metadata-saml

Jump to:

Identifying the Entity | Contacts | Organization Information | Login and Discovery User Interface Elements (MDUI, etc.) | Connection Endpoints | Signing and Encryption Keys | Qualifications and Capabilities (Entity Attributes, etc.) | Publisher Information | Other Information | SAML Specifications Documents



InCommon metadata is the instantiation of the Trust Registry described in Trusted Relationships for Access Management: The InCommon Model.

InCommon metadata contains information about every entity (Identity Provider or Service Provider) known within the InCommon Federation.

Identifying the Entity

All of each entity's metadata is contained in an `<EntityDescriptor>` XML element with an `entityID` XML attribute. This entityID must be globally unique and, therefore, must in the form of a URL rooted in the entity's organization's domain, as described in Entity ID. For more information, see:

- md:EntityDescriptor (and entityID) Syntax

Contacts

These elements provide contact information for people who have various roles (administrative, technical, security, and support) for the entity, as described in Contacts information. For more information, see:

- mdui:ContactPerson Syntax

Organization Information

The <Organization> element provides information about the organization that is legally responsible for the entity, including the organization's legal name, preferred display name, and home page URL. This information is vetted by InCommon and stored in the metadata for all of the organization's entities.

- md:Organization Syntax

Login and Discovery User Interface Elements (MDUI, *etc.*)

These elements provide information to help end users to navigate the handoffs between a Service Provider and the user's Identity Provider during discovery and login, as described in User interface elements and Error Handling URL. For more information, see:

- mdui:UIInfo (User Interface Elements) Syntax
- mdui:DisplayName Syntax
- mdui:Logo Syntax
- mdui:Description Syntax
- mdui:InformationURL Syntax
- mdui:PrivacyStatementURL Syntax
- md:IDPSSODescriptor Syntax (for errorURL)

Connection Endpoints

These are URLs of the entity's SAML service endpoints, as described in IdP SSO Settings (IDPSSODescriptor) and SP SSO Settings (SPSSODescriptor). For more information see:

Registrar Information

This element identifies the registration authority (*i.e.*, the entity's federation) that enrolled this entity, verified its contacts, and reviewed its entity attributes (when review is required). For more information, see:

- mdrpi:RegistrationInfo Syntax

Publisher Information

In addition to the information provided for each entity, there is information that allows you to verify the organization (in this case, InCommon) that publishes the metadata that you retrieve.

- For a metadata aggregate listing all entities, the publisher is provided in the `<mdrpi:PublicationInfo>` element. For aggregates published by InCommon, this is `https://incommon.org`. For more information, see:
  - mdrpi:PublicationInfo Syntax
- For metadata retrieved from an MDQ service, the publisher is, implicitly, the organization responsible for the MDQ server. If the MDQ server utilizes TLS for communication, its authenticity can be verified from its X.509 server certificate.
- In all cases, the retrieved `<Signature>` element can be (and should be) used to verify that the information was signed by the private key held by the expected publisher.

Other Information

The following metadata elements also appear in InCommon metadata:

- shibmd:Scope Syntax
- md:AttributeConsumingService Syntax

SAML Specifications Documents

The SAML representation of InCommon metadata is defined in

- Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0 – Errata Composite, SAML V2.0 Metadata Extension for Entity Attributes, and
- SAML V2.0 Metadata Extensions for Login and Discovery User Interface Version 1.0.

Please see the OASIS SAML Wiki for current versions of these documents. Other specifications may apply in specific circumstances, as noted in the pages linked below. (Note: Per the eduGAIN Policy Framework, the "md:" XML namespace prefix indicated below does not always appear in distributed metadata. In particular, InCommon-registered metadata does not include the prefix.)

- md:IDPSSODescriptor Syntax
- md:SPSSODescriptor Syntax

Signing and Encryption Keys

These are the signing and encryption keys associated with the Connection Endpoints to verify authenticity and provide privacy of the information exchanged, as described in Signing and Encryption Keys.

Qualifications and Capabilities (Entity Attributes, *etc*.)

Qualifications and capabilities are formal assertions of specific information about the entity, generally related to how it should be treated by other entities, as described in Qualifications and Capabilities (Entity Attributes, etc.).

For more information, see:

- mdattr:EntityAttributes Syntax

- md:AttributeConsumingService Syntax
- md:EntityDescriptor (and entityID) Syntax
- md:IDPSSODescriptor Syntax
- md:Organization Syntax
- md:SPSSODescriptor Syntax
- mdattr:EntityAttributes Syntax
- mdrpi:PublicationInfo Syntax
- mdrpi:RegistrationInfo Syntax
- mdui:ContactPerson Syntax
- mdui:Description Syntax
- mdui:DisplayName Syntax
- mdui:InformationURL Syntax
- mdui:Logo Syntax
- mdui:PrivacyStatementURL Syntax
- mdui:UIInfo (User Interface Elements) Syntax
- shibmd:Scope Syntax