MetadataForSP

The Metadata topic covers the general structure of metadata for any entity. This topic will specifically cover the parts that describe an SP. This is an overview of how to create metadata **about** an SP, which you will **give** to an IdP. If you're looking for the reverse, that's here.

> **Shibboleth-Specific Tip**
>
> When first starting out, you can usually begin by relying on the SP software to generate an initial set of metadata about itself, once you've configured it, by accessing a URL like **`https://service.example.org/Shibboleth.sso/Metadata`**
>
> This will only help if you've already configured the SP's entityID and credentials, and properly established the web server's virtual hostname information. Even then, it may not be exactly what you need, but it should be helpful to look at and edit from.

General Structure

SP metadata is contained within the `<md:SPSSODescriptor>` role element. As with all roles, you **MUST** include the proper `protocolSupportEnumeration` value to reflect the protocol families the SP supports, as descibed in the Metadata topic. Failure to do so will prevent the IdP from recognizing the SP properly.

An SP role typically includes the following descriptive information:

- the public key(s) used by the SP for authentication and encryption
- endpoints of various types for communicating with it
- explicitly supported name identifier formats, if any
- descriptions of the "services" offered by the SP and the SAML attributes required by them

The order of all this information is significant, which you can refer to the schema for, but the most common elements included would be present in the following order:

- `<md:KeyDescriptor>` (can be omitted, but rarely)
- `<md:SingleLogoutService>` (if any)
- `<md:NameIDFormat>` (if any)
- `<md:AssertionConsumerService>` (always at least one)
- `<md:AttributeConsumingService>` (rare today, but good practice to include)

Keys

Refer to the MetadataKeyDescriptor topic for assistance with describing keys.

> **Shibboleth-Specific Tip**
>
> The keys you identify in the metadata **MUST** match the keys you configure into the SP as credentials. If they don't match, your SP may be unable to decrypt information from the IdP, or will be unable to negotiate SOAP connections to query for attributes.

Logout

If your SP supports SAML 2.0 Single Logout, you will need to include one or more `<md:SingleLogoutService>` endpoint elements in the metadata.

> **Shibboleth-Specific Tip**
>
> The `Location` attribute of Logout endpoints is derived from the logout handlers defined in the SP. As with all SP handlers, the locations will typically be of the form `scheme` + `vhost` + "/Shibboleth.sso" + `Location`, where `Location` is determined from the handler element in the configuration.
>
> The elements must also include a `Binding` attribute, which can be copied directly from the handler element in the configuration.
>
> Note that each virtual host (combination of scheme, hostname, and port) operating within a particular SP **MUST** have its own set of endpoints expressed in the metadata.

Documenting Identifiers

An SP can identify specific "formats" of SAML name identifiers that it supports by listing each supported `Format` URI inside a `<md:NameIDFormat>` element. If it doesn't care (perhaps because it relies solely on SAML attributes), it can omit this element from its metadata.

Shibboleth-Specific Tip

This isn't used all that often for Shibboleth SPs, which tend to be more attribute-centric in the use of SAML, but the Shibboleth IdP software can utilize this information in its format selection process.

Assertion Consumer Services

SPs support SSO protocols by including one or more `<md:AssertionConsumerService>` endpoint elements in their metadata. These are the locations to which the IdP will eventually send the user at the SP. By enumerating them in the metadata, the IdP can ensure that the user's information is sent only to authorized locations.

For technical reasons, these endpoint elements have to carry an additional `index` XML attribute, which should generally contain a small positive integer. The index values should be unique across all the like-named elements within the role.

Shibboleth-Specific Tip

The `Location` attribute of SSO endpoints is derived from the assertion consumer services defined in the SP. As with all SP handlers, the locations will typically be of the form `scheme` + `vhost` + "/Shibboleth.sso" + `Location`, where `Location` is determined from the handler element in the configuration.

The elements must also include a `Binding` attribute, which can be copied directly from the handler element in the configuration. You can generally copy the `index` attribute as well.

Note that each virtual host (combination of scheme, hostname, and port) operating within a particular SP **MUST** have its own set of endpoints expressed in the metadata.

Documenting Attributes

An SP typically requires some number of SAML attributes to perform its function. Metadata can be used to advertise these requirements in terms of "service offerings" that can be referenced in a request for authentication. An SP can define multiple services or service levels, with accompanying human-readable descriptions, to drive the development of IdP user interface components.

Each "service" is expressed using an `<md:AttributeConsumingService>` element that contains descriptive elements and a list of `<md:RequestedAttribute>` elements (based on type **saml:AttributeType**) that identify required or optional attributes and/or values.

Examples

These examples are written to reflect the typical default configuration of a Shibboleth SP, but obviously specifics may vary. Note that it's very important that what you support match what you advertise. For example, if you have not properly integrated single logout into your application and user interface, then don't claim to support it.

