NIH Shibboleth 1.3 IDP Configuration

NIH IDP Configuration and User support IDP Configuration: **[Shibboleth 1.3]**

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.

idp.xml:

Add the following RelyingParty (set signingCredential and nameMapping to proper values for your setup):

<RelyingParty name="https://federation.nih.gov/FederationGateway" signingCredential="incommon_cred" schemaHack="true" forceAttributePush="true" singleAssertion="true">

<NameID nameMapping="hashib_mapping"/>

</RelyingParty>

<RelyingParty name="https://soadev.nih.gov/FederationGateway" signingCredential="incommon_cred" schemaHack="true" forceAttributePush="true" singleAssertion="true">

<NameID nameMapping="hashib_mapping"/>

</RelyingParty>

resolver.xml:

Make sure that you are releasing both EPPN and OID as there is a bug in Shibb 1.3 which requires both of them to be released. If only OID is released; the scope parameter won't be added to the attribute value, that's the reason where both these attributes should be released. ***(Send EPPN as non-smart scoped using its OID number as definition - ensure that you have urn:mace:dir:attribute-def:eduPersonPrincipalName defined elsewhere in resolver.xml as a smart scoped attribute.):***

<SimpleAttributeDefinition id="urn:oid:1.3.6.1.4.1.5923.1.1.1.6" lifeTime="28800" sourceName="urn:mace:dir:attribute-def:eduPersonPrincipalName">

<AttributeDependency requires="urn:mace:dir:attribute-def:eduPersonPrincipalName"/>

</SimpleAttributeDefinition>

arp.site.xml:

<Rule>

<Target>

<Requester matchFunction="urn:mace:shibboleth:arp:matchFunction:exactShar">https://federation.nih.gov/FederationGateway</Requester>

</Target>

<Attribute name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6">

<AnyValue release="permit"/>

</Attribute>

</Rule>

<Rule>

<Target>

<Requester matchFunction="urn:mace:shibboleth:arp:matchFunction:exactShar">https://soadev.nih.gov/FederationGateway</Requester>

</Target>

<Attribute name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6">

<AnyValue release="permit"/>

</Attribute>

</Rule>

More information is available from https://spaces.at.internet2.edu/display/SHIB/AlternateProfiles

FAQ:-

Q) Having concern that when an IDP releases this attribute "urn:oid:1.3.6.1.4.1.5923.1.1.1.6" to other Shibboleth SPs that expect a scoped attribute as SPs prefer oid format rather than name. If IDP doesn't scope the attribute and pass the scope as part of value itself it may break their apps.

A) No it won't break any application with other SPs as this attribute is profiled in that way.

https://mail.internet2.edu/wws/arc/shibboleth-users/2009-01/msg00156.html

Q) Isn't "urn:oid:1.3.6.1.4.1.5923.1.1.1.6" same as EPPN, eduPersonPrincipalName?

A) Yes both are same but the value for EEPN is not inline scope.

Attribute xmlns:typens="**urn:mace:shibboleth:1.0**" AttributeName="**urn:mace:dir:attribute-def:eduPersonPrincipalName**" AttributeNamespace="**urn:mace:shibboleth:1.0:attributeNamespace:uri**">

<AttributeValue Scope="**university.edu**" xsi:type="**typens:AttributeValueType**">**someone**</AttributeValue>

Value for urn:oid:1.3.6.1.4.1.5923.1.1.1.6 is inline scope.

Attribute xmlns:typens="**urn:mace:shibboleth:1.0**" AttributeName="**urn:oid:1.3.6.1.4.1.5923.1.1.1.6**" AttributeNamespace="**urn:mace:shibboleth:1.0:attributeNamespace:uri**">

<AttributeValue xsi:type="**typens:AttributeValueType**">someone@university.edu (mailto:someone@university.eduAttributeValue>

Since our SP cannot process the scope parameter we are requesting the universities to release both these (EPPN and urn:oid:1.3.6.1.4.1.5923.1.1.1.6) attributes in the above format.

At the minimum these are the attributes we are requesting:-

urn:mace:dir:attribute-def:eduPersonPrincipalName
urn:mace:dir:attribute-def:mail
urn:mace:dir:attribute-def:sn
urn:mace:dir:attribute-def:givenName
urn:oid:1.3.6.1.4.1.5923.1.1.1.6

NOTE: You can release additional attributes in the rule by adding additional <Attribute> entries. What additional attributes you release should be determined on a case by case basis. For NIH, we will request the following attributes will be required for all LOA1 Service Providers:

Given name of person -required as agreed upon MOA w/InCommon - will not break an application

Surname of person -required as agreed upon MOA w/InCommon - will not break an application

LOA - assumed 1 - not required for LOA 1 apps - will certainly lead to lively discussions with Silver ...

Contact email address = mail attribute (internal MACE discussion) required as agreed upon MOA w/InCommon - may break an application

This should be an email address to allow contacting the person. It need not be an institution assigned address, but should be an address at which the person normally received work-related email. It will not be displayed to others except administrators and those people the person is choosing to collaborate with.

Unique identifier - required as agreed upon MOA w/InCommon - will break an application EPPN - required AND EPTID if available

Out of band - we would like to know if the institute recycles the EPPN

Institution Affiliation - required as agreed upon MOA w/InCommon - may break an application

As per suggestion of MACE we have created an NIH Namespace(https://federation.nih.gov/FederationGateway/MACENamespaces/). Below is a sample Actual namespace to be posted week of July 7th - top level only ...threw in a child attribute to give us something to think about ... will lead to larger organizational discussions later.

Example Values:-

Dartmouth	http://federation.nih.gov/participant/Dartmouth
Duke University	http://federation.nih.gov/participant/DukeUniversity
Duke University Medical Center	http://federation.nih.gov/participant/DukeUniversity/MedicalCenter
Sloan Kettering	http://federation.nih.gov/participant/SloanKettering

End User support:

We would like to gather some additional support information to assist both the application owner and/or end-user. Our intent is to gather into a general support matrix that we hope will be useful for others. Please provide answers to the questions listed below. Any other relevant information you would like to provide is greatly appreciated.

- Do most end users already have an account assigned to them? If not, how is one assigned?
- Would an end user know what their user account is?
- Would they recognize it by another name such as NetID?
- Do you have a support/helpdesk group we should route your users to?
    - What are their business hours and after hours contact information?
- We understand that its possible that some of your college/medical centers not know that there is an IDP in place. If that is the case - whom should they contact?
- How would you like us to direct/route end user support questions?

Please contact NIHISCSupport@mail.nih.gov **for any questions regarding the interop.**

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.**