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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 January 2008 (10.01.2008)

PCT

(10) International Publication Number
WO 2008/005909 A2

(51) International Patent Classification:
G06F 15/16 (2006.01)

(21) International Application Number:
PCT/US2007/072622

(22) International Filing Date: 2 July 2007 (02.07.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
1589/DEL/2006 5 July 2006 (05.07.2006) IN

(71) Applicant *(for all designated States except US)*: **MOTOROLA, INC.** [US/US]; 1303 East Algonquin Road, Schaumburg, Illinois 60196 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **SAKLIKAR, Samir Dilipkumar,** [IN/IN]; B-15, Madhav Nagar, Rafi Ahmed Kidwai Road, Wadala, Mumbai, Maharashtra 400031 (IN). **SAHA, Subir,** [IN/IN]; D4 Samhita Vintage, 16th D Cross, 1st Main, Pai La, Bangalore, Karnataka 560016 (IN).

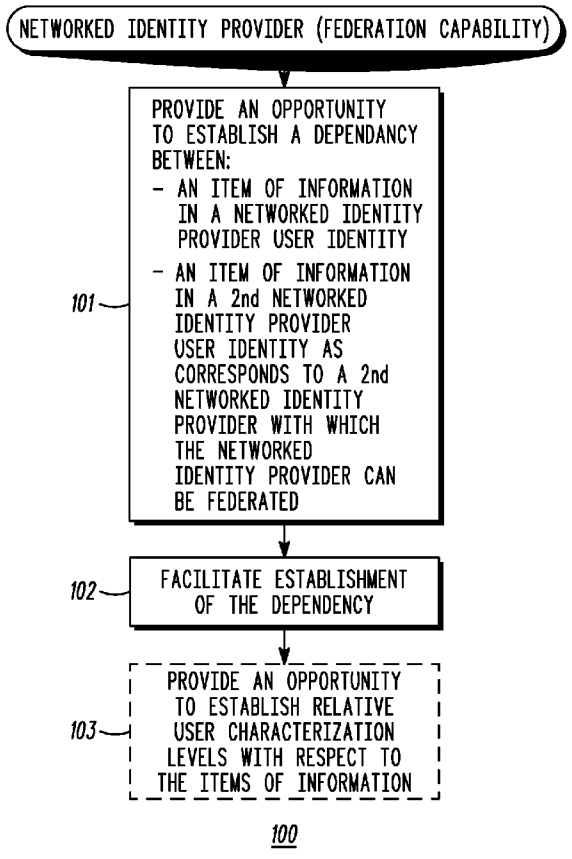
(74) Agents: **NICHOLS, Daniel K.,** et al.; 1303 East Algonquin Road, Schaumburg, Illinois 60196 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, 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, 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, LT, LU, LV, MC, MT, 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).

[Continued on next page]

(54) Title: INFORMATION DEPENDENCY FORMULATION AND USE METHOD AND APPARATUS



(57) Abstract: A networked identity provider can provide (101) an opportunity to a user to establish a dependency between, on the one hand, at least one item of information in a first networked identity provider user identity as is maintained by that networked identity provider and, on the other hand, at least one item of information in a second networked identity provider with which the first networked identity provider can be federated. This networked identity provider can then facilitate establishment (102) of that dependency. These teachings will further support the provision of an opportunity (103) to also establish relative user characterization levels with respect to these items of information to thereby influence subsequent sharing of identity information as between the first and the second networked identity providers.

WO 2008/005909 A2

Published:

— *without international search report and to be republished upon receipt of that report*

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.

INFORMATION DEPENDENCY FORMULATION AND USE METHOD AND APPARATUS

Technical Field

[0001] This invention relates generally to networked identity providers and more particularly to networked identity providers having a federation capability.

Background

[0002] Networked identity providers of various kinds are known in the art. Many identity providers, for example, are accessible and/or provide their corresponding services via the Internet. Such identity providers typically maintain separate identity records for their various authorized users. Such identity records often contain more than more identification information (such as name, email address, password, and so forth). In many cases such identity records also contain information that comprises or otherwise reflects various user preferences and/or characterizing information as pertains relatively specifically to each user.

[0003] Identity federation technologies such as Liberty Alliance are also known in the art. The Liberty Alliance comprises a consortium that supports the formation and promulgation of standards-based specifications for federated identity and identity-based Web services. Such technologies permit, for example, the storage and control of identity information for registered users in user profiles (often denoted as "identity services"). Such technologies provide for a certain amount of information sharing with respect to such networked identity providers. (Those skilled in the art will understand that such sharing is typically between an identity provider and a so-called service provider (which is a term typically used to identify an identity information consumer in identity federation parlance).)

[0004] Unfortunately, for the most part, these efforts tend to maintain a paradigm where each networked identity provider often maintains such information in relative confinement. This likely holds true, at least in part, out of a desire to maintain the user's privacy; as noted, such identity information can comprise user preferences

and/or user details that, at least in some cases, a given user will likely prefer to retain in at least some degree of confidence. This also tends to hold true, at least in part, because some identity provider prefer to control and/or own this information for business reasons. Control over a user's information and preferences, for example, can be a control point to ensure that user's loyalty. This, in turn, tends to restrict the capabilities of users from conveniently using multiple sets of identity information from different identity providers in aggregation.

[0005] As a result, present identity federation technologies fall considerably short of their potential. The problem seems intractable – information from multiple sources can often be usefully leveraged in combination to benefit the user but existing privacy concerns and practices stymie such sharing.

Brief Description of the Drawings

[0006] The above needs are at least partially met through provision of the Information dependency formulation and use method and apparatus described in the following detailed description, particularly when studied in conjunction with the drawings, wherein:

[0007] FIG. 1 comprises a flow diagram as configured in accordance with various embodiments of the invention;

[0008] FIG. 2 comprises a schematic screen shot as configured in accordance with various embodiments of the invention;

[0009] FIG. 3 comprises a schematic screen shot detail as configured in accordance with various embodiments of the invention;

[0010] FIG. 4 comprises a schematic screen shot detail as configured in accordance with various embodiments of the invention;

[0011] FIG. 5 comprises a communications flow diagram as configured in accordance with various embodiments of the invention;

[0012] FIG. 6 comprises a flow diagram as configured in accordance with various embodiments of the invention; and

[0013] FIG. 7 comprises a block diagram as configured in accordance with various embodiments of the invention.

[0014] Skilled artisans will appreciate that elements in the figures are illustrated for simplicity and clarity and have not necessarily been drawn to scale. For example, the dimensions and/or relative positioning of some of the elements in the figures may be exaggerated relative to other elements to help to improve understanding of various embodiments of the present invention. Also, common but well-understood elements that are useful or necessary in a commercially feasible embodiment are often not depicted in order to facilitate a less obstructed view of these various embodiments of the present invention. It will further be appreciated that certain actions and/or steps may be described or depicted in a particular order of occurrence while those skilled in the art will understand that such specificity with respect to sequence is not actually required. It will also be understood that the terms and expressions used herein have the ordinary meaning as is accorded to such terms and expressions with respect to their corresponding respective areas of inquiry and study except where specific meanings have otherwise been set forth herein.

Detailed Description

[0015] Generally speaking, these various embodiments are suitable for use with a networked identity provider that has federation capability. Pursuant to these teachings, this networked identity provider can provide an opportunity to a user to establish a dependency between, on the one hand, at least one item of information in a first networked identity provider user identity as is maintained by that networked identity provider and, on the other hand, at least one item of information in a second networked identity provider with which the first networked identity provider can be federated. This networked identity provider can then facilitate establishment of that dependency.

