How To connect an EduGain Shibboleth Service Provider to the CTA Grouper Authorization Infrastructure

Exchange the SP metadata with Grouper Attribute Authority:
Send your SP medatada file to the Help desk: grouper-helpdesk@oact.inaf.it and in your working copy of the Shibboleth SP follow these steps:

a. Copy grouper Attribute Authority Metadata (https://grouper.oact.inaf.it/Shibboleth.sso/Metadata) in the path:
/etc/shibboleth/CTA-grouper-metadata.xml

b. Modify “shibboleth2.xml” by adding the line :

```
<!-- Loads and trusts a metadata for the grouper Attribute Authority-->
<MetadataProvider type="XML" path="/etc/shibboleth/CTA-grouper-metadata.xml "/>
```

- Modify “shibboleth2.xml” by adding this new AttributeResolver:

```
<!-- Attribute and trust options you shouldn't need to change. -->
<AttributeExtractor type="XML" validate="true" path="attribute-map.xml"/>
<AttributeResolver type="Query" subjectMatch="true"/>
        <AttributeResolver type="SimpleAggregation" attributeId="eppn" format="urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified">
        <Entity>https://grouper.oact.inaf.it/idp/shibboleth</Entity>
</AttributeResolver>
```

- Edit “attribute-map.xml” to resolve the new attribute “isMemberOf” and “eduPersonEntitlement”

```
<Attribute name="urn:mace:dir:attribute-def:eduPersonEntitlement" id="entitlement" />
<Attribute name="urn:oid:1.3.6.1.4.1.5923.1.1.1.7" id="entitlement" />
...
<Attribute name="urn:oid:1.2.840.113556.1.666.1" id="isMemberOf"/>
```

- Configure the policy of the SP by editing "attribute-policy.xml" to retrieve “isMemberOf” and “eduPersonEntitlement” attributes:

```
<!-- Require isMemberOf and eduPersonEntitlement to be released only by Grouper AA -->
<afp:AttributeRule attributeID="isMemberOf">
<afp:PermitValueRule xsi:type="basic:AttributeIssuerString" value="https://grouper.oact.inaf.it/idp/shibboleth" />
</afp:AttributeRule>
<afp:AttributeRule attributeID="eduPersonEntitlement">
<afp:PermitValueRule xsi:type="basic:AttributeIssuerString" value="https://grouper.oact.inaf.it/idp/shibboleth" />
</afp:AttributeRule>
```

- Restart the shibd service

- log-in on the application protected by the SP and see if the attributes “isMemberOf” and “eduPersonEntitlement” are released by checking the /Shibboleth.sso/Session page of your SP.

acknowledgement section:

thanks to Marco Malavolti malavolti@garr.it
and to the GARR consortium. http://www.garr.it/