Endpoints in Metadata

The term *endpoint* refers to a URL location in entity metadata that is explicitly declared to support a particular SAML protocol, binding, and/or profile. At runtime, a relying party routinely checks endpoints in metadata to minimize the possibility of spoofing or phishing. Thus the accuracy of endpoint URLs in metadata is crucial, contributing to the overall security of the SAML exchange.

This page and its child pages provide guidance to deployers of SAML software in the InCommon Federation:

- Endpoints in IdP Metadata
- Endpoints in SP Metadata

In general, the recommendations found on these pages (and their child pages) will maximize interoperability among Federation participants. In practice, a deployer supports those bindings and protocols that meet the particular needs of their federation partners. It's important, however, that deployers include endpoints in metadata that accurately reflect the deployment's software configuration, otherwise runtime errors will occur.

Message Flows

Usually an SP issues a SAML V2.0 authentication request using the HTTP-Redirect binding. The IdP typically returns the response using SAML V2.0 HTTP-POST. Since message-level encryption was introduced in Version 2.0 of SAML Web Browser SSO, the IdP usually includes attributes and encrypts the assertion in the POSTed response. Thus the SP need not query for attributes in the usual SAML V2.0 flow.

Other exchanges are possible of course. One alternative is for the IdP to return a so-called *artifact* to the SP in lieu of the actual assertion. The SP then turns around and issues an artifact resolution request to the IdP via SOAP. Not all implementations support artifact resolution, so check your documentation for details.

In a perfect world, all deployments would support browser-facing SAML V2.0 Web Browser SSO, in which case SOAP-based attribute query and artifact resolution become mostly unnecessary. This would dramatically simplify the deployment of SAML in the Federation.

General Requirements

All new metadata registered by InCommon, both IdP and SP metadata, MUST support SAML V2.0 Web Browser SSO. Specific requirements, recommendations, and guidelines are enumerated on the child pages to this wiki topic.

Resources

- https://wiki.shibboleth.net/confluence/display/CONCEPT/FlowsAndConfig