[0016] By one approach, if desired, these teachings will further support the provision of an opportunity to also establish relative user characterization levels with respect to these items of information to thereby influence subsequent sharing of identity information as between the first and the second networked identity providers.

This permits, for example, varying privacy levels to be established for these various items of information.

[0017] These teachings also provide for allowing query responses to be formed using the aforementioned dependencies. By one approach, for example, this dependency information can serve in the first instance to identify useful information as may reside at another networked identity provider or providers. If desired, the aforementioned relative user characterization levels can then serve to determine which of the networked identity providers shall use the information of the other(s) to form the desired response to the query.

[0018] So configured, privacy and other related concerns regarding importance, priority, and the like are readily accommodated in a manner that is both relatively intuitive for the user and also likely to meet the user's needs in this regard. At the same time, information as held by a plurality of networked identity providers can be relatively available for cross-linked usage to facilitate the formation of rich, well-informed query responses that are more likely to yield a desirable result for the user. Those skilled in the art will recognize and appreciate that these teachings are relatively simple to implement.

[0019] These and other benefits may become clearer upon making a thorough review and study of the following detailed description. Referring now to the drawings, and in particular to FIG. 1, these teachings are readily employed in conjunction with networked identity providers and particularly networked identity providers that have a federation capability as is known in the art.

[0020] By one approach, a corresponding process 100 provides 101 an opportunity to establish a dependency between items of information as are maintained by a plurality of networked identity providers. The networked identity provider extends this opportunity to, for example, a user. (As used herein, "user" will be understood to refer to a person but may also encompass automata as acts on behalf of a person or that acts in a more unilateral manner.) This opportunity can comprise an opportunity to establish a dependency between, on the one hand, at least one item of information in a first networked identity provider user identity as is maintained by the first networked identity provider and, on the other hand, at least one item of

information in a second networked identity provider user identity as corresponds to a second networked identity provider with which the first networked identity provider can be federated.

[0021] There are various ways by which the networked identity provider can provide this opportunity. As but one illustration in this regard, and with momentary reference to FIG. 2, this opportunity can be extended via a browser-based interface 201. By one approach, this browser-based interface 201 (as offered, for example, by the aforementioned first networked identity provider) can provide a display area 202 for federation information. One or more items of information comprising, in this illustrative example, user preferences 203 and 204 are also displayed to thereby refresh the user's recollection with respect to their expressed choices in this regard. Candidate and/or already-linked other networked identity providers 205 and 206 are also presented in an area where dependencies are shown and/or facilitated.

[0022] By one approach, a standard cursor 207 mechanism can serve to facilitate the manipulation of one or more of these displayed elements. For example, the aforementioned dependency creation opportunity can comprise, in part, the opportunity to select and drag a given user preference into a given networked identity provider space. Such click and drag facilities are well known in the art and require no further elaboration here.

[0023] Referring again to FIG. 1, as noted, this process 100 extends an opportunity to establish a dependency between items of user identity information. By one approach this can relate to networked identity provider user identities that both relate to a same user. If desired, however, these networked identity provider user identities can relate to different users. So configured, a dependency establishment opportunity could be provided as regards an item of information in a first networked identity provider user identity as corresponds to a first user and an item of information in a second networked identity provider user identity as corresponds to a second, different user.

[0024] As shown, this opportunity relates to two items of information and two networked identity provider user identities. Those skilled in the art, however, will recognize and understand that this opportunity can be extended to encompass three or

more such items of information/networked identity provider user identities as may be desired. Only two such items are shown here for the sake of simplicity and clarity and not as a point of limitation.

[0025] This process 100 then provides for facilitating 102 establishment of this dependency. This can comprise receiving from a user a selection of at least one of the items of information. Referring again to FIG. 2, for example, this can comprise the user using the cursor 207 to select a given one of the items of information represented by the user-identified preference items 203 and 204. This step of establishing a dependency can further comprise receiving from the user a selection of a target second networked identity provider. Again as noted above, this can comprise the user using the cursor 207 to drag a previously selected user-identified preference item 203 or 204 to a user-selected networked identity provider 205 or 206. In general, the first networked identity provider and the selected second networked identity provider should be capable of establishing and maintaining a state of federation between themselves. It is not necessary, however, that such a state exist at the time of initiating facilitation of the dependency establishment process.

[0026] In general, establishing such a dependency as between two items of information contained in networked identity provider user identities as maintained at different networked identity providers entails establishing a user-based policy that uses information contained in each of these networked identity provider user identities to thereby provide a user-based policy that comprises a composite policy containing information that may be relatively unique to each of the networked identity provider user identities. By one approach, this user-based policy can be established at whichever of the first and second networked identity providers the user selects (wherein the selection can be relatively direct or indirect as the case may be).

[0027] Referring again to FIG. 1, to better inform and guide this process, this process 100 will further optionally accommodate providing 103 an opportunity to establish relative user characterization levels with respect to these items of information in the first and second networked identity provider user identities to thereby influence subsequent sharing of identity information as between the first and second networked identity providers. The user characterization itself can vary as

desired with the application setting, user requirements and preferences, and so forth. Some illustrative examples include, but are not limited to, characterizations regarding value of the information, importance of the information, priority of the information, and so forth. By one approach, this user characterization can usefully comprise a characterization regarding privacy.

[0028] To illustrate, and referring now to FIG. 3, when the user has selected a particular item of information and a target networked identity provider during the dependency establishment process described above, the user is then presented with an opportunity to establish relative levels of privacy expectation and treatment to be accorded such information items. In this illustrative example, this comprises a first opportunity 301 that will permit the user to establish the item of information as corresponds to the first networked identity provider to be more private and a second opportunity 302 that permits the user to instead establish the item of information as corresponds to the second networked identity provider to be more private.

[0029] A lack of a selection in this regard can be taken as a user representation that neither item of information has a relatively higher level of privacy expectation. Lack of a selection from the user may also serve as a trigger for a default system-wide policy to set in. One illustration in this regard would be a policy that all health-related information always defaults to a relatively higher privacy level in the absence of a specific user selection in this regard. If desired, such a policy selection can be based, at least in part, on some user characterization and a policy that is viewed as being most suitable to this category of users (as determined, for example, by the aforementioned user characterization). Also, if desired, such a decision may be reached based on some negotiation between the two involved identity providers themselves using resolution criteria of choice and a negotiation protocol as may be appropriate to the needs, requirements, and/or limitation of a given application setting.

[0030] So configured, such relative degrees of user characterization requirements can be used, for example, to control and determine where the aforementioned user-based policy will be established and maintained (and hence which of the networked identity providers will have possession of information from the other networked identity provider). Generally speaking, when the user

characterization requirement comprises a privacy characterization, this can serve to ensure that the networked identity provider having the higher privacy rating will be the entity to access the item of information from the other networked identity provider. This, in turn, aids in preventing more private information from being accessed by a less private (and perhaps less trusted) entity.

[0031] As noted above, this process 100 readily accommodates the establishment of user-based policies. As one illustrative example in this regard, and referring now to FIG. 4, following the above-described initial dependency-creation steps, the user can be presented with an opportunity to select from amongst a plurality of candidate policies 401 and 402. In this illustrative example the candidate policies are pre-configured (for example, by the networked identity provider itself). If desired, this may be supplemented or supplanted by an opportunity for the user to themselves construct a particular policy. In this illustrative example provided, cuisine user preference information from a first networked identity provider is used with user medical information from a second networked identity provider to form corresponding policies that can be used, for example, when responding to subsequent queries regarding user preferences.

