IdP Updating the Home Organisation Description

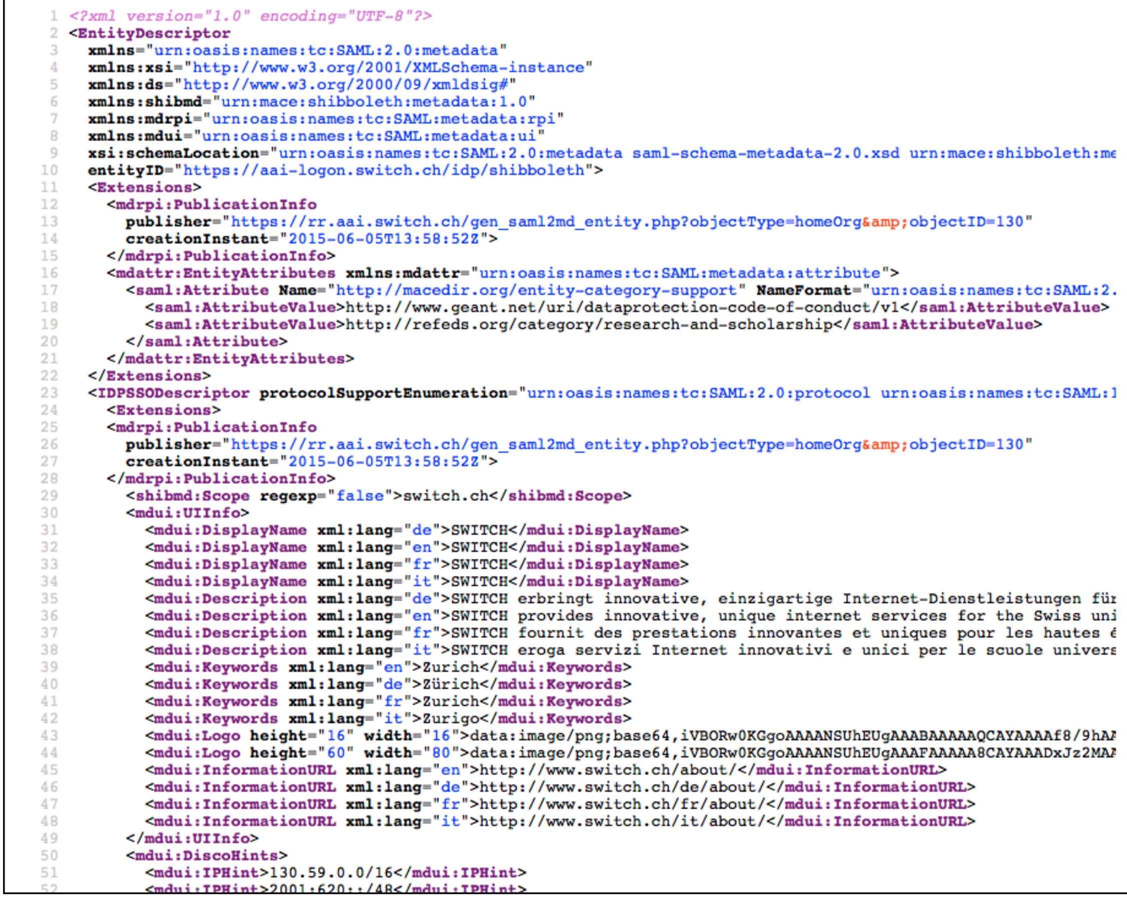
Changes in Resource Registry

SWITCH

SWITCHaai Team
aai@switch.ch

What technically defines your Identity Provider in SWITCHaai or eduGAIN?

