Shib 2.0 IDP Changes and Attributes

IDP Configuration: **[Shibboleth 2.0]**

To interoperate with NIH the following changes/additions need to be made to the Shibboleth configuration files (examples are from NIH/InCommon interop on a Shibboleth IdP running HA_Shib):

SAML signing cert

Please make sure that your IDP signing cert hasn't expired and it is loaded up to date in the InCommon metadata as our SP doesn't accept the assertions signed by an expired certificate.

1) Attributes

Make sure attribute-resolver.xml is configured to generate the attributes:

urn:mace:dir:attribute-def:mail
urn:mace:dir:attribute-def:sn
urn:mace:dir:attribute-def:givenName

NIH prefers that EPPN be delivered with the name "urn:oid:1.3.6.1.4.1.5923.1.1.1.6", and with scopetype inline.

If you prefer not to change the default behavior, you can create a new attribute definition. You should use whatever sourceAttributeID you are already using for "eduPersonPrincipalName"

In attribute-resolver.xml:

Inline scope version of OID form of EPPN to support NIH SPs

```
<resolver:AttributeDefinition id="urn:oid:1.3.6.1.4.1.5923.1.1.1.6-with-inline-scope"
                              xsi:type="Scoped"
                              xmlns="urn:mace:shibboleth:2.0:resolver:ad"
                              scope="[YOUR_INSTITUTION_HERE].edu"
                              sourceAttributeID="[YOUR_EPPN_SOURCE_HERE]">
  <resolver:Dependency ref="[YOUR_DEPENDENCY_HERE]" />
  <resolver:AttributeEncoder xsi:type="SAML1ScopedString"
                             xmlns="urn:mace:shibboleth:2.0:attribute:encoder"
                             name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
                             scopeType="inline"/>
  <resolver:AttributeEncoder xsi:type="SAML2ScopedString"
                             xmlns="urn:mace:shibboleth:2.0:attribute:encoder"
                             name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
                             friendlyName="eduPersonPrincipalName"
                             scopeType="inline"/> </resolver:AttributeDefinition>
```

More info

https://spaces.at.internet2.edu/display/SHIB2/SAML1ScopedStringAttributeEncoder

2) Attribute Release

In attribute-filter.xml release these attributes to NIH:

NIH: release oid version of EPPN, email, surname, givenName.

```
<AttributeFilterPolicy>
  <PolicyRequirementRule xsi:type="basic:OR">
    <basic:Rule xsi:type="basic:AttributeRequesterString" value="https://federation.nih.gov/FederationGateway" />
    <basic:Rule xsi:type="basic:AttributeRequesterString" value="https://soadev.nih.gov/FederationGateway" />
  </PolicyRequirementRule>
```

```
  <AttributeRule attributeID="urn:oid:1.3.6.1.4.1.5923.1.1.1.6-with-inline-scope">
    <PermitValueRule xsi:type="basic:ANY" />
  </AttributeRule>
  <AttributeRule attributeID="email">
    <PermitValueRule xsi:type="basic:ANY" />
  </AttributeRule>
  <AttributeRule attributeID="surname">
    <PermitValueRule xsi:type="basic:ANY" />
  </AttributeRule>
  <AttributeRule attributeID="givenName">
    <PermitValueRule xsi:type="basic:ANY" />
  </AttributeRule>
</AttributeFilterPolicy>
```

3) Adjust ShibbolethSSOProfile

In the Shibboleth 1.3 instructions forceAttributePush is set true. For Shibboleth 2 the equivalent is includeAttributeStatement. You could change the default behavior of the profile, or set it specifically for the NIH SPs in relying-party.xml.

To set it for NIH SPs only, in relying-party.xml (you can put this after the end of the DefaultRelyingParty element):

```
 NIH: includeAttributeStatement true for ShibbolethSSOProfile
<RelyingParty id="https://federation.nih.gov/FederationGateway"
            provider="[YOUR_IDP_URN_HERE]"
            defaultSigningCredentialRef="[YOUR_INCOMMON_CREDENTIAL_HERE">
  <ProfileConfiguration xsi:type="saml:ShibbolethSSOProfile"
                  includeAttributeStatement="true"/>
</RelyingParty>
<RelyingParty id="https://soadev.nih.gov/FederationGateway"
            provider="[YOUR_IDP_URN_HERE]"
            defaultSigningCredentialRef="[YOUR_INCOMMON_CREDENTIAL_HERE">
  <ProfileConfiguration xsi:type="saml:ShibbolethSSOProfile"
                  includeAttributeStatement="true"/>
</RelyingParty>
```

More info http://groups.google.com/group/shibboleth-users/browse_thread/thread/ef5ea6086a2c1c9e

4) Test Link after the completion of above steps:

https://soadev.nih.gov/FederationGateway

Please contact NIHISCSupport@mail.nih.gov once you have successfully logged in.