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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 December 2012 (20.12.2012)

WIPO | PCT

(10) International Publication Number
WO 2012/174354 A1

(51) International Patent Classification:
H04W 12/06 (2009.01)

(21) International Application Number:
PCT/US2012/042629

(22) International Filing Date:
15 June 2012 (15.06.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
13/161,028 15 June 2011 (15.06.2011) US

(71) Applicant *(for all designated States except US)*: **ORACLE INTERNATIONAL CORPORATION** [US/US]; 500 Oracle Parkway, M/S 5op7, Redwood Shores, California 94065 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **POLLOCK, Jason** [CA/NZ]; 3 Monowai Road, Johnsonville, Wellington, 6037 (NZ).

(74) Agents: **MEYER, Sheldon, R.** et al.; Fliesler Meyer LLP, 650 California Street, Fourteenth Floor, San Francisco, California 94108 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, 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, 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).

Published:

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

(54) Title: SYSTEMS AND METHODS OF INTEGRATING OpenID WITH A TELECOMMUNICATIONS NETWORK

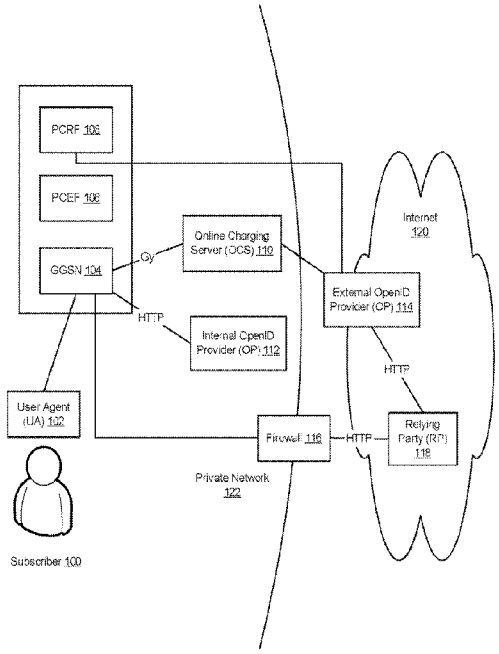

FIGURE 1

(57) Abstract: A solution is described which allows mobile devices to specify that certain sites are allowed to be logged into based on the device credentials alone. The solution integrates OpenID with a telecommunications network in order to verify the user's identity. This verification is based on the trust that the telecom carrier has to identify the subscriber at the GGSN. The solution splits the OpenID Provider (OP) into two systems - an internal OP and an external OP. The external OP can reside in the public network and can allow the user to authenticate with a password. The internal OP resides in the private network of the carrier and is directly connected to the GGSN such that it is only reachable from the GGSN.

WO 2012/174354 A1

SYSTEMS AND METHODS OF INTEGRATING OpenID WITH A TELECOMMUNICATIONS NETWORK

FIELD OF THE INVENTION

[0001] The current invention relates generally to mobile communications and telecommunication networks and in particular to authenticating mobile devices in telecommunication networks.

BACKGROUND

[0002] In recent years, people have been accessing Internet services more and more frequently from their mobile devices. For example, smart phones, tablets, personal digital assistants (PDAs) and other handheld computers have now become almost fully integrated with most Web sites and can access a wide variety of services on the Internet. Many of these services require the subscriber of a mobile device to be authenticated, such as by assigning a username, password to the user. However, due to the compact size and limited keyboard capabilities of such devices, it can be quite unpleasant for a subscriber to enter a username and password or other authentication information using the device.

[0003] There have been numerous standards proposed, some of which attempt to at least partially address the authentication issues for mobile devices. One such existing standard is Generic Bootstrapping Architecture (GBA), which allows applications on the handset to authenticate themselves to a network service, using the SIM card to provide authentication. Under this standard, users can be authenticated if they own a valid identity on a Home Location Register (HLR) or a Home Subscriber Server (HSS). The authentication is

based on a shared secret key, where one key is located in the user's mobile phone and the other is on the HLR/HSS.

[0004] Another standard entitled OpenID has attempted to reduce the number of identities that each owner possesses by allowing users to consolidate their digital identities. Under this open standard, users can be authenticated in a decentralized manner. For example, when a user agent (UA) invokes a particular service, that service can query an open ID provider (OP) which will authenticate the user agent on behalf of the service that is relying on the OP. In this manner, the relying party or service can ensure that the user is authenticated based on a shared secret, which has been previously established between the relying party and the OP.

[0005] Even in light of such standards, a number of limitations and shortcomings are still left unaddressed. For example, most common authentication mechanism for OpenID implementations remains a username and password combination, which can be burdensome on mobile subscribers due to the reasons previously mentioned. At least one solution integrating OpenID with GBA has been proposed, however it is quite likely that such a solution would require the telecommunication companies to buy additional network hardware, require application developers to modify their code and also require the handset unit to change as well. Not surprisingly, solutions that require such a change in the entire ecosystem of the telecommunications network have not been able to gain significant traction.

