IdP Endpoints

Endpoints in IdP Metadata

This topic outlines requirements and recommendations regarding endpoints in IdP metadata registered by InCommon. Endpoints in Metadata are crucial to the overall security and interoperability of SAML protocol exchanges.

An *endpoint in metadata* signals support for a specific profile of SAML. In particular, all IdPs in InCommon metadata MUST support *SAML2 Web Browser SSO* by including certain browser-facing SSO endpoints in metadata. Support for any other profile is strictly OPTIONAL.

✓ **Keep it simple!**

InCommon recommends that site administrators *publish IdP metadata with as few endpoints as possible*. It is sufficient for IdP metadata to *advertise support for SAML2 Web Browser SSO on the front channel only*. Advertised support for other protocols, especially back-channel protocols, should be avoided in published metadata unless you have a specific need.

Endpoint Requirements

The requirements and recommendations outlined in this section apply to both new and existing IdP metadata.

IdP metadata MUST include a `SingleSignOnService` endpoint that supports the SAML2 `HTTP-Redirect` binding. A `SingleSignOnService` endpoint that supports the SAML2 `HTTP-POST` binding SHOULD also be included in IdP metadata since some SAML SP deployments favor that particular binding. Support for both bindings is strongly RECOMMENDED.

⚠ **Browser-facing SSO endpoints**

All IdP metadata MUST satisfy the following requirements:

- A `SingleSignOnService` endpoint that supports the SAML2 `HTTP-Redirect` binding is REQUIRED
- A `SingleSignOnService` endpoint that supports the SAML2 `HTTP-POST` binding is RECOMMENDED

All IdP owners are strongly encouraged to include both of the above endpoints in metadata.

ⓘ **Single logout endpoints**

A single topic covering Single Logout Endpoints in both IdP and SP metadata is found elsewhere in this wiki.

❗ **Avoid SAML2 attribute query endpoints**

A SAML2 `AttributeService` endpoint is not required in IdP metadata in order to support Browser SSO. Such an endpoint is generally only needed if you operate a standalone attribute authority in support of research platforms or specialized applications making use of attributes from multiple organizations at the same time. If you don't know if this applies to you, it probably doesn't. If you have a SAML2 `AttributeService` endpoint in metadata, you SHOULD remove it.

Recommendations for New IdPs

Like all IdPs, a new IdP MUST support SAML2 Web Browser SSO as outlined in the previous section. To simplify setup and testing, endpoints that advertise support for other SAML profiles SHOULD NOT be advertised in **new** IdP metadata. IdP owners are advised to incrementally add new capabilities as their deployment matures.

⚠ **Endpoints in new IdP metadata**

It is strongly RECOMMENDED that **new** IdP metadata contain two (and only two) endpoints:

- A `SingleSignOnService` endpoint that supports the SAML2 `HTTP-Redirect` binding
- A `SingleSignOnService` endpoint that supports the SAML2 `HTTP-POST` binding

These browser-facing SSO endpoints are relatively easy to set up, test, and maintain.

The following endpoints are especially NOT RECOMMENDED in **new** IdP metadata:

- SAML1 endpoints of any kind
- SAML2 `SingleLogoutService` endpoints
- Any endpoint that supports a SOAP binding, including:
  - Any `ArtifactResolutionService` endpoint
  - Any `AttributeService` endpoint

Your IdP software may support some or all of the above (which may turn out to be useful) but publishing those endpoints in metadata involves a commitment that should be delayed until your IdP deployment has sufficiently matured. If you actually need to publish one of those endpoints at a later time (`SingleLogoutService` being a likely case), you can always add it to your metadata as the need arises.

Technical Details

All IdPs SHOULD include both of the following endpoints in metadata. It is strongly RECOMMENDED that new IdP metadata contain only these two endpoints, at least initially.

SAML endpoints in IdP metadata

```
<!-- SAML V2.0 browser-facing SSO endpoints -->
<md:SingleSignOnService xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
    Location="https://idp.example.org/idp/profile/SAML2/Redirect/SSO"/>
<md:SingleSignOnService xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
    Location="https://idp.example.org/idp/profile/SAML2/POST/SSO"/>
```

Note that the browser-facing `<md:SingleSignOnService>` endpoints should run on the default SSL/TLS port (443).

Other Issues

- IdP Endpoints for SAML1
- SLO Endpoints