MetadataForIdP

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

Shibboleth-Specific Tip

When first starting out, the IdP generates an initial metadata file during the installation process and copies it to **metadata/idp-metadata.xml**. It will contain the entityID and credentials generated by the installation process.

Whether that file is ever used is a very deployment-dependent question because it depends on whether you are participating in a "federation" or not, and how that federation handles the collection of metadata from the participants. As a general rule, it's a good idea to have an accurate metadata file available that describes your deployment. You should take the time to understand the metadata structure and content, and change or add to it as required as you make changes to your system.

General Structure

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

The use of the `<md:AttributeAuthorityDescriptor>` role is generally a compatibility requirement for supporting legacy or other SPs that rely on queries for attributes. In most cases, much of the role content will be identical across the two.

An IdP role typically includes the following descriptive information:

- the public key(s) used by the IdP for authentication and encryption
- endpoints of various types for communicating with it
- explicitly supported identifier formats, if any
- explicitly supported attributes, if any

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.

For an `<md:IDPSSODescriptor>`:

- `<md:KeyDescriptor>` (can be omitted, but rarely)
- `<md:ArtifactResolutionService>` (only needed if supporting response by artifact)
- `<md:SingleLogoutService>` (if any)
- `<md:NameIDFormat>` (if any)
- `<md:SingleSignOnService>` (always at least one)
- `<saml:Attribute>` (rare today, but may be reasonable to include)

For an `md:AttributeAuthorityDescriptor>`:

- `<md:KeyDescriptor>` (can be omitted, but rarely)
- `<md:AttributeService>` (always at least one)
- `<md:NameIDFormat>` (if any)
- `<saml:Attribute>` (rare today, but may be reasonable 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 IdP as credentials (see V2 or V3 documentation). If they don't match, SPs will generally be unable to accept assertions from or make queries to the IdP.

Artifact Resolution

SAML includes the ability to rely on redirects containing small strings called "artifacts" that the consuming site uses to pull the complete message. This is much more commonly used in the IdP->SP direction, so some IdPs may need to support an inbound SOAP endpoint to perform artifact->message resolution.

Logout

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

Documenting Identifiers

An IdP can identify specific "formats" of SAML name identifiers that it supports by listing each supported `Format` URI inside a `<md:NameIDFormat>` element.

Shibboleth-Specific Tip

This isn't used at all by the Shibboleth SP software.

Single Sign-On Services

IdPs support SSO protocols by including one or more `<md:SingleSignOnService>` endpoint elements in their metadata. These are the locations to which the SP (or some other web site acting on its behalf) will send the user to the IdP with a protocol-specific request of some kind.

Attribute Services

IdPs that support attribute queries document this by including the additional `<md:AttributeAuthorityDescriptor>` role in their metadata containing one or more `<md:AttributeService>` endpoint elements. These are the SOAP endpoints to which SPs or other software may send SAML attribute queries.

Documenting Attributes

An IdP can enumerate the SAML attributes that it can supply (subject to policy) to SPs. This is essentially informational in most cases.

Shibboleth-Specific Tip

This isn't used at all by the Shibboleth SP software.

Examples

These examples are written to reflect the typical default configuration of a Shibboleth IdP, but obviously specifics can vary. Note that it's very important that what you support match what you advertise. For example, if you don't support artifact resolution (perhaps because of IdPStatelessClustering), then don't advertise it.

Complete Example Supporting SAML 2.0 and the Shibboleth profile of SAML 1.1

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

  <md:IDPSSODescriptor protocolSupportEnumeration="urn:mace:shibboleth:1.0 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:ArtifactResolutionService Location="https://idp.example.org:8443/idp/profile/SAML1/SOAP
/ArtifactResolution"
      Binding="urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding" index="1"/>
    <md:ArtifactResolutionService Location="https://idp.example.org:8443/idp/profile/SAML2/SOAP
/ArtifactResolution"
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" index="2"/>

    <md:NameIDFormat>urn:mace:shibboleth:1.0:nameIdentifier</md:NameIDFormat>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>

    <md:SingleSignOnService Location="https://idp.example.org/idp/profile/Shibboleth/SSO"
      Binding="urn:mace:shibboleth:1.0:profiles:AuthnRequest"/>
    <md:SingleSignOnService Location="https://idp.example.org/idp/profile/SAML2/POST/SSO"
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
    <md:SingleSignOnService Location="https://idp.example.org/idp/profile/SAML2/POST-SimpleSign/SSO"
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST-SimpleSign"/>
    <md:SingleSignOnService Location="https://idp.example.org/idp/profile/SAML2/Redirect/SSO"
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"/>
    <md:SingleSignOnService Location="https://idp.example.org/idp/profile/SAML2/SOAP/ECP"
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"/>
 </md:IDPSSODescriptor>

  <md:AttributeAuthorityDescriptor 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:AttributeService Location="https://idp.example.org:8443/idp/profile/SAML1/SOAP/AttributeQuery"
      Binding="urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding"/>
    <md:AttributeService Location="https://idp.example.org:8443/idp/profile/SAML2/SOAP/AttributeQuery"
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"/>

    <md:NameIDFormat>urn:mace:shibboleth:1.0:nameIdentifier</md:NameIDFormat>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>

  </md:AttributeAuthorityDescriptor>

  <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">http://www.example.org/</md:OrganizationURL>
  </md:Organization>

</md:EntityDescriptor>
```