Using Other Software

> **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).

The Use of Other SAML Software

For a complete list of software recommended for use in the InCommon Federation, see the parent Software Guidelines wiki page. Here we discuss the use of other SAML software implementations, in particular, Microsoft AD FS 2.0.

Contents

General Considerations

If you choose not to use one of the recommended SAML software implementations, be advised that you may incur additional deployment costs and/or experience operational challenges. In extreme cases, you may cause interoperability issues with your federation partners. While the use of recommended software is not guaranteed to eliminate all problems, experience has shown that the likelihood of issues is greatly increased if you don't.

The impact of your software choices depends to a certain extent on your role(s) in the Federation. For an Identity Provider, the primary responsibility is to authenticate users and issue accurate assertions about them. In most cases, deficiencies in software products will not negatively impact your ability to do so, but occasional disruptions in service are likely, especially if your deployment lacks appropriate metadata support, in which case your ability to handle operational changes made by Service Providers will be limited and manual.

A Service Provider on the other hand is principally concerned with securing its systems and maintaining a sufficient degree of protection of its resources. In addition to the reliability issues noted above, a lack of metadata support can in some cases limit an SP's ability to deal with a compromised signing key of an IdP partner. The use of metadata in the Federation is tightly orchestrated to address various risks that aren't adequately addressed by manually configuring metadata in the fashion that many products do.

> **The interoperability and security implications of metadata refresh!**
>
> It is **strongly recommended** that InCommon SPs and IdPs **refresh and verify metadata** at least daily. Regular metadata refresh promotes interoperability, protects users against spoofing and phishing, and is a necessary precaution in the event of key compromise. Failure to refresh metadata exposes Federation users to unnecessary risk.

Visit the Metadata Consumption wiki page for more information about metadata refresh.

Certificates in Metadata

In general, SAML implementations have varying degrees of support for X.509 certificates in metadata, which leads to known and well understood interoper ability issues. These software limitations need to be factored into the software decision-making process.

In particular, to fully support key rollover, implementations MUST support the following features:

1. An implementation MUST be able to consume and utilize two signing keys bound to a single role descriptor. There are two cases that MUST be supported:
   a. `<md:KeyDescriptor use="signing">` and `<md:KeyDescriptor use="signing">` in a single role descriptor
   b. `<md:KeyDescriptor use="signing">` and `<md:KeyDescriptor>` in a single role descriptor
2. If an implementation supports inbound encryption, it MUST be configurable with up to two decryption keys.
3. An implementation MAY support (i.e., consume and utilize) multiple encryption keys per role descriptor in metadata. In particular, the implementation MAY support two `<md:KeyDescriptor>` elements (with no `use` XML attribute) in a single role descriptor, but this is not strictly required since it can usually be avoided in practice.

Consult your software documentation to better understand its capabilities. Indeed, evaluate software capabilities with respect to certificate handling *before* you deploy, if at all possible.

Microsoft AD FS

Although Microsoft AD FS is not recommended for general use in the InCommon Federation, it is specifically called out here for two reasons:

1. Due to its relationship with Active Directory, it is likely AD FS will find significant usage regardless of recommendations
2. It turns out that AD FS 2.0 *can* be successfully used in some limited circumstances, so the goal here is to outline at least one such use case

By far the dominant deployment scenario in the InCommon Federation involves an IdP-only campus interoperating with one or more SP-only Sponsored Partners. In this and similar situations, **AD FS 2.0 can be successfully deployed as an Identity Provider** if all of the following are true:

- *Use pysFEMMA to refresh and verify metadata* (since AD FS 2.0 will not consume SAML metadata whose root element is an `<md:EntitiesDescriptor>` element)
- *Ensure that all SP partners support and use SAML V2.0* (since AD FS 2.0 does not support SAML V1.1)
- *Ensure that all SP partners follow InCommon recommendations regarding certificates in metadata*. Specifically:
    - *certificates should be self-signed* (since AD FS 2.0 will actually try to check any CRLs or OCSP endpoints contained in the certificate)
    - *certificates should not be expired* (since AD FS 2.0 will not consume an `<md:EntityDescriptor>` element that contains an expired certificate)
    - *certificates should not be shared* (some versions of AD FS 2.0 will not consume two `<md:EntityDescriptor>` elements that contain the same certificate)
    - *redundant certificates should be avoided* (since AD FS 2.0 will not consume an `<md:EntityDescriptor>` element containing more than one encryption key)
- *Ensure that no SP partners include a `<samlp:Scoping>` element in the `AuthnRequest`* (since AD FS 2.0 will reject such a request)

Recognizing the limitations of AD FS, the international REFEDs community is calling upon Microsoft to address this situation. Visit the adfstoolkit.org web site to add your voice to this effort.

Another good source of relevant information is the Microsoft Interoperability page in the Shib wiki.