

IdP 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 IdP Metadata

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



New IdPs **SHOULD** avoid advertising SAML1 endpoints in metadata.

Technical Details

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

- IdPs **MUST** include one and only one TLS-protected `<md:SingleSignOnService>` endpoint that supports the Shibboleth 1.x AuthnRequest protocol.
- IdPs **MAY** include an `<md:ArtifactResolutionService>` endpoint that supports the SAML V1.1 SOAP binding and therefore the SAML V1.1 Browser/Artifact profile. This endpoint **MUST** be protected by SSL/TLS unless message-based signing is used.
- IdPs **SHOULD** include an `<md:AttributeService>` endpoint that supports the SAML V1.1 SOAP binding. This endpoint **MUST** be protected by SSL/TLS unless message-based signing is used.
- IdPs **MUST** support the proprietary `urn:mace:shibboleth:1.0:nameIdentifier` transient name identifier format.

SAML1 Endpoints in IdP Metadata

```
<!-- SAML V1.1 -->
<md:SingleSignOnService
  xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
  Binding="urn:mace:shibboleth:1.0:profiles:AuthnRequest"
  Location="https://idp.example.org/idp/profile/Shibboleth/SSO"/>
<md:AttributeService
  xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
  Binding="urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding"
  Location="https://idp.example.org:8443/idp/profile/SAML1/SOAP/AttributeQuery"/>
<md:ArtifactResolutionService index="1"
  xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
  Binding="urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding"
  Location="https://idp.example.org:8443/idp/profile/SAML1/SOAP/ArtifactResolution"/>
```

Note that the browser-facing `<md:SingleSignOnService>` endpoint runs on the default TLS port (443) while the back-channel endpoints typically run on some non-standard port (such as 8443 in the examples above).