Recommended Practices
for the
InCommon Federation

Tom Scavo
@trscavo

Outline

1. Preparing to publish your metadata
2. Publishing an EntityDescriptor in metadata
3. Characteristics of an EntityDescriptor in metadata

In a sense, you become a member of the InCommon Federation when you publish an EntityDescriptor in metadata (2). However, you will discover that most of the work is preparation for this big event (1).

Pre-preparation

IdP or SP?

Terminology:
Identity Provider (IdP)
Service Provider (SP)

Are you an IdP or SP (or both)?

- IdP: Audit your identity management system
- SP: Domesticate your application
  - Consider deploying an IdP

SAML Software

Terminology:
Security Assertion Markup Language (SAML)

Choosing a SAML software implementation

- Support SAML V2.0 Web Browser SSO
- Fully supports SAML metadata

Recommendations:

- Shibboleth
- SimpleSAMLphp

Software Deployment

Deploying and testing the software

- IdP: deploy both an IdP and an SP
- SP: deploy both an IdP and an SP (or leverage public IdP)
  - ProtectNetwork.org
  - TestShib.org

https://spaces.internet2.edu/x/36eKAQ

Identity Provider Discovery

Two options:

1. Centralized Discovery Service
2. Embedded Discovery Service (in SP)

https://spaces.internet2.edu/x/FgEFAQ

Federated Error Handling

Federated Error Handling is a centralized service for SPs.

IdPs: Include an errorURL in metadata

https://spaces.internet2.edu/x/kJOVAQ

Publishing Metadata

Preparing your Metadata

You'll need the following information:

- entityID
- certificates
- endpoints
- contacts
- UI elements
- requested attributes

https://spaces.internet2.edu/x/5YKKAQ

Accessing the Federation Manager

Up to two site administrators per organization.

InCommon Operations will issue you login credentials. (We are in the process of deploying mobile-based, two-factor authentication technology.)

https://spaces.internet2.edu/x/hofNAQ

Creating the EntityDescriptor

Metadata is stored as SAML metadata in an `<md:EntityDescriptor>` element.

But you don't need to know XML. Metadata is entered via HTML forms.

Maintaining the EntityDescriptor

Things change. For example:

Keys in metadata expire or otherwise need to migrate in/out of metadata (key rollover).

https://spaces.internet2.edu/x/vAEFAQ

Configuring Metadata Refresh

Automatically refresh metadata at least daily.

(An optimal configuration will attempt to refresh metadata every hour.)

https://spaces.internet2.edu/x/JwQjAQ

Metadata Characteristics

Entity ID

The `entityID` is immutable.

https://spaces.internet2.edu/x/eAUjAQ

Certificates in Metadata

Long-lived, self-signed certificates with 2048-bit keys are recommended.

https://spaces.internet2.edu/x/boY0

Endpoints in Metadata

Support for SAML V2.0 Web Browser SSO is required:

- IdPs support HTTP-Redirect binding
- SPs support HTTP-POST binding

https://spaces.internet2.edu/x/IImKAQ

Contacts in Metadata

Technical contact and administrative contact in metadata are required.

https://spaces.internet2.edu/x/BomKAQ

User Interface Elements in Metadata

Every entity needs a human-readable name. A logo is recommended.

https://spaces.internet2.edu/x/2YGKAQ

Requested Attributes in SP Metadata

SPs list attributes in metadata.

https://spaces.internet2.edu/x/8YGKAQ