[0032] Those skilled in the art will recognize and appreciate that the foregoing steps can be implemented in any of a wide variety of ways. For the purposes of illustration and not by way of limitation, a description of an exemplary scenario in this regard will now be provided. Referring to FIG. 5, in this scenario, a given user is using a browser as is known in the art. These teachings are readily applicable for use with wireless as well as direct connection browser platforms.

[0033] In this example the user uses their browser to present their username and password 501 to a cuisine-based networked identity provider to thereby login with the latter. Once logged in, the user then clicks 502 on a provided link to enable the federation functionality of the cuisine-based networked identity provider. In this example the cuisine-based networked identity provider responds by providing 503 a profile display for the user that prompts the user for federation enablement specifics. This can comprise, for example, providing a page that displays a plurality of cuisine-based items of information as comprise the user's identity profile. Each such item can

further include a check box. So configured, the user can be prompted to check on the check-box for items of information for which the user wishes to create a federation-enabled dependency.

[0034] In this example the user selects 504 a particular cuisine-based item of information for which a federation-enabled dependency is desired. This can comprise, as disclosed above, also identifying the target networked identity provider as well as a given user-selected relative level for a given user characterization (such as, for example, a given level of privacy to be accorded to the item of information). In this illustrative embodiment, the cuisine-based networked identity provider then responds by redirecting 505 the user's browser to the target networked identity provider (which in this example comprises a health information-based networked identity provider).

[0035] By one approach, this latter transaction can comprise a new element that is added to an AuthnRequest as is already known in the art. This new element could take the form, for example, of <profileLink> (A more detailed illustrative example in this regard appears further below). This new element can indicate to the recipient networked identity provider that in addition to seeking to establish a federation there is also identity information to be linked in a dependent manner. In a case where the user characterization (such as privacy) has been set relatively low by the user in the previous steps, this transaction can also include the corresponding item of information itself that is to be linked to information at the health-based networked identity provider. In a case where the user characterization had been set relatively high, such information could be withheld and the recipient networked identity provider could instead be compelled or requested to provide the item of information to the cuisine-based networked identity provider.

[0036] By one approach, this transaction can further include an assertion from the cuisine-based networked identity provider to indicate that the user has already been authenticated by the cuisine-based networked identity provider. This can serve to prove to the health-based networked identity provider, for example, that the cuisine-based networked identity provider is also a networked identity provider for this particular user. This, in turn, can be used by the health-based networked identity

provider to permit subsequent acceptance of other assertions or submissions as proffered by the cuisine-based networked identity provider.

[0037] The user's browser can act upon the redirection message 505 by forwarding the provided AuthnRequest message 506 (as known in the art and as modified as described above) to the health-based networked identity provider. In this illustrative example the latter responds with a login request 507 to which the user replies with their login information 508. The health-based networked identity provider then analyzes 509 the AuthnRequest message including the dependency content described above. This analysis can comprise, for example, identifying the various elements described above and facilitating a cooperative use of this content.

[0038] In this illustrative example the health-based networked identity provider then responds with page content 510 to confirm for that user that the dependency request is acknowledged and will be honored. This page can further comprise, for example, one or more prompts to encourage the user to identify one or more specific items of information in the identity profile for this user at this health-based networked identity provider that are to be linked with the provided item of information from the cuisine-based networked identity provider. The user in turns provides their selection 511 in this regard. The health-based networked identity provider then prompts 512 the user to specify a particular policy that relies upon the aforementioned items of information.

When the user provides the policy information response 513, the health-based networked identity provider then redirects 514 the user's browser back to the cuisine-based networked identity provider. This redirection message can comprise a federation Response message that includes additional content as per these teachings. In particular, this additional content can comprise further information regarding the established dependency. In this example, this might comprise, for instance, information regarding which cuisine-based networked identity provider items of information have been linked with items of information at the health-based networked identity provider. This information can further comprise, for example, a network address for a location within the health-based networked identity provider where a query regarding this dependency can be directed. If desired, when adopting this

approach, a different network address (such as a different uniform resource locator) can be provided for each individual element of the linked identity profile. (It would also be possible to provide a different URL (for example, "https://112.12.12.12/policy1") rather than a more revelatory URL (such as "www.health.com/policy1") to better ensure that the one provider will not know in which informational domain the dependency has been established.)

[0039] The user's browser then forwards that Response 515 to the cuisine-based networked identity provider which then stores 516 at least the aforementioned network address. Information 517 can then be provided to the user to indicate a successful conclusion of the federation and dependency establishment activity.

[0040] In the above example, the cuisine-based networked identity provider provided its item of information to the health-based networked identity provider because the user established a relatively low privacy level for the cuisine-related information. Those skilled in the art will recognize that this process can be readily modified to accommodate a scenario where the initial networked identity provider has, instead, a relatively high privacy level. In such a case, the cuisine-based networked identity provider would proceed as described above though while retaining its information. The health-based networked identity provider would then include its item of information in its Response message. Upon receiving this information, the cuisine-based networked identity provider would then carry out the policy-establishment activity described above. This could include, for example, presenting an additional message via the user's browser to inform the health-based networked identity provider of the network address where the dependency result can now be accessed.

[0041] The various processes described above provide for establishment of informational dependencies in a federation-enabled operational environment where, if desired, informational sharing can be controlled, directed, and/or informed through use of user-specified characterizations regarding the information. As is also noted above, this can further comprise using such dependencies to form multi-identity

policies capable of representing user preferences or circumstances in a rich yet protected manner.

[0042] Referring now to FIG. 6, further elaboration with respect to such processes will be presented. By this process 600, upon receiving 601 a query regarding a user for whom the receiving networked identity provider has a corresponding user identity, the receiving networked identity provider then effectively determines 602 whether the query requires access to a dependent item of information that is held by a different federated networked identity provider. When true, and when the information in question is not available to the networked identity provider, generally speaking the networked identity provider nevertheless uses the corresponding user-created dependency to facilitate responding to this query.

[0043] This can comprise, for example, receiving a query and associating that query with a particular network address as was established by another networked identity provider pursuant to the processes set forth above, where the whole of the required information is held, at least in part, for just such a purpose. So configured, the user gains access in a relatively transparent manner to a desired response notwithstanding that the original receiving networked identity provider did not, in fact, have direct access to all of the information required to form the desired response. At the same time, the receiving networked identity provider is able to facilitate, in a knowing manner, a suitable response to the query notwithstanding that, in this scenario, the receiving networked identity provider does not have actual access to the underlying item of information at the other networked identity provider(s).

[0044] When the receiving networked identity provider determines 602 instead that the query does require dependently linked information but that the dependent information is, in fact, available to the receiving networked identity provider, this process 600 can simply provide for that receiving networked identity provider using 604 that dependent item of information to facilitate responding to the query. This can comprise, for example, accessing an internal (to the receiving networked identity provider) network address where the receiving networked identity provider has previously placed the dependent item(s) of information and/or a corresponding user-specified policy.

[0045] So configured, networked identity providers are able to more fully respond to a given query without also requiring that all items of information be disclosed to all other federated networked identity providers. This, in turn, permits the user to assign and rely upon any number of user characterizations regarding such information (including but not limited to the use of any number of user-assigned levels as correspond to such user characterizations).

[0046] Those skilled in the art will appreciate that the above-described processes are readily enabled using any of a wide variety of available and/or readily configured platforms, including partially or wholly programmable platforms as are known in the art or dedicated purpose platforms as may be desired for some applications. Referring now to FIG. 7, an illustrative approach to such a platform will now be provided.