Complete Example Supporting SAML 2.0 and SAML 1.1

```
<md:EntityDescriptor entityID="https://service.example.org/shibboleth" validUntil="2010-01-01T00:00:00Z">

  <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol urn:oasis:names:tc:SAML:
2.0:protocol">

    <md:KeyDescriptor>
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>
           ... base64-encoded certificate elided ...
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>

    <md:SingleLogoutService Location="https://service.example.org/Shibboleth.sso/SLO/SOAP"
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"/>
    <md:SingleLogoutService Location="https://service.example.org/Shibboleth.sso/SLO/Redirect"
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"/>
    <md:SingleLogoutService Location="https://service.example.org/Shibboleth.sso/SLO/POST"
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
    <md:SingleLogoutService Location="https://service.example.org/Shibboleth.sso/SLO/Artifact"
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact"/>

    <md:AssertionConsumerService Location="https://service.example.org/Shibboleth.sso/SAML2/POST" index="1"
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
    <md:AssertionConsumerService Location="https://service.example.org/Shibboleth.sso/SAML2/POST-SimpleSign"
index="2"
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST-SimpleSign"/>
    <md:AssertionConsumerService Location="https://service.example.org/Shibboleth.sso/SAML2/Artifact" index="3"
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact"/>
    <md:AssertionConsumerService Location="https://service.example.org/Shibboleth.sso/SAML2/ECP" index="4"
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:PAOS"/>
    <md:AssertionConsumerService Location="https://service.example.org/Shibboleth.sso/SAML/POST" index="5"
      Binding="urn:oasis:names:tc:SAML:1.0:profiles:browser-post"/>
    <md:AssertionConsumerService Location="https://service.example.org/Shibboleth.sso/SAML/Artifact" index="6"
      Binding="urn:oasis:names:tc:SAML:1.0:profiles:artifact-01"/>

    <md:AttributeConsumingService index="1">
      <md:ServiceName xml:lang="en">Sample Service</md:ServiceName>
      <md:ServiceDescription xml:lang="en">An example service that requires a human-readable identifier and
optional name and e-mail address.</md:ServiceDescription>

      <md:RequestedAttribute FriendlyName="eduPersonPrincipalName" Name="urn:mace:dir:attribute-def:
eduPersonPrincipalName" NameFormat="urn:mace:shibboleth:1.0:attributeNamespace:uri"/>
      <md:RequestedAttribute FriendlyName="mail" Name="urn:mace:dir:attribute-def:mail" NameFormat="urn:mace:
shibboleth:1.0:attributeNamespace:uri"/>
      <md:RequestedAttribute FriendlyName="displayName" Name="urn:mace:dir:attribute-def:displayName"
NameFormat="urn:mace:shibboleth:1.0:attributeNamespace:uri"/>

      <md:RequestedAttribute FriendlyName="eduPersonPrincipalName" Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
      <md:RequestedAttribute FriendlyName="mail" Name="urn:oid:0.9.2342.19200300.100.1.3" NameFormat="urn:oasis:
names:tc:SAML:2.0:attrname-format:uri"/>
      <md:RequestedAttribute FriendlyName="displayName" Name="urn:oid:2.16.840.1.113730.3.1.241" NameFormat="
urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>

    </md:AttributeConsumingService>

  </md:SPSSODescriptor>

  <md:Organization>
    <md:OrganizationName xml:lang="en">Example Organization, Ltd.</md:OrganizationName>
    <md:OrganizationDisplayName xml:lang="en">Example Organization</md:OrganizationDisplayName>
    <md:OrganizationURL xml:lang="en">https://service.example.org/</md:OrganizationURL>
  </md:Organization>

</md:EntityDescriptor>
```

Complete Example Supporting SAML 1.1 Only

```
<md:EntityDescriptor entityID="https://service.example.org/shibboleth" validUntil="2010-01-01T00:00:00Z">

  <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol">

    <md:KeyDescriptor>
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>
           ... base64-encoded certificate elided ...
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>

    <md:AssertionConsumerService Location="https://service.example.org/Shibboleth.sso/SAML/POST" index="5"
      Binding="urn:oasis:names:tc:SAML:1.0:profiles:browser-post"/>
    <md:AssertionConsumerService Location="https://service.example.org/Shibboleth.sso/SAML/Artifact" index="6"
      Binding="urn:oasis:names:tc:SAML:1.0:profiles:artifact-01"/>

    <md:AttributeConsumingService index="1">
      <md:ServiceName xml:lang="en">Sample Service</md:ServiceName>
      <md:ServiceDescription xml:lang="en">An example service that requires a human-readable identifier and
optional name and e-mail address.</md:ServiceDescription>
      <md:RequestedAttribute FriendlyName="eduPersonPrincipalName" Name="urn:mace:dir:attribute-def:
eduPersonPrincipalName" NameFormat="urn:mace:shibboleth:1.0:attributeNamespace:uri"/>
      <md:RequestedAttribute FriendlyName="mail" Name="urn:mace:dir:attribute-def:mail" NameFormat="urn:mace:
shibboleth:1.0:attributeNamespace:uri"/>
      <md:RequestedAttribute FriendlyName="displayName" Name="urn:mace:dir:attribute-def:displayName"
NameFormat="urn:mace:shibboleth:1.0:attributeNamespace:uri"/>
    </md:AttributeConsumingService>

  </md:SPSSODescriptor>

  <md:Organization>
    <md:OrganizationName xml:lang="en">Example Organization, Ltd.</md:OrganizationName>
    <md:OrganizationDisplayName xml:lang="en">Example Organization</md:OrganizationDisplayName>
    <md:OrganizationURL xml:lang="en">https://service.example.org/</md:OrganizationURL>
  </md:Organization>

</md:EntityDescriptor>
```