3.1 Configure Shibboleth SP - shibboleth2.xml

We have prepared two files with reasonable defaults for connecting an SP to SWAMID. One is for a shibboleth SP behind an Apache web server and the other is for a shibboleth SP behind an IIS web server. You need to change EntityID and any other values containing the string **example.org** in the file to the public FQDN (Fully Qualified Domain Name) of your host. Note that registering a fully functional SP with SWAMID usually requires you to have a FQDN for your service in DNS that is visible on the public Internet. It is possible to register internal development instances in the SWAMID testing metadata that points to localhost or other internal DNS names but this is discouraged for production services.

If you have followed the installation guides in this wiki so far, you should rename the downloaded file, edit it and rename it to shibboleth2.xml and put it in the SHIB_HOME directory (/etc/shibboleth on linux c:\opt\shibboleth-sp\etc\shibboleth on Windows, if you haven't changed that during installation).

The latest published SWAMID example main configuration file for Shibboleth Service Provider 3 is published at mds.swamid.se/entity-configurations/Shibboleth-SP/v3/. Below is the latest versions included from the publication repository.

swamid-apache-shibboleth2.xml without standard installation comments and examples

```
<SPConfig xmlns="urn:mace:shibboleth:3.0:native:sp:config"
    xmlns:conf="urn:mace:shibboleth:3.0:native:sp:config"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    clockSkew="180">
    <ApplicationDefaults entityID="https://swamidsp.example.org/shibboleth"
                         REMOTE_USER="subject-id eppn pairwise-id persistent-id"
                         metadataAttributePrefix="Meta-">

        <Sessions lifetime="28800" timeout="3600" relayState="ss:mem"
                  redirectLimit="exact"
                  checkAddress="false" handlerSSL="true" cookieProps="http" sameSiteFallback="true">

            <Logout>SAML2 Local</Logout>

            <SessionInitiator type="Chaining" Location="/DS/Login" id="swamid-ds-default" relayState="cookie">
                <SessionInitiator type="SAML2" acsIndex="1" acsByIndex="false" template="bindingTemplate.html"/>
                <SessionInitiator type="Shib1" acsIndex="5"/>
                <SessionInitiator type="SAMLDS" URL="https://service.seamlessaccess.org/ds/"/>
            </SessionInitiator>

            <md:AssertionConsumerService Location="/SAML2/POST" index="1"
                Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                conf:ignoreNoPassive="true"/>

            <Handler type="MetadataGenerator" Location="/Metadata" signing="false"/>
            <Handler type="Status" Location="/Status" acl="127.0.0.1 ::1"/>
            <Handler type="Session" Location="/Session" showAttributeValues="false"/>
            <Handler type="DiscoveryFeed" Location="/DiscoFeed"/>

            <md:ArtifactResolutionService Location="/Artifact/SOAP" index="1"
                Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"/>

        </Sessions>

        <Errors supportContact="webmaster@example.org"
            helpLocation="/about.html"
            styleSheet="/shibboleth-sp/main.css"/>

        <MetadataProvider type="MDQ" id="mdq.swamid.se" ignoreTransport="true" cacheDirectory="mdq.swamid.se"
                    baseUrl="https://mds.swamid.se/">
            <MetadataFilter type="Signature" certificate="md-signer2.crt"/>
            <MetadataFilter type="RequireValidUntil" maxValidityInterval="2419200"/>
        </MetadataProvider>

        <!-- "Old" way -->
        <!--
        <MetadataProvider
                type="XML"
                url="https://mds.swamid.se/md/swamid-idp-transitive.xml"
                backingFilePath="swamid-idp-transitive.xml" reloadInterval="14400">
            <MetadataFilter type="Signature" certificate="md-signer2.crt" verifyBackup="false" />
        </MetadataProvider>
```

```
        -->

        <AttributeExtractor type="XML" validate="true" reloadChanges="false" path="attribute-map.xml"/>

        <AttributeExtractor type="Metadata" errorURL="errorURL" DisplayName="displayName"
registrationAuthority="registrationAuthority"/>
        <!-- more attributes please check https://shibboleth.atlassian.net/wiki/spaces/SP3/pages/2065334447
/MetadataAttributeExtractor -->

        <AttributeResolver type="Query" subjectMatch="true"/>

        <AttributeFilter type="XML" validate="true" path="attribute-policy.xml"/>

        <CredentialResolver type="File" key="sp-key.pem" certificate="sp-cert.pem"/>
    </ApplicationDefaults>
    <SecurityPolicyProvider type="XML" validate="true" path="security-policy.xml"/>

    <ProtocolProvider type="XML" validate="true" reloadChanges="false" path="protocols.xml"/>

</SPConfig>
```

