Draft requirements for a shared PILOT Social2SAML gateway service

Operational

1. Initially, this service will be offered as a pilot; it is not a production service. It will be run as a single instance; there is no failover.
2. The goal is to get a simple service operational quickly, and evaluate the use of and demand for the service, and learn more about requirements. Because this is a pilot, it may be shut down on short notice. -- consequently, use at your risk.
3. The SLA associated with the GW will provide 8 X 5 coverage (business hours, Ann Arbor). There will be NO 7 X 24 coverage.
4. Initially this service will be scoped to InCommon members.
5. The gateway will, at least initially, assert the `unspecified` authentication context URI. A future version of the gateway might assert other `AuthnContext` URIs depending on the LoA of the social IdP. For example, some social IdPs (e.g., Google) are certified LoA-1 by ICAM so it would be great if the gateway could proxy an appropriate `AuthnContext` URI in this case (but there are technical issues, which is why this capability shouldn't be expected from the initial gateway deployment).
6. The browser user should only have to traverse a single Discovery Service; they should not be forced to traverse multiple DSs. (ie they shouldn't have to select "social gateway" from the local DS, and then select a specific social IDP when they reach the GW)
7. The GW will be stateless; it will not include anything resembling a Person Registry; it will not remember anything about a browser user who traverses the GW.
8. The GW is just a translator; it maps the values in the received assertion from a social identity provider to values in a SAML Assertion sent by the GW. The GW does NOT add any attributes to the SAML Assertion that are are sourced from any other sources.
9. The GW will have NO support for per-attribute or per-SP attribute filtering when constructing the SAML Assertion.
10. The GW will not attempt to address the use case of associating a SAML account and a separate social account with a single person. If this is a requirement, then the application at the SP will have to provide this functionality. This so-called "account linking" functionality is out of scope for this discussion.

Usage

1. A browser user receiving an invitation is NOT required to login from the IDP contained in the invite email

Mode 1 -- SP uses Embedded Discovery Service

Use Case: Browser User goes to an SP, and is redirected to a local Discovery Service. The DS displays some set of SAML IDPs and some set of social IDPs. The user selects an IDP, is returned to the SP, which then redirects the user to the selected IDP. For social IDPs, the user is redirected to an appropriate social-to-saml gateway, along with information indicating which social identity provider the GW should use. The GW redirects the browser user to the social identity site, the user authenticates if necessary, approves the release of some attributes, and is returned to the GW. The GW builds an appropriate SAML Assertion, and forwards the browser user to the original SP. (Note, the browser user has transparently crossed the GW, but has never seen a browser screen presented by the GW.) The SP validates the SAML Assertion, and passes control to the application.

This Use Case can be initiated with either the Invitation model (user receives an email containing a url; goes to that url; use case above initiates) or with the Self registration Model (user obtains a url, goes to that url, use case initiates). In the Invitation Model, it is the responsibility of the Application at the SP to remember which permissions or group memberships were assigned to the social user.

GW -- Handling of input, and outputs

1. SP can pass a token to the GW (indicating session at SP?); GW must return it
2. GW MUST forward to the SP the original payload from IDP in an unmolested way (I believe this refers to the Assertion coming from the social IDP, in its native format) -- see issue down below ...
3. the GW should map and then forward individual attributes ....
    a. we need to define syntax, semantics for Assertions produced by GW

Outstanding Issues

1. Should the GW forward the original assertion (the one from the social provider) ? If yes, then Google and Facebook require that each target SP register with them, and we need to figure out a way to pass that identifier to the GW.
2. Which social IDPs should the central GW support ?

DRAFT Sample text for CIO Letter

Over the last several months representatives of our campus have been participating in the discussions sponsored by the InCommon/MACE Social Identity Working Group. I think that this discussion has served an important role in understanding the roles that social identities can play in Higher Education. Recently, this group has developed a set of requirements for a centrally run gateway capable of mapping identities from social network providers (eg google, yahoo. facebook, etc) to SAML Assertions that could be consumed by the Shibboleth SP software. There are Research SPs on our campus that would find this to be a valuable way to broaden access to their sites. In addition, our campus is searching for ways to allow a variety of adjuncts in the community to gain short-term access to our LMS system; this gateway would allow that functionality without requiring that we issue Brown identities to all of these people.

We feel that prototyping and testing such a gateway is an important effort, and our campus is willing to participate in this effort through the incubator and service validation stages, for a period of six months. I feel that this testing will help to refine our understanding of needs and cost models. Operating this sort of gateway provides a great way for the community to learn as a group. We understand that there is some risk involved here, and that this may not become a full production service.

I would strongly encourage Netplus to initiate the first steps of creating a pilot service and conducting a proof-of-concept..