Social-to-SAML Gateway Attributes

Social-to-SAML Gateway Attributes

The following attributes contribute to a minimal gateway attribute bundle:

1. `eduPersonTargetedID` (`ePTID`)
2. `eduPersonPrincipalName` (`ePPN`)
3. `mail`
4. `displayName` OR (`givenName` AND `sn`)

Recommendations:

- Set `ePPN` to the user's email address
    - Use `ePPN` at your own risk
- Set the `mail` attribute to the user's email address
- Set the person name as appropriate
- Optionally set the `NameID` to one of the following:
    1. the user's email address
    2. `ePTID` (i.e., a SAML2 Persistent `NameID`)
    3. SAML2 Transient `NameID` (default)

The most difficult mapping is `ePTID`. The goal is to assert a value of `ePTID` that persists with or without the gateway in the middle.

Recall that `ePTID` is a triple: (IdP `entityID`, SP `entityID`, persistent opaque blob)

All three components must persist regardless of whether or not the gateway is functioning as an intermediary. For the Google OpenID Gateway, we can do this as follows.

Let's assume that the `entityID` of the Google IdP is:

`https://www.google.com/accounts/o8/id`

and the entityID of the end SP is:

`https://fm.incommon.org/sp`

(The latter is in fact the `entityID` of the Federation Manager.) Then the `ePTID` computed and asserted by the gateway is given by the triple:

IdP `entityID`: `https://www.google.com/accounts/o8/id`
SP entityID: `https://fm.incommon.org/sp`
User ID: `persistent_opaque_value`

This remains true even if the Google OpenID Gateway goes away.