

Metadata Registration Practice Statement



This policy is deprecated. The current version of the policy is published at: <https://www.incommon.org/federation/mrps/>

Metadata Registration Practice Statement

InCommon maintains a registry of organizationally valid SAML metadata. Entity metadata is aggregated, vetted, signed, and published periodically at well-known HTTP locations.

Note: This Metadata Registration Practice Statement applies to the InCommon [Export Aggregate](#) only.

1. Registration of an Organization
 - a. An organization that wishes to register metadata in the InCommon Federation signs a legal document called the InCommon [Participation Agreement](#).
 - i. Data includes the name of the organization.
 - b. The InCommon Registration Authority (RA) verifies the organization name against third-party information sources.
2. Registration of Organizational Representatives
 - a. Executive
 - i. The InCommon Executive for an organization is identified on the Participation Agreement.
 1. Data includes email address and phone number
 - ii. The RA verifies the identity of the Executive via out-of-band methods.
 - b. Site Administrator
 - i. The Executive identifies one or more Site Administrators for the organization.
 1. Data includes email address and phone number
 - ii. The RA verifies the identity of a Site Administrator via a combination of automated processes and out-of-band methods. A Site Administrator is granted access to the InCommon [Federation Manager](#), a web application for managing entity metadata.
 - c. Delegated Administrator
 - i. A Site Administrator identifies Delegated Administrators for the organization as needed. This is an optional role.
 1. Data includes email address
 - ii. The RA verifies the identity of a Delegated Administrator by sending the Delegated Administrator an email invitation confirmation. A Delegated Administrator accesses the Federation Manager using a federated credential.
3. Production of Entity Metadata
 - a. Supported XML Schema
 - i. InCommon metadata conforms to and validates against the XML schema listed in the [OASIS Security Assertion Markup Language \(SAML\) V2.0 Metadata specification](#).
 - ii. InCommon metadata also conforms to various extension schema. A complete list of extension schema required for exported metadata is documented on the [Interfederation Technical Policy](#) page.
 - b. Registration of Entity Metadata
 - i. Optionally, a Delegated Administrator submits entity metadata to the Site Administrator via the Federation Manager. A Site Administrator must approve all such entity metadata registration requests.
 - ii. A Site Administrator submits entity metadata to the Federation Operator (FedOp) via the Federation Manager.
 - iii. The RA vets and approves all metadata updates submitted by the Site Administrator.
 - c. Augmentation of Entity Metadata
 - i. The FedOp adds an `<md:Organization>` element to each entity descriptor. The value of `<md:OrganizationName>` element is verified as described above.
 - ii. The FedOp adds an `<mdrpi:RegistrationInfo>` extension element to each entity descriptor. The value of the `registrationAuthority` XML attribute is `"https://incommon.org"`.
 - iii. The FedOp adds zero or more `<mdattr:EntityAttributes>` extension elements to each entity descriptor, including:
 1. entity attributes denoting entity categories (such as the Research & Scholarship entity category)
 2. identity assurance qualifiers
4. Production of Metadata Aggregate
 - a. Normally the FedOp signs and publishes metadata once every business day, at predetermined times according to published [hours of operation](#). Occasionally the FedOp will produce metadata at other times, upon special request or solely at its own discretion.
 - b. To begin the metadata production process, the FedOp aggregates entity metadata and wraps the entity descriptors in a top-level `<md:EntitiesDescriptor>` element.
 - c. The FedOp 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.
 - d. 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"`.
5. Metadata Signing and Publication
 - a. The InCommon Key Authority signs one or more [Metadata Aggregates](#) with a private offline key protected by multiple layers of access control. A rigorous [Metadata Signing Process](#) is followed.
 - b. The corresponding public key is bound to a [Metadata Signing Certificate](#) used by metadata clients to bootstrap a secure metadata refresh process.
 - c. Signed metadata aggregates are published to a well-known public [Metadata Server](#).