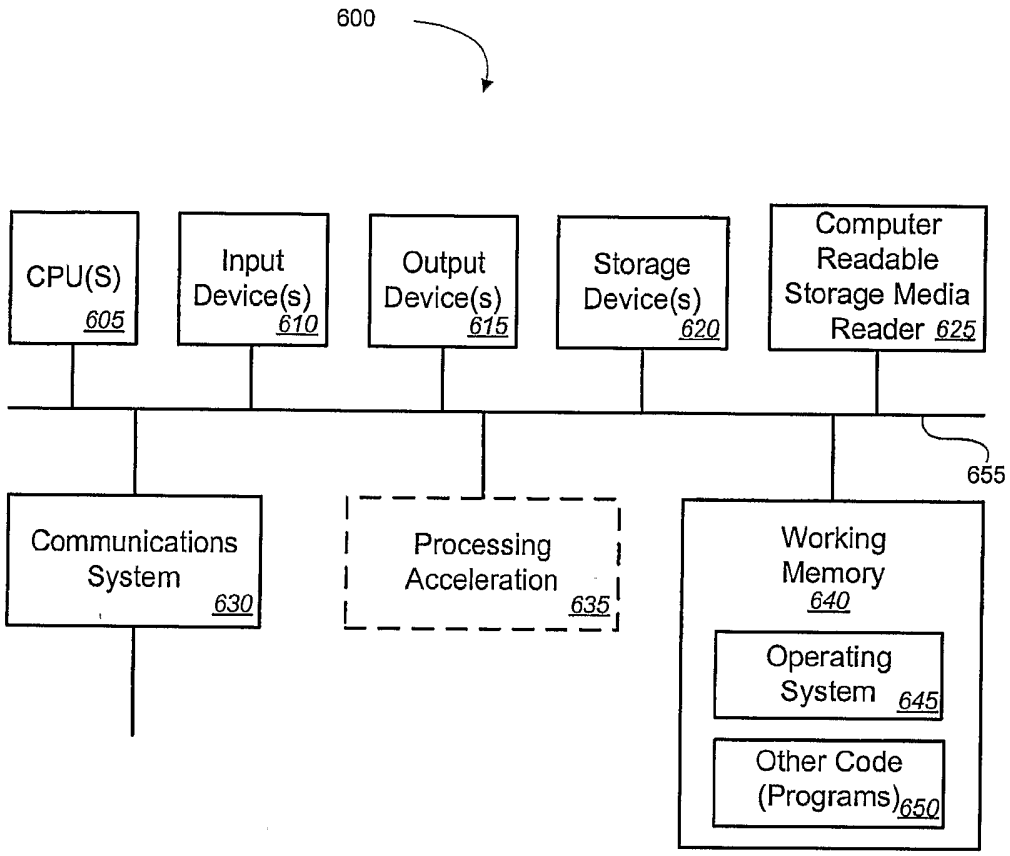

600
CPU(S)
605
Input
Device(s)
610
Output
Device(s)
615
Storage
Device(s)
620
Computer
Readable
Storage Media
Reader 625
655
Communications
System
630
Processing
Acceleration
635
Working
Memory
640
Operating
System 645
Other Code
(Programs) 650

Fig. 6

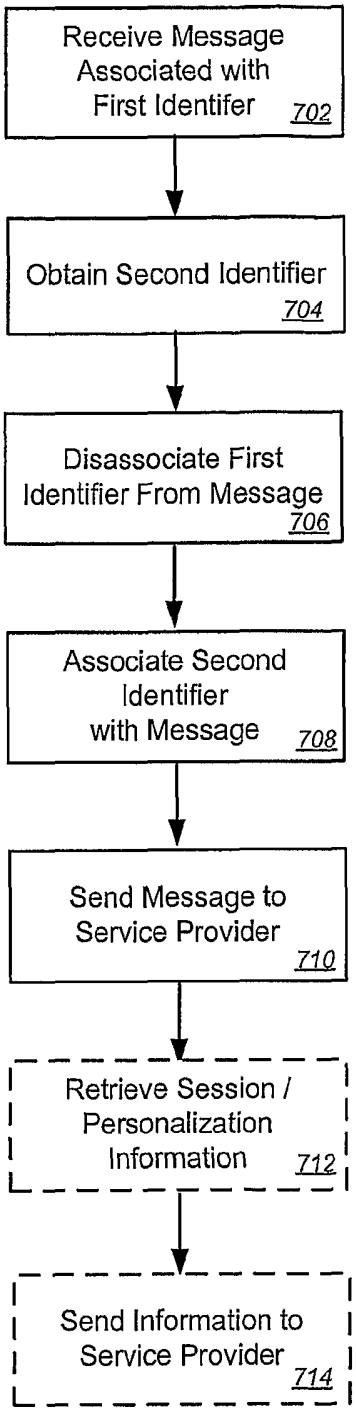

Receive Message Associated with First Identifer 702
Obtain Second Identifier 704
Disassociate First Identifier From Message 706
Associate Second Identifier with Message 708
Send Message to Service Provider 710
Retrieve Session / Personalization Information 712
Send Information to Service Provider 714

