InCommon Federation Metadata Registration Practice Statement

Publication Date: August 9, 2019

Repository ID TI.136.1
Author InCommon Federation
Sponsor Ann West, Associate Vice President, Trust and Identity, Internet2
Version 2.0

Superseded documents:
https://spaces.at.internet2.edu/display/InCFederation/Metadata+Registration+Practice+Statement

Content

1. Definitions and Terminology **3**

2. Introduction and Applicability **3**

3. Participant Eligibility and Ownership **4**

4. Registration Representatives **4**

4.1 Registration Authority 4

4.2 InCommon Executive (Executive) 4

4.3 Site Administrator 5

4.4 Delegated Administrator 5

5. Metadata Format **5**

6. Entity Eligibility and Validation **6**

6.1 Entity Registration 6

6.2 EntityID Format 7

6.3 Scope Format 7

6.4 Entity Validation 7

7. Entity Management **7**

7.1 Entity Change Requests 7

7.2 Entity Augmentation made by Federation Operator 8

7.3 Unsolicited Entity Changes 8

7.4 Metadata Aggregate Production 8

7.5 Metadata Signing and Publication 9

8. References **10**

9. Attribution **11**

1. Definitions and Terminology

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

The following definitions are used in this document:

Federation - Identity Federation. An association of organizations that come together to securely exchange information as appropriate about their users and resources to enable collaborations and transactions. Unless otherwise noted, “Federation” is synonymous with the InCommon Federation within this document.

Federation Participant (Participant) - An organization that has joined the Federation by agreeing to be bound by the Participant Agreement in writing.

Federation Operator - Organisation providing the infrastructure for Authentication and Authorization to Participants.

Participant Agreement - A document describing the obligations, rights, and expectations of the Participant and the Federation Operator. [InCommon-PA]

Entity - A discrete component that a Participant wishes to register and describe in the metadata. This is typically an Identity Provider or Service Provider.

Registry - System used by the Federation Operator to register entity metadata. This may be via a self-service tool or via other manual processes.

Registered Representatives - Individuals authorized to act on behalf of the Participant. These may take on different roles with different rights attached to them.

2. Introduction and Applicability

This document describes the metadata registration practices of the Federation Operator with effect from the publication date shown at the start of this document. All new entity registrations performed on or after that date SHALL be processed as described here until the document is superseded.

This document SHALL be published on the Federation website at https://www.incommon.org/federation/mrps. Updates to the documentation SHALL be accurately reflected in entity metadata.

An entity that does not include a reference to a registration policy MUST be assumed to have been registered under a historic, undocumented registration practice regime. Requests to re-evaluate a given entity against a current MRPS MAY be made to the Federation helpdesk.

3. Participant Eligibility and Ownership

Participants of the Federation are eligible to make use of the Federation Operator's Registry to register entities. Registration requests from other sources SHALL NOT be accepted.

The procedure for becoming a Participant of the Federation is published on the InCommon website. See [Join-InCommon].

The participation procedure verifies that the prospective Participant has legal capacity, and requires that all Participants enter into a contractual relationship with the Federation Operator by agreeing to the Participant Agreement. The Federation Operator makes checks based on the legal name provided.

The membership process also identifies and verifies Registered Representatives, who are permitted to act on behalf of the organization in dealings with the Federation Operator. The Federation Operator requires formal written notice from a Participant to designate its InCommon Executive. The identity of the InCommon Executive is verified via live, real-time conversation. The designated InCommon Executive, in turn, designates Site Administrators.

The process also establishes a canonical name for the Federation Participant. The canonical name of a member MAY change during the membership period, for example as a result of corporate name changes or mergers. The Participant organization's canonical name is disclosed in the entity's SAML v2.0 `<md:OrganizationName>` element [SAML-Metadata-OS].

4. Registration Representatives

4.1 Registration Authority

The InCommon Registration Authority consists of InCommon staff who are authorized to review, accept for publication or reject, submissions of participant metadata.

4.2 InCommon Executive (Executive)

The InCommon Executive represents the Participant in all decisions and delegations of authority for the responsibilities of Participants. Among other duties, the Executive designates the Participant's Site Administrators.

The Federation Operator maintains a confidential record of the Executive. Data includes the Executive's name and email address.

For additional information, see the InCommon website. [InCommon-Roles].

