IdP 2.2: what’s new?

SWITCH

Serving Swiss Universities

Patrik Schnellmann
patrik.schnellmann@switch.ch

Bern, 15. June 2010

Recap: changes from IdP 1.3 to 2

- Attribute Push profile is default (no more backchannel requests)
- Embedded certificates in metadata
- SAML names of attributes changed from “urn:mace:...” to “urn:oid:...”
- entityID URL format (e.g. https://sp.example.org/shibboleth)
- No more separate cronjobs to download metadata

Download of attribute-filter.xml

```
<Service id="shibboleth.AttributeFilterEngine"
  xsi:type="attribute-afp:ShibbolethAttributeFilteringEngine"
   configurationResourcePollingFrequency="3600000"
   configurationResourcePollingRetryAttempts="128">
  <ConfigurationResource xsi:type="resource:FileBackedHttpResource”
url="https://rr.aai.switch.ch/switchaai/example.org/
attribute-filter.xml"
file="/opt/shibboleth-idp/conf/attribute-filter.xml"/>
</Service>
```

- Download attribute-filter.xml every hour (3’600 s)
- If not successful, retry
- Stop retrying after 128 attempts

What ~~is~~ will be new in IdP 2.2?

- Proxy support for (file backed) URL Metadata Provider
- requireValidMetadata instead of maintainExpiredMetadata
- XML Schema duration syntax instead of integers (ms)
- IdP status handler: uptime is shown

```
<MetadataProvider
  id="URLMD”
  xsi:type="FileBackedHTTPMetadataProvider"
  xmlns="urn:mace:shibboleth:2.0:metadata"
  metadataURL="http://metadata.aai.switch.ch/metadata.switchaai.xml"
  backingFile="/opt/shibboleth-idp/metadata/metadata.switchaai.xml"
  requireValidMetadata="true"
  maxRefreshDelay="PT1H"
  proxyHost="proxy.example.org" proxyPort="8080"
  proxyUser="proxy" proxyPassword="secret"
  requestTimeout="PT5S">
  <!-- ... -->
</MetadataProvider>
```

Questions?

Q & A

http://www.switch.ch/aai

aai@switch.ch