[0006] Telecommunications companies and mobile network operators (MNOs) already have a trust relationship with the mobile device and the subscriber. It would be desirable to export that trust relationship from the handset to Internet services. It would also be advantageous to export this trust while minimizing the number changes among the numerous entities that are involved and while addressing the deficiencies mentioned above. Applicant has identified these, as well as other needs that currently exist in the art in coming to conceive the subject matter of the present disclosure.

SUMMARY OF INVENTION

[0007] In accordance with various embodiments, a solution is described which allows a user of a mobile device to specify that certain sites are allowed to be logged into based on the device credentials alone. The solution integrates OpenID with a telecommunications network in order to verify the user's identity. This verification is based on the trust that the telecom carrier has and can use to identify the mobile device and the subscriber at the Gateway GPRS Support Node (GGSN).

[0008] The process for identifying the subscriber is based on splitting an OpenID provider (OP) into two systems, an internal OP and an external OP. The external OP can reside in the public network and can allow the user to authenticate with a password. The internal OP resides in the private network of the carrier and is directly connected to the GGSN such that it is only reachable from the GGSN. The process for identifying the subscriber begins when a mobile device (user agent) invokes a relying party (RP) service. The RP can query an external OP, requesting a validation uniform resource locator (URL) for the subscriber. The RP redirects the user agent (UA) to a validation URL on the internal OP provider. The internal OP can validate the subscriber by IP address or if the subscriber elects, a user name and password. The internal OP redirects the US back to an accepted URL provided by the RP. The RP can then validate the response with the external OP.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] FIGURE 1 is a system-level illustration of integrating the OpenID with a telecommunication network, in accordance with various embodiments of the invention.

[0010] FIGURE 2 is an illustration of a page presented to a UA once it is redirected to the internal OP, in accordance with various embodiments of the invention.

[0011] FIGURE 3 is a flow chart illustration of integrating OpenID with a telecommunications network, in accordance with various embodiments of the invention.

[0012] FIGURE 4 is a sequence diagram of integrating OpenID with the telecom network, in accordance with various embodiments of the invention.

DETAILED DESCRIPTION

[0013] The invention is illustrated by way of example and not by way of limitation in the figures of the accompanying drawings in which like references indicate similar elements. References to embodiments in this disclosure are not necessarily to the same embodiment, and such references mean at least one. While specific implementations are discussed, it is understood that this is done for illustrative purposes only. A person skilled in the relevant art will recognize that other components and configurations may be used without departing from the scope and spirit of the invention.

[0014] In the following description, numerous specific details are set forth to provide a thorough description of the invention. However, it will be apparent to those skilled in the art that the invention may be practiced without these specific details. In other instances, well-known features have not been described in detail so as not to obscure the invention.

[0015] In accordance with various embodiments described throughout this disclosure, a solution is described to enable a user of a mobile device to specify that certain sites are allowed to be logged in based on the device credentials alone. The solution integrates OpenID with a telecommunications network in order to verify the user's identity. This verification is based on the trust that the telecom carrier has and can use to identify the mobile device and the subscriber at the Gateway GPRS Support Node (GGSN).

[0016] Currently, OpenID often requires the user to log in using a username and password. A typical OpenID flow can work as follows:

1. The user agent (UA) invokes a relying party (RP), providing an identifier
2. The RP queries the OpenID provider (OP), requesting the validation uniform resource locator (URL) for the subscriber
3. The RP redirects the UA to the validation URL on the OP

4. The OP validates the subscriber by any means, typically a username/password combination
5. The OP redirects the UA back to the "accepted" URL provided by the RP.
6. The RP validates the response with the OP.

[0017] A change in this situation can utilize the trust that the carrier has that they can identify the phone (and therefore the subscriber) at the Gateway General Packet Radio Service Support Node (GGSN). If the GGSN can identify the subscriber, it should be able to export that trust to the RP. In order to export this trust, the Open ID flow can become the following:

1. The UA invokes the RP, providing an identifier
2. The RP queries an external OpenID provider (OP), requesting the validation URL for the subscriber
3. The RP redirects the UA to the validation URL on the Internal OP
4. The internal OpenID provider (OP) validates the subscriber by IP address, or if the subscriber has elected, a username/password
5. The internal OP redirects the UA back to the "accepted" URL provided by the RP
6. The RP validates the response with the external OP.