4.3 Site Administrator

A Site Administrator (SA) is a Participant's primary responsible party for registering and maintaining the organization's policies and technical data related to the Participant's participation in the InCommon Federation. SA responsibilities include submitting and updating Participant's federation metadata in the Federation Registry. Site Administrators are assigned by the Participant's InCommon Executive. Each Participant can designate up to two Site Administrators.

The Federation Operator maintains a confidential record of Site Administrators. Data includes the Site Administrator's name and email address.

For additional information, see the InCommon website. [InCommon-Roles].

4.4 Delegated Administrator

A Delegated Administrator (DA) is an optional Registration Representative role. A DA manages a subset of the Participant's entity metadata as delegated by a Site Administrator.

A Site Administrator identifies Delegated Administrators for the Participant as needed. A Delegated Administrator's access scope is limited to a subset of the Site Administrator's access.

The Federation Operator maintains the record of Delegated Administrators. Data includes the Delegated Administrator's name and email address.

5. Metadata Format

The InCommon Federation metadata SHALL conform to and validate against the OASIS Security Assertion Markup Language (SAML) V2.0 Metadata specification ([SAML-Metadata]).

The InCommon metadata SHALL conform to extension schemas required to support inter-federation via eduGAIN. A complete list of extension schema required for export metadata can be found in the InCommon Federation Library. See [Interfederation-Policy].

Metadata for all entities registered by the Federation Operator SHALL make use of the SAML metadata extension ([SAML-Metadata-RPI-V1.0]) to indicate that the Federation Operator is the

registrar for the entity and to detail the version of the MRPS statement that applies to the entity. The following is a non-normative example:

```
<md:Extensions>
  <mdrpi:RegistrationInfo registrationAuthority="https://incommon.org"/>
…
</md:Extensions>
```

6. Entity Eligibility and Validation

6.1 Entity Registration

The process by which a Federation Participant can register an entity is described in the Federation Manager User Guide. See [FM-Guide].

A Site Administrator SHALL submit entity metadata to the Federation Operator (FedOp) via the Registry tool (Federation Manager).

A Delegated Administrator MAY submit entity metadata to the Site Administrator via the Federation Manager. A Site Administrator SHALL approve all such entity metadata registration requests.

The Federation Operator, specifically the Registration Authority (RA) SHALL review and approve critical metadata updates submitted by the Site Administrator. Routine syntax checking and non-critical updates MAY be performed by an automated process within the Registry tool (Federation Manager).

The Federation Operator SHALL verify the Participant's right to use particular domain names in relation to entityID attributes and, for Identity Provider entities, any scope elements.

The right to use a domain name SHALL be established in one of the following ways:

- A Participant's canonical name matches registrant information shown in WHOIS.
- Domain Control Validation - See InCommon Federation Participant Domain Use Policy ([Domain-Use-Policy]) for details.
- A Participant MAY be granted the right to make use of a specific domain name through a permission letter from the domain owner on a per-entity basis. Permission SHALL NOT be regarded as including permission for the use of sub-domains.

6.2 EntityID Format

Values of the entityID attribute registered MUST be an absolute URI using the http, https or urn schemes.

https-scheme URIs are RECOMMENDED to all Participants.

http-scheme and https-scheme URIs used for entityID values MUST contain a host part whose value is a DNS domain.

For additional information, see [Entity-Id].

6.3 Scope Format

For Identity Provider entities, scopes MUST be rooted in the DNS domain namespace, expressed in lowercase. Multiple scopes are allowed.

Regular expressions representing scopes MAY NOT be used.

6.4 Entity Validation

On entity registration, the Federation Operator (and/or the Registry software) SHALL carry out entity validation checks. These checks include:

- Ensuring the entity meets the requirements of InCommon Baseline Expectations in Trust in Federation [Baseline].
- Ensuring metadata is correctly formatted;
- Ensuring applicable protocol endpoints are properly protected with TLS / SSL certificates.

7. Entity Management

Once a Participant has joined the Federation any number of entities MAY be added, modified or removed by the Participant. IdP registrations are normally limited to one IdP per Participant. Participants MAY purchase additional IdP registrations.

7.1 Entity Change Requests

Any request for entity addition, change or removal from a Federation Participant needs to be communicated from or confirmed by their respective Registered Representatives.

