Sirtfi Metadata Aggregates

Why create a Sirtfi Metadata Aggregate?

Sirtfi provides a mechanism to identify federation participants that comply with a baseline of best practices in operational security and are willing to participate in collaborative incident response. As a Service Provider (SP), you may have good reason to restrict authentication to only those Identity Providers asserting Sirtfi Compliance. Sirtfi was first developed as a reaction to key Research Collaborations wanting to do just this! The Research and Education Sector is a target for online attacks and it is essential that we as a community are able to contain and resolve an incident within our federated network. By creating metadata aggregates, a federation participant is able to ensure that it only interacts with the entities that it trusts.

How to create a Metadata Aggregate?

The following section provides detailed instructions on how this can be done for Sirtfi with the use of pyFF Federation Feeder or Shibboleth Metadata Aggregator. You may wish to add additional logic to require REFEDS Research and Scholarship Entity Category as well as Sirtfi.

pyFF Federation Feeder

The following example pyFF pipeline, loads the eduGAIN metadata from mds.edugain.org and after filtering out all Entities from the local federation and all Entities that do not assert Sirtfi compliance moves on to create three new metadata aggregates :

- One that contains only the Identity Providers
- One that contains only the Service Providers
- One that contains both Identity and Service Providers

```
### Load eduGAIN Metadata ###
- load:
  # Load from the eduGAIN Metadata URL
  - http://mds.edugain.org/feed-sha256.xml as edugain-md certs/eduGAIN-signer-ca.pem

### Replace the value of '###YOUR-REG-AUTH###' with your registrationAuthority to exclude the entities of your
federation. ###
- select:
  - "edugain-md!//md:EntityDescriptor[md:Extensions/mdrpi:RegistrationInfo/@registrationAuthority and not(md:
Extensions/mdrpi:RegistrationInfo/@registrationAuthority='###YOUR-REG-AUTH###')]"

### Select only the Entities that assert Sirtfi Compliance
- select:
  - "edugain-md!//md:EntityDescriptor[md:Extensions/mdattr:EntityAttributes/saml:Attribute/@Name='urn:oasis:
names:tc:SAML:attribute:assurance-certification' and md:Extensions/mdattr:EntityAttributes/saml:Attribute/saml:
AttributeValue='https://refeds.org/sirtfi']"


### Fork to produce the Interfederation Identity Providers Metadata ### Replace the value of '###YOUR-
ENTITIESDESCRIPTOR-NAME-FOR-INTERFEDERATION###' and '###YOUR-ENTITIESDESCRIPTOR-ID-FOR-INTERFEDERATION###' with
the values of XML attributes "Name" and "ID" choosed for your interfederation metadata stream ###
- fork:
  - select:
     - "edugain-md!//md:EntityDescriptor[md:IDPSSODescriptor]"
  - xslt:
     stylesheet: tidy.xsl
  - finalize:
     Name: ###YOUR-ENTITIESDESCRIPTOR-NAME-FOR-INTERFEDERATION###
     ID: ###YOUR-ENTITIESDESCRIPTOR-ID-FOR-INTERFEDERATION###
     cacheDuration: PT5H
     validUntil: P5D
  - sign:
     key: certs/sign.key
     cert: certs/sign.crt
  - publish:
     - output/my-interfederation-idp-metadata.xml

### Fork to produce the Interfederation Service Providers Metadata ###
### Replace the value of '###YOUR-ENTITIESDESCRIPTOR-NAME-FOR-INTERFEDERATION###' and '###YOUR-
ENTITIESDESCRIPTOR-ID-FOR-INTERFEDERATION###' with the values of XML attributes "Name" and "ID" choosed for your
interfederation metadata stream ###
- fork:
  - select:
     - "edugain-md!//md:EntityDescriptor[md:SPSSODescriptor]"
  - xslt:
     stylesheet: tidy.xsl
  - finalize:
     Name: ###YOUR-ENTITIESDESCRIPTOR-NAME-FOR-INTERFEDERATION###
     ID: ###YOUR-ENTITIESDESCRIPTOR-ID-FOR-INTERFEDERATION###
     cacheDuration: PT5H
     validUntil: P5D
  - sign:
     key: certs/sign.key
     cert: certs/sign.crt
  - publish:
     - output/my-interfederation-sp-metadata.xml

### Produce the Interfederation Metadata ###
### Replace the value of '###YOUR-ENTITIESDESCRIPTOR-NAME-FOR-INTERFEDERATION###' and '###YOUR-
ENTITIESDESCRIPTOR-ID-FOR-INTERFEDERATION###' with the values of XML attributes "Name" and "ID" choosed for your
interfederation metadata stream ###
- xslt:
  stylesheet: tidy.xsl
- finalize:
  Name: ###YOUR-ENTITIESDESCRIPTOR-NAME-FOR-INTERFEDERATION###
  ID: ###YOUR-ENTITIESDESCRIPTOR-ID-FOR-INTERFEDERATION###
  cacheDuration: PT5H
  validUntil: P5D
- sign:
  key: certs/sign.key
  cert: certs/sign.crt
- publish:
  - output/my-interfederation-metadata.xml
```

Shibboleth Metadata Aggregator

This tool is under development. Please check their homepage for the latest updates at https://shibboleth.net/products/metadata-aggregator.html