Shibboleth13Differences

Different between Shibboleth 1.3 and 2.0

General Questions

What makes Shibboleth 2.0 different from Shibboleth 1.3?

Shibboleth 2.0 is built primarily on SAML 2.0 and includes a large number of functionality improvements based on the community's substantial experience with Shibboleth 1.3. Most of the details of these changes are discussed in this FAQ. Shibboleth 2.0 is fully backward compatible with Shibboleth 1.3, both from 2.0 SP to 1.3 IdP and from 1.3 SP to 2.0 IdP.

How has the default Shibboleth profile changed?

Shibboleth 1.3 and earlier were primarily implementations of the Shibboleth profile, of SAML 1.1. This profile included some proprietary extensions, such as the authentication request profile. It also made use of a direct query to a separate portion of the IdP, called an Attribute Authority, to retrieve attributes.

The default profile used by Shibboleth 2.0 is a fully compliant implementation of the SAML 2.0 Web Browser SSO Profile. Attributes are now by default included in an encrypted SAML 2.0 assertion sent from the IdP to the SP. This does not reduce the privacy or security features of Shibboleth and should result in easier deployment.

How has metadata changed?

Shibboleth 1.3 and Shibboleth 2.0 both rely on the SAML 2.0 metadata standard. The same metadata file can be used by providers of both SAML versions. New SAML 2.0 functionality is located at different endpoints. However, to take advantage of the new encryption capabilities of Shibboleth 2.0, the providers need to have access to the public keys of their partners. This is much simpler to implement if the provider's key or certificate is placed directly into the metadata, and there are no other built-in mechanisms supplied for this purpose. Please see BuildAFederation for more information.

How has the use of attributes changed?

Shibboleth 1.x strongly encouraged the use of a URI to identify SAML attributes, and this continues to be the heavily preferred default for Shibboleth 2.0. However, Shibboleth 1.3 and earlier versions included eduPerson-based examples that rely on a specialized namespace delegated by the MACE-Dir working group. This has been superseded in most cases by the SAML 2.0 specification's LDAP/X.500 attribute profile, which names attributes using the `URN:OID` namespace. The default configuration files supplied with the software will be compatible with both legacy and OID-based names for maximum interoperability.

This decision has no bearing on the rules and administration of the `urn:mace` URN namespace or URL-based naming. All formally delegated namespaces remain valid, but please follow good practices when naming your own attributes.

Finally, a significantly simplified set of rules for attribute syntax in SAML 2.0 assertions have been adopted by the MACE-Dir working group to increase interoperability with other SAML implementations. The Shibboleth software includes a variety of improvements to maximize its ability to both produce and consume as many syntax variants as possible, and is much more extensible in this regard.

What will Shibboleth 2.0 interoperate with?

Shibboleth should interoperate with any compliant SAML 2.0, 1.1, or 1.0 implementation, within the constraints of each specification and the profiles it supports. SAML leaves many details, particularly in the area of security, to implementers. Products with good support for SAML 2.0 metadata will be simpler to integrate.

Shibboleth will also interoperate with Microsoft's ADFS product and other implementations of its proprietary WS-Federation profile.

Backward compatibility extends to the Shibboleth 1.3 software, and any other conformant implementations of the Shibboleth Protocols and Profiles specification. Significant compatibility with Shibboleth 1.2 should be expected but is not guaranteed.

Identity Provider Questions

How has the identity provider changed?

The Shibboleth IdP has been completely redesigned for version 2.0.

What changes do I need to make in my IdP's metadata?

The only change that you **must** make is a change to the URLs used by your identity provider. All of the profile endpoints in Shibboleth take the form `<scheme>://<host>:<port>/<servlet-context>/profile/<profile-path>`. In most cases you will use `https` as the scheme and `idp` as your servlet context path. The default locations for profile paths are listed below:

Path	Associated Profile

/Status	Provides status information about the IdP
/Metadata/SAML	Provides SAML metadata for the IdP
/Shibboleth/SSO	The Shibboleth 1.3 SSO profile
/SAML1/SOAP/AttributeQuery	SAML 1 attribute query using the SOAP binding
/SAML1/SOAP /ArtifactResolution	SAML 1 artifact query using the SOAP binding
/SAML2/POST/SSO	SAML 2 SSO profile using the HTTP-POST binding
/SAML2/POST-SimpleSign/SSO	SAML 2 SSO profile using the HTTP-POST-Simplesign binding
/SAML2/Redirect/SSO	SAML 2 SSO profile using the HTTP-Redirect binding
/SAML2/SOAP/AttributeQuery	SAML 2 attribute query using the SOAP binding
/SAML2/SOAP /ArtifactResolution	SAML 2 artifact resolution query using the SOAP binding

Other changes may be necessary in order to enable particular functionality. For example, if you wish to support SAML 2 you need to list SAML 2 in the your supported protocols and add SAML 2 endpoints to the IdPSSO and AttributeAuthority roles.

The IdPUpgrades topic has more information about upgrading from 1.3 to 2.x.

Service Provider Questions

How has the SP changed?

The Shibboleth Native SP is structurally similar to the first generation software but incorporates many internal changes to reduce software conflicts, improve portability and manageability, and provide more options for application integration. Most of the software's configuration files have been redesigned, but without altering the overall deployment model.