Shibboleth SP attribute checker example - Require REFEDS SIRTFI and REFEDS Research and Scholarship

This example is based on the based on How to configure Shibboleth SP attribute checker. Please see that wiki page for further information on how to use Shibboleth SP attribute checker.

Shibboleth Service Provider (SP) provides a hook for performing attribute checks for required attributes and a attribute extractor for fetching Identity Provider (IdP) metadata attributes where the login was performed. Without require any changes to the service the end user'will get an error message. THe example contains an a possiblity for the end user to send a detailed error report to their Identity Provider support contact.

In this example the Identity Provider is tested for

- metadata declaration for support of REFEDS SIRTFI v1; and
- attribute release based on REFEDS R&S v1.3.

Attribute Checker Handler

The AttributeChecker validates the user session against attributes specified as a required. If requirements are fulfilled, the login completes otherwise an error page is displayed instead. Note that the required attributes have to be "hard coded" here and kept in sync with the required attributes expressed in the Metadata.

Configuration

Add a sessionHook for attribute checker: sessionHook="/Shibboleth.sso/AttrChecker" to ApplicationDefaults. Add also the metadataAttributePrefix="Meta-" (This will be explained later).

In context: /etc/shibboleth/shibboleth2.xml -> ApplicationDefault element

```
<ApplicationDefaults entityID="https://<HOST>/shibboleth"
  REMOTE_USER="eppn persistent-id targeted-id"
  signing="front" encryption="false"
  sessionHook="/Shibboleth.sso/AttrChecker"
  metadataAttributePrefix="Meta-" >
```

Add the attribute checker handler with the list of required attributes to Sessions.

/etc/shibboleth/shibboleth2.xml -> Sessions element

If you want to describe more complex scenarios with required attributes, operators such as "AND" and "OR" are available.

```
<Handler type="AttributeChecker" Location="/AttrChecker" template="attrChecker.html" flushSession="true">
  <AND>
    <!-- Check for REFEDS SIRTFI Assurance Declaration in metadata -->
    <Rule require="Meta-AssuranceCertification">https://refeds.org/sirtfi</Rule>
    <!-- Check for REFEDS R&S compliant attribute release -->
    <Rule require="eppn"/>
    <Rule require="mail"/>
    <OR>
      <Rule require="displayName"/>
      <AND>
        <Rule require="givenName"/>
        <Rule require="surname"/>
      </AND>
    </OR>
  </AND>
</Handler>
```

Now we have an session hook for the attribute checker to check specified attributes before a user login is completed.

Add the AttributeExtractor element of the type metadata next to the already existing type XML: (<AttributeExtractor type="XML" validate="true" path="attribute-map.xml"/>)

For customization and error checks on the error page (attrChecker.html) we want to enable the "Attribute Extractor" with the type "metadata" to be able to fetch IdP attributes from the metadata feed. The attributes we need is the email addresses of the IdP support and security contacts. We've already added metadataAttributePrefix to the ApplicationDefaults element.

/etc/shibboleth/shibboleth2.xml -> ApplicationDefault element

```
<!-- Extracts support information for IdP from its metadata. -->
<AttributeExtractor type="Metadata" errorURL="errorURL" DisplayName="displayName"
                    InformationURL="informationURL" PrivacyStatementURL="privacyStatementURL"
                    OrganizationURL="organizationURL">
  <ContactPerson id="Support-Contact"  contactType="support" formatter="$EmailAddress" />
  <ContactPerson id="Other-Contact"  contactType="other" formatter="$EmailAddress" />
  <Logo id="Small-Logo" height="16" width="16" formatter="$_string"/>
</AttributeExtractor>
```

When you modify shibboleth2.xml you can test validity of the configuration file with command "shibd -t". If configuration file is still valid XML you can now restart your shibboleth with "sudo service shibd restart". Shibboleth should anyways reload configuration file if it detects any change on it.

Add attribute definition for the metadata Assurance Certification attribute

To be able to check for REFEDS SIRTFI you need to add a definition for the metadata based attribute Assurance Certification. We've already added metadataAttributePrefix to the ApplicationDefaults element in shibboleth2.xml.