[0047] This networked identity provider 700 can comprise a processor 701 that operably couples to a first memory 702, a second memory 703, and a third memory 704. In this illustrative embodiment the first memory 702 has a user identity for a user of the networked identity provider 700 stored therein. (More typically, of course, this will actually comprise a large plurality of user identities for a corresponding number of users; for the sake of simplicity and clarity, however, this description relates to only a single such user identity.) By one approach this user identity can be relatively complete and include, for example, corresponding identity information, preferences, and so forth. In the alternative, if desired, a fourth optional memory 705 can serve to retain, in whole or in part, such content. Also in this illustrative embodiment, the second memory 703 has information regarding federation status with other networked identity providers stored therein while the third memory 704 has information regarding the aforementioned user-established user identity information dependencies between the networked identity provider 700 and other networked identity providers with which the networked identity provider 700 has a federation stored therein.

[0048] The process 701, in turn, is configured and arranged (via, for example, corresponding programming as will be well understood by those skilled in the art) to provide the aforementioned opportunity to establish dependencies between at least

one item of information in a first networked identity provider user identity and at least one other item of information in another networked identity provider user identity with which the networked identity provider 700 can be federated and further to facilitate the establishment of such a dependency. This can comprise, if desired, further configuring and arranging the processor 701 to establish such dependencies as a function, at least in part, of user-assigned levels of user characterization to thereby control which of the networked identity providers is provided with user identity information from an opposing networked identity provider. It will also be understood that such a processor 700 can further be configured and arranged to formulate query replies (at least to user-authorized queries) in a manner that leverages the availability of such dependencies.

[0049] Those skilled in the art will recognize and understand that such an apparatus 700 may be comprised of a plurality of physically distinct elements as is suggested by the illustration shown in FIG. 7. It is also possible, however, to view this illustration as comprising a logical view, in which case one or more of these elements can be enabled and realized via a shared platform. It will also be understood that such a shared platform may comprise a wholly or at least partially programmable platform as are known in the art.

[0050] As noted above, these transactions can be facilitated using a new element that is added to an AuthnRequest as is already known in the art, or if desired, can be used independently of such existing messages as the AuthnRequest message. More specific illustrative examples in this regard will now be presented.

[0051] A first element <LinkCreate> can be used to create a link between profile elements of a Data Service 1 with a Data Service 2. This element can be sent from one Web Service Provider (who wants to set up the dependency) to another Web Service Provider (with whom the dependency is to be set). This request can be sent, for example, to a target URL that is exposed by the Destination Web Service Provider for receiving requests related to establishing federation. It is possible, however, that a new URL (specific to receiving resolves for Dependency Creation) may be standardized and exposed if desired.

[0052] The following information can be sent in the <LinkCreate> Request:

[0053] A Local Dependency Identifier – A unique identifier that identifies this dependency in this domain of the Originating Web Service Provider. It may, if desired, be in the form of a URL.

[0054] A Subject – The User for whom this dependency is being established. This element identifies the subject within the domain of the Originating Web Service Provider (that is, the one originating the LinkCreate Request).

[0055] A User Characterization Level – A level defining whether the Originating Web Service Provider is at a higher or lower User Characterization level with respect to the destination Web Service Provider, for this particular set of Profile Elements (as decided, for example, by the following parameter).

[0056] A Set of Data Services (Profile) Elements – The content of this element can be decided, for example, by the user of the Web Service Provider and can reflect, for example, whatever profile elements within the domain of the Originating Web Service Provider that the user wants to create a link with some other profile elements in the domain of the Destination Web Service Provider. By one approach, if desired, this set can be null when the Originating Web Service Provider is at a higher user characterization level that the Destination Web Service Provider.

[0057] By one approach, each element of this parameter would contain the Profile Type (Personal Profile, Employee Profile, and so forth) as well as the exact Profile Parameter that is being linked with the Destination Web Service Provider.

[0058] A <LinkCreateResponse> element can be sent in response to the above element and can contain the status of the Link request. By one approach this element can contain the following information:

[0059] Status – This indicates a success or a failure in processing the LinkCreate Request. It may also contain appropriate error codes, if there was some failure in executing a <LinkCreate> request. For example, a "User Characterization level not agreeable" message can be sent back if the User Characterization level as suggested by the Originating Web Service Provider is not acceptable to the Destination Web Service Provider. This may happen either because of a User decision, an applicable policy, or some applicable global policy.

[0060] A Local Dependency Identifier – A unique identifier that identifies this dependency in this domain of the Destination Web Service Provider. It may be in the form of a URL. It would be used by the Originating Web Service Provider to identify this dependency, resolve it, or delete it.

[0061] Subject – The User for whom this dependency is being established. This element can identify the subject within the domain of the Destination Web Service Provider (the one who is accepting the LinkCreate Request).

[0062] A User Characterization Level – A level defining whether the Destination Web Service Provider is at a higher or lower User Characterization level with respect to the Originating Web Service Provider, for this particular set of Profile Elements (as decided by the following parameter). This will preferably conform to the User Characterization Level that was indicated within the <LinkCreate> Request. For example, if the Originating Web Service Provider claimed to be at a higher User Characterization level, then the Destination Web Service Provider will preferably agree to be at a lower User Characterization level.

[0063] A Set of Data Services (Profile) Elements – The content of this element can be decided, for example, based on those elements for which the User agrees to have a dependency established from the Destination Web Service Provider to the Originating Web Service Provider. By one approach, if desired, this set can be null when the Destination Web Service Provider has a higher user characterization level as in such a case, no profile element information is shared with the Originating Web Service Provider (who is at a lower user characterization level).

[0064] A request comprising a <LinkResolve> element can serve to resolve a dependency between two Web Service Providers as established by the above <LinkCreate> process. This element would be sent typically from any Web Service Provider to the other. It is not mandated that it be necessarily sent by the Web Service Provider that had initiated the <LinkCreate> request. For example, it may be sent by the Web Service Provider that had responded to the <LinkCreate> request. Such flexibility allows in setting up the links from one Web Service Provider to another, but having them resolved from any Web Service Provider, wherever a Query was made. In general, the User Characterization levels as selected by the User should be

honored when resolving the dependencies as Identity Information should preferably not travel from a higher User Characterization to a Lower User Characterization -level Web Service Provider. This request can be targeted towards the URL that was exposed by the Resolvee Web Service Provider as its Local Dependency Identifier during the Link Creation process.

[0065] The following information can be sent in this <LinkResolve> Request:

[0066] A Local Dependency Identifier – The unique identifier that identifies this particular dependency in the Resolver Web Service Provider domain. It may be in the form of a URL. This is used by the Resolvee Web Service Provider to verify whether the appropriate dependency is being triggered.

[0067] A Subject – The User for whom this dependency is being resolved. This element identifies the subject within the domain of the Resolver Web Service Provider (the one who is originating the <LinkResolve> Request).

[0068] A Set of Data Services (Profile) Elements and Values – The content of this element can be decided, for example, based on the Profile Elements which were linked during the <LinkCreate> process and can reflect, for example, whatever profile elements and their associated values within the domain of the Originating Web Service Provider for which a link has been created and is being resolved with some other profile elements in the domain of the Destination Web Service Provider. By one approach, if desired, this set can be null when the Originating Web Service Provider is at a higher user characterization level than the Destination Web Service Provider.

[0069] A <LinkResolveResponse> element can be sent in response to a Link Resolve Request. It is sent towards the Resolver Web Service Provider who had issued the Link Resolve request to resolve the dependency that was setup between the two different information profiles at the respective Web Service Provider.