Fig. 7

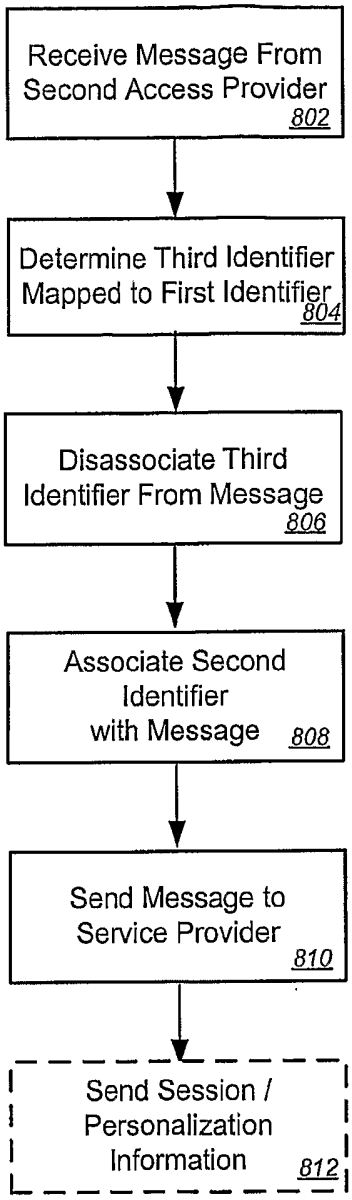

Receive Message From Second Access Provider
802
Determine Third Identifier Mapped to First Identifier
804
Disassociate Third Identifier From Message
806
Associate Second Identifier with Message
808
Send Message to Service Provider
810
Send Session / Personalization Information
812

Fig. 8

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US2004/037461

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00 H04L29/06 H04L29/12

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)
IPC 7 G06F H04L

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

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 02/102016 A (KONINKLIJKE KPN N.V; ERGEZINGER, SIEGRIED; KEISINGER; THIERBACH, HEIKO) 19 December 2002 (2002-12-19) page 7, line 13 - page 10, line 12 page 19, line 26 - page 21, line 7 page 22, line 20 - page 24, line 14	1-37
X	WO 02/33516 A (SAFEWEB, INC) 25 April 2002 (2002-04-25) abstract page 9, line 15 - page 11, line 4 page 22, line 17 - page 23, line 11 page 14, line 12 - page 16, line 28	1-37

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in 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 document 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 another 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	Date of mailing of the international search report
23 February 2005	02/03/2005

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Horn, M.P.

3

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US2004/037461

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 01/65380 A (IPRIVACY LLC) 7 September 2001 (2001-09-07) abstract	1,2,24, 25,34
Y	page 3, line 6 - page 4, line 1	3-23, 26-33, 35-37
Y	US 2003/140225 A1 (BANKS DAVID MURRAY ET AL) 24 July 2003 (2003-07-24) abstract paragraph '0007! - paragraph '0046!	3-23, 26-33, 35-37

3

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US2004/037461

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 02102016 A	19-12-2002	DE 10154546 A1	15-05-2003
		EP 1253760 A1	30-10-2002
		WO 02102016 A2	19-12-2002
		EP 1386470 A2	04-02-2004
		US 2004139204 A1	15-07-2004
		EP 1263187 A2	04-12-2002
		US 2002156732 A1	24-10-2002
WO 0233516 A	25-04-2002	US 2004230820 A1	18-11-2004
		AU 3038802 A	29-04-2002
		WO 0233516 A2	25-04-2002
WO 0165380 A	07-09-2001	AU 4177701 A	12-09-2001
		WO 0165380 A1	07-09-2001
		US 2001034709 A1	25-10-2001
US 2003140225 A1	24-07-2003	GB 2372344 A	21-08-2002
		EP 1362318 A1	19-11-2003
		WO 02067158 A1	29-08-2002