/etc/shibboleth/attribute-map.xml -> Attributes element

```
<!-- Metadata based attribute for Assurance Certification -->
<Attribute name="urn:oasis:names:tc:SAML:attribute:assurance-certification" id="AssuranceCertification"/>
```

Logging of missing requirements

Shibboleth SP doesn't track nor log failed logins due to missing attributes. The Shibboleth SP web server can be used for "pixel tracking". This means that you load an image (eg: containing only one transparent pixel) from the web server from where you can monitor logs and observe access for you image. In the url of the image you can also insert details you want to see, eg: Authentication source (IdP) and missing attributes. This technique is used in attrChecker-html below.

Replace the image with your existing one from the following code or comment it out if you dont need it. Example below loads track.png from document root and adds variables like "idp" containing the entityID of the authentication source and "miss" denoting missing attributes.

Template customization

Replace the attrChecker.html that is located in the "/etc/shibboleth" directory with the template below. If you don't want to edit it by yourself, you can use the ready made template. The template has links to external components such as jquery and bootstrap. They are fetched on the fly from third party sources.

There is two checks if the IdP declare support SIRTFI is done due to the the Assurance Certifcation attribute can contain other values than SIRTFI and the possibility to check for specific values is not possible. The first check is to see if Assurance Certfication is missing and the second is check for when there is a Assurance Certification but now other contact address, i.e. security contact. Furthermore the name checks is speical due to that name in R&S is either displayName or sn and givenName.

All attribute names, except the one for Assurance Certification, in the template are based on the standard mappings in the Shibboleth SP distribution.

attrChecker.html

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE html
        PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
        "DTD/xhtml1-strict.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
        <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/>
        <link rel="stylesheet" type="text/css" href="<shibmlp styleSheet/>" />
  <script type='text/javascript' src='//ajax.googleapis.com/ajax/libs/jquery/1.10.2/jquery.min.js'></script>
  <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.6/css/bootstrap.min.css"
integrity="sha384-1q8mTJOASx8j1Au+a5WDVnPi2lkFfwwEAa8hDDdjZlpLegxhjVME1fgjWPGmkzs7" crossorigin="anonymous">

        <title>Login failed due to missing user attributes or missing security requirements</title>
  <script>
    $(document).ready(function() {
        $("#textarea").val(
         $('#textarea').val().replace(/\ \*\ (\r\n|\n|\r)/ig,"")
        );
        var mailto = "<shibmlp Meta-Support-Contact/>";
        var target = "<shibmlp target />";
```

```
        var target = target.replace("&#58;", ":");
        mailto = mailto.split("&#58;").pop();
        $("#email").attr('href','mailto:' + mailto + '?subject=Attributes missing for ' + encodeURIComponent
(target) + '&cc=<shibmlp supportContact/>' + '&body=' + encodeURIComponent(document.getElementById('textarea').
value));

        $('#showdetails').click(function() {
          $('#details').slideToggle("fast");
        });
        $('#showdetails2').click(function() {
          $('#details').slideToggle("fast");
        });
        document.getElementById("support").innerHTML=mailto;
        document.getElementById("support2").innerHTML=mailto;
    });
  </script>
</head>

