# Example of a standard attribute resolver for Shibboleth IdP v5 and above

This is an example of a standard attribute resolver for SWAMID 2.0 in a Shibboleth IdP which contains definitions of alla attribute defined in SWAMID's Entity Category attribute release in SWAMID. Check the comments in the XML and replace any values as needed. Furthermore, check that you read the attributes from the correct data source.

The latest published SWAMID example standard resolver for Shibboleth Identity Provider is published at https://mds.swamid.se/entity-configurations/Shibboleth-IdP/v4/attribute-resolver.xml. Below is the latest version included from the publication repository.
The repository is in the process of being re-tagged for IdPv5. The v4 files work just fine with IdPv5.

```
<?xml version="1.0" encoding="UTF-8"?>
<!--
    This file is an EXAMPLE configuration file for use within the
    SWAMID federation containing lots of example attributes, encoders,
    and a couple of example data connectors.

    Not all attribute definitions or data connectors are demonstrated, but
    a variety of LDAP attributes, some common to Shibboleth deployments and
    many not, are included.

    Deployers should refer to the Identity Provider documentation

    https://wiki.shibboleth.net/confluence/display/IDP4/AttributeResolverConfiguration

    for a complete list of components and their options.
-->
<AttributeResolver
        xmlns="urn:mace:shibboleth:2.0:resolver"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="urn:mace:shibboleth:2.0:resolver http://shibboleth.net/schema/idp/shibboleth-
attribute-resolver.xsd">

    <!-- ========================================== -->
    <!--      Attribute Definitions                 -->
    <!-- ========================================== -->

    <!-- Schema: Core schema attributes-->
    <AttributeDefinition xsi:type="Simple" id="uid">
        <InputDataConnector ref="myLDAP" attributeNames="uid"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:uid" encodeType="false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:0.9.2342.19200300.100.1.1" friendlyName="uid"
encodeType="false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Simple" id="mail">
        <InputDataConnector ref="myLDAP" attributeNames="mail"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:mail" encodeType="false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:0.9.2342.19200300.100.1.3" friendlyName="mail"
encodeType="false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Simple" id="homePhone">
        <InputDataConnector ref="myLDAP" attributeNames="homePhone"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:homePhone" encodeType="false"
/>
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:0.9.2342.19200300.100.1.20" friendlyName="
homePhone" encodeType="false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Simple" id="homePostalAddress">
        <InputDataConnector ref="myLDAP" attributeNames="homePostalAddress"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:homePostalAddress"
encodeType="false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:0.9.2342.19200300.100.1.39" friendlyName="
homePostalAddress" encodeType="false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Simple" id="mobileNumber">
```

```
        <InputDataConnector ref="myLDAP" attributeNames="mobile"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:mobile" encodeType="false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:0.9.2342.19200300.100.1.41" friendlyName="
mobile" encodeType="false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Simple" id="pagerNumber">
        <InputDataConnector ref="myLDAP" attributeNames="pager"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:pager" encodeType="false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:0.9.2342.19200300.100.1.42" friendlyName="pager"
encodeType="false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Simple" id="sn">
        <InputDataConnector ref="myLDAP" attributeNames="sn"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:sn" encodeType="false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:2.5.4.4" friendlyName="sn" encodeType="false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Simple" id="cn">
        <InputDataConnector ref="myLDAP" attributeNames="cn"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:cn" encodeType="false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:2.5.4.3" friendlyName="cn" encodeType="false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Simple" id="locality">
        <InputDataConnector ref="myLDAP" attributeNames="l"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:l" encodeType="false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:2.5.4.7" friendlyName="l" encodeType="false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Simple" id="stateProvince">
        <InputDataConnector ref="myLDAP" attributeNames="st"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:st" encodeType="false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:2.5.4.8" friendlyName="st" encodeType="false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Simple" id="street">
        <InputDataConnector ref="myLDAP" attributeNames="street"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:street" encodeType="false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:2.5.4.9" friendlyName="street" encodeType="
false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Simple" id="o">