swamid-IIS-shibboleth2.xml without standard installation comments and examples

```
<SPConfig xmlns="urn:mace:shibboleth:3.0:native:sp:config"
    xmlns:conf="urn:mace:shibboleth:3.0:native:sp:config"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    clockSkew="180">

    <InProcess logger="native.logger">
        <ISAPI normalizeRequest="true" safeHeaderNames="true">
            <Site id="1" name="swamidsp.example.org" scheme="https" port="443"/>
        </ISAPI>
    </InProcess>

    <RequestMapper type="Native">
        <RequestMap>
            <Host name="swamidsp.example.org">
                <Path name="myswamidapp" requireSession="true"  authType="shibboleth"/>
            </Host>
        </RequestMap>
    </RequestMapper>

    <ApplicationDefaults entityID="https://swamidsp.example.org/shibboleth"
                         REMOTE_USER="subject-id eppn pairwise-id persistent-id"
                         metadataAttributePrefix="Meta-">
        <Sessions lifetime="28800" timeout="3600" relayState="ss:mem"
                  redirectLimit="exact"
                  checkAddress="false" handlerSSL="true" cookieProps="http" sameSiteFallback="true">

            <Logout>SAML2 Local</Logout>

            <SessionInitiator type="Chaining" Location="/DS/Login" id="swamid-ds-default" relayState="cookie">
               <SessionInitiator type="SAML2" acsIndex="1" acsByIndex="false" template="bindingTemplate.html"/>
                <SessionInitiator type="Shib1" acsIndex="5"/>
                <SessionInitiator type="SAMLDS" URL="https://service.seamlessaccess.org/ds/"/>
            </SessionInitiator>

            <md:AssertionConsumerService Location="/SAML2/POST" index="1"
                Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                conf:ignoreNoPassive="true"/>

            <Handler type="MetadataGenerator" Location="/Metadata" signing="false"/>
            <Handler type="Status" Location="/Status" acl="127.0.0.1 ::1"/>

            <Handler type="Session" Location="/Session" showAttributeValues="false"/>

            <Handler type="DiscoveryFeed" Location="/DiscoFeed"/>
```

```
            <md:ArtifactResolutionService Location="/Artifact/SOAP" index="1"
                Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"/>
        </Sessions>

        <Errors supportContact="webmaster@example.org"
            helpLocation="/about.html"
            styleSheet="/shibboleth-sp/main.css"/>

        <MetadataProvider type="MDQ" id="mdq.swamid.se" ignoreTransport="true" cacheDirectory="mdq.swamid.se"
                    baseUrl="https://mds.swamid.se/">
            <MetadataFilter type="Signature" certificate="md-signer2.crt"/>
            <MetadataFilter type="RequireValidUntil" maxValidityInterval="2419200"/>
        </MetadataProvider>

        <!-- "Old" way -->
        <!--
          <MetadataProvider
                type="XML"
                url="https://mds.swamid.se/md/swamid-idp-transitive.xml"
                backingFilePath="swamid-idp-transitive.xml" reloadInterval="14400">
            <MetadataFilter type="Signature" certificate="md-signer2.crt" verifyBackup="false" />
        </MetadataProvider>
        -->

        <AttributeExtractor type="XML" validate="true" reloadChanges="false" path="attribute-map.xml"/>

        <AttributeExtractor type="Metadata" errorURL="errorURL" DisplayName="displayName"
registrationAuthority="registrationAuthority"/>
        <!-- more attributes please check https://shibboleth.atlassian.net/wiki/spaces/SP3/pages/2065334447
/MetadataAttributeExtractor -->

        <AttributeResolver type="Query" subjectMatch="true"/>

        <AttributeFilter type="XML" validate="true" path="attribute-policy.xml"/>

        <CredentialResolver type="File" use="signing"
            key="sp-signing-key.pem" certificate="sp-signing-cert.pem"/>
        <CredentialResolver type="File" use="encryption"
            key="sp-encrypt-key.pem" certificate="sp-encrypt-cert.pem"/>

    </ApplicationDefaults>

    <SecurityPolicyProvider type="XML" validate="true" path="security-policy.xml"/>

    <ProtocolProvider type="XML" validate="true" reloadChanges="false" path="protocols.xml"/>

</SPConfig>
```

Errorhandling

The "<Errors .... /> assumes that http://example.org/about.html leads to some form of help page and that webmaster@example.org is the right contact address for your service. Change according to taste.

Additional setup steps

After you save this file as /etc/shibboleth/shibboleth2.xml, download https://mds.swamid.se/md/md-signer2.crt and save as /etc/shibboleth/md-signer.crt (or your windows equivalent). Take care to verify the fingerprint of this certificate as published on https://mds.swamid.se/md/. Finally you must generate a keypair for your SP. This keypair is not the same as the certificate of your service and is used to secure SAML protocol messages between SWAMID IdPs and your service. Usually you do this by running the following command

shibboleth key generation

```
# shib-keygen -h example.com
```

At this point you should be able to restart the shibd process. If you get errors or if shibd refuses to start, make sure you don't have syntax error in any of your XML files. The system logs should provide clues about what may have gone wrong. If necessary increase the shibboleth log level to DEBUG.

If shibd restarts ok, you should be able to point a browser at (or use curl to download) **https://example.com/Shibboleth.sso/Metadata** which should contain a PEM encoded version of your newly generated SP keypair. At this point you are read to register this metadata with SWAMID.