My First SP - Mod mellon

Please start here if you want to connect your service to the SURFconext platform

This is a description how to set up an SP in SURFconext using Apache and the module mod_mellon. It might be a good choice for SPs with very simple requirements. When in doubt, using SimpleSAMLphp or Shibboleth is probably a good choice. This manual is still quite basic.

For more background and options for mod mellon, see: https://github.com/latchset/mod_auth_mellon

SURFconext Metadata

Take note that the metadata and the metadata locations used for the test and production environments of SURFconext differ. This example uses TEST urls. Please change to production where appropriate.

- **Test:** https://metadata.test.surfconext.nl/idp-metadata.xml
- **Production:** https://metadata.surfconext.nl/idp-metadata.xml, for certificate see https://metadata.surfconext.nl

Install things

```
apt install apache2 libapache2-mod-auth-mellon
a2enmod auth_mellon
service apache2 restart
```

Configure Apache to work for your application. Set up HTTPS with a working certificate and a high score on https://ssllabs.com/ssltest and/or https://internet.nl.

Configure SURFconext IdP metadata

Generate a SAML keypair to use for mellon and download SURFconext IdP metadata.

```
mkdir /etc/apache2/mellon/
cd !^

openssl req -newkey rsa:3072 -new -x509 -days 3652 -nodes -out saml.pem -keyout saml.key

curl -O https://metadata.test.surfconext.nl/idp-metadata.xml
```

Configure virtual host

Add the following to your virtual host (assuming it lives on https://your.example.domain).

```
<Location />
    MellonSPentityId "https://your.example.domain"
    MellonSPCertFile /etc/apache2/mellon/saml.pem
    MellonSPPrivateKeyFile /etc/apache2/mellon/saml.key

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

    MellonOrganizationName "en" "Your Organization Name"
    MellonOrganizationDisplayName "en" "Your Organization Name"
    MellonOrganizationURL "en" "https://www.example.org"

    MellonSecureCookie On
    MellonCookieSameSite None
</Location>

<Location /secret>
    AuthType "Mellon"
    Require valid-user
    MellonEnable "auth"
</Location>
```

Reload Apache.

The configuration above requires login for URL path /secret.

Browse to the path /secret on your vhost. This should now redirect to SURFconext (error message about unknown SP).

The following URL should now give output: `https://your.example.domain/mellon/metadata`.

Supply this URL to SURFconext (via SP dashboard or to SURFconext support). It will be configured on their end.

Authenticate and authorize users

Authentication might now just work.

You receive information about the user in environment variables, named like this:

`REMOTE_USER`

(which attribute's value ends up in REMOTE_USER is defined by the MellonUser directive)

`MELLON_urn:mace:attribute-def:eduPersonPrincipalName`

etc.

See the Mellon documentation for more information.

It's also possible to add more Mellon* directives to the Apache config. Including directives to authorize users (e.g. only allow users with eduPersonAffiliation = employee) with MellonRequire.

That's all folks

Let us know if you have any questions at support@surfconext.nl.