TITLE

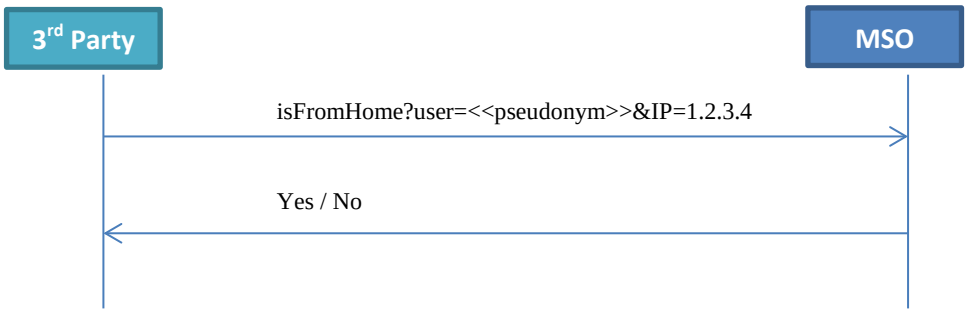
SERVICE ACCESS LOCATING

DESCRIPTION

As required, detailed embodiments of the present invention are disclosed herein; however, it is to be understood that the disclosed embodiments are merely exemplary of the invention that may be embodied in various and alternative forms. The figures are not necessarily to scale; some features may be exaggerated or minimized to show details of particular components. Therefore, specific structural and functional details disclosed herein are not to be interpreted as limiting, but merely as a representative basis for teaching one skilled in the art to variously employ the present invention.

One non-limiting aspect of the present invention relates to a way for 3rd party services to determine if the user is accessing their service from their home. Today, some MSOs have deployed Zero Sign-On (ZSO) service where, based on the IP address of the connection, they can determine who the user is (of course, with a fair degree of certainty, not 100%). A lot of services have a great need for this knowledge (home access). For example, this could be a factor used in letting the user perform certain transactions (financial, otherwise) without additional validation (out-of-band, like sending an SMS to the user conforming that they are the ones performing the transaction). Another example could be determining if content access may be allowed. MSOs can benefit, financially, by exposing this information to authorized 3rd parties.