<body>
  <div id="msg"/>
    <div class="container">
      <!--PixelTracking without Assurance Certification-->
          <shibmlpifnot Meta-AssuranceCertification>
      <img title="track" src="/track.png?idp=<shibmlp entityID/>&miss=-SIRTFI<shibmlpifnot
displayName><shibmlpifnot givenName>-displayName</shibmlpifnot></shibmlpifnot><shibmlpifnot
givenName><shibmlpifnot displayName>-givenName</shibmlpifnot></shibmlpifnot><shibmlpifnot sn><shibmlpifnot
displayName>sn</shibmlpifnot></shibmlpifnot><shibmlpifnot mail>-mail</shibmlpifnot><shibmlpifnot eppn>-
eduPersonPrincipalName</shibmlpifnot>" alt="" width="1" height="1" />
          </shibmlpifnot>
      <!--PixelTracking with Assurance Certification but without Other Contact (Security)-->
          <shibmlpif Meta-AssuranceCertification><shibmlpifnot Meta-Other-Contact/>
      <img title="track" src="/track.png?idp=<shibmlp entityID/>&miss=-SIRTFI<shibmlpifnot
displayName><shibmlpifnot givenName>-displayName</shibmlpifnot></shibmlpifnot><shibmlpifnot
givenName><shibmlpifnot displayName>-givenName</shibmlpifnot></shibmlpifnot><shibmlpifnot sn><shibmlpifnot
displayName>sn</shibmlpifnot></shibmlpifnot><shibmlpifnot mail>-mail</shibmlpifnot><shibmlpifnot eppn>-
eduPersonPrincipalName</shibmlpifnot>" alt="" width="1" height="1" />
          </shibmlpifnot></shibmlpif>
      <!--PixelTracking with Assurance Certification and Other Contact (Security)-->
          <shibmlpif Meta-AssuranceCertification><shibmlpif Meta-Other-Contact/>
      <img title="track" src="/track.png?idp=<shibmlp entityID/>&miss=<shibmlpifnot displayName><shibmlpifnot
givenName>-displayName</shibmlpifnot></shibmlpifnot><shibmlpifnot givenName><shibmlpifnot displayName>-
givenName</shibmlpifnot></shibmlpifnot><shibmlpifnot sn><shibmlpifnot displayName>sn</shibmlpifnot><
/shibmlpifnot><shibmlpifnot mail>-mail</shibmlpifnot><shibmlpifnot eppn>-eduPersonPrincipalName</shibmlpifnot>"
alt="" width="1" height="1" />
          </shibmlpif></shibmlpif>
      <div class="hero-unit">
        <h2>Login failed due to missing user attributes or missing security requirements</h2>
          <p>
          You could unfortunately not login to to our service <shibmlp target />, because your home
organisation <shibmlpif Meta-displayName>(<shibmlp Meta-displayName />)</shibmlpif> did not provide all
information about you that is needed by this service or that your home organisation Identity Provider doesn't
fulfil the service's security requirements.
          </p>
          <a href="#" id="showdetails">Show details</a>
                <br/>
          <div id="details" style="display:none">
<hr>
                  <!-- Report non REFEDS SIRTFI  dual check no enitity categories in metadata and entity
categories without other contact in metadata -->
                  <shibmlpifnot Meta-AssuranceCertification><h3 class='warning text-danger'>Missing SIRTFI
requirement</h3><p class='warning text-danger'>The service you tried to access require that the <shibmlpif Meta-
displayName><shibmlp Meta-displayName /></shibmlpif> Identity Provider fulfils and declares support for the
security incident response trust framework REFEDS SIRTFI (https://refeds.org/sirtfi).</p></shibmlpifnot>
                  <shibmlpif Meta-AssuranceCertification><shibmlpifnot Meta-Other-Contact/><h3 class='warning
text-danger'>Missing SIRTFI requirement</h3><p class='warning text-danger'>The service you tried to access
require that the <shibmlpif Meta-displayName><shibmlp Meta-displayName /></shibmlpif> Identity Provider fulfils
and declares support for the security incident response trust framework REFEDS SIRTFI (https://refeds.org
/sirtfi).</p></shibmlpifnot></shibmlpif>

          <h3>Attribute requirements</h3>
                  <p>The following user information in form of SAML attributes is requested by this service.
```

```
Required but missing attribute values are marked in red.</p>
          <div class="row">
            <div class="col-sm-5">
              <table class="table table-sm">
                <thead>
                  <tr><th colspan=2>Connection summary</th></tr>
                </thead>
                <tr>
                  <th>Time</th>
                  <td><shibmlp now/> UTC</td>
                </tr>
                <tr>
                  <th>SP</th>
                  <td><shibmlp target /></td>
                </tr>
                <tr>
                  <th> </th>
                  <td> </td>
                </tr>
                <tr>
                  <th>IdP</th>
                  <td><shibmlp Meta-displayName /></td>
                </tr>
                <tr>
                   <td>entityId</td>
                   <td><shibmlp entityID/></td>
                </tr>
                <tr>
                  <td>Contact</td>
                  <td id="support"><shibmlp Meta-Support-Contact/></td>
                </tr>
              </table>
            </div>
            <div class="col-sm-7">
              <table class="table table-sm">
                <thead>
                  <tr>
                    <th>Attribute</th>
                    <th>Value</th>
                  </tr>
                </thead>
                <tbody>
<!--TableStart-->
<tr <shibmlpifnot displayName><shibmlpifnot givenName> class='warning text-danger'</shibmlpifnot><
/shibmlpifnot>>
        <td>displayName</td>
        <td><shibmlp displayName /></td>
        <td></td>
</tr>
<tr <shibmlpifnot givenName><shibmlpifnot displayName> class='warning text-danger'</shibmlpifnot><
/shibmlpifnot>>
        <td>givenName</td>
        <td><shibmlp givenName /></td>
</tr>
<tr <shibmlpifnot sn><shibmlpifnot displayName> class='warning text-danger'</shibmlpifnot></shibmlpifnot>>
        <td>sn</td>
        <td><shibmlp sn /></td>
</tr>
<tr <shibmlpifnot mail> class='warning text-danger'</shibmlpifnot>>
        <td>mail</td>
        <td><shibmlp mail /></td>
</tr>
<tr <shibmlpifnot eppn> class='warning text-danger'</shibmlpifnot>>
        <td>eduPersonPrincipalName</td>
        <td><shibmlp eppn /></td>
</tr>
<tr>
        <td>eduPersonTargetedID</td>
        <td><shibmlp persistent-id /></td>
</tr>
<tr>
```