[0070] The following information can be to be sent in the <LinkResolveResponse> Request:

[0071] Status – This indicates a success or a failure in processing the LinkResolve request. It may also contain appropriate error codes, if there was some failure in executing a <LinkResolve> request. For example, “Dependency not found”

can be sent back if there is no dependency between the two Web Service Providers as identified for this particular subject and the given dependency identifier.

[0072] A Local Dependency Identifier – The unique identifier that identifies this particular dependency in the Resolvee Web Service Provider domain. It may be in the form of a URL.

[0073] A Subject – The User for whom this dependency is being resolved. This element can identify the subject within the domain of the Resolvee Web Service Provider (the one who is responding to the <LinkResolve> Request).

[0074] A Set of Data Services (Profile) Elements and Values – The content of this element can be decided, for example, based on those profile elements and their values for which the User agrees to have a dependency established from the Destination Web Service Provider to the Originating Web Service Provider. By one approach, if desired, this set can be returned after the execution of a Policy within the domain of the Destination Web Service Provider, which is associated with the Local Dependency Identifier for this dependency.

[0075] In any of the above, the User Characterization levels may be considered to be one or more of, but not limited to, levels corresponding to Privacy, Importance, Value, or Priority.

[0076] A <LinkDelete> element can be used to delete a link/dependency that was created between Profile elements of Data Service 1 with Data Service 2. It can be sent from one Web Service Provider (who wants to delete the dependency) to another Web Service Provider (with whom the dependency is to be set). This request can typically be sent to the URL that is exposed by the Destination Web Service Provider for receiving requests related to de-establishing federation. It is also possible, however, that it be sent to the URL that was exposed in the Local Dependency Identifier during the Link Creation process.

[0077] The following information can be sent in the <LinkDelete> Request:

[0078] A Local Dependency Identifier – The unique identifier that identified this dependency in this domain. It may be in the form of a URL.

[0079] A Subject – The User for whom this dependency is being deleted. This element can identify the subject within the domain of the Originating Web Service Provider (the one who is originating the LinkDelete Request).

[0080] A <LinkDeleteResponse> element can be sent in response to the <LinkDelete> request. It can confirm to the Web Service Provider that the specific dependency that was identified in the <LinkDelete> request for this particular subject has been deleted. Neither of the involved Web Service Providers need try to resolve this dependency any further. By one approach, such an attempt to resolve such a deleted dependency could result in an error equivalent to "Dependency not found."

[0081] The following information can be sent in the <LinkDeleteResponse> element:

[0082] A Local Dependency Identifier – The unique identifier that identified this dependency in this domain. It may be in the form of a URL.

[0083] A Subject – The User for whom this dependency is being deleted. This element identifies the subject within the domain of the Destination Web Service Provider (the one who is sending the LinkDeleteResponse).

[0084] When the User has federated and setup a dependency between two information profiles, they can also have the option to set up rules/policies to govern how the Profile Data elements from the two profiles can interact with each other. For purposes of this particular illustrative example, the term Policy is used to reflect User-defined personalization-related policies that control the system behavior as per User expectations. The meaning of the term is thus more generic than the "Access-control" connotation that is often associated with "Policy." By one approach, if desired, this Policy can be associated with the Local Dependency URL that identifies a dependency within a given domain.

[0085] There are different potential usages of such User-defined rules/policies. Here are some illustrative examples in this regard:

[0086] Rules/Policies are used in the same domain, where they belong and are stored. This would happen, for example, when the User federates some other profile information from some other Web Service Provider to a present Web Service

Provider, but writes the policy/rule that works over these two pieces of User information at this Web Service Provider itself. Herein, the Web Service Provider can store the Policy in any format that is most suitable for it since there is no need to share these policies with other domains. Hence, the Policy representation format can indeed be proprietary. It may be appropriate, however, that at least a conversion mechanism be allowed so that Policies can be shared if and when the need arises.

[0087] Policies are usable in different domains. Here, a Policy that is written in one domain (by one Web Service Provider or Identity Provider) needs to be shared with another domain. Such sharing can be for any of a variety of reasons. The following are some examples in this regard.

[0088] The compete rule/policy itself is being returned to the Web Service Provider, since it is determining some Service Behavior, that must be executed by the Web Service Provider so as to give the appropriate benefit to the User. Here, the Rule/Policy can be returned to the Web Service Provider in the Query result. (For example, the Web Service Provider makes a Query regarding Call-routing related preferences. The Web Service Provider may return a rule indicating something like, "When I get a call from Paul, reject it.")

[0089] The Policy is owned by a certain domain/ Web Service Provider, but it needs to be shared with the other Web Service Provider. Here, the Policy needs to be shared to the other Web Service Provider notwithstanding that the other Web Service Provider has not agreed to share its profile information because the User wants the behavior from one Web Service Provider to be applicable at another Web Service Provider (though for a different set of Profile Data). (For example, an Airline Reservation counter is selecting movies/games that should be accessible to the User during her long flight. The User has Music and Video Preferences stored by one Web Service Provider, whereas her Gaming-related preferences are stored with another Web Service Provider. She has a rule with her Video-related Web Service Provider stating that if she did not like the book (based on federation and profile linking with her library/reading preferences), then she is not interested in seeing the corresponding movie. In this example the User would like that same experience for her Gaming-related preferences. This lays the need for the rule/policy to travel from the Video-

related Web Service Provider towards the Gaming- Web Service Provider so that it can apply the same rule to give a similar experience to the User.)

[0090] Those skilled in the art will recognize that a wide variety of modifications, alterations, and combinations can be made with respect to the above described embodiments without departing from the spirit and scope of the invention, and that such modifications, alterations, and combinations are to be viewed as being within the ambit of the inventive concept.

We claim:

1. A method for facilitating establishing a dependency as between items of information at networked identity providers comprising:
at a first networked identity provider having a federation capability:
providing an opportunity to establish a dependency between:
at least one item of information in a first networked identity provider user identity as is maintained by the first networked identity provider; and
at least one item of information in a second networked identity provider user identity as corresponds to a second networked identity provider with which the first networked identity provider can be federated;
facilitating establishment of the dependency.

2. The method of claim 1 wherein facilitating establishment of the dependency comprises receiving from a user a selection of at least one of the items of information.

3. The method of claim 2 wherein at least one of the items of information comprises at least one user-identified preference.

4. The method of claim 1 wherein the first networked identity provider user identity and the second networked identity provider user identity both relate to a same user.

5. The method of claim 1 wherein the first networked identity provider user identity and the second networked identity provider user identity each relate to a different user.

6. The method of claim 1 wherein facilitating establishment of the dependency comprises receiving from a user a selection of the second networked identity provider.

7. The method of claim 1 further comprising:

providing an opportunity to establish relative user characterization levels with respect to the at least one item of information in the first networked identity provider user identity and the at least one item of information in a second networked identity provider user identity to thereby influence subsequent sharing of identity information as between the first and second networked identity providers.

8. The method of claim 1 wherein facilitating establishment of the dependency comprises establishing a user-based policy that uses:

information in the first networked identity provider user identity; and

information in the second networked identity provider user identity;

to thereby provide a user-based policy that comprises a composite policy containing information that is relatively unique to each of the networked identity provider user identities.

9. The method of claim 8 wherein establishing the user-based policy further comprises establishing the user-based policy at whichever of the first and second networked identity providers the user selects.

10. The method of claim 9 wherein establishing the user-based policy at whichever of the first and second networked identity providers the user selects comprises establishing the user-based policy at whichever of the first and second networked identity providers the user identifies as having a higher relative degree of user characterization requirements.