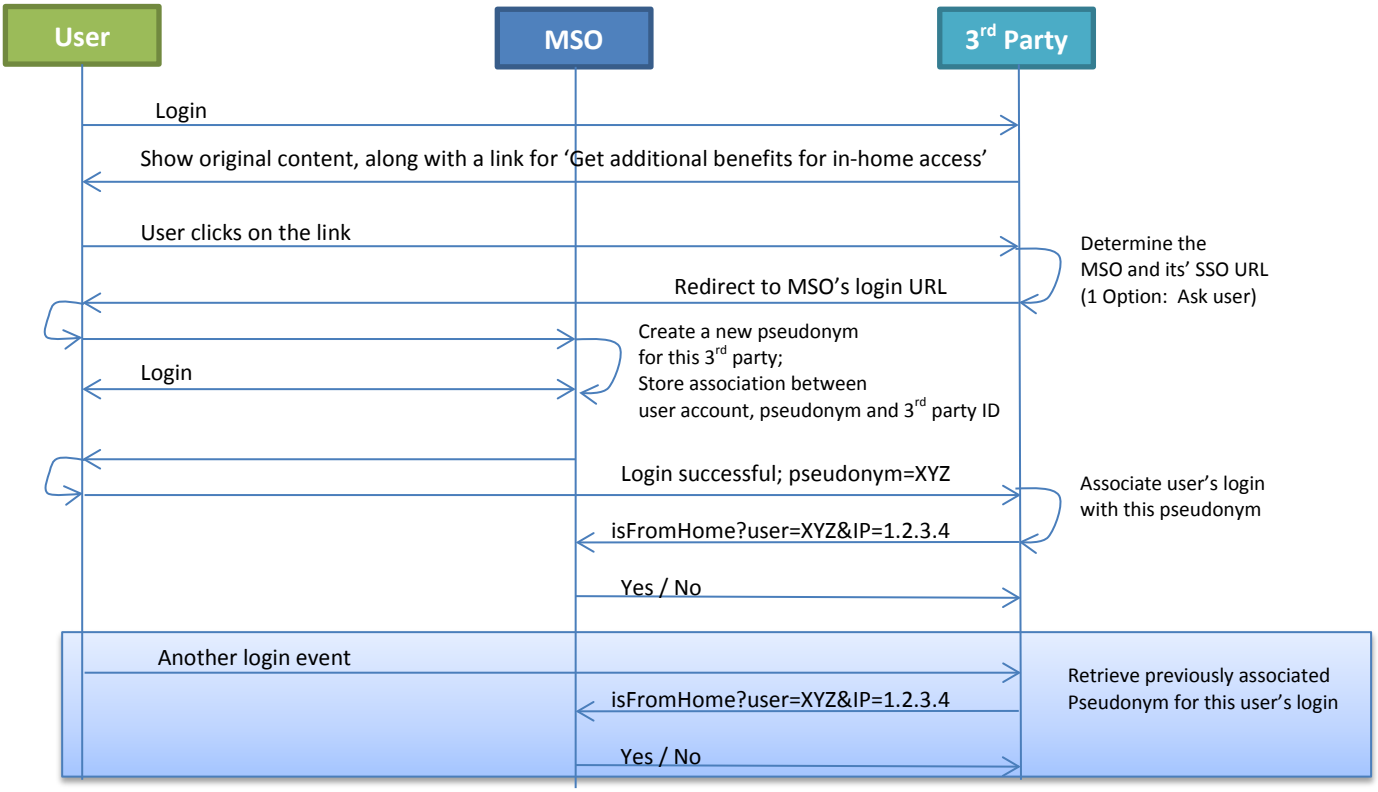
One non-limiting aspect of the present invention a primary way for any 3rd party to know if the user is accessing their service from home is to enable the 3rd party to query the MSO at run-time. The parameters passed in the query include a pseudonym for the user accessing the service and the IP address used by the user. Thus, at a high-level, the service could look like:



MSO will ensure that the 3rd party is authorized to query on behalf of the user. Also, MSO needs a way to obtain the user's account identifier from the given pseudonym. (Note: A pseudonym is used between the 3rd party and the MSO, as the MSO may not want to share the actual account identifier with the 3rd party.) These two requirements can be provide in accordance wth the present invention as shown below, called Option 1 and Option 2.

Option 1: Direct integration between the 3rd party and the MSO

In this option, there is a direct connection/integration between the 3rd party and the MSO. The flow is shown below.



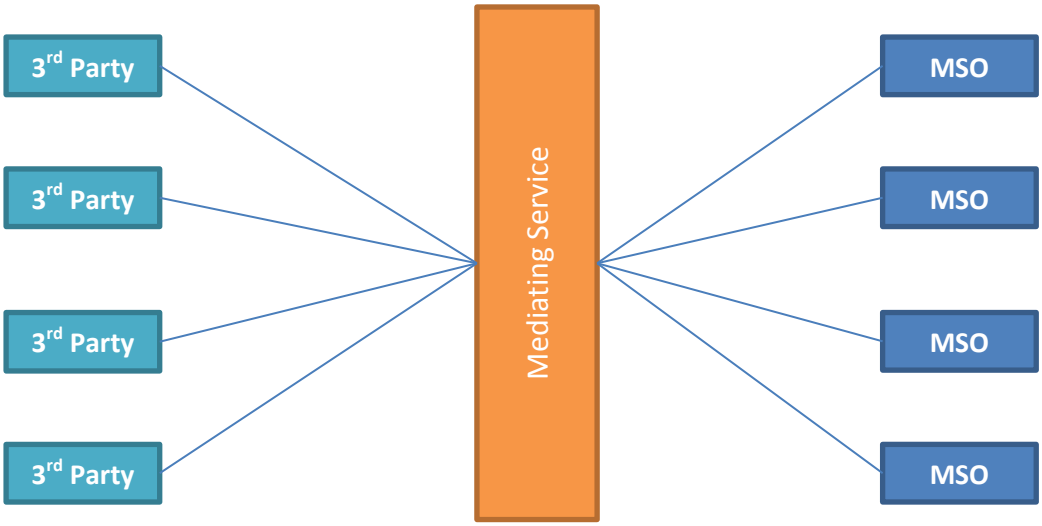
In the above figure, 3rd party systems are directly integrated with MSO's systems. The flow is described below.

