Konfigurera metadatahämtning i Shibboleth Identity Provider för SAML

> Konfigurationerna under denna sida fungerar endast för Shibboleth 3 eller senare. För simpleSAMLphp och ADFS kan konfigurationsexemplen endast användas som inspiration.

SWAMID är en en multilateral identitetsfederation där alla identitetsutgivare pratar direkt med alla tjänster. Detta innebär att en identitetsutgivare måste ha tillgång till tjänsternas metadata när en användare vill logga in i tjänsten. I princip finns två sätt att göra detta, dels genom att med jämna mellanrum hämta metadata för alla tjänster och dels genom att dynamiskt hämta metadata vid behov. Traditionellt har SWAMID endast tillhandahållit den fulla nedladdningen men från och med våren 2023 går det även använda den dynamiska metoden.

När identitetsutgivaren hämtar hem metadata från SWAMID ska den verifiera att det är metadata signerat av SWAMID som hämtas hem och används. För denna signering använder SWAMID en PKI-baserad krypteringsnyckel. För att genomföra denna kontroll behöver SWAMIDs signeringscertfikat laddas ner, installeras och konfigureras i identitetsutgivaren.

Hämta och spara certifikatet från SAML Metadata and Trust

Hämta certifkatsfilen md-signer2.crt från https://mds.swamid.se/md/md-signer2.crt och verifiera att det är rätt nyckel genom att kontrollera fingerprint. Spara sedan certfikatsfilen på den plats i filsystemet som anges nedan om du gjort standardinstallation av Shibboleth IdP.

Linux

```
/opt/shibboleth-idp/credentials/md-signer2.crt
```

Windows

```
C:/Program Files (x86)/Shibboleth/IdP/credentials/md-signer2.crt
```

Konfigurera hur metadata hämtas och sparas av Shibboleth IdP

Om du väljer att hämta full eller dynamisk metadata från SWAMID är en riskbedömning. Fördelen med att automatiskt hämta det fulla metadatat är att du alltid har en färsk kopia av SWAMIDs metadata men det betyder också att tjänsten förbrukar mycket mer ramminne eftersom IdPn håller allt metadata i primärminnet. En annan effekt av att hämta och använda det fulla metadatat från SWAMID är att det tar mycket längre tid att starta IdP-tjänsten. För att minska minnesåtgången har SWAMID stöd för att IdPn dynamiskt hämta metadata när en användare ska logga in i tjänsten. För att detta ska vara snabbt cachar IdP använd metadata under en period så att den inte behöver hämtas varje gång. Nackdelen med den dynamiska hämtningen av metadata är att SWAMIDs metadata tjänst alltid måste vara tillgänglig och detta har löst via en feltollerant teknisk lösning.

Dynamiskt hämta metadata från SWAMID

Stoppa in följande block XML på relevant plats i metadata-providers.xml dynamiskt hämta SWAMIDs metadata inklusive SP:s från eduGAIN.

```
<!-- SWAMID MDQ METADATA PROVIDER -->
<MetadataProvider id="DynamicEntityMetadata" xsi:type="DynamicHTTPMetadataProvider"
         connectionRequestTimeout="PT2S"
         connectionTimeout="PT2S"
         socketTimeout="PT4S">
     <MetadataFilter xsi:type="SignatureValidation" requireSignedRoot="true"
               certificateFile="%{idp.home}/credentials/md-signer2.crt" />
     <MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P14D"/>
          <MetadataQueryProtocol>https://mds.swamid.se/</MetadataQueryProtocol>
</MetadataProvider>
```

Hämta metadata aggregat över alla registrerade tjänster automatiskt från SWAMID

Stoppa in följande block XML på relevant plats i metadata-providers.xml för att hämta SWAMIDs metadata över alla registrerade tjänster i SWAMID och från interfederationssamarbeten.

Hämta metadata för SWAMID 2.0 med följande konfiguration:

```
<!-- SWAMID 2.0 METADATA PROVIDER -->
<MetadataProvider id="Swamid2MD" xsi:type="FileBackedHTTPMetadataProvider" xmlns="urn:mace:shibboleth:2.0:
metadata"
                metadataURL="http://mds.swamid.se/entities/md/swamid-2.0.xml"
                backingFile="%{idp.home}/metadata/swamid-2.0.xml">
        <MetadataFilter xsi:type="SignatureValidation" requireSignedMetadata="true"
                        certificateFile="%{idp.home}/credentials/md-signer2.crt" />
        <MetadataFilter xsi:type="EntityRoleWhiteList">
                <RetainedRole>md:SPSSODescriptor</RetainedRole>
        </MetadataFilter>
</MetadataProvider>
```

Hämta och använda metadata från SWAMIDs testfederation

Använd endast denna konfiguration om du planerar att registrera din IdP i SWAMIDs testfederation.

Vid behov så kan även metadata för SWAMIDs testfederation läggas till för att tillåta realistiska tester för ej driftsatta tjänsteleverantörer (SP):

```
<!-- SWAMID TEST METADATA PROVIDER -->
<MetadataProvider id="Swamid2MD" xsi:type="FileBackedHTTPMetadataProvider" xmlns="urn:mace:shibboleth:2.0:
metadata"
                metadataURL="http://md.swamid.se/md/swamid-testing-1.0.xml"
                backingFile="%{idp.home}/metadata/swamid-testing-1.0.xml">
        <MetadataFilter xsi:type="SignatureValidation" requireSignedMetadata="true"
                        certificateFile="%{idp.home}/credentials/md-signer2.crt" />
        <MetadataFilter xsi:type="EntityRoleWhiteList">
                <RetainedRole>md:SPSSODescriptor</RetainedRole>
        </MetadataFilter>
</MetadataProvider>
```