11. A method for facilitating responding to a query using an established dependency between items of information at networked identity providers comprising:

at a first networked identity provider having a federation capability:

receiving a query regarding a user for whom the first networked identity provider has a corresponding user identity;

determining that the query requires access to at least one item of information that depends on another at least one item of information at a different networked

identity provider identity, wherein the first networked identity provider is federated with the different networked identity provider, the at least one item of information that corresponds to the different networked identity provider user identity is not available to the first networked identity provider, and a user-created dependency exists with respect to the at least one item of information that corresponds to a different networked identity provider user identity;

using the user-created dependency to facilitate responding to the query.

12. The method of claim 11 wherein using the user-created dependency to facilitate responding to the query comprises permitting the different networked identity provider to use the at least one item of information that depends on another at least one item of information at the different networked identity provider to form a response to the query without disclosing that at least one item of information to the first networked identity provider.

13. The method of claim 12 wherein permitting the different networked identity provider to use the at least one item of information further comprises permitting the different networked identity provider to use the at least one item of information as a function, at least in part, of user-assigned levels of at least one user characterization as correspond to the user-created dependency.

14. The method of claim 13 wherein permitting the different networked identity provider to use the at least one item of information as a function, at least in part, of user-assigned levels of at least one user characterization as correspond to the user-created dependency further comprises permitting the different networked identity provider to use the at least one item of information because a user-assigned level of at least one user characterization as corresponds to the item of information that corresponds to a different network identity provider has a higher relative level for the user characterization as compared to the at least one user characterization as corresponds to the item of information at the first networked identity provider.

15. The method of claim 13 wherein the at least one user characterization comprises at least one of:

a characterization regarding privacy;

a characterization regarding value;

a characterization regarding importance.

a characterization regarding priority.

16. The method of claim 12 wherein permitting the different networked identity provider to use the at least one item of information that depends on another at least one item of information at a different networked identity provider identity to form a response to the query without disclosing that at least one item of information to the first networked identity provider further comprises the first networked identity provider providing information to the different networked identity provider to vouch for user authorization regarding the different networked identity provider's authorization to form the response.

17. The method of claim 11 further comprising:

determining that the query requires access to at least one item of information at the first networked identity provider that depends on another at least one item of information at the different networked identity provider identity, wherein:

the first networked identity provider is federated with the different networked identity provider; and

the another at least one item of information at the different networked identity provider identity is available to the first networked identity provider pursuant to a user-created dependency that exists with respect to the at least one item of information that depends on another at least one item of information at the different networked identity provider user identity;

using the another at least one item of information at the first networked identity provider to facilitate responding to the query.

18. A networked identity provider comprising:

a first memory having stored therein a user identity for a user of the network identity provider;

a second memory having stored therein information regarding federation status with other networked identity providers;

a third memory having stored therein information regarding user-established user identity information dependencies between the networked identity provider and other networked identity providers with which the networked identity provider has a federation;

a processor that is operably coupled to the first, second, and third memory and that is configured and arranged to:

provide an opportunity to establish a dependency between:

at least one item of information in a first networked identity provider user identity; and

at least one item of information in another networked identity provider user identity with which the networked identity provider can be federated; and

facilitate establishment of the dependency.

19. The networked identity provider of claim 18 wherein the processor is further operably configured and arranged to provide an opportunity to establish the dependency as a function, at least in part, of user-assigned levels of user characterization to thereby control which of the networked identity providers is provided with user identity information from an opposing networked identity provider.

20. The networked identity provider of claim 18 wherein the processor is further configured and arranged to use at least one such dependency when formulating a reply to a user-authorized query.

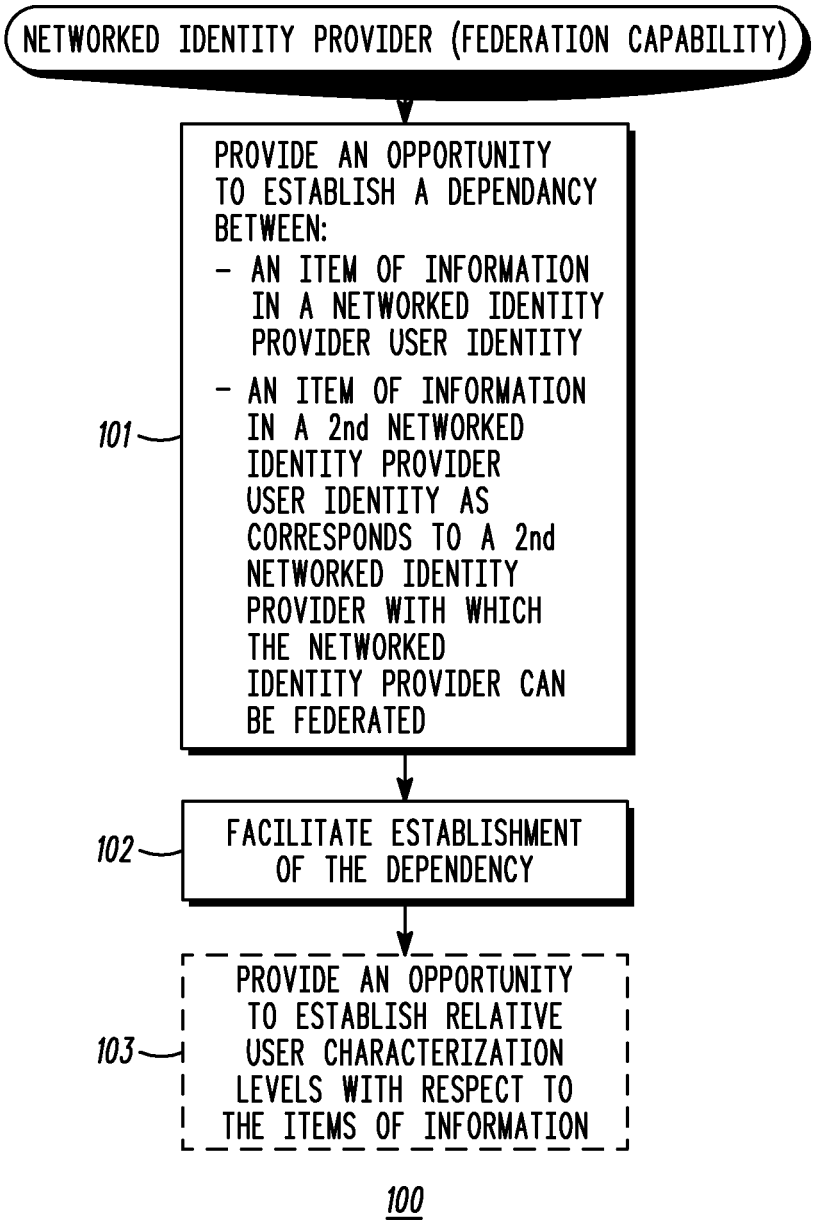

NETWORKED IDENTITY PROVIDER (FEDERATION CAPABILITY)
PROVIDE AN OPPORTUNITY TO ESTABLISH A DEPENDANCY BETWEEN:
- AN ITEM OF INFORMATION IN A NETWORKED IDENTITY PROVIDER USER IDENTITY
- AN ITEM OF INFORMATION IN A 2nd NETWORKED IDENTITY PROVIDER USER IDENTITY AS CORRESPONDS TO A 2nd NETWORKED IDENTITY PROVIDER WITH WHICH THE NETWORKED IDENTITY PROVIDER CAN BE FEDERATED
101
FACILITATE ESTABLISHMENT OF THE DEPENDENCY
102
PROVIDE AN OPPORTUNITY TO ESTABLISH RELATIVE USER CHARACTERIZATION LEVELS WITH RESPECT TO THE ITEMS OF INFORMATION
103
100

