Technical questions and issues

Shared practice recommendations: A discussion starter

It would be to all our benefits if we could agree to follow the same conventions to the extent feasible with regard to attribute and value syntax and semantics across implementations. That is, it would be good if Google and Twitter were known by the same identifier whether one was using the UT System gateway, the Penn State Gateway, or a native SP backdoor approach. To the extent we can converge on common practices, it will be easier for adopters of one solution to migrate to another if needed.

The first step would be to identify which items of information would benefit from standardization. A discussion starter list follows below:

Item	Description	Proposed syntax
Gateway Identifier	A value that uniquely identifies the gateway used (if any)	URI
Social Provider Identifier	A value that uniquely identifies one of the social providers (e.g., one for Google, Facebook, Twitter, Yahoo,....)	URI
Display Name	A human-friendly representation of the authenticated user's name	displayName
Given Name		givenName
Surname	A surname or surname component	sn
Principal Name	A scoped user identifier	ePPrincipalName
Email Address	The user's email	mail
Directed Identifier	A unidirectional identifier, unique to a triple of IdP, SP and user	ePTargetedId

Discussion areas about the Social Identity Protocols being ingested and gatewayed to SAML:

Conversation Point	Applicable to any Context	Context 1: Federation centric 'Social' Identity Service	Context 2: Institutional centric 'Social' Identity Service	Context 3: Federated SP, SP centric 'Social' Identity Service	Context 4: Standalone Service (non federated)
What are the dimensions of ongoing support for the given context? (e.g costs borne by SP's, impact to end users...)					
How should required attributes be dealt with?					
When 'user' is specified, what are the possible ways to appropriately identify them with a unique identifier?					
What is available as data is 'passed through' to the interior environment?					
What are the benefits / drawbacks of running a gateway in this context?					
What do I have to do as a Service Provider to leverage this particular model?				You may have additional registrations to perform for your service for each endpoint you want to allow in	