Notes-ConferenceCall-March-14-2011

As of March 2011, there are already several gateway implementations that translate social identities to SAML Assertions. There seems to be one overriding reason for the strong interest in this approach -- applications and service providers would only have to support a single framework for authentication; no matter what sort of credentials or service a browser user used to authenticate, the information describing that event (and attributes describing the user) would be presented to the application in a single standard fashion. Just as importantly, applications would not have to be modified, adding support for various protocols and mechanisms; the gateway approach insulates them from that uncertainty.

Chris Phillips shared a Gliffy diagram of some possible configurations:
https://spaces.at.internet2.edu/display/socialid/March14-conf+call+notes|OpenID:display/socialid/March14-conf+call+notes|\

All of the current gateway implementations only function in one direction: from the authentication source to the application.

However, the gateway is functioning as a proxy of sorts; it represents the user to the application. Not surprisingly, there are a number of issues that need to be addressed in a standard fashion:

-- which entity does the application think is making the assertions?

Consensus --

1) in SAML terms, the entityID will be the GW (since its the asserting entity).

2) Problems obtaining attribute values. Many of the collaboration sites which would use this support want the user to present several PII-attributes (eg name, email, identifier for this principal from the social provider). However, not all social authentication providers will share this information (especially email). As a result, the application may have to present a "user profile" form the first time a user connects, and ask the user to self-assert various values.

3) Should the GW indicate which social identity provider was used for authentication ? Or is it sufficient for the GW to assert the associated LoA ?

-- social identities are at LoA 1 (decreed by the US government).

-- most campus identities are also (currently) at LoA 1. However, there was consensus that a campus-asserted identity was "stronger" than a social identity. Should the GW differentiate social, campus bronze, silver in some sort of LoA assertion ?

Consensus -- GW should assert both authN source and forward any LoA value that it receives; the application can use application context + whatever algorithm it wants to determine how it wants to treat an incoming Assertion (eg any SP can decide that social + LOA 1 --> treat as LOA 0)

4) Does the GW compute an LoA value ?

Consensus -- NO. Social identities are LoA 1; GW forwards any eduPersonAssurance attributes or Bronze/Silver assertion that it receives.

Let any further categorization emerge from experience and practice...

RI -- (conjecture) IC assurance program will recommend SAML value -- authn Context, not the attribute; rather than something made up for edu...

4) How to represent LoA -- question was asked, but no conclusion.... needs an answer

5) How should the GW map attributes provided by social identity providers to SAML Attributes ? (Note -- AI -- need a list of which attributes are provided by the various social providers)

-- are there any Attributes that are "generated" by the GW ? (eg the identity of the social identity provider?)

Other relevant ideas:

Should the GW include something in its Assertions to indicate that it is a GW (so apps don't have to match against a list of entityIDs).

because of liberty roots, SAML includes IDP chaining, which is relevant

SAML Assertions contain an element that could be used to hold the identity of the social identity provider; unfortunately, this was determined to be too hard to implement in the shibboleth v2.2.x IDP

In the UK, the Athens GW represents 200 or so campuses; each of those is represented in UK metadata; so the GW is transparent to the SPs

There was interest in requesting that the Federation operate a GW, representing google, facebook, yahoo, etc. It wasn't clear how this would work in an inter-federation scenario