Draft requirements for a Social2SAML gateway service

This page is being used to develop the requirements for a Phase 1 Production Social-to-SAML Gateway. It could be run locally by a campus, or be a shared service that would be available to InCommon members.

Scope

1. Support for Google OpenID has been demonstrate
2. Prioritize other Social Identity Providers that are required:
    a. Facebook
    b. Yahoo
    c. ?

Functionality

1. The GW is just a translator; it maps the values in the assertion received from a social identity provider to values in a SAML assertion sent to the service provider. The GW does NOT add any attributes to the SAML assertion that are sourced from any other sources.
2. 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.
3. The browser user should only have to traverse a single Discovery Service; the user should not be forced to traverse multiple DSs (e.g., the user shouldn't have to select "social gateway" from the local DS, and then select a specific social IDP when they reach the GW).
4. The GW will not initially include an invitation service. However, campus-based invitation services should be able to easily use the gateway.
5. It will be transparent to the SP whether gateway or native social protocol support is used.

Management

1. The gateway can operate in either of two modes -- we need to specify which mode is needed first:
    a. a gateway (local or in the cloud) serving an entire campus (campus-level admins configure SPs to use the gateway, and there is some model for delegated administration)
    b. a gateway serving a single SP (SP admins at your campus configure their apps to use the gateway directly)
2. The gateway would include a Gateway Manager function that would allow the admin to specify, on a per SP basis:
    a. which social providers can be used (i.e., the gateway would export endpoints which the SP could use to connect through to those social providers)
    b. which algorithm is used to compute eduPersonTargetedID (ePTID) and eduPersonPrincipalName (ePPN) attributes (see next section)
    c. for the enterprise model, manage individual SPs

Attributes

1. Attributes available from various providers, and draft mappings
2. The Gateway will assert the following attributes (if provided by the social identity provider):
    a. eduPersonTargetedID
    b. eduPersonPrincipalName
    c. mail
    d. givenName
    e. sn (surName)
3. The mail, givenName, and sn attributes always pass through the Gateway as-is. eduPersonTargetedID (ePTID) and eduPersonPrincipalName (ePPN) will be computed based on the choice made in the Gateway Manager.
4. The gateway will, at least initially, assert the unspecified AuthnContext 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).
5. The GW will have NO support for per-attribute or per-SP attribute filtering when constructing the SAML Assertion. A future version of the gateway may leverage RequestedAttributes in SP metadata.
6. 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.
7. The gateway should be able to assert a persistent identifier for the user that is:
    a. predictable in advance, on a per-user basis
    b. persistent; multiple gateway instances would assert the same value

Open Questions

1. What would you anticipate using as the key identifier for social identities? email address? other?
2. Is email a required attributed? In other words, is there interest in a social IdP that does not assert email?
3. Is there a model for including "people" with social identities in groups defined in the campus ldap directory ?