FIG. 1

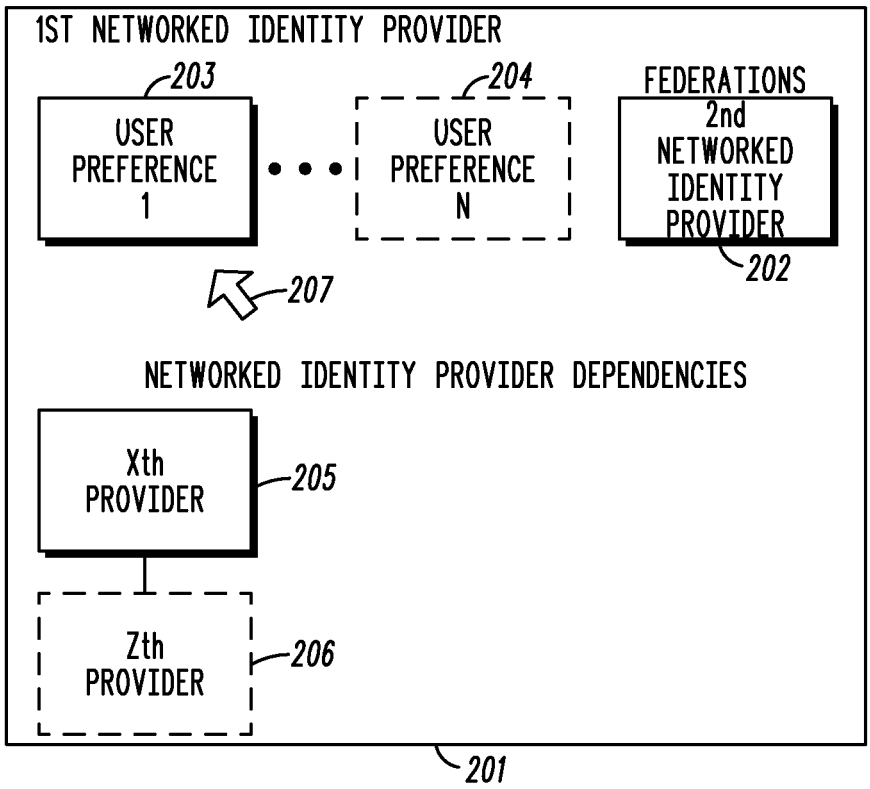


FIG. 2

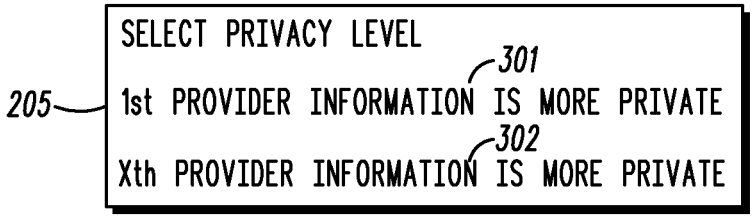


FIG. 3

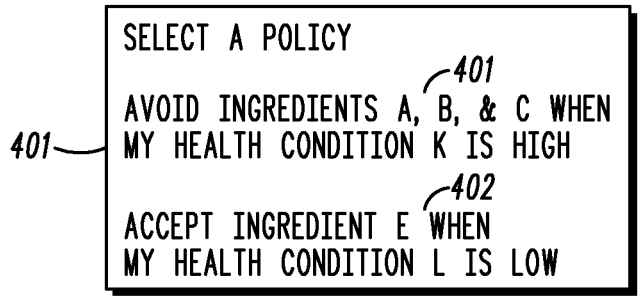


FIG. 4

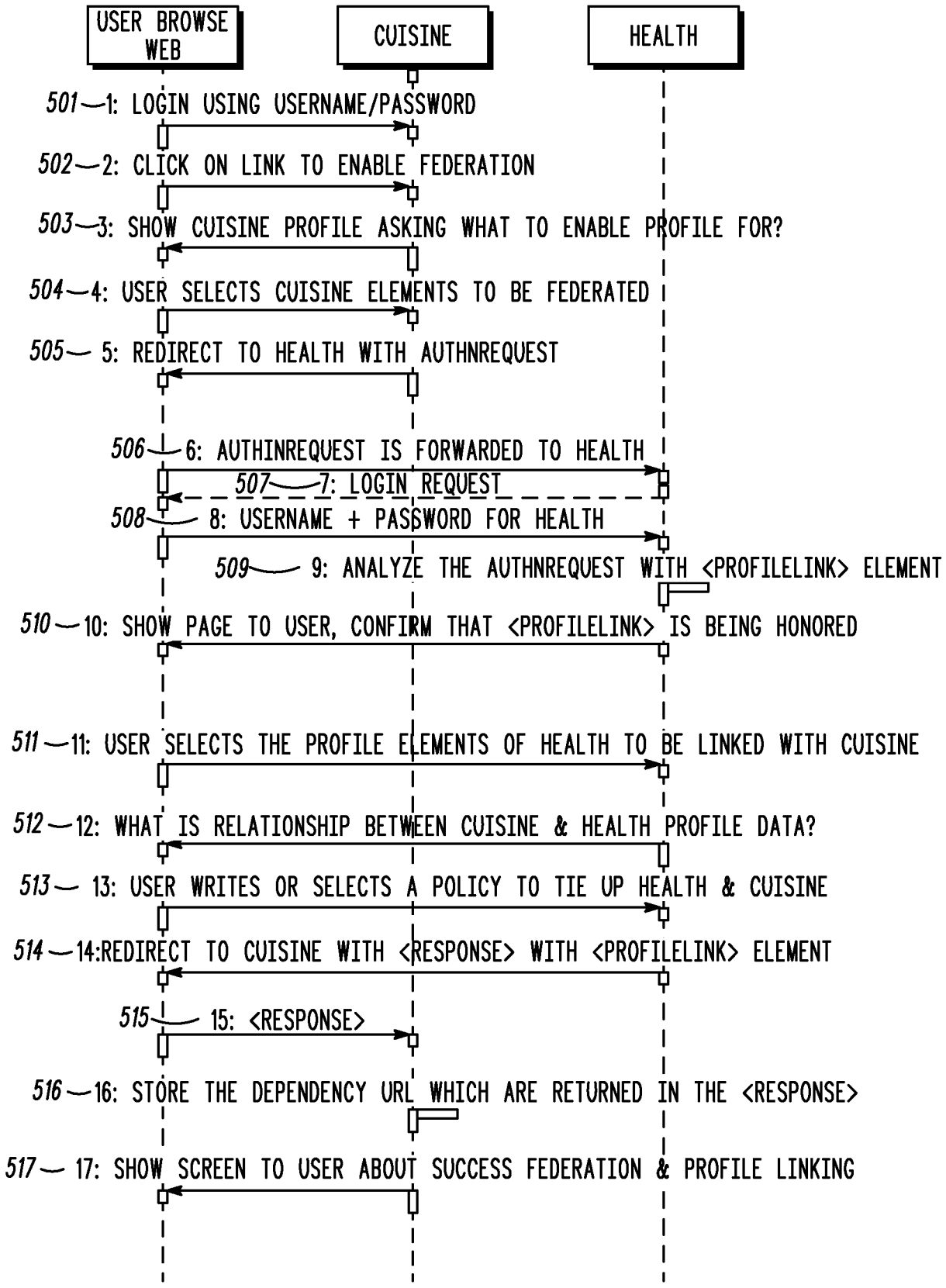

USER BROWSE WEB
CUISINE
HEALTH
501 1: LOGIN USING USERNAME/PASSWORD
502 2: CLICK ON LINK TO ENABLE FEDERATION
503 3: SHOW CUISINE PROFILE ASKING WHAT TO ENABLE PROFILE FOR?
504 4: USER SELECTS CUISINE ELEMENTS TO BE FEDERATED
505 5: REDIRECT TO HEALTH WITH AUTHNREQUEST
506 6: AUTHINREQUEST IS FORWARDED TO HEALTH
507 7: LOGIN REQUEST
508 8: USERNAME + PASSWORD FOR HEALTH
509 9: ANALYZE THE AUTHNREQUEST WITH <PROFILELINK> ELEMENT
510 10: SHOW PAGE TO USER, CONFIRM THAT <PROFILELINK> IS BEING HONORED
511 11: USER SELECTS THE PROFILE ELEMENTS OF HEALTH TO BE LINKED WITH CUISINE
512 12: WHAT IS RELATIONSHIP BETWEEN CUISINE & HEALTH PROFILE DATA?
513 13: USER WRITES OR SELECTS A POLICY TO TIE UP HEALTH & CUISINE
