TN - Recommendations on Common Standards

This section contains a set of recommendations on "standard" definitions for interfaces and data encoding across the boundatries where the various components must interact.

1. Attributes

Native SAML implementations are already using standard interfaces between web servers and application to provide the information that has been asserted by an IDP. In addition, these implementations are also leveraging a standard set of attribute syntax and semantics. These also provide a framework that can be easily extended to accommodate new attributes. The more consistent the Social-to-SAML mappings are across gateways, the easier it will be to transition away from gateways to native multi-protocol SPs.

1.1 Principles

1. Everything must be expressed in a manner that is independent of whether a native or GW implementation is being used.
2. Different social identity providers should be represented by different uri values (this is the same convention used with every other saml idp provider). This is essential for implementing Discovery in a seamless fashion. Its not necessary that every GW in the world use the same identifier for each social identity provider. Clearly, though, consistency would a good thing.
3. A given person's identifier from a given social IdP should be the same, regardless of which gateway it passed through
4. Since different Social IdPs may use different attributes to carry the user identifier, the gateway should use different attribute names to carry a given Social IdP's user identifier.
5. The SP should be able to determine which Gateway (if any) processed the request. (eg an SP might trust one GW but not another)
6. The SP should be able to determine which social IDP authenticated the user and issued the initial assertions.
7. The various social IDPs assert a variety of PII information; different providers assert different information. Any asserted PII should be mapped to the appropriate ldap/SAML attribute. 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.
8. Consistency is desirable in several areas
    a. Organization Identifiers--or Why EntityID was Guaranteed to be Misused

1.2 Gateways Mapping Social-IDP Provided Information to SAML Assertions

(similar to a profile, set down some specific rules)

1. The entityID value asserted by a Gateway as the Issuer MUST be a concatenation of (a gateway identifier) + (the social identity provider), since different GWs might use different values to represent a specific social identity provider.
2. The resulting entityID will NOT be parseable, but will be mappable (mapping file)
3. The value in the Subject/ NameID element MUST be the user identifier asserted by the social IDP. (eg a google account from one GW MUST be the same as a google account from another GW).
    a. NOTE For instance, a social-SAML gateway, or a Virtual Organization, could assert a google user identity. If they both both asserted a user identity of X@ google, presumably it is the same person being asserted by two different entities. NOTE -- accounts are different from email addresses, even though with some social providers there might have the same value).
4. The identity of the social IDP MUST be passed in the XXX attribute, and encoded as follows:
    a. Google -
5. The identity of the processing Gateway (if any) MUST be encoded as the YYY attribute
6. The identity of the browser user MUST be encoded as an attribute, and using different attribute names to represent identities coming from different social providers; using a different uri gives you the opportunity to tell GW implementers what to do
7.

We need to do an appropriate study of what all the identifiers in the social space are -- we might end up with different attributes from different providers, or different syntax in some cases.

Future Proofing SAML Assertions Containing Social IdP-Provided Information

- There will be any number of gateways in use in the near term

2. Discovery

(some text about the rules between the SP and the GW, when it comes to Discovery related issues)