A Registered Representative SHALL make these changes via the InCommon Federation Registry tool (Federation Manager).

In emergency cases where a Participant is unable to user Federation Manager to make the necessary changes, the Federation Operator MAY delete metadata for a Federation Participant via other request methods, such as an email, supplemented with an additional check, submitted by a Registered Representative.

7.2 Entity Augmentation made by Federation Operator

The Federation Operator SHALL add an `<md:Organization>` element to each entity metadata registered in the InCommon Federation, as described in [3. Participant Eligibility and Ownership].

The Federation Operator SHALL add an `<md:RegistrationInfo>` element to each entity metadata to note that the entity is registered by the InCommon Federation. The value of the `registrationAuthority` XML attribute is "https://incommon.org".

The Federation Operator MAY add zero or more `<mdattr:EntityAttributes>` extension elements to an entity metadata. These entity attributes denote entity categories (such as the Research & Scholarship entity category) and/or identity assurance qualifiers. For more information, see [Entity-Categories].

7.3 Unsolicited Entity Changes

The Federation Operator may amend or modify the Federation metadata at any time in order to:

- Ensure the security and integrity of the metadata;
- Comply with interFederation agreements;
- Improve interoperability;
- Add value to the metadata.

Changes will be communicated to Registered Representatives for the entity.

7.4 Metadata Aggregate Production

The Federation Operator SHALL sign and publish metadata once every business day, at predetermined times according to published hours of operation. See [Hours].

The Federation Operator MAY occasionally publish metadata at an alternate time upon special request or to ensure the integrity and availability of the metadata aggregate.

To begin the metadata production process, the Federation Operator aggregates entity metadata and wraps the entity descriptors in a top-level `<md:EntitiesDescriptor>` element.

The Federation Operator adds an expiration date to the metadata aggregate. The value of the `validUntil` XML attribute on the top-level `<md:EntitiesDescriptor>` element is a date two (2) weeks into the future.

The FedOp adds an `<mdrpi:PublicationInfo>` child element to the top-level `<md:EntitiesDescriptor>` element. The value of the publisher XML attribute is "https://incommon.org".

7.5 Metadata Signing and Publication

The Federation Operator signs and publishes metadata [Metadata]. Metadata is available in a number of different formats and streams, to fit the needs of different consumers.

Metadata is signed using a secure process that prevents malicious or insider access to the signing key.

The corresponding public key is bound to a metadata signing certificate, available in our Metadata Service documentation [Metadata]. The signing certificate is used by metadata consumers to bootstrap a secure metadata refresh process.

Signed metadata published to a well-known public Metadata Distribution Server. See [Metadata]

8. References

[Baseline] InCommon Baseline Expectations for Trust in Federation: https://incommon.org/federation/baseline/

[Domain-Use-Policy] http://doi.org/10.26869/TI.53.1

[Entity-Categories] https://spaces.at.internet2.edu/display/federation/Badging+service+with+entity+categories

[Entity-Id] https://spaces.at.internet2.edu/display/federation/entity+id

[FM-Guide] https://spaces.internet2.edu/display/federation/federation+manager

[Hours] https://www.incommon.org/about/hours-of-operation/

[InCommon-PA] InCommon Participant Agreement: https://incommon.org/wp-content/uploads/2019/04/Participation-Agreement-20180312-Rvw-Copy1.pdf

[InCommon-Roles] https://www.incommon.org/about/roles/

[Interfederation-Policy] https://spaces.at.internet2.edu/display/federation/Interfederation+Technical+Policy

[Join-InCommon] https://www.incommon.org/join-incommon

[Metadata] https://spaces.at.internet2.edu/x/2wR0C

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[SAML-Metadata] OASIS Security Assertion Markup Language (SAML) V2.0 Metadata specification: https://wiki.oasis-open.org/security

[SAML-Metadata-OS] OASIS Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0: http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf.

[SAML-Metadata-RPI-V1.0] SAML V2.0 Metadata Extensions for Registration and Publication Information Version 1.0. 03 April 2012. OASIS Committee Specification 01. http://docs.oasis-open.org/security/saml/Post2.0/saml-metadata-rpi/v1.0/cs01/saml-metadata-rpi-v1.0-cs01.html.

9. Attribution

This document is developed using the REFEDS Metadata Registration Practice Statement template v1.1.