Example of a standard attribute filter for Shibboleth IdP

This is an example of a standard entity category based attribute filter for SWAMID 2.0 in a Shibboleth IdP.

Prerequisites:

- The Identity Provider home organisation is willing to release attributes based on SWAMID entity categorisation of services.
- The attribute resolver in Shibboleth is configured to prepare the following attributes:
  - transientId
  - eduPersonTargetedID
  - eduPersonPrincipalName
  - norEduPersonNIN
  - email
  - displayName
  - commonName
  - givenName
  - surname
  - eduPersonAssurance
  - eduPersonScopedAffiliation
  - eduPersonAffiliation
  - organizationName
  - norEduOrgAcronym
  - countryName
  - friendlyCountryName
  - schacHomeOrganization
  - schacHomeOrganizationType

attribute-filter.xml for Shibboleth IDP 3.2.1 and newer

```
<?xml version="1.0" encoding="UTF-8"?>

<AttributeFilterPolicyGroup id="ShibbolethFilterPolicy"
        xmlns="urn:mace:shibboleth:2.0:afp"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="urn:mace:shibboleth:2.0:afp http://shibboleth.
net/schema/idp/shibboleth-afp.xsd">

<!--  Release the transient ID to anyone -->
<AttributeFilterPolicy id="releaseTransientIdToAnyone">
    <PolicyRequirementRule xsi:type="ANY" />

    <AttributeRule attributeID="transientId">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
</AttributeFilterPolicy>




<AttributeFilterPolicy id="releasePermanentIdToAnyone">
   <PolicyRequirementRule xsi:type="ANY" />
   <!-- As of Shib3.2.1 persistentId is automatically released and
processed in saml-nameid.xml -->

   <AttributeRule attributeID="eduPersonTargetedID">
      <PermitValueRule xsi:type="ANY" />
```

```
   </AttributeRule>
</AttributeFilterPolicy>



<!-- GEANT Data protection Code of Conduct -->
<AttributeFilterPolicy id="releaseToCoCo">
    <PolicyRequirementRule xsi:type="EntityAttributeExactMatch"
        attributeName="http://macedir.org/entity-category"
        attributeValue="http://www.geant.net/uri/dataprotection-code-of-
conduct/v1" />

    <AttributeRule attributeID="displayName">
        <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="
true" />
    </AttributeRule>
    <AttributeRule attributeID="commonName">
        <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="
true" />
    </AttributeRule>
    <AttributeRule attributeID="email">
        <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="
true" />
    </AttributeRule>
    <AttributeRule attributeID="eduPersonPrincipalName">
        <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="
true" />
    </AttributeRule>
    <AttributeRule attributeID="eduPersonScopedAffiliation">
        <PermitValueRule xsi:type="AND">
            <Rule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
            <Rule xsi:type="OR">
                <Rule xsi:type="Value" value="faculty" ignoreCase="true" />
                <Rule xsi:type="Value" value="student" ignoreCase="true" />
                <Rule xsi:type="Value" value="staff" ignoreCase="true" />
                <Rule xsi:type="Value" value="alum" ignoreCase="true" />
                <Rule xsi:type="Value" value="member" ignoreCase="true" />
                <Rule xsi:type="Value" value="affiliate" ignoreCase="true"
/>
                <Rule xsi:type="Value" value="employee" ignoreCase="true"
/>
                <Rule xsi:type="Value" value="library-walk-in" ignoreCase="
true" />
            </Rule>
        </PermitValueRule>
    </AttributeRule>
    <AttributeRule attributeID="eduPersonAffiliation">
        <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="
true" />
    </AttributeRule>
    <AttributeRule attributeID="schacHomeOrganization">
        <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="
```

```
true" />
    </AttributeRule>
    <AttributeRule attributeID="schacHomeOrganizationType">
        <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="
true" />
    </AttributeRule>
</AttributeFilterPolicy>



<!-- REFEDS Research and Schoolarship -->
<AttributeFilterPolicy id="releaseToRandS">
    <PolicyRequirementRule xsi:type="EntityAttributeExactMatch"
        attributeName="http://macedir.org/entity-category"
        attributeValue="http://refeds.org/category/research-and-
scholarship" />

    <AttributeRule attributeID="displayName">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
    <AttributeRule attributeID="givenName">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
    <AttributeRule attributeID="surname">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
    <AttributeRule attributeID="email">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
    <AttributeRule attributeID="eduPersonPrincipalName">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
    <AttributeRule attributeID="eduPersonScopedAffiliation">
        <PermitValueRule xsi:type="OR">
            <Rule xsi:type="Value" value="faculty" ignoreCase="true" />
            <Rule xsi:type="Value" value="student" ignoreCase="true" />
            <Rule xsi:type="Value" value="staff" ignoreCase="true" />
            <Rule xsi:type="Value" value="alum" ignoreCase="true" />
            <Rule xsi:type="Value" value="member" ignoreCase="true" />
            <Rule xsi:type="Value" value="affiliate" ignoreCase="true" />
            <Rule xsi:type="Value" value="employee" ignoreCase="true" />
            <Rule xsi:type="Value" value="library-walk-in" ignoreCase="
true" />
        </PermitValueRule>
    </AttributeRule>
</AttributeFilterPolicy>



<!-- entity-category-swamid-research-and-education -->
<AttributeFilterPolicy id="entity-category-research-and-education">
```

```
    <PolicyRequirementRule xsi:type="AND">