        <InputDataConnector ref="staticAttributes" attributeNames="o"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:o" encodeType="false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:2.5.4.10" friendlyName="o" encodeType="false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Simple" id="ou">
        <InputDataConnector ref="myLDAP" attributeNames="ou"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:ou" encodeType="false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:2.5.4.11" friendlyName="ou" encodeType="false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Simple" id="title">
        <InputDataConnector ref="myLDAP" attributeNames="title"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:title" encodeType="false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:2.5.4.12" friendlyName="title" encodeType="
false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Simple" id="postalAddress">
        <InputDataConnector ref="myLDAP" attributeNames="postalAddress"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:postalAddress" encodeType="
false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:2.5.4.16" friendlyName="postalAddress"
encodeType="false" />
    </AttributeDefinition>
```

```
    <AttributeDefinition xsi:type="Simple" id="postalCode">
        <InputDataConnector ref="myLDAP" attributeNames="postalCode"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:postalCode" encodeType="
false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:2.5.4.17" friendlyName="postalCode" encodeType="
false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Simple" id="postOfficeBox">
        <InputDataConnector ref="myLDAP" attributeNames="postOfficeBox"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:postOfficeBox" encodeType="
false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:2.5.4.18" friendlyName="postOfficeBox"
encodeType="false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Simple" id="telephoneNumber">
        <InputDataConnector ref="myLDAP" attributeNames="telephoneNumber"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:telephoneNumber" encodeType="
false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:2.5.4.20" friendlyName="telephoneNumber"
encodeType="false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Simple" id="givenName">
        <InputDataConnector ref="myLDAP" attributeNames="givenName"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:givenName" encodeType="false"
/>
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:2.5.4.42" friendlyName="givenName" encodeType="
false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Simple" id="initials">
        <InputDataConnector ref="myLDAP" attributeNames="initials"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:initials" encodeType="false"
/>
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:2.5.4.43" friendlyName="initials" encodeType="
false" />
    </AttributeDefinition>

    <!-- Schema: inetOrgPerson attributes-->
    <AttributeDefinition xsi:type="Simple" id="departmentNumber">
        <InputDataConnector ref="myLDAP" attributeNames="departmentNumber"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:departmentNumber" encodeType="
false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:2.16.840.1.113730.3.1.2" friendlyName="
departmentNumber" encodeType="false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Simple" id="displayName">
        <InputDataConnector ref="myLDAP" attributeNames="displayName"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:displayName" encodeType="
false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:2.16.840.1.113730.3.1.241" friendlyName="
displayName" encodeType="false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Simple" id="employeeNumber">
        <InputDataConnector ref="myLDAP" attributeNames="employeeNumber"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:employeeNumber" encodeType="
false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:2.16.840.1.113730.3.1.3" friendlyName="
employeeNumber" encodeType="false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Simple" id="employeeType">
        <InputDataConnector ref="myLDAP" attributeNames="employeeType"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:employeeType" encodeType="
false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:2.16.840.1.113730.3.1.4" friendlyName="
employeeType" encodeType="false" />
```

```
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Simple" id="jpegPhoto">
        <InputDataConnector ref="myLDAP" attributeNames="jpegPhoto"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:jpegPhoto" encodeType="false"
/>
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:0.9.2342.19200300.100.1.60" friendlyName="
jpegPhoto" encodeType="false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Simple" id="preferredLanguage">
        <InputDataConnector ref="myLDAP" attributeNames="preferredLanguage"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:preferredLanguage"
encodeType="false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:2.16.840.1.113730.3.1.39" friendlyName="
preferredLanguage" encodeType="false" />
    </AttributeDefinition>

    <!-- Schema: eduPerson attributes -->
    <AttributeDefinition xsi:type="Simple" id="eduPersonAffiliation">
        <InputDataConnector ref="myLDAP" attributeNames="eduPersonAffiliation" />
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:eduPersonAffiliation"
encodeType="false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:1.3.6.1.4.1.5923.1.1.1.1" friendlyName="
