Shibboleth - Administering the Campus Federation

Stephanie Obodda - 2020-12-02 - 0 Comments - in Shibboleth Single Sign On

1. What is Involved, and Why It Is Important

1.1 Metadata

At run time, the various Shibboleth components exchange messages over SSL/TLS tunnels; sometimes, they sign and encrypt XML documents. The components are doing this in a way that is transparent to the browser users; browser users doNOT have to know aything about PKI, certificate, etc. However, the Shibboleth site admin does have to know something about this.

Each Shibboleth component has a public and private key. One major difference, tho, from a conventional PKI environment is that the Shibboleth metadata provides the trust. In a conventional PKI environment, the chain of CAs that has signed a cetificate provide the trust. The Shibboleth metadata for a Federation typically contains self-signed certificates; path validation of a certificate provides no additional value above and beyond the trust obtained from the metadata. Having access to the metadata does not simplify the process of breaking the trust or impersonating an entity; consequently, the metadata is always available for download by anyone.

It is the responsibility of the local Shibboleth site admin to maintain the metadata (including removing/correcting entries whose keys have been compromised), to digitally sign the metadata, and to make it available for download.

1.2 Attribute Definitions, and Attribute Release Policies

These XML files are used to tell the IdP 1) which attributes are available and where they are sourced from (LDAP, SQL, static, produced by a scirpt run within the IdP, etc), and 2) define the policies controlling which attributes and values are released to which SP, or groups of SPs. The local policy is defined here.

2. Overview of the Metadata Process

1. The metadata is stored on the IdP machines, and the signed version is published from those machines.
2. The file brown-unsigned-metadata.xml contains the version of record of the

metadata for the "campus federation".

3. Entries in this XML file are added, deleted, and edited per requests from user sites. The file is divided into two EntityGroups -- one for a few off-campus sites that are useful, and the other contains the on-campus sites. Several of the ARPs rely on the EntityGroup name for the on-campus SPs.
4. A script (publish-meta.sh) signs this file, and copies it to the file system locations from which it is published. Signing is done with the samlsign utility (from the Shibboleth SP package).
5. UNC is about to release a GUI java servlet to aid in managing Federation metadata.

3. Overview of the Attribute Management Process

1. attribute-resolver.xml defines the locally available attributes; attribute-filter.xml defines the policies controlling release. Documentation on both is available here.

Tags

Service Center