[0018] FIGURE 1 is a system-level illustration of integrating the OpenID with a telecommunication network, in accordance with various embodiments of the invention. Although this diagram depicts components as logically separate, such depiction is merely for illustrative purposes. It will be apparent to those skilled in the art that the components portrayed in this figure can be combined or divided into separate software, firmware and/or hardware. Furthermore, it will also be apparent to those skilled in the art that such components, regardless of how they are combined or divided, can execute on the same computing device or can be distributed among different computing devices connected by one or more networks or other suitable communication means.

[0019] As illustrated, the OpenID provider (OP) can be split into two separate systems, an internal OP 112 and an external OP 114. The term network can encompass at least two separate networks – the public network (e.g. Internet) 120 accessible to all entities; and the internal private network 122 of the telecom provider. Access to the private network is controlled and it is usually separated from the public network by way of a firewall 116 or other security measures. The external OP can reside in the public network and can allow the subscriber 100 to authenticate with a password. The internal OP resides in the private network of the carrier and is directly connected to the GGSN 104 such that it is only reachable from the GGSN. The process for identifying the subscriber begins when a mobile device (UA 102) invokes a relying party (RP) service 118. The RP can query an external OP 114, requesting a validation URL for the subscriber. The RP redirects the user agent (UA) to a validation URL on the internal OP provider 112. The internal OP can validate the subscriber by IP address or if the subscriber elects, a user name and password. The internal OP redirects the UA back to an accepted URL provided by the RP 118. The RP can then validate the response with the external OP.

[0020] In accordance with an embodiment, the GGSN can employ a Policy Control Rule Function (PCRF) 108 and a Policy Control Enforcement Function (PCEF) 106 to apply policies to the communications involving the carrier's subscribers. These components encompass Service Data Flow (SDF) detection, policy enforcement and flow-based charging functionalities. In addition, the GGSN can connect to an online charging server (OCS) 110, which is a system for allowing communication service providers to charge their subscribers in real time, based on service usage. Some (or all) of these components can play a roll in controlling access to the internal OP, as will be described in more detail later in this document.

[0021] FIGURE 2 is an illustration of a page presented to a UA once it is redirected to the internal OP, in accordance with various embodiments of the invention. It should be noted that

this page is only an example and should not be construed to restrict all of the embodiments to require a user name and password combination upon first login.

[0022] As illustrated, on the internal OP, when the user agent (UA) is redirected there, the UA can be presented with a page to authenticate with a username and password combination. This page can also include an option to allow the device to log in without a password in the future. The UA is asked for a username/password. They are also given the option of allowing future logins from the device to that service to be password-free. In accordance with an embodiment, the UA will always be prompted for a password the first time the service is used, and the UA can elect to enable or disable the password-free login at any time.

[0023] In accordance with an embodiment, in order to allow password-free authentication, access to the Internal OP must be protected. Otherwise, if the Internal OP is accessible from any device other than the GGSN, it may be possible for a third party to emulate the UA and gain access to the RP.

[0024] In accordance with an embodiment, the solution can rely on splitting the OP into two systems. An External OP behaves as a regular OP, allowing the user to authenticate with a password. An Internal OP, on the other hand, is directly connected to the GGSN, and only reachable from the GGSN. Since the Internal OP is only reachable from the GGSN, it reduces the authentication problem to one of access control to the Internal OP. In accordance with various embodiments, the following are several methods of performing this access control:

1. The PCEF/PCRF on the GGSN is able to perform deep packet inspection (DPI), and able to perform validation on specific parts of the URL.
2. The PCEF/PCRF are able to receive real-time rule updates with specified IP address and ports.
3. The GGSN is able to initiate a new charging session for all connections to a specific IP address.

[0025] Deep Packet Inspection

[0026] In accordance with an embodiment, if the PCEF/PCRF are able to perform DPI, the Mobile Station International Subscriber Directory Number (MSISDN) for the subscriber is encoded into the request to the OP. The PCEF can then validate that URL, discarding all requests that do not contain an MSISDN which matches the subscriber profile. If the subscriber has previously decided that the UA is allowed to have device-authenticated access to the RP, the Internal OP will then return a success response.

[0027] Real Time Rule Updates

[0028] In accordance with an embodiment, if the PCEF/PCRF are able to perform real-time updates, the External OP will allocate a port on the Internal OP. It will then construct a rule for the UA's MSISDN, allowing access to that port, passing this rule to the PCRF. The PCRF will update the PCEF, and then report success back to the External OP. The External OP will then inform the RP of the hostname/port combination to use on the Internal OP for access. The UA will then open a connection to that hostname and port. Since the rule is matched, the PCEF will allow the GGSN to connect to the UA to the Internal OP. The Internal OP trusts the GGSN, so it will report success to the authentication request. When the RP contacts the External OP to validate the response, the External OP will release the allocation and remove the rule from the PCRF.

[0029] New Charging Session

[0030] In accordance with an embodiment, if the GGSN is able to initiate a new charging session for each socket connection to a specific IP address, the ability of the OCS system can be used to perform real-time account modifications to perform this connection validation. As a non-limiting example, Oracle Network Charging and Control (NCC) product line provides this ability.