eduPersonAffiliation" encodeType="false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Simple" id="eduPersonEntitlement">
        <InputDataConnector ref="myLDAP" attributeNames="eduPersonEntitlement"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:eduPersonEntitlement"
encodeType="false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:1.3.6.1.4.1.5923.1.1.1.7" friendlyName="
eduPersonEntitlement" encodeType="false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Simple" id="eduPersonNickname">
        <InputDataConnector ref="myLDAP" attributeNames="eduPersonNickname"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:eduPersonNickname"
encodeType="false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:1.3.6.1.4.1.5923.1.1.1.2" friendlyName="
eduPersonNickname" encodeType="false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Simple" id="eduPersonPrimaryAffiliation">
        <InputDataConnector ref="myLDAP" attributeNames="eduPersonPrimaryAffiliation"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:eduPersonPrimaryAffiliation"
encodeType="false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:1.3.6.1.4.1.5923.1.1.1.5" friendlyName="
eduPersonPrimaryAffiliation" encodeType="false" />
    </AttributeDefinition>

    <!-- Use this if the eduPersonPrincipalName is stored in myLDAP -->
    <!--
    <AttributeDefinition xsi:type="Prescoped" id="eduPersonPrincipalName">
        <InputDataConnector ref="myLDAP" attributeNames="eduPersonPrincipalName"/>
        <AttributeEncoder xsi:type="SAML1ScopedString" name="urn:mace:dir:attribute-def:eduPersonPrincipalName"
encodeType="false" />
        <AttributeEncoder xsi:type="SAML2ScopedString" name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6" friendlyName="
eduPersonPrincipalName" encodeType="false" />
    </AttributeDefinition>
    -->

    <!-- Or this if you want a scoped eduPersonPrincipalName. Change the attributeNames as appropriate to your
LDAP -->
    <AttributeDefinition xsi:type="Scoped" id="eduPersonPrincipalName" scope="%{idp.scope}">
        <InputDataConnector ref="myLDAP" attributeNames="uid"/>
        <AttributeEncoder xsi:type="SAML1ScopedString" name="urn:mace:dir:attribute-def:eduPersonPrincipalName"
encodeType="false" />
        <AttributeEncoder xsi:type="SAML2ScopedString" name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6" friendlyName="
eduPersonPrincipalName" encodeType="false" />
    </AttributeDefinition>
```

```
    <AttributeDefinition xsi:type="Prescoped" id="eduPersonPrincipalNamePrior">
        <InputDataConnector ref="myLDAP" attributeNames="eduPersonPrincipalNamePrior"/>
        <AttributeEncoder xsi:type="SAML1ScopedString" name="urn:oid:1.3.6.1.4.1.5923.1.1.1.12" encodeType="
false" />
        <AttributeEncoder xsi:type="SAML2ScopedString" name="urn:oid:1.3.6.1.4.1.5923.1.1.1.12" friendlyName="
eduPersonPrincipalNamePrior" encodeType="false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Scoped" id="eduPersonScopedAffiliation" scope="%{idp.scope}">
        <InputDataConnector ref="myLDAP" attributeNames="eduPersonAffiliation"/>
        <AttributeEncoder xsi:type="SAML1ScopedString" name="urn:mace:dir:attribute-def:
eduPersonScopedAffiliation" encodeType="false" />
        <AttributeEncoder xsi:type="SAML2ScopedString" name="urn:oid:1.3.6.1.4.1.5923.1.1.1.9" friendlyName="
eduPersonScopedAffiliation" encodeType="false" />
    </AttributeDefinition>

    <!-- filteredLDAPEduPersonAssurance script which checks if the user has AL2 or AL3 in LDAP and releases
them together with appropriate similar RAF attributes -->
    <!-- AL3 is only released if the SP has requested Refeds MFA authentication context -->
    <!-- Output of this script must be used in the eduPersonAssurance attribute definition -->
    <!-- NOTE WELL - You must ensure that you only release attribute values that your organisation has approval
for! Read through this code and understand it fully before using it! -->
    <AttributeDefinition id="filteredLDAPEduPersonAssurance" xsi:type="ScriptedAttribute">
        <InputDataConnector ref="myLDAP" attributeNames="eduPersonAssurance"/>
        <InputDataConnector ref="staticAttributes" attributeNames="allowedLDAPEduPersonAssurance"/>
        <Script><![CDATA[
            logger = Java.type("org.slf4j.LoggerFactory").getLogger("net.shibboleth.idp.attribute.resolver.
eppnbuilder");
            mfaPrincipalName = "https://refeds.org/profile/mfa";
            al3Assurance = "http://www.swamid.se/policy/assurance/al3"
            al2Assurance = "http://www.swamid.se/policy/assurance/al2"
            rafMedium = "https://refeds.org/assurance/IAP/medium"
            rafHigh = "https://refeds.org/assurance/IAP/high"
            rafLocalEnterprise = "https://refeds.org/assurance/IAP/local-enterprise"
            rafCappuccino = "https://refeds.org/assurance/profile/cappuccino"
            rafEspresso = "https://refeds.org/assurance/profile/espresso"
            try {
              // Loop over the eduPersonAssurance values stored in the backend
              for(i = 0; i < eduPersonAssurance.getValues().size(); i++)
              {
                value = eduPersonAssurance.getValues().get(i);
                // Check value against the static attribute id allowLDAPEduPersonAssurance which contains the
values we can process below
                if (allowedLDAPEduPersonAssurance.getValues().contains(value))
                {
                  // If the user has AL2 in our backend, we add AL2, rafLocalEnterprise and rafMedium to
eduPersonAssurance.
