Metadata Migration Process

Deprecated

Note that this page has been deprecated. The information it contains is no longer current.

Metadata Migration Process

This document describes how to safely migrate to one of the new metadata aggregates in timely fashion.

On June 30, 2014, the fallback metadata aggregate will be synced with the production metadata aggregate; that is, after June 30, *all metadata aggregates published by the InCommon Federation will be signed using the SHA-256 digest algorithm*.

To avoid a potential problem with your metadata consumption process, here's what you need to do prior to June 30, 2014:

1. Migrate to a metadata aggregate that is signed using the SHA-256 digest algorithm
2. Obtain an authentic copy of the metadata signing certificate
3. Reconfigure your metadata client software

Choose a Metadata Aggregate

No later than June 30, 2014, *migrate to either the production aggregate or the preview aggregate*. The two aggregates are identical. If your SAML deployment is a production deployment, migrate to the production aggregate; otherwise migrate to the preview aggregate.

To determine whether or not your deployment supports the SHA-256 digest algorithm, apply the Metadata Migration Algorithm to your deployment. Better yet, point your configuration at the production metadata aggregate and see if it works.

For more information: Metadata Aggregates

Bootstrap your Trusted Metadata Process

Before migrating to a new metadata aggregate, *bootstrap your trusted metadata process with an authentic copy of the new metadata signing certificate*. The new metadata aggregates are signed with the same trusted signing key that we've always used but the corresponding signing certificate is different.

Obtain an authentic copy of the metadata signing certificate

The key pair used to sign and verify metadata have **not** changed but *the certificate wrapper on the public key has changed*. To avoid confusion, download and install a fresh copy of the metadata signing certificate.

For more information: Metadata Signing Certificate

Reconfigure your Metadata Client Software

The final step is to *reconfigure your metadata client software*. There are three metadata clients that meet the basic requirements of a SAML deployment in the InCommon Federation:

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

We provide detailed documentation for Shibboleth and simpleSAMLphp, but to our knowledge, no one is using pysFEMMA in conjunction with Microsoft AD FS. If you are, please describe your experiences to the help@incommon.org support address. For more information: Metadata Client Software