Software Guidelines

Community Review in progress!

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 (participants@incommon.org).

This document provides guidance for choosing an appropriate SAML software implementation for use in the InCommon Federation.

SAML V2.0 Implementation Profile

Conformance to the SAML V2.0 Implementation Profile for Federation Interoperability is strongly encouraged!

There are numerous commercial and open-source implementations of the SAML Web Browser SSO Profiles. In what follows, we apply two basic requirements that filter the set of implementations down to a small, manageable subset. There are other requirements that could be applied; the two chosen here are deemed most beneficial to InCommon Federation participants.

Contents

Software Recommendations

InCommon recommends the following SAML software implementations:

Recommended SAML Software

1. Shibboleth
2. simpleSAMLphp

A few details about each of the recommended software implementations are given in the following subsections. Consult the corresponding product documentation to determine currently supported versions and platforms.

Shibboleth

The Shibboleth Consortium offers a number of federation software products, including a SAML IdP and a SAML SP (they are distinct products). Both are free and open source.

- Home: http://shibboleth.net/
- Docs: https://wiki.shibboleth.net/
- Mailing lists: http://shibboleth.net/community/lists.html

Shibboleth has strong metadata management capabilities for multilateral federation. See the wiki for detailed instructions for configuring Shibboleth for metadata refresh.

simpleSAMLphp

UNINETT leads the open-source simpleSAMLphp project, which offers both a SAML IdP and SAML SP (written in PHP).

- Home: http://simplesamlphp.org/
- Docs: http://simplesamlphp.org/docs/stable/
- Mailing lists: http://simplesamlphp.org/lists

The simpleSAMLphp software distribution includes a separate module for automated metadata management. Although not as tightly integrated as the Shibboleth metadata client, the simpleSAMLphp metarefresh module will consume the entire InCommon metadata aggregate (and even larger aggregates). Instructions how to configure simpleSAMLphp for metadata refresh are provided elsewhere in this wiki.

Choose your software carefully!

InCommon does not *require* participants to use any particular SAML software implementation. Regardless of your software choice, you have the same rights and responsibilities as any other participant in the InCommon Federation but make sure you understand the consequences of Using Other Software for federation purposes.

Using Microsoft AD FS

Although Microsoft AD FS is not recommended for general use in the InCommon Federation, *AD FS 2.0 can be successfully deployed as an Identity Provider* in certain limited situations. Visit the Using Other Software child page for more information about using AD FS.

Software Requirements

Terminology. A *metadata consumer* is a specific SAML software implementation plus a metadata client. The latter may be distributed with the SAML implementation itself or by a third party.

Two necessary conditions for a metadata consumer to be recommended for use in the InCommon Federation are:

1. The metadata consumer must correctly consume InCommon metadata.
2. The metadata consumer must conform to the OASIS SAML V2.0 Metadata Interoperability Profile.

Basic Metadata Consumption

A metadata consumer satisfies the first requirement if it can refresh and verify metadata as outlined on the Metadata Consumption wiki page. To our knowledge, there are only three such metadata consumers:

1. Shibboleth
2. simpleSAMLphp
3. Microsoft AD FS 2.0 + pysFEMMA

Since Metadata Consumption is a critical function of any SAML deployment, the above list intentionally aligns with the list of recommended Metadata Client Software documented elsewhere in this wiki.

Metadata Interoperability

The SAML V2.0 Metadata Interoperability Profile specifies requirements for both metadata producers and metadata consumers. As consumers, *Shibboleth and simpleSAMLphp conform to the Metadata Interoperability Profile* but the AD FS 2.0 metadata consumer does not since it processes certificates in metadata in ways that are specifically excluded by the Profile:

- AD FS 2.0 will not consume an `<md:EntityDescriptor>` element that contains an expired certificate.
- AD FS 2.0 will actually try to check any CRLs or OCSP endpoints that might be contained in the certificate.

Since AD FS 2.0 does not conform to the Metadata Interoperability Profile, and because it has other interoperability issues that limit its use as fully functioning SAML software, it is not recommended for general use in the InCommon Federation.

Legacy Use of SAML V1.1

The Federation supports metadata that enables interoperability with both the modern SAML V2.0 standard and the earlier/legacy SAML V1.1 standard. While most participants will primarily use SAML V2.0, the use of SAML V1.1 remains possible, and is required by some participants for legacy reasons.

Participants are strongly encouraged to choose software that supports at least SAML V2.0 to ensure the greatest degree of interoperability. Note that the use of metadata with SAML V1.1 is generally not supported by any software other than the two recommended above.

Refer to the SAML wiki page for additional information.