[0031] As in the Real Time Rule Update method, the External OP will allocate a port on the Internal OP. It will then inform the OCS of the port allocation, which will update the UA's profile with the information. Prior to sending the TCP SYN to the Internal OP, the GGSN will

initiate a new charging session to the OCS, providing the IP address and port in the request. The OCS will then validate the IP address and Port against the allocation list, only responding with a success to the charging request if they match. As above, since the Internal OP trusts the GGSN, it is able to report success to the authentication request. When the RP contacts the External OP to validate the response, the External OP will release the allocation and update the UA's profile on the OCS.

[0032] FIGURE 3 is a flow chart illustration of integrating OpenID with a telecommunications network, in accordance with various embodiments of the invention. Although this figure depicts functional steps in a particular sequence for purposes of illustration, the process is not necessarily limited to this particular order or steps. One skilled in the art will appreciate that the various steps portrayed in this figure can be changed, rearranged, performed in parallel or adapted in various ways. Furthermore, it is to be understood that certain steps or sequences of steps can be added to or omitted from this process, without departing from the spirit and scope of the invention.

[0033] As illustrated in step 300, the process begins when a user agent invokes a service on a relying party and provides an identifier to the relying party. The relying party then transmits a request to validate the user agent to the external OpenID provider (step 302) and also redirects the user agent to the internal OpenID provider (step 304). The internal OP validates the subscriber by IP address or by username/password, as shown in step 306. In step 308, the internal OP redirects the user agent back to the accepted URL provided by the relying party. Finally, the relying party confirms the response with the external OP, as shown in step 310.

[0034] FIGURE 4 is a sequence diagram of integrating OpenID with the telecom network, in accordance with various embodiments of the invention. It is noted that similarly to other figures described herein, the sequence of steps is shown only for purposes of illustration and is not necessarily intended to limit all embodiments to the particular order or steps. One skilled in the art will appreciate that the various steps portrayed in this figure can be changed,

rearranged, performed in parallel or adapted in various ways. Furthermore, it is to be understood that certain steps or sequences of steps can be added to or omitted from this process, without departing from the spirit and scope of the invention.

[0035] As illustrated in FIGURE 4, the process for identifying the subscriber begins when the UA 400 (e.g. web browser on the subscriber's mobile device) invokes a service on the RP 402. Upon invoking the service, the UA typically provides its identifier to the RP. The RP receives this identifier and uses it to contact the external OP 404, requesting validation of the UA. The RP also responds to the UA, redirecting the UA to the internal OP 406. Since access to the internal OP is limited to the GGSN, when the UA reaches the internal OP, it is validated. Once validated, the internal OP redirects the UA to an accepted URL provided by the RP. Finally, the RP can confirm the validation of the UA with the external OP.

[0036] Throughout the various contexts described in this disclosure, the embodiments of the invention further encompass computer apparatus, computing systems and machine-readable media configured to carry out the foregoing systems and methods. In addition to an embodiment consisting of specifically designed integrated circuits or other electronics, the present invention may be conveniently implemented using a conventional general purpose or a specialized digital computer or microprocessor programmed according to the teachings of the present disclosure, as will be apparent to those skilled in the computer art.

[0037] Appropriate software coding can readily be prepared by skilled programmers based on the teachings of the present disclosure, as will be apparent to those skilled in the software art. The invention may also be implemented by the preparation of application specific integrated circuits or by interconnecting an appropriate network of conventional component circuits, as will be readily apparent to those skilled in the art.

[0038] The various embodiments include a computer program product which is a storage medium (media) having instructions stored thereon/in which can be used to program a general purpose or specialized computing processor(s)/device(s) to perform any of the features presented herein. The storage medium can include, but is not limited to, one or

more of the following: any type of physical media including floppy disks, optical discs, DVDs, CD-ROMs, microdrives, magneto-optical disks, holographic storage, ROMs, RAMs, PRAMS, EPROMs, EEPROMs, DRAMs, VRAMs, flash memory devices, magnetic or optical cards, nanosystems (including molecular memory ICs); and any type of media or device suitable for storing instructions and/or information. The computer program product can be transmitted in whole or in parts and over one or more public and/or private networks wherein the transmission includes instructions which can be used by one or more processors to perform any of the features presented herein. In certain embodiments, the transmission may include a plurality of separate transmissions. In accordance with one or more embodiments, the computer readable storage medium is non-transitory in nature.

[0039] The foregoing description of the preferred embodiments of the present invention has been provided for purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise forms disclosed. Many modifications and variations can be apparent to the practitioner skilled in the art. Embodiments were chosen and described in order to best explain the principles of the invention and its practical application, thereby enabling others skilled in the relevant art to understand the invention.