514 14:REDIRECT TO CUISINE WITH <RESPONSE> WITH <PROFILELINK> ELEMENT
515 15: <RESPONSE>
516 16: STORE THE DEPENDENCY URL WHICH ARE RETURNED IN THE <RESPONSE>
517 17: SHOW SCREEN TO USER ABOUT SUCCESS FEDERATION & PROFILE LINKING

FIG. 5

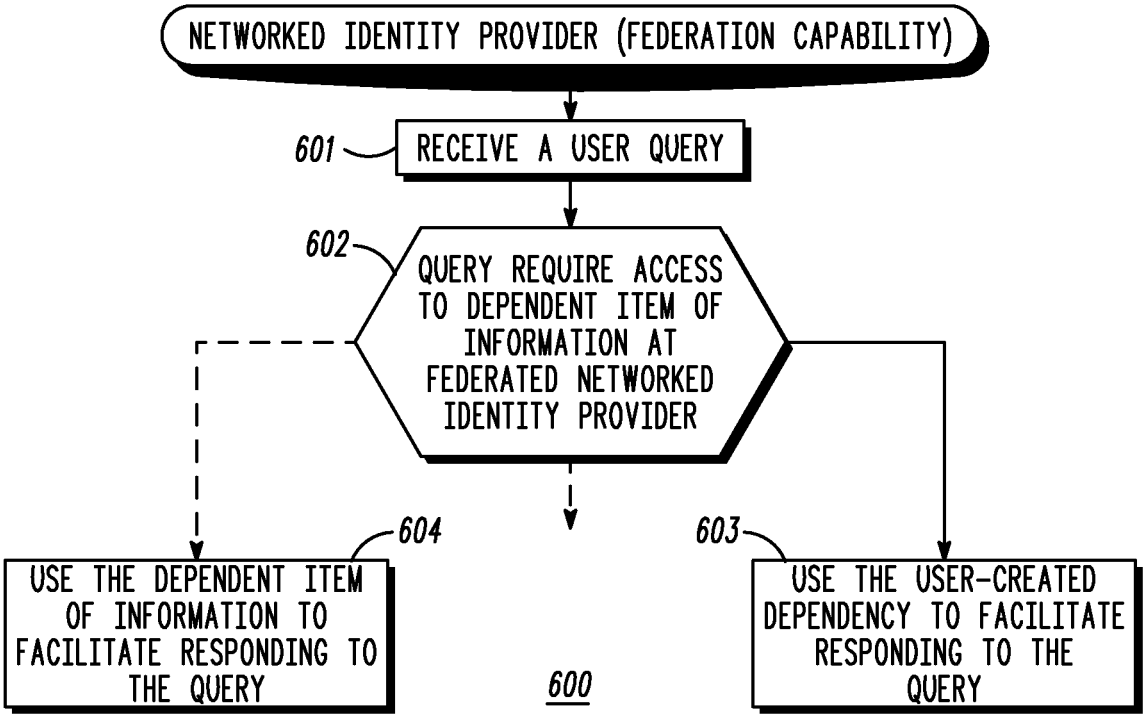

NETWORKED IDENTITY PROVIDER (FEDERATION CAPABILITY)
601
RECEIVE A USER QUERY
602
QUERY REQUIRE ACCESS TO DEPENDENT ITEM OF INFORMATION AT FEDERATED NETWORKED IDENTITY PROVIDER
604
USE THE DEPENDENT ITEM OF INFORMATION TO FACILITATE RESPONDING TO THE QUERY
603
USE THE USER-CREATED DEPENDENCY TO FACILITATE RESPONDING TO THE QUERY
600

FIG. 6

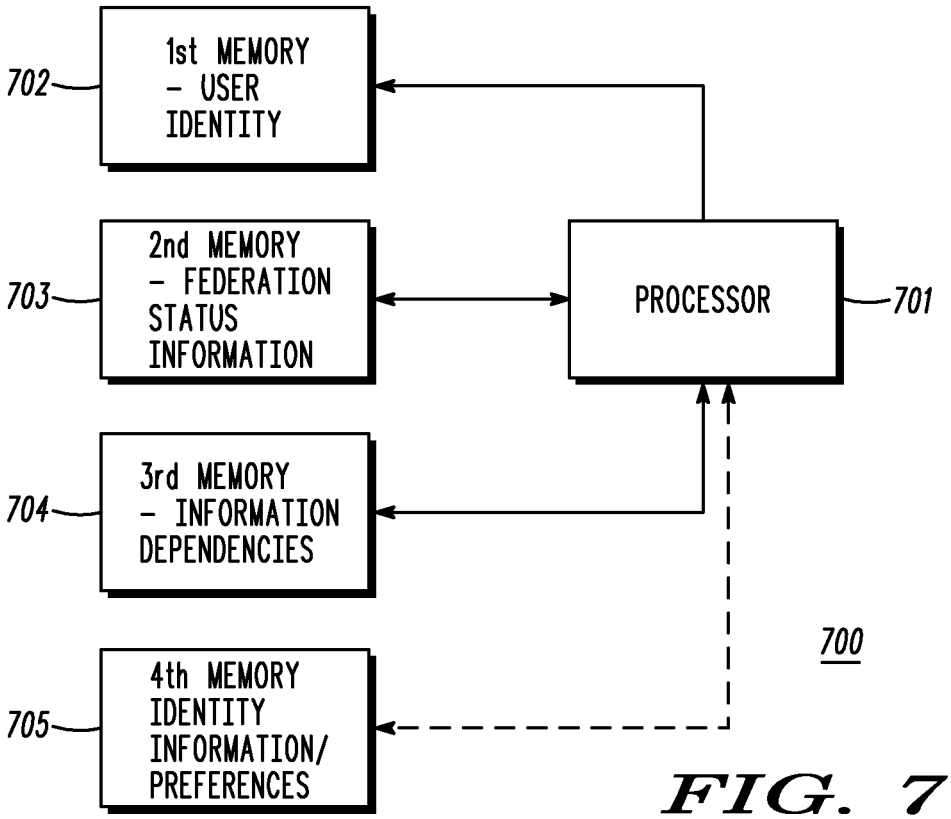

702
1st MEMORY - USER IDENTITY
703
2nd MEMORY - FEDERATION STATUS INFORMATION
PROCESSOR
701
704
3rd MEMORY - INFORMATION DEPENDENCIES
700
705
4th MEMORY IDENTITY INFORMATION/ PREFERENCES

FIG. 7