```
        <td>eduPersonScopedAffiliation (optional)</td>
        <td><shibmlp affiliation /></td>
</tr>
<!--TableEnd-->
               </tbody>
             </table>
           </div>
         </div>
         Email template for your IdP Administrator
<textarea id="textarea" style="width:100%;height:100px;">
Dear <shibmlpif Meta-displayName><shibmlp Meta-displayName /></shibmlpif> IdP Administrator

I tried to log in to a service with the entityID "<shibmlp target />" today (<shibmlp now />). Unfortunately,
the login failed because the <shibmlpif Meta-displayName><shibmlp Meta-displayName /></shibmlpif> Identity
Provider did not release the requested user attributes to this service or doesn't fulfil the security and
incident handling requirements in REFEDS SIRTFI. To be able to access this service, I kindly ask you to ensure
that our Identity Provider fulfil the requirements needed by the service <shibmlp target /> so that I can log
into it. Please find a summary of the login attempt below.

<shibmlpifnot Meta-AssuranceCertification>The service I tried to access require that the <shibmlpif Meta-
displayName><shibmlp Meta-displayName /></shibmlpif> Identity Provider fulfils and declares support for the
security incident response trust framework REFEDS SIRTFI (https://refeds.org/sirtfi).
</shibmlpifnot><shibmlpif Meta-AssuranceCertification><shibmlpifnot Meta-Other-Contact/>The service I tried to
access require that the <shibmlpif Meta-displayName><shibmlp Meta-displayName /></shibmlpif> Identity Provider
fulfils and declares support for the security incident response trust framework REFEDS SIRTFI (https://refeds.
org/sirtfi).
</shibmlpifnot></shibmlpif>
The attributes that were not released to the service are (REFEDS R&S):
<shibmlpifnot displayName> * displayName
</shibmlpifnot><shibmlpifnot givenName> * givenName
</shibmlpifnot><shibmlpifnot sn> * sn
</shibmlpifnot><shibmlpifnot mail> * mail
</shibmlpifnot><shibmlpifnot eppn> * eduPersonPrincipalName
</shibmlpifnot><shibmlpifnot persistent-id> * eduPersonTargetedID (only if eduPersonPrincipalName is
reasignable to another user)
</shibmlpifnot><shibmlpifnot affiliation> * eduPersonScopedAffiliation (optional)
</shibmlpifnot><shibmlpif displayName><shibmlpif givenName><shibmlpif sn><shibmlpif mail><shibmlpif
eppn><shibmlpif persistent-id><shibmlpif affiliation> * no missing attributes!</shibmlpif></shibmlpif><
/shibmlpif></shibmlpif></shibmlpif></shibmlpif></shibmlpif>

Connection summary:
 * IdP:      <shibmlp entityID/> (<shibmlp Meta-displayName />)
 * SP:       <shibmlp target />
 * Time:     <shibmlp now/> UTC

Best Regards</textarea>
<hr>
</div>
          <p>
Please contact your home organisations helpdesk (here: <span id="support2"><shibmlp Meta-Support-Contact/><
/span>) and request attribute release for missing attributes or declare that they fulfil the security
requirements. To do this, click on the button below. This will open your mail program with the needed technical
information to resolve this issue. You can add additional information and review the email before sending it.
Alternatively you can copy and paste the request from the  <a href="#" id="showdetails2">details</a> text box.
          </p>
          <a id="email" class="btn btn-primary btn-large" href="#">Report Problem to your Home Organisation's
Helpdesk</a>
        </div>
      </div>
    </div>
  </div>
</body>
</html>
```