                  if (value == al2Assurance)
                  {
                    filteredLDAPEduPersonAssurance.addValue(value);
                    filteredLDAPEduPersonAssurance.addValue(rafMedium);
                    filteredLDAPEduPersonAssurance.addValue(rafCappuccino);
                    filteredLDAPEduPersonAssurance.addValue(rafLocalEnterprise);
                  }
                  // If the user has AL3 in our backend...
                  if (value == al3Assurance)
                  {
                    // Following ascertains if the SP has requested Refeds MFA
                    if (profileContext)
                    {
                      authenticationContext = profileContext.getSubcontext("net.shibboleth.idp.authn.context.
AuthenticationContext");
                      if(authenticationContext)
                      {
                        requestedPrincipalContext = authenticationContext.getSubcontext("net.shibboleth.idp.
authn.context.RequestedPrincipalContext");
                        if(requestedPrincipalContext)
                        {
                          matchingPrincipal = requestedPrincipalContext.getMatchingPrincipal();
                          if (matchingPrincipal && matchingPrincipal.getName() == mfaPrincipalName)
```

```
                            {
                              // User is AL3 and we are logging in with MFA, release AL3 assurance, rafHigh and
rafEspresso
                              filteredLDAPEduPersonAssurance.addValue(value);
                              filteredLDAPEduPersonAssurance.addValue(rafHigh);
                              filteredLDAPEduPersonAssurance.addValue(rafEspresso);
                            }
                          }
                        }
                      }
                    }
                  }
                }
              } catch(err) {
                  // Put a warning in the logs, might be wrong in LDAP, or this script! The static variables will
still be released.
                  logger.info("eduPersonAssurance not set in LDAP.");
              }
        ]]>
        </Script>
    </AttributeDefinition>

    <!-- eduPersonAssurance - output from script above together with the base RAF and AL1 that are always
released -->
    <!-- NOTE WELL: Your organisation must be approved for at least AL1 to use this! -->
    <AttributeDefinition xsi:type="Simple" id="eduPersonAssurance">
        <InputAttributeDefinition ref="filteredLDAPEduPersonAssurance" />
        <InputDataConnector ref="staticAttributes" attributeNames="refedsAssuranceFramework assuranceLevel1"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:eduPersonAssurance"
encodeType="false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:1.3.6.1.4.1.5923.1.1.1.11" friendlyName="
eduPersonAssurance" encodeType="false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Simple" id="eduPersonOrcid">
        <InputDataConnector ref="myLDAP" attributeNames="eduPersonOrcid"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:eduPersonOrcid" encodeType="
false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:1.3.6.1.4.1.5923.1.1.1.16" friendlyName="
eduPersonOrcid" encodeType="false" />
    </AttributeDefinition>

    <!-- Deprecated eduPersonUniqueId -->
    <!--
    <AttributeDefinition xsi:type="Scoped" id="eduPersonUniqueId" scope="%{idp.scope}">
        <InputDataConnector ref="myLDAP" attributeNames="uid"/>
        <AttributeEncoder xsi:type="SAML1ScopedString" name="urn:oid:1.3.6.1.4.1.5923.1.1.1.13" encodeType="
false" />
        <AttributeEncoder xsi:type="SAML2ScopedString" name="urn:oid:1.3.6.1.4.1.5923.1.1.1.13" friendlyName="
eduPersonUniqueId" encodeType="false" />
    </AttributeDefinition>
    -->

    <!-- Schema: norEdu* attributes -->
    <AttributeDefinition xsi:type="Simple" id="norEduPersonLegalName">
        <InputDataConnector ref="myLDAP" attributeNames="norEduPersonLegalName"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:norEduPersonLegalName"
encodeType="false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:1.3.6.1.4.1.2428.90.1.10" friendlyName="
norEduPersonLegalName" encodeType="false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Simple" id="norEduPersonNIN">
        <InputDataConnector ref="myLDAP" attributeNames="norEduPersonNIN"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:norEduPersonNIN" encodeType="
false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:1.3.6.1.4.1.2428.90.1.5" friendlyName="
norEduPersonNIN" encodeType="false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Simple" id="norEduPersonLIN">
```

```
        <InputDataConnector ref="myLDAP" attributeNames="norEduPersonLIN"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:norEduPersonLIN" encodeType="
