Metadata Signing and Update

For Shibboleth 2 Deployments

SWITCH

Serving Swiss Universities

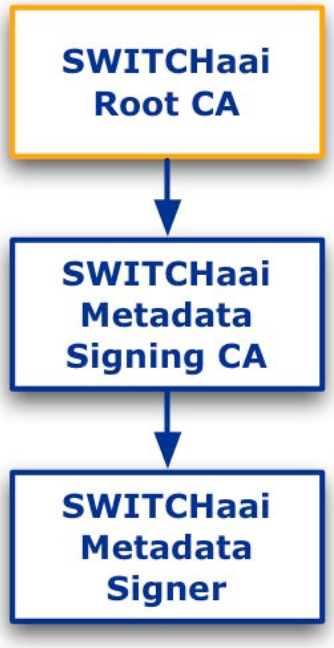
Patrik Schnellmann
patrik.schnellmann@switch.ch

Metadata Signing and Update

- The new certificate hierarchy for AAI metadata signing
- How to trust the trust anchor
- Configuration of the trust anchor for Shibboleth
- Metadata refresh for Shibboleth

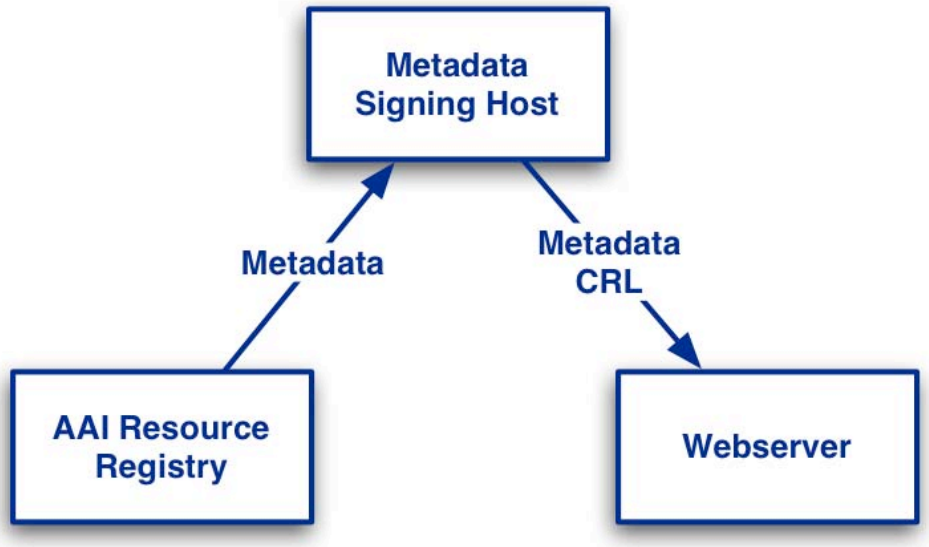
Metadata Signing - Certificate Hierarchy

- Trust anchor for SWITCHaai Metadata



⇨ https://www.switch.ch/pki/aai/

Metadata Provisioning Infrastructure



- To be used for Shibboleth 2 deployments (no changes for IdP/SP 1.3)
- URLs
  http://metadata.aai.switch.ch/metadata.switchaai.xml
  http://metadata.aai.switch.ch/metadata.aaitest.xml
  http://crl.aai.switch.ch/SWITCHaaiRootCA.crl
  http://crl.aai.switch.ch/SWITCHaaiMetadataSigningCA2008.crl

How to trust the trust anchor

```
$ curl -O http://ca.aai.switch.ch/SWITCHaaiRootCA.crt.pem

$ openssl x509 -in SWITCHaaiRootCA.crt.pem \
 -fingerprint -sha1 -noout

SHA1 Fingerprint=
3C:E2:5A:E0:9D:B4:BB:2B:FD:33:3C:22:80:39:F7:FC:4A:F9:2C:E9
```

Compare the fingerprint with the fingerprint on https://www.switch.ch/pki/aai/

One-Liner:

```
curl http://ca.aai.switch.ch/SWITCHaaiRootCA.crt.pem |
openssl x509 -fingerprint -sha1 -noout
```

Trust anchor configuration (IdP 2.1)

relying-party.xml

```
<security:TrustEngine id="shibboleth.MetadataTrustEngine"
                      xsi:type="security:StaticPKIXSignature">

        <security:ValidationInfo
                    id="SWITCHaaiFederationCredentials"
                    xsi:type="security:PKIXFilesystem">

    <security:Certificate>
      /opt/shibboleth-idp/credentials/SWITCHaaiRootCA.crt.pem
    </security:Certificate>

  </security:ValidationInfo>
</security:TrustEngine>
```

Metadata configuration (IdP 2.1)

relying-party.xml

```
<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"
 maintainExpiredMetadata="false"
 cacheDuration="3600">

 <MetadataFilter xsi:type="SignatureValidation"
  xmlns="urn:mace:shibboleth:2.0:metadata"
  trustEngineRef="shibboleth.MetadataTrustEngine"
  requireSignedMetadata="true" />

</MetadataProvider>
```

⇨ The IdP reloads the metadata before it expires.
No external cronjob needed in version 2.

Keep your metadata up-to-date!

metadata.switchaai.xml

```
<EntitiesDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  Name="urn:mace:switch.ch:SWITCHaai"
  validUntil="2008-11-18T10:00:01Z"
  cacheDuration="P1D"
  ...>
  ...
```

- Metadata validity of 5 days
- IdP's are required to refresh metadata at least once a day
  hourly refreshes are recommended

Summary

Main changes concerning metadata

- New metadata trust anchor
- Metadata validity limited to 5 days

Benefits

- Increased reliability and security of SWITCHaai
- Less interoperability problems using IdP built-in metadata refresh