SP Endpoints for SAML1

This document contains **DRAFT** material intended for discussion and comment by the InCommon participant community. Comments and questions should be sent to the InCommon participants mailing list.

SAML1 Endpoints in SP Metadata

This page gives guidance and recommendations regarding legacy SAML1 endpoints in SP metadata.

New SPs SHOULD avoid advertising SAML1 endpoints in metadata.

Every SP that supports SAML V1.1 Web Browser SSO MUST include an `<md:AssertionConsumerService>` endpoint that supports the Browser /POST profile. The Browser/Artifact profile MAY be supported as well.

Technical Details

Support for *SAML V1.1 Web Browser SSO* is OPTIONAL:

- SPs MUST include an SSL/TLS-protected `<md:AssertionConsumerService>` endpoint that supports the SAML V1.1 Browser/POST profile.
- SPs MAY include an SSL/TLS-protected `<md:AssertionConsumerService>` endpoint that supports the SAML V1.1 Browser/Artifact profile.

SAML1 Endpoints in SP Metadata

```
<!-- SAML V1.1 -->
<md:AssertionConsumerService index="1"
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    Binding="urn:oasis:names:tc:SAML:1.0:profiles:browser-post"
    Location="https://sp.example.org/sso/SAML1/POST"/>

<md:AssertionConsumerService index="2"
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    Binding="urn:oasis:names:tc:SAML:1.0:profiles:artifact-01"
    Location="https://sp.example.org/sso/SAML1/Artifact"/>
```

Note that the browser-facing `<md:AssertionConsumerService>` endpoint runs on the default TLS port (443) as shown in the examples above.