Its SAML2 Metadata



```xml
<?xml version="1.0" encoding="UTF-8"?>
<EntityDescriptor
  xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  xmlns:shibmd="urn:mace:shibboleth:metadata:1.0"
  xmlns:mdrpi="urn:oasis:names:tc:SAML:metadata:rpi"
  xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui"
  xsi:schemaLocation="urn:oasis:names:tc:SAML:2.0:metadata saml-schema-metadata-2.0.xsd urn:mace:shibboleth:me
  entityID="https://aai-logon.switch.ch/idp/shibboleth">
  <Extensions>
    <mdrpi:PublicationInfo
      publisher="https://rr.aai.switch.ch/gen_saml2md_entity.php?objectType=homeOrg&amp;objectID=130"
      creationInstant="2015-06-05T13:58:52Z">
    </mdrpi:PublicationInfo>
    <mdattr:EntityAttributes xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
      <saml:Attribute Name="http://macedir.org/entity-category-support" NameFormat="urn:oasis:names:tc:SAML:2.
        <saml:AttributeValue>http://www.geant.net/uri/dataprotection-code-of-conduct/v1</saml:AttributeValue>
        <saml:AttributeValue>http://refeds.org/category/research-and-scholarship</saml:AttributeValue>
      </saml:Attribute>
    </mdattr:EntityAttributes>
  </Extensions>
  <IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol urn:oasis:names:tc:SAML:1
    <Extensions>
    <mdrpi:PublicationInfo
      publisher="https://rr.aai.switch.ch/gen_saml2md_entity.php?objectType=homeOrg&amp;objectID=130"
      creationInstant="2015-06-05T13:58:52Z">
    </mdrpi:PublicationInfo>
      <shibmd:Scope regexp="false">switch.ch</shibmd:Scope>
      <mdui:UIInfo>
        <mdui:DisplayName xml:lang="de">SWITCH</mdui:DisplayName>
        <mdui:DisplayName xml:lang="en">SWITCH</mdui:DisplayName>
        <mdui:DisplayName xml:lang="fr">SWITCH</mdui:DisplayName>
        <mdui:DisplayName xml:lang="it">SWITCH</mdui:DisplayName>
        <mdui:Description xml:lang="de">SWITCH erbringt innovative, einzigartige Internet-Dienstleistungen für
        <mdui:Description xml:lang="en">SWITCH provides innovative, unique internet services for the Swiss uni
        <mdui:Description xml:lang="fr">SWITCH fournit des prestations innovantes et uniques pour les hautes é
        <mdui:Description xml:lang="it">SWITCH eroga servizi Internet innovativi e unici per le scuole univers
        <mdui:Keywords xml:lang="en">Zurich</mdui:Keywords>
        <mdui:Keywords xml:lang="de">Zürich</mdui:Keywords>
        <mdui:Keywords xml:lang="fr">Zurich</mdui:Keywords>
        <mdui:Keywords xml:lang="it">Zurigo</mdui:Keywords>
        <mdui:Logo height="16" width="16">data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAABAAAAAQCAYAAAAf8/9hAA
        <mdui:Logo height="60" width="80">data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAAFAAAAA8CAYAAADxJz2MAA
        <mdui:InformationURL xml:lang="en">http://www.switch.ch/about/</mdui:InformationURL>
        <mdui:InformationURL xml:lang="de">http://www.switch.ch/de/about/</mdui:InformationURL>
        <mdui:InformationURL xml:lang="fr">http://www.switch.ch/fr/about/</mdui:InformationURL>
        <mdui:InformationURL xml:lang="it">http://www.switch.ch/it/about/</mdui:InformationURL>
      </mdui:UIInfo>
      <mdui:DiscoHints>
        <mdui:IPHint>130.59.0.0/16</mdui:IPHint>
        <mdui:IPHint>2001:620::/48</mdui:IPHint>
```

Does metadata change when IdP is upgraded?

No, but revising some parts of metadata still is recommended.

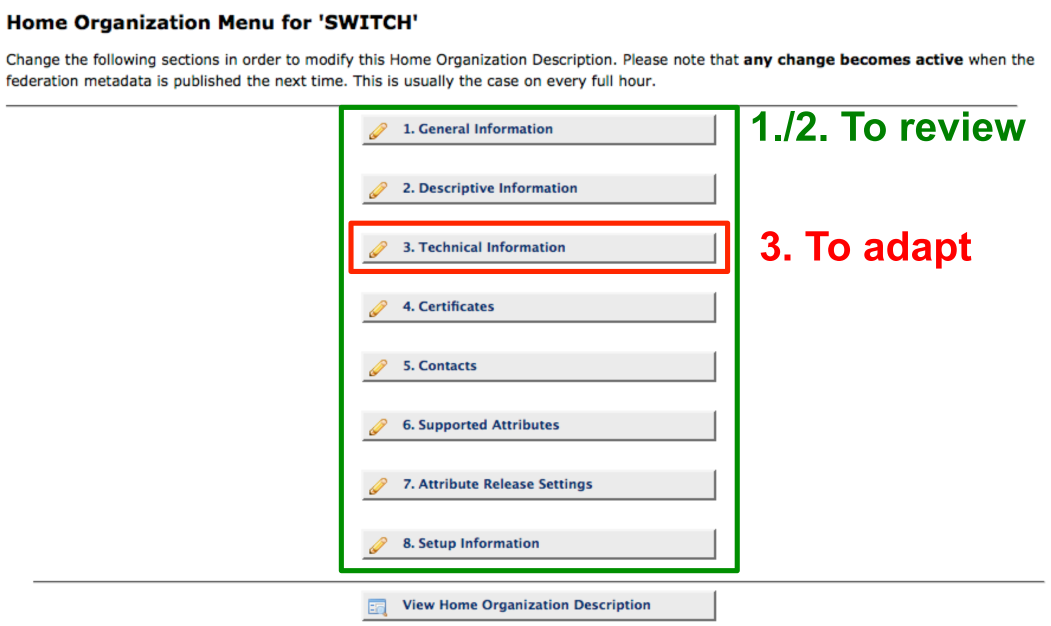
IdPv2 vs IdPv3 Metadata

- **Endpoint URLs stay the same! ☺**
  - Unlike upgrade vom IdPv1 to IdPv2
  - Therefore, no metadata/Resource Registry change needed in general

- However, **some changes still recommended**:
  1. Review the Home Organisation Description
  2. Change URL for Attribute Authority
  3. Remove Unnecessary Endpoints

- To change metadata, **change Home Organisation description**
  - Apply change in AAI Resource Registry: https://rr.aai.switch.ch

Home Organisation Description



Home Organization Menu for 'SWITCH'

Change the following sections in order to modify this Home Organization Description. Please note that **any change becomes active** when the federation metadata is published the next time. This is usually the case on every full hour.

