Connecting a mod_auth_mellon SP to eduTEAMS

This guide describes how mod_auth_mellon can be configured as a SAML Service Provider for eduTEAMS.

mod_auth_mellon is an authentication module for Apache. It authenticates the user against a SAML 2.0 IdP, and grants access to directories depending on attributes received from the IdP. It used to be maintained by Uninett, but is now in the community. The code and documentation can be found at https://github.com/latchset/mod_auth_mellon.

This guide assumes you're using a Debian-based Linux distribution, and you have installed and enabled the mod-auth-mellon module.

1. mod_auth_mellon

We suggest populating the global configuration options with the following. Edit your **auth_mellon.conf** file to read as follows:

```
##############################################################################
# Global configuration for mod_auth_mellon. This configuration is shared by
# every virtual server and location in this instance of apache.
##############################################################################

# MellonCacheSize sets the maximum number of sessions which can be active
# at once. When mod_auth_mellon reaches this limit, it will begin removing
# the least recently used sessions. The server must be restarted before any
# changes to this option takes effect.
# Default: MellonCacheSize 100
MellonCacheSize 100

# MellonCacheEntrySize sets the maximum size for a single session entry in
# bytes. When mod_auth_mellon reaches this limit, it cannot store any more
# data in the session and will return an error. The minimum entry size is
# 65536 bytes, values lower than that will be ignored and the minimum will
# be used.
# Default: MellonCacheEntrySize 196608

# MellonLockFile is the full path to a file used for synchronizing access
# to the session data. The path should only be used by one instance of
# apache at a time. The server must be restarted before any changes to this
# option takes effect.
# Default: MellonLockFile "/var/run/mod_auth_mellon.lock"
MellonLockFile "/var/run/mod_auth_mellon.lock"

# MellonPostDirectory is the full path of a directory where POST requests
# are saved during authentication. This directory must writable by the
# Apache user. It should not be writable (or readable) by other users.
# Default: None
# Example: MellonPostDirectory "/var/cache/mod_auth_mellon_postdata"

# MellonPostTTL is the delay in seconds before a saved POST request can
# be flushed.
# Default: MellonPostTTL 900 (15 mn)
MellonPostTTL 900

# MellonPostSize is the maximum size for saved POST requests
# Default: MellonPostSize 1048576 (1 MB)
MellonPostSize 1048576

# MellonPostCount is the maximum amount of saved POST requests
# Default: MellonPostCount 100
MellonPostCount 100

##############################################################################
# End of global configuration for mod_auth_mellon.
##############################################################################
```

Next, add a location under the web server that will be protected, requiring a SAML authentication (and authorization if you require).

You will add this snippet after the global configuration, in the file **auth_mellon.conf**.

```
<Location />

   MellonEnable info

   MellonEndpointPath /mellon/

   MellonSPMetadataFile /etc/apache2/mellon/[your_sp]_mellon_metadata.xml

   MellonSPPrivateKeyFile /etc/apache2/mellon/https_[your_sp]_mellon_metadata.
key

   MellonSPCertFile /etc/apache2/mellon/https_[your_sp]_mellon_metadata.cert

   MellonIdPMetadataFile /etc/apache2/mellon/eduTEAMS-metadata.xml

   MellonOrganizationURL "en" "mellon test for https://www.eduteams.org"
```

```
   MellonUser "urn:oasis:names:tc:SAML:attribute:subject-id"

   MellonUser "urn:oid:1.3.6.1.4.1.5923.1.1.1.13"

</Location>

<Location /private>
   AuthType Mellon
   MellonEnable auth
   Require valid-user
</Location>

Note you can also use MellonRequire to allow for access based on attributes
sent for the user
```

1a Authorisation within Apache

You can use the directive MellonRequire within your apache <Location> directives.

```
MellonCond <attribute name> <value> [<options>]
```

eg

```
MellonCond "urn:oid:1.3.6.1.4.1.5923.1.1.1.13" "<your eduTEAMS identifier>@edu
teams.org"
```

1b. Authorisation in code

mod_mellon will create a number of environment variables within your Apache instance.

See an example on the right.