false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:1.3.6.1.4.1.2428.90.1.4" friendlyName="
norEduPersonLIN" encodeType="false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Simple" id="norEduPersonBirthDate">
        <InputDataConnector ref="myLDAP" attributeNames="norEduPersonBirthDate"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:norEduPersonBirthDate"
encodeType="false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:1.3.6.1.4.1.2428.90.1.3" friendlyName="
norEduPersonBirthDate" encodeType="false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Simple" id="norEduOrgUniqueIdentifier">
        <InputDataConnector ref="myLDAP" attributeNames="norEduOrgUniqueIdentifier"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:norEduOrgUniqueIdentifier"
encodeType="false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:1.3.6.1.4.1.2428.90.1.7" friendlyName="
norEduOrgUniqueIdentifier" encodeType="false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Simple" id="norEduOrgUnitUniqueIdentifier">
        <InputDataConnector ref="myLDAP" attributeNames="norEduOrgUnitUniqueIdentifier"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:
norEduOrgUnitUniqueIdentifier" encodeType="false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:1.3.6.1.4.1.2428.90.1.8" friendlyName="
norEduOrgUnitUniqueIdentifier" encodeType="false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Simple" id="norEduOrgNIN">
        <InputDataConnector ref="myLDAP" attributeNames="norEduOrgNIN"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:norEduOrgNIN" encodeType="
false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:1.3.6.1.4.1.2428.90.1.12" friendlyName="
norEduOrgNIN" encodeType="false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Simple" id="norEduOrgUniqueNumber">
        <InputDataConnector ref="myLDAP" attributeNames="norEduOrgUniqueNumber"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:norEduOrgUniqueNumber"
encodeType="false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:1.3.6.1.4.1.2428.90.1.1" friendlyName="
norEduOrgUniqueNumber" encodeType="false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Simple" id="norEduOrgUnitUniqueNumber">
        <InputDataConnector ref="myLDAP" attributeNames="norEduOrgUnitUniqueNumber"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:norEduOrgUnitUniqueNumber"
encodeType="false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:1.3.6.1.4.1.2428.90.1.2" friendlyName="
norEduOrgUnitUniqueNumber" encodeType="false" />
    </AttributeDefinition>

    <!-- Schema: SCHema for ACademia (SCHAC) -->
    <!-- This takes the norEduPersonNIN and returns the date of birth part. -->
    <!-- Uncomment InputAttributeDefinition if norEduPersonNIN is generated by a script or InputDataConnector
if it is an attribute in LDAP -->
    <AttributeDefinition xsi:type="RegexSplit" id="schacDateOfBirth" regex="^((18|19|20)?[0-9]{2}((0[0-9])|
(10|11|12))((([0-2][0-9])|(3[0-1]))|((6[1-9])|([7-8][0-9])|(9[0-1])))).*$">
        <!-- <InputAttributeDefinition ref="norEduPersonNIN"/> -->
        <!-- <InputDataConnector ref="myLDAP" attributeNames="norEduPersonNIN" /> -->
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:schacDateOfBirth" encodeType="
false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:1.3.6.1.4.1.25178.1.2.3" friendlyName="
schacDateOfBirth" encodeType="false" />
    </AttributeDefinition>

    <!-- This is a multi-value attribute that can be used for many use cases, for example the European Student
Identifier (ESI). -->
```

```
    <AttributeDefinition xsi:type="Simple" id="schacPersonalUniqueCode">
        <InputDataConnector ref="myLDAP" attributeNames="schacPersonalUniqueCode" />
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:schacPersonalUniqueCode"
encodeType="false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:1.3.6.1.4.1.25178.1.2.14" friendlyName="
schacPersonalUniqueCode" encodeType="false" />
    </AttributeDefinition>

    <!-- Alternative to above for when European Student Identifier (ESI) is not included in
schacPersonalUniqueCode, uuid part is existing in another -->
    <!-- LDAP attribute and needs to be concatenated with the first part of the string to form the complete
schacPersonalUniqueCode. This example -->
    <!-- simply uses the fictional attribute ExterntStudentUID. This needs to be changed in three places to the
attribute you are actually using! -->
    <!--
    <AttributeDefinition xsi:type="ScriptedAttribute" id="schacPersonalUniqueCode">
        <InputDataConnector ref="myLDAP" attributeNames="ExterntStudentUID" />
        <Script>
                 <![CDATA[
                logger = Java.type("org.slf4j.LoggerFactory").getLogger("net.shibboleth.idp.attribute.resolver.
