

EndpointReference

Overview

The [WS-Addressing specification](#) and its [SOAP binding](#) provide a way to represent information about a web service endpoint in XML using the <wsa:EndpointReference> element.

Section 2.3 of the [ID-WSF Discovery Service Specification](#) defines a profile of this mechanism that carries additional information relevant to securing web services, without the complexity of the WS-SecurityPolicy standard.

The data specific to ID-WSF is encapsulated in the <wsa:Metadata> extension point, and includes identifiers that describe the type of service offered, the SAML entityID of the service, and one or more <disco:SecurityContext> elements that identify the "security mechanism" and associated token(s) to use with the service. In this way, the consumer of a service can choose to implement particular mechanisms and can dynamically select the right ones at runtime when contacting different services.

The full range of predefined mechanisms is found in the [ID-WSF Security Mechanisms Core Specification](#) and can be extended as needed.

Relevance to Solution

For the purposes of our use case, we will pass Endpoint References conforming to this profile in a SAML attribute in which the Name of the attribute corresponds to the value found in the EPR's <disco:ServiceType> element. These EPRs will typically be used to identify the endpoint at which the Identity Provider's ID-WSF Single Sign-On Service lives, and how it is secured.

Endpoint Reference Example

A typical EPR might look like this:

```
<wsa:EndpointReference xmlns:wsa="http://www.w3.org/2005/08/addressing">
  <wsa:Address>https://idp.example.org/idp/profiles/WSF/SSO</wsa:Address>
  <wsa:Metadata xmlns:disco="urn:liberty:disco:2006-08">
    <disco:Abstract>ID-WSF Single Sign-On Service</disco:Abstract>
    <disco:ServiceType>urn:liberty:ssos:2006-08</disco:ServiceType>
    <disco:ProviderID>http://idp.example.org/idp/shibboleth</disco:ProviderID>
    <sbef:Framework xmlns:sbef="urn:liberty:sb" version="2.0"/>
    <disco:SecurityContext>
      <disco:SecurityMechID>urn:liberty:security:2005-02:ClientTLS:peerSAMLV2</disco:SecurityMechID>
      <sec:Token xmlns:sec="urn:liberty:security:2006-08" ref="#ID" usage="urn:liberty:security:tokenusage:2006-08:SecurityToken"/>
    </disco:SecurityContext>
  </wsa:Metadata>
</wsa:EndpointReference>
```