1./2. To review

3. To adapt

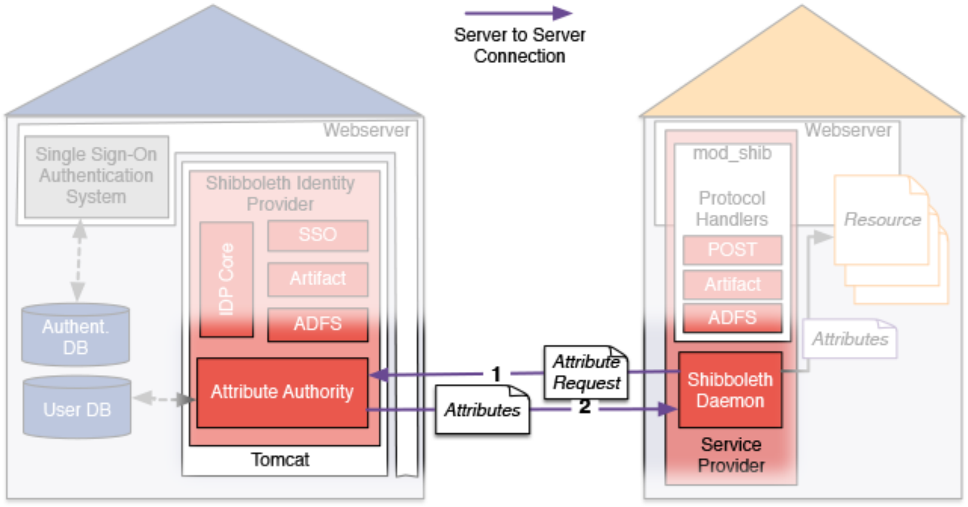
1. Review the Home Organisation Description

In particular review and adapt if necessary:

- **1. General Information**
  - Interfederation Support (option only available if Interfederation Access Declaration has been signed. More information on https://www.switch.ch/aai/support/documents/interfederation/).
- **2. Descriptive Information**
  - Update/Revise IP ranges and Domain Hints (used for IdP discovery)
- **5. Contacts**
  - Please ensure only non-personal email addresses are listed. Ideally also add helpdesk phone numbers.
- **7. Attribute Release Settings**
  - Default attribute release policies. Consider to release all R&S attributes!

2. Change URL for Attribute Authority

Recommendation for IdPv2 has been so far:
Separate port (i.e. 8443) or IP for IdP Attribute Authority (AA)



2. Change URL for Attribute Authority

New Recommendation for IdP:
Use same IP and same Port (443) for Attribute Authority (AA).

Why?

Easier configuration because:

- only one Apache <VirtualHost>
- one domain name and one certificate
- no X.509 client authentication needed anymore (SP still checks IdP webserver certificate with IdP's metadata)
- Attribute Queries are hardly used anymore (but will become important again for support of edu-ID)

But how is the attribute query still secured without X.509 client authentication by the Service Provider?

SP signs attribute query request with his private key (message signing), the IdP checks signature with SP's public key in metadata.

2. Change URL for Attribute Authority

What to adapt in Resource Registry then?

In "3. Technical Information" change the URLs for:

- "Attribute Service"
- "Artifact Resolution Service"

Make sure they point to the URL configured during the Identity Provider deployment. Typically the **URLs change from** e.g.:

https://aai-login.example.org:8443/idp/... or https://aai-aa.example.org/idp/...

to

https://aai-login.example.org/idp/...

3. Remove Unnecessary Endpoints

Which endpoints to remove?

Generally it's better to only have published in metadata what is needed and used.

So, in "3. Technical Information" consider removing end points that are hardly used.

Candidates to remove:

- "**Single Sign On Service**" with "SAML2 HTTP POST SimpleSign" binding
- "**Artifact Resolution Service**" with "SAML1 SOAP" binding
- "**Attribute Service**" with "SAML1 SOAP" binding

But only remove them after verifying they are not used ...

3. Remove Unnecessary Endpoints

How to check if a profile and binding can be removed?

Check if it has been used within last few months.
If not, remove it from Resource Registry.

How to check if it has been used?

Check log files. To find if SAML1 SOAP binding logins in 2015:

```
$ cd /opt/shibboleth-idp/logs/
$ grep 'urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding' \
  idp-process-2015-*.log
```

Returns information (i.e. time, SP) when binding was used the last time.