eppnbuilder");
                try {
                        if (ExterntStudentUID) {
                                value=ExterntStudentUID.getValues().get(0);
                                if (value != null) {
                                        schacPersonalUniqueCode.getValues().add("urn:schac:personalUniqueCode:
int:esi:ladok.se:externtstudentuid-" + value);
                                }
                        }
                } catch (err) {
                        logger.info("Error: " + err);
                }
                ]]>
        </Script>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:schacPersonalUniqueCode"
encodeType="false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:1.3.6.1.4.1.25178.1.2.14" friendlyName="
schacPersonalUniqueCode" encodeType="false" />
    </AttributeDefinition>
    -->

    <!-- Static Attributes -->
    <AttributeDefinition xsi:type="Simple" id="co">
        <InputDataConnector ref="staticAttributes" attributeNames="co"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:co" encodeType="false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:0.9.2342.19200300.100.1.43" friendlyName="co"
encodeType="false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Simple" id="c">
        <InputDataConnector ref="staticAttributes" attributeNames="c"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:c" encodeType="false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:2.5.4.6" friendlyName="c" encodeType="false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Simple" id="schacHomeOrganization">
        <InputDataConnector ref="staticAttributes" attributeNames="schacHomeOrganization"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:schacHomeOrganization"
encodeType="false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:1.3.6.1.4.1.25178.1.2.9" friendlyName="
schacHomeOrganization" encodeType="false" />
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Simple" id="schacHomeOrganizationType">
        <InputDataConnector ref="staticAttributes" attributeNames="schacHomeOrganizationType"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:schacHomeOrganizationType"
encodeType="false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:1.3.6.1.4.1.25178.1.2.10" friendlyName="
schacHomeOrganizationType" encodeType="false" />
    </AttributeDefinition>
```

```
    <AttributeDefinition xsi:type="Simple" id="norEduOrgAcronym">
        <InputDataConnector ref="staticAttributes" attributeNames="norEduOrgAcronym"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:norEduOrgAcronym" encodeType="
false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:1.3.6.1.4.1.2428.90.1.6" friendlyName="
norEduOrgAcronym" encodeType="false" />
    </AttributeDefinition>

    <!-- Schema: SAML Subject ID Attributes -->
    <AttributeDefinition xsi:type="Scoped" id="samlSubjectID" scope="%{idp.scope}">
        <InputDataConnector ref="myLDAP" attributeNames="%{idp.persistentId.sourceAttribute}"/>
        <AttributeEncoder xsi:type="SAML2ScopedString" name="urn:oasis:names:tc:SAML:attribute:subject-id"
friendlyName="subject-id" encodeType="false" />
    </AttributeDefinition>

    <!-- Schema: SAML Subject ID Attributes (alternative example) -->
    <!-- Use this if your idp.persistentId.sourceAttribute contains invalid characters like underscore or full
stop (period).
    <AttributeDefinition id="preSamlSubjectID" xsi:type="ScriptedAttribute">
        <InputDataConnector ref="myLDAP" attributeNames="%{idp.persistentId.sourceAttribute}"/>
        <Script><![CDATA[
            logger = Java.type("org.slf4j.LoggerFactory").getLogger("net.shibboleth.idp.attribute.resolver.
