ADFSMetadataProfile

SAML Metadata Profile

- An ADFS-compliant role descriptor's `protocolSupportEnumeration` MUST include the value `http://schemas.xmlsoap.org/ws/2003/07/secext`
- An IdP MUST include a `<IDPSSODescriptor>` element and a `<SingleSignOnService>` element with a `Binding` value of `http://schemas.xmlsoap.org/ws/2003/07/secext`
- An SP MUST include a `<SPSSODescriptor>` element and an `<AssertionConsumerService>` element with a `Binding` value of `http://schemas.xmlsoap.org/ws/2003/07/secext`. A `<SingleLogoutService>` endpoint MAY be included (with the same `Binding` value).

Note that the ADFS protocol does not support a callback or query from the SP to the IdP, and therefore no `<KeyDescriptor>` is required in the `<SPSSODescriptor>` element.

ADFS Configuration and Metadata

In the ADFS Trust Policy, the General tab includes Federation Service URI and endpoint URL values that define the ADFS site. These map to the `entityI` and endpoint `Location` in the `<SingleSignOnService>` and `<AssertionConsumerService>` elements respectively.

A typical ADFS deployment supports both IdP and SP functionality because the ADFS service is a gateway that handles both roles at the same time. The same endpoint URL is therefore able to both handle requests for SAML tokens and process incoming SAML tokens.

Example Metadata

An example representing a typical ADFS site configuration follows:

```
<EntityDescriptor entityID="https://foo.example.org/adfs">
  <IDPSSODescriptor protocolSupportEnumeration="http://schemas.xmlsoap.org/ws/2003/07/secext">
    <KeyDescriptor use="signing">
      <ds:KeyInfo>
        <ds:X509Data>
          <ds:X509Certificate>...base64 signing key...</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </KeyDescriptor>
    <SingleSignOnService Binding="http://schemas.xmlsoap.org/ws/2003/07/secext"
        Location="https://foo.example.org/adfs/ls/clientlogon.aspx"/>
  </IDPSSODescriptor>
  <SPSSODescriptor protocolSupportEnumeration="http://schemas.xmlsoap.org/ws/2003/07/secext">
    <AssertionConsumerService Binding="http://schemas.xmlsoap.org/ws/2003/07/secext"
        Location="https://foo.example.org/adfs/ls/clientlogon.aspx"/>
  </SPSSODescriptor>
</EntityDescriptor>
```