

Nyckelrullning 2016 - Shibboleth Identity Provider v3

Det är enkelt att ändra signeringsnyckel och metadataflöde i Shibboleth IdP v3. Det enda du behöver göra är att hämta ner nya publika signeringsnyckeln och därefter ändra i filen metadata-providers.xml.

1. Ladda ner den nya publika signeringsnyckeln [md-signer2.crt](#) och spara den under `%{idp.home}/credentials/`. `%{idp.home}` är baskatalogen för din shibbolethinstallation (oftast `/opt/shibboleth-idp/` om du använt standard värden på en linux maskin).
2. Verifiera nyckeln

```
openssl x509 -noout -fingerprint -sha256 -in %{idp.home}/credentials/md-signer2.crt
Output skall bli
SHA256 Fingerprint=A6:78:5A:37:C9:C9:0C:25:AD:5F:1F:69:22:EF:76:7B:C9:78:67:67:3A:AF:4F:8B:EA:A1:A7:6D:
A3:A8:E5:85
```

3. Ändra publik signeringsnyckel för SWAMID i metadata-providers.xml till den nya filen, `certificateFile="%{idp.home}/credentials/md-signer2.crt"`
4. Ändra vilket metadataflöde som ska laddas hem från SWAMID i metadata-providers.xml, `metadataURL="http://mds.swamid.se/md/swamid-2.0.xml"`
5. Starta om Shibboleth och titta i loggarna att allt startar ordentligt.

Ändring i metadata-providers.xml

```
...
<MetadataProvider id="SWAMIDURLMD" xsi:type="FileBackedHTTPMetadataProvider" xmlns="urn:mace:shibboleth:2.0:
metadata"
    metadataURL="http://mds.swamid.se/md/swamid-2.0.xml"
    backingFile="%{idp.home}/metadata/swamid-2.0.xml">
    <MetadataFilter xsi:type="SignatureValidation" requireSignedRoot="true"
        certificateFile="%{idp.home}/credentials/md-signer2.crt" />
    <MetadataFilter xsi:type="EntityRoleWhiteList">
        <RetainedRole>md:SPSSODescriptor</RetainedRole>
    </MetadataFilter>
</MetadataProvider>
...
```