eppnbuilder");
                // Script to replace underscore with %5F
                try {
                        // If idp.persistentId.sourceAttribute is not uid, then you need to amend the content
of the script
                        source=uid.getValues().get(0);
                        source=source.replaceAll("_", "=5F");
                        source=source.replaceAll("[\.]", "=2E");
                        preSamlSubjectID.getValues().add(source);
                }
                catch(err) {
                        logger.info("Error: " + err);
                }
                ]]>
        </Script>
    </AttributeDefinition>

    <AttributeDefinition xsi:type="Scoped" id="samlSubjectID" scope="%{idp.scope}">
        <InputAttributeDefinition ref="preSamlSubjectID" />
        <AttributeEncoder xsi:type="SAML2ScopedString" name="urn:oasis:names:tc:SAML:attribute:subject-id"
friendlyName="subject-id" encodeType="false" />
    </AttributeDefinition>
    -->

    <AttributeDefinition xsi:type="Scoped" id="samlPairwiseID" scope="%{idp.scope}">
        <InputDataConnector ref="computed" attributeNames="computedId"/>
        <AttributeEncoder xsi:type="SAML2ScopedString" name="urn:oasis:names:tc:SAML:attribute:pairwise-id"
friendlyName="pairwise-id" encodeType="false" />
    </AttributeDefinition>

    <!-- Deprecated SWAMID eduPersonTargetedID -->
    <AttributeDefinition xsi:type="SAML2NameID" id="eduPersonTargetedID" nameIdFormat="urn:oasis:names:tc:SAML:
2.0:nameid-format:persistent">
        <InputDataConnector ref="StoredId" attributeNames="persistentId"/>
        <AttributeEncoder xsi:type="SAML1XMLObject" name="urn:oid:1.3.6.1.4.1.5923.1.1.1.10" encodeType="false"
/>
        <AttributeEncoder xsi:type="SAML2XMLObject" name="urn:oid:1.3.6.1.4.1.5923.1.1.1.10" friendlyName="
eduPersonTargetedID" encodeType="false" />
    </AttributeDefinition>

    <!-- Swedish eID Framework, personalIdentityNumber. Release norEduPersonNIN if it only contains numbers
(filter out interim numbers) -->
    <!-- Uncomment InputAttributeDefinition if norEduPersonNIN is generated by a script or InputDataConnector
if it is an attribute in LDAP -->
    <AttributeDefinition xsi:type="RegexSplit" id="personalIdentityNumber" regex="^((18|19|20)?[0-9]{2}((0[0-9])
|(10|11|12))(([0-2][0-9])|(3[0-1]))|((6[1-9])|([7-8][0-9])|(9[0-1])))[0-9]{4})$">
        <!-- <InputAttributeDefinition ref="norEduPersonNIN"/> -->
        <!-- <InputDataConnector ref="myLDAP" attributeNames="norEduPersonNIN" /> -->
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:personalIdentityNumber"
```

```
encodeType="false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:1.2.752.29.4.13" friendlyName="
personalIdentityNumber" encodeType="false" />
    </AttributeDefinition>

    <!-- mailLocalAddress is used for services that may need access to more than one mail address for the user
-->
    <AttributeDefinition xsi:type="Simple" id="mailLocalAddress">
        <InputDataConnector ref="myLDAP" attributeNames="mailLocalAddress"/>
        <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:mailLocalAddress" encodeType="
false" />
        <AttributeEncoder xsi:type="SAML2String" name="urn:oid:2.16.840.1.113730.3.1.13" friendlyName="
mailLocalAddress" encodeType="false" />
    </AttributeDefinition>

    <!-- ========================================== -->
    <!--      Data Connectors                       -->
    <!-- ========================================== -->

    <!-- Example Static Connector -->
    <DataConnector id="staticAttributes" xsi:type="Static">
         <Attribute id="o">
            <Value>ORGANIZATION_NAME</Value>
        </Attribute>
        <Attribute id="norEduOrgAcronym">
            <Value>ORGANIZATION_ACRONYM</Value>
        </Attribute>
        <Attribute id="c">
            <Value>ISO_COUNTRY_CODE</Value>
        </Attribute>
        <Attribute id="co">
            <Value>ISO_COUNTRY_NAME</Value>
        </Attribute>
        <Attribute id="schacHomeOrganization">
            <Value>SCHAC_HOME_ORG_DOMAIN_NAME</Value>
        </Attribute>
        <Attribute id="schacHomeOrganizationType">
            <Value>urn:schac:homeOrganizationType:eu:higherEducationInstitution</Value>
<!-- This value is for EU higher education institution, other allowed values are:
            - urn:schac:homeOrganizationType:eu:educationInstitution
            - urn:schac:homeOrganizationType:int:NREN
            - urn:schac:homeOrganizationType:int:universityHospital