If you do not want multi-valued attributes to create many 0...n numbered variables, set

```
 MellonMergeEnvVars  Off
```

and this will give you eg

```
[MELLON_urn:oid:
1_3_6_1_4_1_5923_1_1_1_7] =>
"value1[;valueX]"
```

```
    [MELLON_NAME_ID]
    [MELLON_NAME_ID_0]
    [MELLON_urn:oid:2_16_840_1_113730_3_1_241]
    [MELLON_urn:oid:2_16_840_1_113730_3_1_241_0]
    [MELLON_urn:oid:2_5_4_4]
    [MELLON_urn:oid:2_5_4_4_0]
    [MELLON_urn:oid:0_9_2342_19200300_100_1_3] => stephen.lovell@geant.org
    [MELLON_urn:oid:0_9_2342_19200300_100_1_3_0] => stephen.lovell@geant.org
    [MELLON_urn:oid:1_3_6_1_4_1_25178_4_1_11] => member@gn4-3.wp5.geant.org
    [MELLON_urn:oid:1_3_6_1_4_1_25178_4_1_11_0] => member@gn4-3.wp5.geant.org
    [MELLON_urn:oid:1_3_6_1_4_1_5923_1_1_1_6] => stephen@acc.eduteams.org
    [MELLON_urn:oid:1_3_6_1_4_1_5923_1_1_1_6_0] => stephen@acc.eduteams.org
    [MELLON_urn:oid:1_3_6_1_4_1_5923_1_1_1_13] =>
0226a866112c6a8c42e226c31d6bf04293de6582@eduteams.org
    [MELLON_urn:oid:1_3_6_1_4_1_5923_1_1_1_13_0] =>
0226a866112c6a8c42e226c31d6bf04293de6582@eduteams.org
    [MELLON_urn:oid:1_3_6_1_4_1_25178_4_1_6] =>
0226a866112c6a8c42e226c31d6bf04293de6582@eduteams.org
    [MELLON_urn:oid:1_3_6_1_4_1_25178_4_1_6_0] =>
0226a866112c6a8c42e226c31d6bf04293de6582@eduteams.org
    [MELLON_urn:oid:1_3_6_1_4_1_5923_1_1_1_7] => urn:geant:eduteams.org:
service:eduteams-acc:group:eduTEAMS#acc.eduteams.org
    [MELLON_urn:oid:1_3_6_1_4_1_5923_1_1_1_7_0] => urn:geant:eduteams.org:
service:eduteams-acc:group:eduTEAMS#acc.eduteams.org
```

Note that mod_mellon will create a series of single value variables named MELLON_var_{0..n}. If MELLON_var is single valued you will see a duplicate called MELLON_var_0

If MELLON_var is multivalued, you will find all values in their own variables eg:

```
    [MELLON_urn:oid:1_3_6_1_4_1_5923_1_1_1_7] => urn:geant:eduteams.org:
service:eduteams-acc:group:eduTEAMS#acc.eduteams.org
    [MELLON_urn:oid:1_3_6_1_4_1_5923_1_1_1_7_0] => urn:geant:eduteams.org:
service:eduteams-acc:group:eduTEAMS#acc.eduteams.org
    [MELLON_urn:oid:1_3_6_1_4_1_5923_1_1_1_7_1] => urn:geant:eduteams.org:
service:eduteams-acc:group:eduTEAMS:gitlab#acc.eduteams.org
    [MELLON_urn:oid:1_3_6_1_4_1_5923_1_1_1_7_2] => urn:geant:eduteams.org:
service:eduteams-acc:group:eduTEAMS:gitlab:admin#acc.eduteams.org
    [MELLON_urn:oid:1_3_6_1_4_1_5923_1_1_1_7_3] => urn:geant:eduteams.org:
service:eduteams-acc:group:eduTEAMS:Developers#acc.eduteams.org
    [MELLON_urn:oid:1_3_6_1_4_1_5923_1_1_1_7_4] => urn:geant:eduteams.org:
service:eduteams-acc:group:eduTEAMS:gitlab:audit#acc.eduteams.org
```

Would be the result of the following assertion:

```
    <ns1:Attribute FriendlyName="eduPersonEntitlement"
                   Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.7"
                   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:
uri"
                   >
       <ns1:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
                           xsi:type="xs:string"
                           >urn:geant:eduteams.org:service:eduteams-acc:group:
eduTEAMS#acc.eduteams.org</ns1:AttributeValue>
       <ns1:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
                           xsi:type="xs:string"
                           >urn:geant:eduteams.org:service:eduteams-acc:group:
eduTEAMS:gitlab#acc.eduteams.org</ns1:AttributeValue>
       <ns1:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
                           xsi:type="xs:string"
                           >urn:geant:eduteams.org:service:eduteams-acc:group:
eduTEAMS:gitlab:admin#acc.eduteams.org</ns1:AttributeValue>
       <ns1:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
                           xsi:type="xs:string"
                           >urn:geant:eduteams.org:service:eduteams-acc:group:
eduTEAMS:Developers#acc.eduteams.org</ns1:AttributeValue>
       <ns1:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
                           xsi:type="xs:string"
                           >urn:geant:eduteams.org:service:eduteams-acc:group:
eduTEAMS:gitlab:audit#acc.eduteams.org</ns1:AttributeValue>
    </ns1:Attribute>
```