CLAIMS

What is claimed is:

1. A system for authenticating users in a telecommunications network, said system comprising:

a gateway node for authenticating mobile devices, each mobile device having an identifier associated therewith;

an internal provider that is connected to the gateway node, wherein the internal provider is reachable only from said gateway node; and

an external provider that receives a request from at least one relying party service to validate a subscriber of a mobile device, and redirects the mobile device to a validation uniform resource identifier (URI) on the internal provider in response to having received said request, wherein the mobile device is validated, and wherein after said validation, the internal provider redirects the mobile device to an accepted URI provided by the relying party service.

2. The system of claim 1, wherein the mobile device is validated by the gateway node performing deep packet inspection, wherein a Mobile Station International Subscriber Directory Number (MSISDN) associated with the subscriber is encoded into the request to the internal provider and wherein the gateway node validates said request by discarding all requests that do not contain the MSISDN that matches the subscriber of said mobile device.

3. The system of claim 1, wherein the mobile device is validated by the gateway node receiving real-time rule updates with specified address and port, wherein the external provider allocates a port on the internal provider and constructs a rule for a Mobile Station International Subscriber Directory Number (MSISDN) associated with the subscriber, said rule granting access to said port for said MSISDN, and wherein said rule is passed to the gateway node.

4. The system of claim 1, wherein the mobile device is validated by the gateway node initiating a new charging session, wherein the external provider allocates a port on the internal provider and informs an online charging server (OCS) of the port allocation, wherein the OCS updates a profile associated with said subscriber, and wherein the OCS validates the mobile device based on said port allocation.

5. The system of claim 1, wherein the gateway node is a Gateway for General Packet Radio Service (GPRS) Support Node (GGSN) that serves as a gateway between a GPRS wireless data network and one or more other networks, and wherein the gateway node further comprises:

a Policy and Charging Enforcement Function (PCEF); and

a Policy Control and Charging Rules Function (PCRF).

6. The system of claim 1, wherein the internal provider renders a page requesting a user name and password, said page further including an option to allow the mobile device to login without a password for subsequent requests.

7. The system of claim 1, wherein the relying party service confirms the validation of the subscriber with the external provider after the mobile device is redirected to the accepted URI provided by the relying party service.

8. A method for authenticating users in a telecommunications network, said method comprising:

receiving a request to validate a subscriber of a mobile device from a relying party service to an external provider;

redirecting the user agent to an internal provider by the relying party;

validating the user agent;

redirecting the user agent to an accepted uniform resource identifier (URI) provided by the relying party; and

validating a response by the relying party with the external provider.

9. The method of claim 8, wherein the request to validate the subscriber of the mobile device is initiated when a user agent invokes a service on a relying party and provides an identifier to the relying party.

10. The method of claim 9, wherein the relying party initiates a request to validate the user agent upon having received the invocation of the service from the mobile device and transmits said request to validate the user agent to an external provider.

11. The method of claim 8, wherein the user agent is connected to a gateway node.

12. The method of claim 8, wherein validating the user agent is implemented by a gateway node performing deep packet inspection, wherein a Mobile Station International Subscriber Directory Number (MSISDN) associated with the subscriber is encoded into the request to the internal provider and wherein the gateway node validates said request by discarding all requests that do not contain the MSISDN that matches the subscriber of said mobile device.

13. The method of claim 8, wherein the user agent is validated by a gateway node receiving real-time rule updates with specified address and port, wherein the external provider allocates a port on the internal provider and constructs a rule for a Mobile Station International Subscriber Directory Number (MSISDN) associated with the subscriber, said

rule granting access to said port for said MSISDN, and wherein said rule is passed to the gateway node.

14. The method of claim 8, wherein the user agent is validated by a gateway node initiating a new charging session, wherein the external provider allocates a port on the internal provider and informs an online charging server (OCS) of the port allocation, wherein the OCS updates a profile associated with said subscriber, and wherein the OCS validates the mobile device based on said port allocation.

15. The method of claim 11, wherein the gateway node is a Gateway for General Packet Radio Service (GPRS) Support Node (GGSN) that serves as a gateway between a GPRS wireless data network and one or more other networks, and wherein the gateway node further comprises:

a Policy and Charging Enforcement Function (PCEF); and

a Policy Control and Charging Rules Function (PCRF).

16. The method of claim 8, wherein the internal provider renders a page requesting a user name and password, said page further including an option to allow the user agent to login without a password for subsequent requests.

17. The method of claim 8, wherein the relying party service confirms the validation of the subscriber with the external provider after the user agent is redirected to the accepted URI provided by the relying party service.

18. The method of claim 8, wherein the user agent is a web browser of the mobile device invoking the relying party service.