1. User logs into 3rd party's web site.
2. As of this moment, 3rd party does not know who is the user's MSO/ISP
3. 3rd party asks the user if they would like this site to recognize accesses from within the user's home (mostly because there is a benefit to the user, for example, less number of steps in certain situations)
4. If the user clicks the link for the above, 3rd party creates a login request to the MSO/ISP and redirects the user to the corresponding MSO/ISP (based off of some public knowledge – like ISP corresponding to a given IP address, or based off of explicit user's choice of who their ISP is).
5. MSO/ISP performs authentication of the user.
6. After successful authentication, MSO/ISP creates a new pseudonym for this user as used when communicating with the current 3rd party.
7. MSO/ISP sends this pseudonym to the 3rd party as a browser redirect

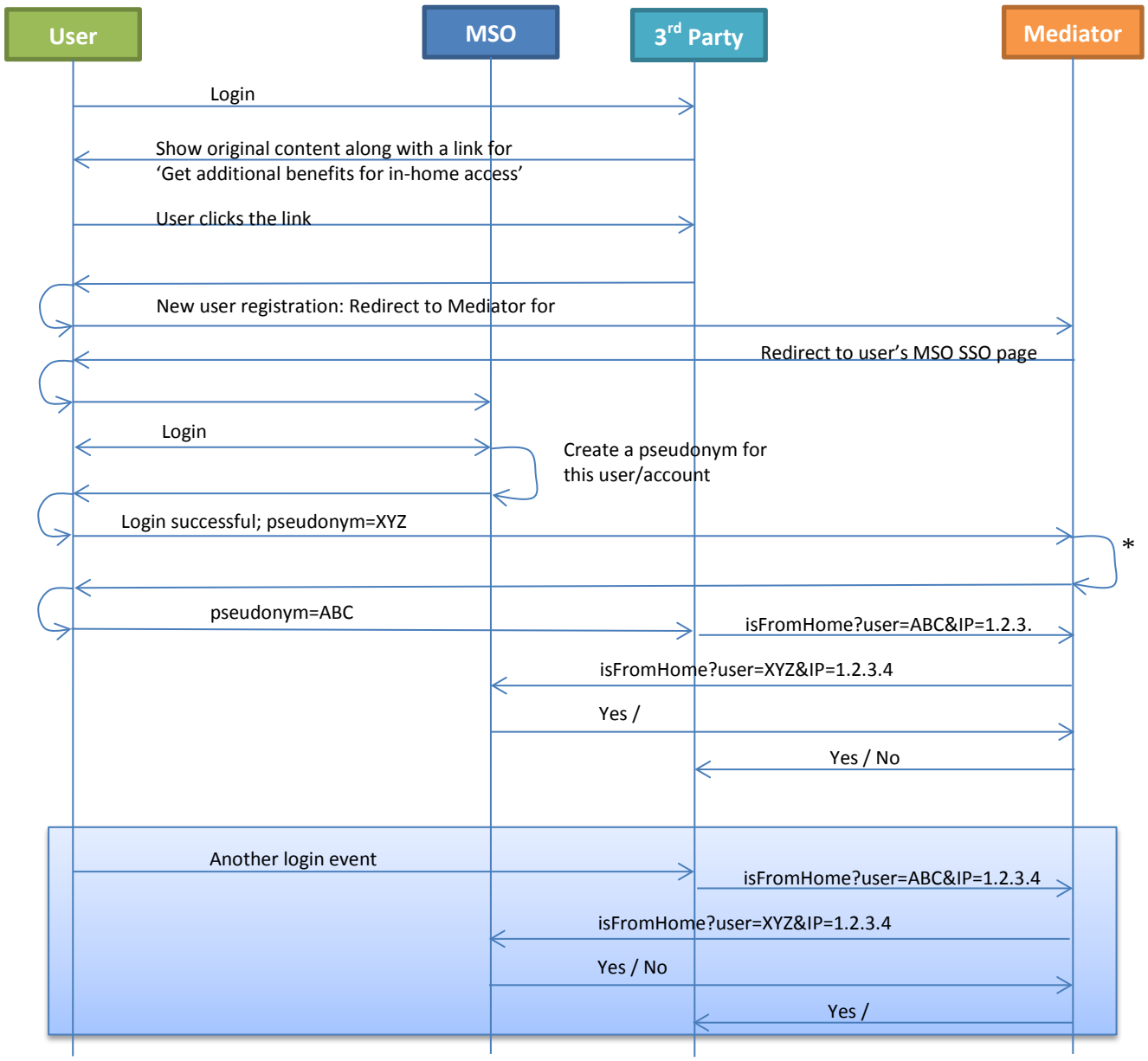
8. 3rd party will associate this pseudonym with the user's account at the 3rd party
9. 3rd party will use this pseudonym to query the MSO/ISP if a given IP address is user's home IP address.
10. MSO/ISP retrieves the account associated with the given pseudonym and 3rd party combination and verifies if the given IP address is the IP address currently allotted to this account.
11. MSO/ISP responds with a Yes or No.