2. Next, download the eduTEAMS metadata

```
mkdir /etc/apache/mellon

wget "https://proxy.acc.eduteams.org/metadata/frontend.xml" -O /etc/apache2
/mellon/eduTEAMS-metadata.xml
```

3. Now generate the metadata for your mellon SP

It is a matter of record that any shell script designed to be useful in setting up a system is not guaranteed to be present. If having installed the Apache auth-mellon package for your system you cannot find the script **mellon_create_metadata.sh** you can source it from the github home of the package ie https://github.com/latchset/mod_auth_mellon

Usage: mellon_create_metadata.sh ENTITY-ID ENDPOINT-URL

Example:

(cd /etc/apache2/mellon or the location you choose to use)

./mellon_create_metadata.sh urn:someservice https://sp.example.org/mellon

```
./mellon_create_metadata.sh https://[your_sp]/mellon/metadata https://
[your_sp]/mellon
```

This will give you three files:

```
https_[your_sp]_mellon_metadata.cert

https_[your_sp]_mellon_metadata.key

https_[your_sp]_mellon_metadata.xml
```

Note - these three files are those we refer to in the file **auth_mellon.conf** (earlier in this document).

Please note that whilst the metadata generated but the mellon_create_metadata.sh script is valid, it is does not contain all elements the eduTEAMS service prefers.

```
<?xml version="1.0"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:
mdattr="urn:oasis:names:tc:SAML:metadata:attribute" xmlns:saml="urn:oasis:
names:tc:SAML:2.0:assertion" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui" xmlns:ds="
http://www.w3.org/2000/09/xmldsig#" entityID="https://[your_sp]/mellon
/metadata">
  <md:Extensions>
    <mdattr:EntityAttributes xmlns:mdattr="urn:oasis:names:tc:SAML:
metadata:attribute">
      <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
Name="http://macedir.org/entity-category" NameFormat="urn:oasis:names:tc:
SAML:2.0:attrname-format:uri">
        <!-- Required for R&S SPs -->
        <saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-
```

```
instance" xmlns:xs="http://www.w3.org/2001/XMLSchema" xsi:type="xs:string"
>http://refeds.org/category/research-and-scholarship</saml:AttributeValue>
        <!-- Required for Production SPs -->
        <saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xmlns:xs="http://www.w3.org/2001/XMLSchema" xsi:type="xs:string"
>http://www.geant.net/uri/dataprotection-code-of-conduct/v1</saml:
AttributeValue>
      </saml:Attribute>


      <!-- Required for SPs supporting Sirtfi -->
      <saml:Attribute Name="urn:oasis:names:tc:SAML:attribute:assurance-
certification" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
>
        <saml:AttributeValue xsi:type="xs:string">https://refeds.org
/sirtfi</saml:AttributeValue>
      </saml:Attribute>


      <!-- Required to signal the requirement for the release of subject-
id -->
      <saml:Attribute Name="urn:oasis:names:tc:SAML:attribute:subject-id:
req" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <saml:AttributeValue>any</saml:AttributeValue>
      </saml:Attribute>
    </mdattr:EntityAttributes>
  </md:Extensions>


  <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:
2.0:protocol" AuthnRequestsSigned="true">
    <md:Extensions>
      <mdui:UIInfo xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui">

        <!-- Required: Change it for your SP -->
        <mdui:DisplayName xml:lang="en">[your_sp_description]</mdui:
DisplayName>

        <!-- Required: Change it for your SP -->
        <mdui:Description xml:lang="en">[your_sp_description_full_sentence]
</mdui:Description>
        <!-- Required for Production: Change it for your SP -->

        <mdui:PrivacyStatementURL xml:lang="en">[your_privacy_policy_url]<
/mdui:PrivacyStatementURL>

        <!-- Required: Change it for your SP -->
        <mdui:Logo width="200" height="200">[your_sp_img_url_200x200]<
/mdui:Logo>
        <mdui:Logo width="16" height="16">[your_sp_img_url_16x16]</mdui:
Logo>

        <!-- Optional: Change it for your SP -->
        <mdui:InformationURL xml:lang="en">https://[your_sp]</mdui:
InformationURL>