19. A non-transitory computer readable storage medium storing a set of instructions executed by one or more processors to cause the one or more processors to perform a sequence of steps comprising:

receiving a request to validate a subscriber of a mobile device from a relying party service to an external provider;

redirecting the user agent to an internal provider by the relying party;

validating the user agent;

redirecting the user agent to an accepted uniform resource identifier (URI) provided by the relying party; and

validating a response by the relying party with the external provider.

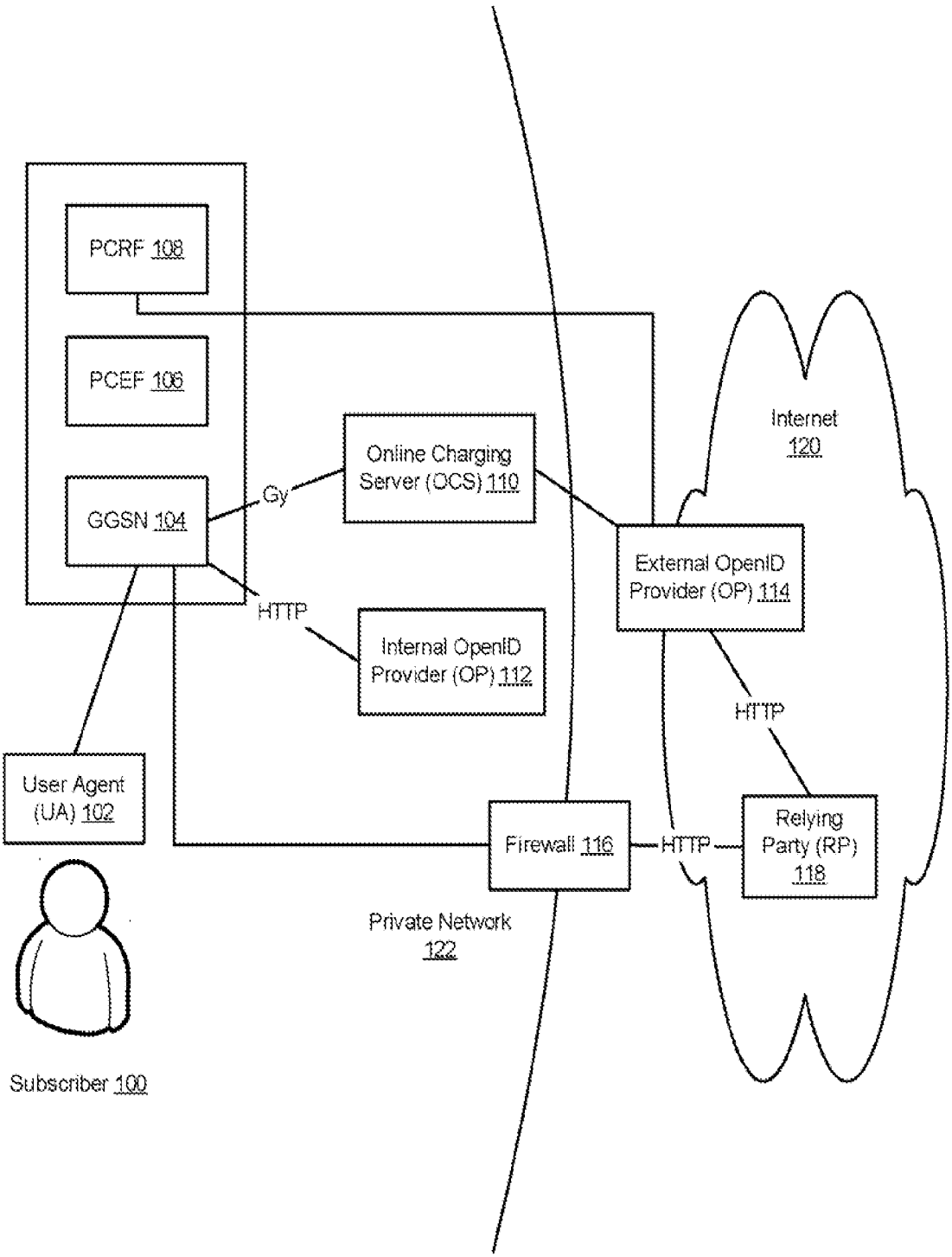
PCRF 108
PCEF 106
GGSN 104
Gy
Online Charging Server (OCS) 110
HTTP
Internal OpenID Provider (OP) 112
Internet 120
External OpenID Provider (OP) 114
HTTP
User Agent (UA) 102
Firewall 116
HTTP
Relying Party (RP) 118
Private Network 122
Subscriber 100