        <Rule xsi:type="OR">
            <Rule xsi:type="EntityAttributeExactMatch"
                attributeName="http://macedir.org/entity-category"
                attributeValue="http://www.swamid.se/category/eu-adequate-
protection" />
            <Rule xsi:type="EntityAttributeExactMatch"
                attributeName="http://macedir.org/entity-category"
                attributeValue="http://www.swamid.se/category/nren-
service" />
            <Rule xsi:type="EntityAttributeExactMatch"
                attributeName="http://macedir.org/entity-category"
                attributeValue="http://www.swamid.se/category/hei-service"
/>
        </Rule>

        <Rule xsi:type="EntityAttributeExactMatch"
            attributeName="http://macedir.org/entity-category"
            attributeValue="http://www.swamid.se/category/research-and-
education" />
    </PolicyRequirementRule>

    <AttributeRule attributeID="givenName">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
    <AttributeRule attributeID="surname">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
    <AttributeRule attributeID="displayName">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
    <AttributeRule attributeID="commonName">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
    <AttributeRule attributeID="eduPersonPrincipalName">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
    <AttributeRule attributeID="eduPersonAssurance">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
    <AttributeRule attributeID="email">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
    <AttributeRule attributeID="eduPersonScopedAffiliation">
        <PermitValueRule xsi:type="OR">
            <Rule xsi:type="Value" value="faculty" ignoreCase="true" />
            <Rule xsi:type="Value" value="student" ignoreCase="true" />
            <Rule xsi:type="Value" value="staff" ignoreCase="true" />
            <Rule xsi:type="Value" value="alum" ignoreCase="true" />
            <Rule xsi:type="Value" value="member" ignoreCase="true" />
            <Rule xsi:type="Value" value="affiliate" ignoreCase="true" />
            <Rule xsi:type="Value" value="employee" ignoreCase="true" />
            <Rule xsi:type="Value" value="library-walk-in" ignoreCase="
```

```
true" />
        </PermitValueRule>
    </AttributeRule>
    <AttributeRule attributeID="organizationName">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
    <AttributeRule attributeID="norEduOrgAcronym">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
    <AttributeRule attributeID="countryName">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
    <AttributeRule attributeID="friendlyCountryName">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
    <AttributeRule attributeID="schacHomeOrganization">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
</AttributeFilterPolicy>



<!-- entity-category-sfs-1993-1153 -->
<AttributeFilterPolicy id="entity-category-sfs-1993-1153">
    <PolicyRequirementRule xsi:type="EntityAttributeExactMatch"
            attributeName="http://macedir.org/entity-category"
            attributeValue="http://www.swamid.se/category/sfs-1993-1153" />

    <AttributeRule attributeID="norEduPersonNIN">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
    <AttributeRule attributeID="eduPersonAssurance">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
</AttributeFilterPolicy>



<!-- Examples of entityId based release to Service Providers -->


<!--
    Release to testshib.org
    Only enable this if you want to test with testshib.org
    This should not be enabled in a production environment
-->
<!--
<AttributeFilterPolicy id="testShib">
    <PolicyRequirementRule xsi:type="Requester" value="https://sp.testshib.
org/shibboleth-sp" />
```

```
    <AttributeRule attributeID="givenName">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
    <AttributeRule attributeID="commonName">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
    <AttributeRule attributeID="surname">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>

</AttributeFilterPolicy>
-->




<!--
    NyA-webben UHR
    This relies on the generated attribute NyAwebbenEntitlement which must
be manually added to attribute-resolver.xml
    Please see the SWAMID wiki for an example
-->
<!--
<AttributeFilterPolicy id="releaseNyAwebbenEntitlement">
    <PolicyRequirementRule xsi:type="OR">
        <Rule xsi:type="Requester" value="https://expert.antagning.se/ecs-
sp" />
        <Rule xsi:type="Requester" value="https://expert.test.antagning.se
/ecs-sp" />
    </PolicyRequirementRule>

    <AttributeRule attributeID="NyAwebbenEntitlement">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
</AttributeFilterPolicy>
-->




<!--
    New TCS Personal
    This relies on the generated attribute tcsPersonalEntitlement which
must be manually added to attribute-resolver.xml
    Please see the SWAMID wiki for an example
-->
<!--
<AttributeFilterPolicy id="releaseTcsPersonalEntitlement">
    <PolicyRequirementRule xsi:type="Requester" value="https://www.
digicert.com/sso" />

    <AttributeRule attributeID="displayName">
        <PermitValueRule xsi:type="ANY" />
```

```
    </AttributeRule>
    <AttributeRule attributeID="eduPersonPrincipalName">
        <PermitValueRule xsi:type="ANY"/>
    </AttributeRule>
    <AttributeRule attributeID="tcsPersonalEntitlement">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
    <AttributeRule attributeID="email">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
    <AttributeRule attributeID="schacHomeOrganization">
        <PermitValueRule xsi:type="ANY"/>
    </AttributeRule>
</AttributeFilterPolicy>
-->



</AttributeFilterPolicyGroup>
```