Option 2: 3rd party integrates with a Mediating Service

For every 3rd party to integrate with every MSO/ISP becomes a N*N problem. That is not viable. Another approach is to let each party integrate with a mediating service, that serves as a hub.



The flow with the mediating service may be as follows:



*Create a new pseudonym for this 3rd party alone, and store the mapping between 3rd party ID, MSO pseudonym and 3rd party pseudonym

The flow shown in the above figure is explained below.

1. User logs into the 3rd party's web site
2. As of this moment, 3rd party does not know who is the user's MSO/ISP
3. 3rd party asks the user if they would like this site to recognize accesses from within the user's home (mostly because there is a benefit to the user, for example, less number of steps in certain situations)

4. If the user clicks the link for the above, 3rd party creates a login request to the Mediator and redirects the user to Mediator's login URL.
5. Mediator creates a login request to the MSO/ISP and redirects the user to the corresponding MSO/ISP (based off of some public knowledge – like ISP corresponding to a given IP address, or based off of explicit user's choice of who their ISP is).
6. MSO/ISP performs authentication of the user.
7. After successful authentication, MSO/ISP creates a new pseudonym for this user.
8. MSO/ISP sends this pseudonym to the Mediator as a browser redirect
9. Mediator will in turn create another pseudonym between the 3rd party and this specific user, and stores that mapping.
10. Mediator sends that pseudonym to the 3rd party web site as a browser redirect
11. 3rd party will associate this pseudonym with the user's account at the 3rd party
12. 3rd party will use this pseudonym to query the Mediator if a given IP address is user's home IP address.
13. Mediator will map the 3rd party given pseudonym to the MSO pseudonym and then query the MSO/ISP
14. MSO/ISP retrieves the account associated with the given pseudonym and verifies if the given IP address is the IP address currently allotted to this account.
15. MSO/ISP responds with a Yes or No.
16. Mediator responds with the above Yes or No response to the 3rd party.

As described above, one non-limiting aspect of the present invention contemplates solving the problem that 3rd parties currently face in knowing if a particular login is from a user's home. For every query, MSOs can charge a fee to the 3rd party.

While exemplary embodiments are described above, it is not intended that these embodiments describe all possible forms of the invention. Rather, the words used in the specification are words of description rather than limitation, and it is understood that various changes may be made without departing from the spirit and scope of the invention. Additionally, the

features of various implementing embodiments may be combined to form further embodiments of the invention.