            - urn:schac:homeOrganizationType:int:NRENAffiliate
            - urn:schac:homeOrganizationType:int:other
-->
        </Attribute>

        <!-- Refeds Assurance Framework and eduPersonAssurance -->
        <!-- Use following in conjunction with scripted attribute filteredEduPersonAssurance -->
        <Attribute id="allowedLDAPEduPersonAssurance">
            <Value>http://www.swamid.se/policy/assurance/al2</Value>
            <Value>http://www.swamid.se/policy/assurance/al3</Value>
        </Attribute>

        <!-- Use following in conjunction with attribute eduPersonAssurance -->
        <Attribute id="assuranceLevel1">
            <Value>http://www.swamid.se/policy/assurance/al1</Value>
            <Value>https://refeds.org/assurance/IAP/low</Value>
        </Attribute>

        <!-- Refeds Assurance Framework static value, used in conjunction with scripted attribute
filteredEduPersonAssurance -->
        <Attribute id="refedsAssuranceFramework">
            <Value>https://refeds.org/assurance</Value>
            <Value>https://refeds.org/assurance/ID/unique</Value>
            <Value>https://refeds.org/assurance/ID/eppn-unique-no-reassign</Value>
            <Value>https://refeds.org/assurance/ATP/ePA-1m</Value>
        </Attribute>

    </DataConnector>
```

```
<DataConnector id="StoredId"
xsi:type="StoredId"
generatedAttributeID="persistentId"
salt="%{idp.persistentId.salt}">
<InputAttributeDefinition ref="%{idp.persistentId.sourceAttribute}"/>
<BeanManagedConnection>MyGlobalDataSource</BeanManagedConnection>
</DataConnector>

<DataConnector id="myLDAP" xsi:type="LDAPDirectory"
    ldapURL="%{idp.attribute.resolver.LDAP.ldapURL}"
    baseDN="%{idp.attribute.resolver.LDAP.baseDN}"
    principal="%{idp.attribute.resolver.LDAP.bindDN}"
    principalCredential="%{idp.attribute.resolver.LDAP.bindDNCredential}"
useStartTLS="%{idp.attribute.resolver.LDAP.useStartTLS:true}"
    trustFile="%{idp.attribute.resolver.LDAP.trustCertificates}">
    <FilterTemplate>
        <![CDATA[
    %{idp.attribute.resolver.LDAP.searchFilter}
        ]]>
    </FilterTemplate>
</DataConnector>

<!-- Example Relational Database Connector -->
<!--
<DataConnector id="mySIS" xsi:type="RelationalDatabase">
    <ApplicationManagedConnection jdbcDriver="oracle.jdbc.driver.OracleDriver"
                                  jdbcURL="jdbc:oracle:thin:@db.example.org:1521:SomeDB"
                                  jdbcUserName="myid"
                                  jdbcPassword="mypassword" />
    <QueryTemplate>
        <![CDATA[
            SELECT * FROM student WHERE gzbtpid = '$resolutionContext.principal'
        ]]>
    </QueryTemplate>

    <Column columnName="gzbtpid" attributeID="uid" />
    <Column columnName="fqlft" attributeID="gpa" />
</DataConnector>
-->

<!-- Example LDAP Connector -->
<!--
<DataConnector id="myLDAP" xsi:type="LDAPDirectory"
    ldapURL="%{idp.attribute.resolver.LDAP.ldapURL}"
    baseDN="%{idp.attribute.resolver.LDAP.baseDN}"
    principal="%{idp.attribute.resolver.LDAP.bindDN}"
    principalCredential="%{idp.attribute.resolver.LDAP.bindDNCredential}"
    useStartTLS="%{idp.attribute.resolver.LDAP.useStartTLS:true}"
    connectTimeout="%{idp.attribute.resolver.LDAP.connectTimeout}"
    trustFile="%{idp.attribute.resolver.LDAP.trustCertificates}"
    responseTimeout="%{idp.attribute.resolver.LDAP.responseTimeout}">
    <FilterTemplate>
        <![CDATA[
            %{idp.attribute.resolver.LDAP.searchFilter}
        ]]>
    </FilterTemplate>
    <ConnectionPool
        minPoolSize="%{idp.pool.LDAP.minSize:3}"
        maxPoolSize="%{idp.pool.LDAP.maxSize:10}"
        blockWaitTime="%{idp.pool.LDAP.blockWaitTime:PT3S}"
        validatePeriodically="%{idp.pool.LDAP.validatePeriodically:true}"
        validateTimerPeriod="%{idp.pool.LDAP.validatePeriod:PT5M}"
        expirationTime="%{idp.pool.LDAP.idleTime:PT10M}"
        failFastInitialize="%{idp.pool.LDAP.failFastInitialize:false}" />
</DataConnector>
-->

<!-- DataConector for pairwise-id (example depends on saml-nameid.properties). -->
<DataConnector id="computed" xsi:type="ComputedId"
    generatedAttributeID="computedId"
    salt="%{idp.persistentId.salt}"
```

```
        algorithm="%{idp.persistentId.algorithm:SHA}"
        encoding="%{idp.persistentId.encoding:BASE32}">

        <InputDataConnector ref="myLDAP" attributeNames="%{idp.persistentId.sourceAttribute}" />

    </DataConnector>


</AttributeResolver>
```