FIGURE 1

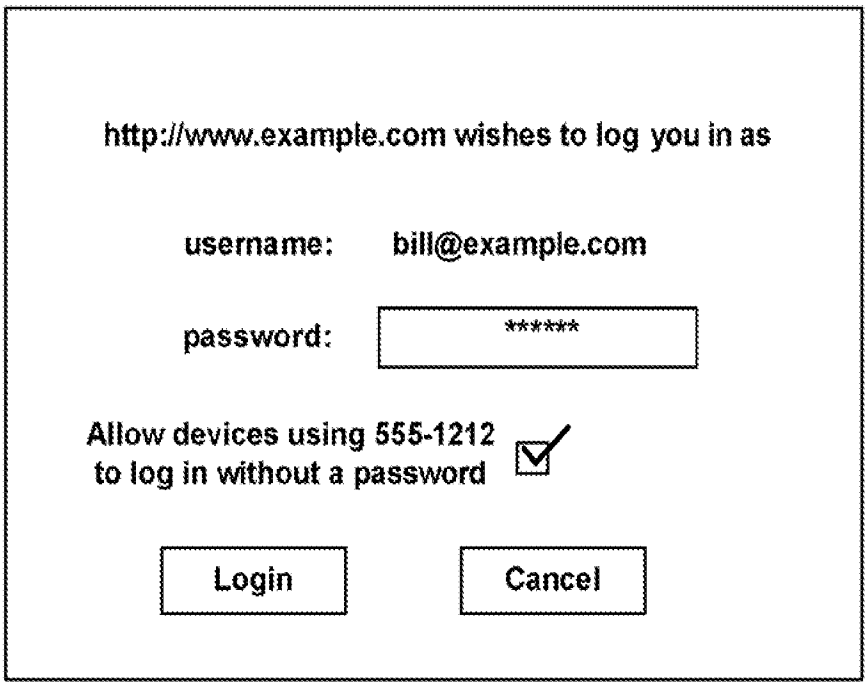
http://www.example.com wishes to log you in as
username: bill@example.com
password: ******
Allow devices using 555-1212
to log in without a password
Login
Cancel

FIGURE 2

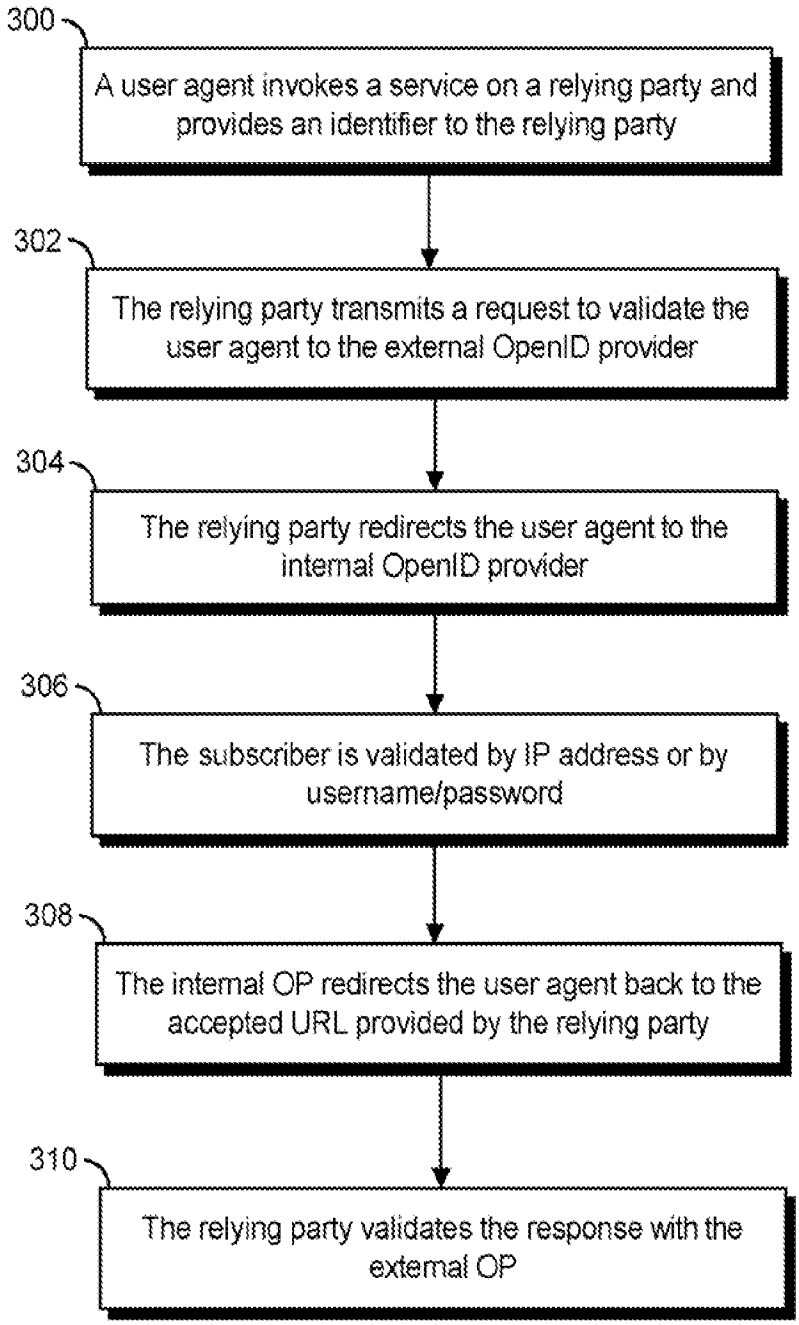
300
A user agent invokes a service on a relying party and provides an identifier to the relying party
302
The relying party transmits a request to validate the user agent to the external OpenID provider
304
The relying party redirects the user agent to the internal OpenID provider
306
The subscriber is validated by IP address or by username/password
308
The internal OP redirects the user agent back to the accepted URL provided by the relying party
310
The relying party validates the response with the external OP