      </mdui:UIInfo>
    </md:Extensions>


    <!-- Required: Change it for your SP -->
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>
{ contents of https_[your_sp]_mellon_metadata.cert }
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <!-- Required: Change it for your SP -->
    <md:KeyDescriptor use="encryption">
```

```
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>
{ contents of https_[your_sp]_mellon_metadata.cert }
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>


    <!-- Optional: Change it for your SP -->
    <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:
HTTP-Redirect" Location="https://[your_sp]/mellon/logout"/>


    <!-- Required -->
    <!--
      In the list below all the attributes are requested. If your SP
       needs fewer attributes, the list has to be modified accordingly
    -->
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:
bindings:HTTP-POST" Location="https://[your_sp]/mellon/postResponse"
index="0"/>

    <md:AttributeConsumingService index="0">
      <md:ServiceName xml:lang="en">[your_sp_description]</md:ServiceName>
      <md:RequestedAttribute Name="urn:oasis:names:tc:SAML:attribute:
subject-id" FriendlyName="subject-id"/>
      <md:RequestedAttribute Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.13"
FriendlyName="eduPersonUniqueId"/>
      <md:RequestedAttribute Name="urn:oid:1.3.6.1.4.1.25178.4.1.6"
FriendlyName="voPersonID"/>
      <md:RequestedAttribute Name="urn:oid:2.5.4.42" FriendlyName="
givenName"/>
      <md:RequestedAttribute Name="urn:oid:2.5.4.4" FriendlyName="sn"/>
      <md:RequestedAttribute Name="urn:oid:2.16.840.1.113730.3.1.241"
FriendlyName="displayName"/>
      <md:RequestedAttribute Name="urn:oid:0.9.2342.19200300.100.1.3"
FriendlyName="mail"/>
      <md:RequestedAttribute Name="urn:oid:1.3.6.1.4.1.25178.4.1.11"
FriendlyName="voPersonExternalAffiliation"/>
      <md:RequestedAttribute Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.9"
FriendlyName="eduPersonScopedAffiliation"/>
      <md:RequestedAttribute Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.7"
FriendlyName="eduPersonEntitlement"/>
      <md:RequestedAttribute Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.11"
FriendlyName="eduPersonAssurance"/>
      <md:RequestedAttribute Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.16"
FriendlyName="eduPersonOrcid"/>
      <md:RequestedAttribute Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
FriendlyName="eduPersonPrincipalName"/>
      <md:RequestedAttribute Name="urn:oid:1.3.6.1.4.1.24552.500.1.1.1.13"
FriendlyName="sshPublicKey"/>
    </md:AttributeConsumingService>
  </md:SPSSODescriptor>



  <!-- Required: Change it for your SP -->
  <md:Organization>
    <md:OrganizationName xml:lang="en">[your_organisation]</md:
OrganizationName>
    <md:OrganizationDisplayName xml:lang="en">[your_organisation]</md:
OrganizationDisplayName>
    <md:OrganizationURL xml:lang="en">[your_organisation_homepage]</md:
OrganizationURL>
  </md:Organization>


  <!-- Required: Change it for your SP -->
  <md:ContactPerson contactType="administrative">
```

```
    <md:EmailAddress>mailto:admin@[your_sp]</md:EmailAddress>
  </md:ContactPerson>


  <!-- Required: Change it for your SP -->
  <md:ContactPerson contactType="technical">
    <md:EmailAddress>mailto:support@[your_sp]</md:EmailAddress>
  </md:ContactPerson>


  <!-- Required for SPs supporting Sirtfi: Change it for your SP -->
  <md:ContactPerson xmlns:remd="http://refeds.org/metadata"
                    contactType="other"
                    remd:contactType="http://refeds.org/metadata
/contactType/security">
    <md:GivenName>[your_sirtifi_contact_name]</md:GivenName>
    <md:EmailAddress>mailto:security@[your_sp]</md:EmailAddress>
  </md:ContactPerson>

</md:EntityDescriptor>
```

2. Apache

All of the configuration to enable mod_mellon, and specify areas of your site to protect are covered above.

3. Restarting the apache2 service

systemctl restart apache2

4. Conclusion

You should now have a working integration of Apache and Shibboleth v3 SP services on your machine.