# Technical Specifications

## Technical Specifications

The following are technical specifications that are supported/implemented in part or in full by various Shibboleth products.

You can find a highly unofficial statement here about FIPS compliance.

### Technical Standards

The formal specifications that define how Shibboleth works span a number of documents. Shibboleth is primarily built on the Security Assertion Markup Language (SAML) standard as defined by the OASIS SSTC. Shibboleth also has formal profile and conformance documents that define additional constraints on top of the base standard.

| Document | Description |
|---|---|
| SAML V1.1 | Specification for SAML V1.1, an OASIS Standard. Describes SAML V1.1 assertions, protocols, bindings, and profiles. |
| SAML V1.x Metadata Profile | Specification for *Metadata Profile for the OASIS Security Assertion Markup Language (SAML) V1.x*, an OASIS Standard. Describes a SAML V2.0 metadata profile for describing SAML V1.x entities. |
| SAML V2.0 | Specification for SAML V2.0, an OASIS Standard. Describes SAML V2.0 assertions, protocols, bindings, profiles, metadata, and authentication context. |
| SAML V2.0 Metadata Interoperability Profile | Specification for *SAML V2.0 Metadata Interoperability Profile*, a profile for using metadata that is self-contained and scalable. |
| Identity Provider Discovery Service Protocol and Profile | Specification for *Identity Provider Discovery Service Protocol and Profile*, an OASIS Committee Spec. Describes a protocol and profile for identity provider discovery. |
| SAML Metadata Extension | Specification for *Metadata Extension for SAML V2.0 and V1.x Query Requesters*, an OASIS Standard. Describes a SAML metadata extension for standalone query requesters. |
| SAML V2.0 Condition for Delegation Restriction Version 1.0 | This document defines a <saml:Condition> type for expressing a chain of intermediaries acting on behalf of the subject of an assertion, requring relying parties to distinguish between direct and indirect access. |
| SAML V2.0 Metadata Extension for Entity Attributes Version 1.0 | This profile defines an extension element for use in attaching SAML attributes to an <md:EntityDescriptor> or <md: EntitiesDescriptor> element, to communicate an arbitrary set of additional information about an entity in its metadata. |
| SAML V2.0 Metadata Interoperability Profile Version 1.0 | This profile describes a set of rules for SAML metadata producers and consumers to follow such that federated relationships can be interoperably provisioned, and controlled at runtime in a secure, understandable, and self-contained fashion. |
| SAMLv2.0 HTTP POST “SimpleSign” Binding | This specification defines a SAML HTTP protocol binding, specifically using the HTTP POST method, and not using XML Digital Signature for SAML message data origination authentication. Rather, a “sign the BLOB” technique is employed wherein a conveyed SAML message is treated as a simple octet string if it is signed. Conveyed SAML assertions may be individually signed using XMLdsig. Security is optional in this binding. This specification is an addition to the bindings described in the SAML V2.0 Bindings specification. |
| SAML v2.0 Metadata Profile for Algorithm Support Version 1.0 | SAML Metadata extension that allow an entity to describe which signature and encryption algorithms are supported |
| SAML V2.0 Metadata Extensions for Login and Discovery User Interface Version 1.0 | This document defines a set of extensions to SAML metadata that provide information necessary for user agents to present effective user interfaces and, in the case of identity provider discovery, recommend appropriate choices to the user. |

| | |
|---|---|
| Shibboleth Protocol Specification | Describes Shibboleth-specific extensions to SAML V1.x. The primary extension specifies an SP-first authentication request. |
| Shibboleth Conformance Specification | Describes conformance standards for the Shibboleth Protocol Specification |

## Deployment Profiles, Best Practices, Etc:

In addition to these standards, note that within specific communities of use, additional profiles may be defined to further constrain options, define attributes, etc. People are welcome to maintain pointers to those here.

| Document | Summary |
|---|---|
| I2MI SAML Attribute Profiles | The Internet2 Middleware Initiative has published profiles for the use of SAML attributes (both SAML V1.x and SAML V2.0). These are best practices and naming standards used by at least InCommon and some other federations. Some of the practices described are implemented directly by Shibboleth 1.x, often in ways that don't permit other approaches. |
| Interoperable SAML 2.0 Web Browser SSO Deployment Profile | A simple, constrained deployment profile of SAML 2 developed for use in several higher-education federations. |

## Historical Documents

Additional documents of historical relevance to the project and our community.

| Document | Summary |
|---|---|
| Shibboleth Architecture document | The last draft located of the original Shibboleth Architecture document that was created prior to constructing the original software. The software today looks much different than it did in the heads of the people who imagined it, but there are also a lot of ideas that survive after all this time. |