FIGURE 3

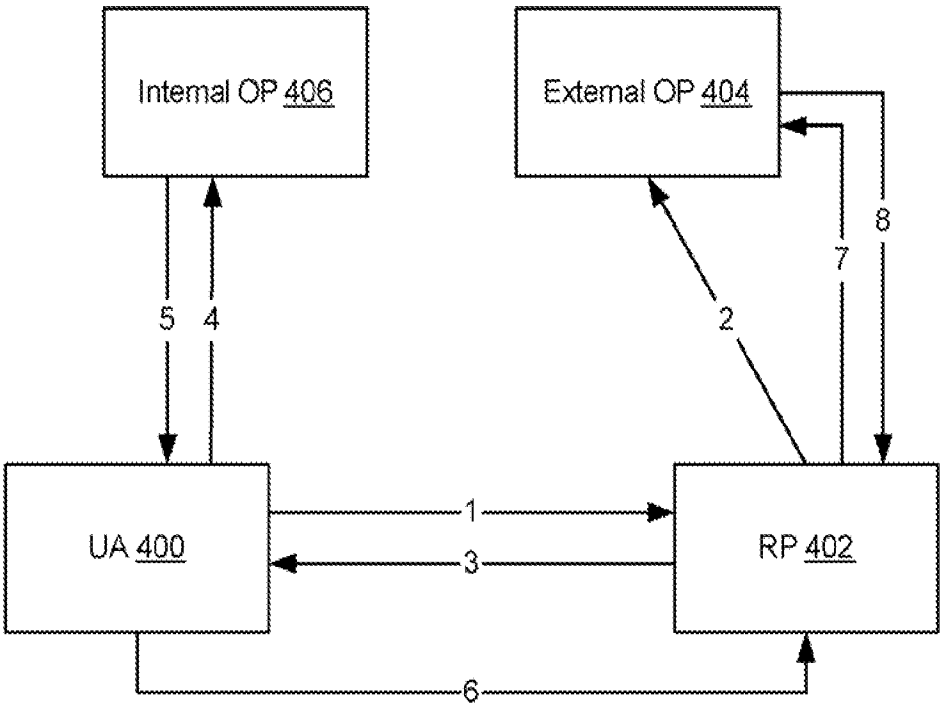

FIGURE 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2012/042629

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W12/06
ADD.

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)
H04L H04W

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 practicable, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2010/041347 A1 (ERICSSON TELEFON AB L M [SE]; HJELM JOHAN [JP]; MATSUMURA TAKESHI [JP]) 15 April 2010 (2010-04-15) abstract paragraph [0017] paragraph [0057] - paragraph [0071] figure 4 -----	1-19
X	WO 03/073783 A1 (ERICSSON TELEFON AB L M [SE]) 4 September 2003 (2003-09-04) abstract paragraph [0066] - paragraph [0067] figure 3 -----	1-19

☐ 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 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
12 September 2012	20/09/2012

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, Fax: (+31-70) 340-3016	Horn, Marc-Philipp

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2012/042629

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2010041347 A1	15-04-2010	EP 2335179 A1	22-06-2011
		JP 2012505436 A	01-03-2012
		US 2011188508 A1	04-08-2011
		WO 2010041347 A1	15-04-2010
WO 03073783 A1	04-09-2003	AU 2003217103 A1	09-09-2003
		CA 2473793 A1	04-09-2003
		CN 1640175 A	13-07-2005
		DE 10392283 T5	14-04-2005
		ES 2281228 A1	16-09-2007
		GB 2401509 A	10-11-2004
		JP 4303130 B2	29-07-2009
		JP 2005519501 A	30-06-2005
		SE 527706 C2	16-05-2006
		SE 0402099 A	26-08-2004
		WO 03073783 A1	04-09-2003