

# InCommon metadata validation procedure

Jump to:

[About the Metadata Validation Procedure](#) | [Entity validation performed by Site Administrator](#) | [Entity validation performed by the Federation Manager](#) | [Entity validation performed by Registration Authority](#) | [Glossary](#)



This document uses normative language (MUST, MAY, SHOULD, etc.) from [RFC2119](#)

## About the Metadata Validation Procedure

This article describes the procedure InCommon performs to validate data elements submitted by Participants during the course of registering an organization and its entity metadata.

Organization validation upon joining InCommon

When an organization joins InCommon and signs the InCommon Participation Agreement, the InCommon Registration Authority (RA) performs validation on an organization's name and website. The same validation also occurs when an organization requests a name or website update.

Metadata Element	Requirement Level	Method	Assessor
OrganizationName	MUST	3 <sup>rd</sup> Party verification (e.g., database such as accreditation listings)	InCommon Registration Authority (RA)
Organization DisplayName	MUST	Same as OrganizationName or a reasonable variant if requested	InCommon RA
OrganizationURL	MUST	Demonstrable Control of domain.	InCommon RA

## Entity validation performed by Site Administrator

The following validations SHOULD be done by the Site Administrator (SA) before the Site Administrator submits an entity to be published into the InCommon metadata.

Metadata Element	Requirement Level	Method	Assessor
errorURL in IdPs	SHOULD	Be a URL that resolves to a document describing how to contact IdP support personnel, or providing a form for contacting IdP support personnel (e.g., to request that attributes be released to an SP).	Site Administrator
Endpoints in IdPs	SHOULD	Contain a SAML V2.0 SingleSignOnService endpoint supporting the HTTP-POST binding.	Site Administrator
Endpoints in IdPs	SHOULD NOT	Contain one or more SAML V2.0 Attribute Authority endpoints, unless for a known use case articulated by the Site Administrator.	Site Administrator
Certificate expirations	SHOULD	The certificate should be long lived (10 years). Not all places can do long lived certs so seek clarification if they want to switch to a long-lived cert before approving.	Site Administrator

## Entity validation performed by the Federation Manager

The following validations are run automatically in Federation Manager (FM) when a Site Administrator submits an entity to be published into the InCommon metadata.

Metadata Element	Requirement Level	Method	Assessor
EntityID	MUST	For <b>new</b> entity descriptors, must be a validly formatted URL.	FM
EntityID	MUST	Be URLs only. Grandfathered URNs are supported.	FM
mdui:Logo	MUST	Be a resolvable URL, using the https:// scheme.	FM
mdui:PrivacyStatementURL	MUST	Be a resolvable URL	FM

Endpoints in IdPs	MUST	Contain a SAML V2.0 SingleSignOnService endpoint supporting the HTTP-redirect binding.	FM
Endpoints in IdPs	MUST	Be a validly formatted URL, using the https:// scheme.	FM
Endpoints in SPs	MUST	Contain at least one AssertionConsumerService endpoint supporting the SAML V2.0 HTTP-POST binding.	FM
Technical, Administrative, Support, Security contacts	MUST	Metadata MUST contain at least one of each: Technical Contact, Administrative Contact, Security Contact.	FM

## Entity validation performed by Registration Authority

The following validations are done by the Registration Authority (RA) when a Site Administrator submits an entity to be published into the InCommon metadata.

Metadata Element	Requirement Level	Method	Assessor
EntityID	MUST	Demonstrable Control of domain.	RA
mdui:DisplayName	MUST	Reasonableness Check	RA
mdui:Description	MUST	Reasonableness Check	RA
shibmd:Scope in IdPs	MUST	Demonstrable Control of domain.	RA
shibmd:Scope in IdPs	SHOULD	Be the root DNS zone for the organization (e.g., <a href="#">campus.edu</a> , <b>not</b> <a href="#">library.campus.edu</a> ).	RA

\* This applies only to new entity submissions. Older entities may contain exceptions.

## Glossary

- MUST** - The Assessor must validate the metadata element. The entered value must meet validation rules before the change is approved.
- SHOULD/SHOULD NOT** - These statements are strong recommendations to the metadata submitter. We strongly recommend that all administrators submitting metadata consult the [metadata submission documentation](#) to determine the best course of action. As they are not mandatory, InCommon Registration Authority will not object to or block the approval of metadata when the recommendation is not followed.
- Demonstrable Control of domain** - There are two methods for validating control of a domain:
  - WHOIS: On a domain's WHOIS record, the Registrant Organization must be the Organization submitting the metadata. Results are archived in the Org's box folder.
  - TXT Record: See the [Domain Control Validation Procedure](#). Results are archived in the Org's box folder.
- Reasonableness Check for Names and Descriptions**
  - High-value names that obviously don't belong to the submitting organization are disallowed. For example, University-X cannot claim to be "Woolworth's" or "Pan Am" or "Compaq Computers."
  - However, limited brand associations are allowed that constrain the relationship appropriately. For example Company-A should not assert "University-X's Job Board" but could assert "University-X's Job Board via Company-A."
  - URLs are not allowed.
  - Domain strings (e.g., [campus.company.com](#)) are allowed but discouraged (see SHOULD) where a name or brief description is more appropriate for human readable elements.
  - Offensive language is discouraged (see SHOULD).
  - It is ultimately up to the Org to ensure violations and infringements are not occurring.