The InCommon Federation Trust Model and the Steward Program

An overview of the impact of the Steward Program on the trust model

August 30, 2016

InCommon Federation Trust Model and the Steward Program

Definition of Terms[1]

Entities - This refers to SAML entities, which are the identity provider and service provider entries in the InCommon Trust Registry (also known as metadata aggregate).

InCommon Executive - The InCommon Executive represents the participant organization regarding all decisions and delegations of authority for the responsibilities of InCommon Participants, including but not limited to, all relevant federation and certificate services.

InCommon Site Administrators - The Site Administrator serves as an organization's primary registrar. The administrator is responsible for registering and maintaining the policies and technical data related to the organization's participation in the InCommon Federation.

Identity Provider - The originating organization for a user. The identity provider software authenticates a user by prompting for and checking a username and password, and provides that information to the Service Provider to use for authorization for access to a service. For the InCommon Federation, the Identity Provider software is typically deployed by a campus or other organization that manages and operates an identity management system and provides federated single sign-on services..

Represented Constituents - The school districts and community colleges represented by a Steward.

Service Provider - The Service Provider software is used to authorize a user for access to a protected resource. When a user attempts to access the resource, the Service Provider sends an authentication request to the Identity Provider. Once authentication is complete, the Service Provider validates the response and provides access to the resource.

Trust Registry - Also known as Metadata or Metadata Aggregate, the trust registry includes all of the information submitted by InCommon Participants. Examples of the information contained are general information about an entity (identity provider or service provider), statements of support for the SAML protocol, certifications that enhance trust, and contact information about those responsible for the entity.

[1] An extensive glossary of InCommon and identity and access management terms is at www.incommon.org/glossary.html

Executive Summary

InCommon establishes the operating principles, technology standards, and data exchange schema that participants use in their trusted interactions with one another, enabling the flow of identity information in a secure and private way.

The policies, procedures, and agreements that InCommon uses for onboarding new participants provide the foundation for the trust structure. InCommon maintains a trust registry (also known as the metadata aggregate) that includes all identity providers and service providers registered in the Federation (these are also known as entities). Each InCommon participant is responsible for submitting the correct information about its entities to the trust registry.

For its part, InCommon maintains the integrity of the trust registry and performs reasonableness checks on the information submitted by the participants. This trust registry enables interoperability between InCommon participants, provides certifications that enhance trust among participants, and includes other information such as contact addresses and links to documentation.

With the addition of the Steward Program, Stewards will act under contract to InCommon for the organizational vetting and metadata management for their “Represented Constituents” (the K-12 schools and community colleges that the Steward serves). InCommon will train the Stewards with the same processes and procedures it uses, and monitor them to assure no material change to the trust model.

This paper outlines how the trust model is maintained in light of the addition of the Steward Program.

Responsibilities - InCommon and Stewards

An organization joining InCommon agrees to the common policies, procedures, and technology standards that form the basis for the trust structure of the federation. By adopting these policies and procedures once, via signing the InCommon Participation Agreement, organizations do not need to negotiate such things with every other organization individually.

InCommon/Internet2 staff complete organizational vetting and identity proofing of the trusted individuals from those organizations (the InCommon Executive and up to two InCommon Site Administrators). The Site Administrators will then have access to the Federation Manager, which is the interface used to submit metadata to the trust registry.

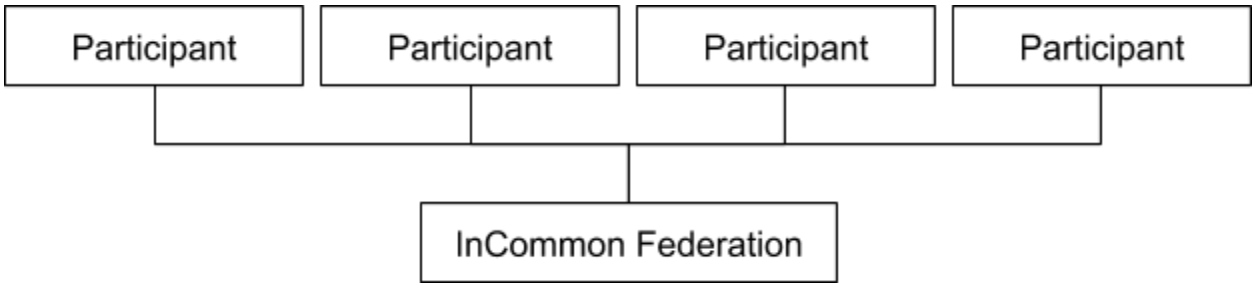
This metadata file is in machine-readable XML format and includes information about the entity, statements of support for the SAML protocol, contact information about those responsible for the entity, and other information. InCommon combines the metadata from all participants into

one file - the metadata aggregate - and publishes that file daily. Vetting, maintaining, and safeguarding the federation metadata is a key role for InCommon.

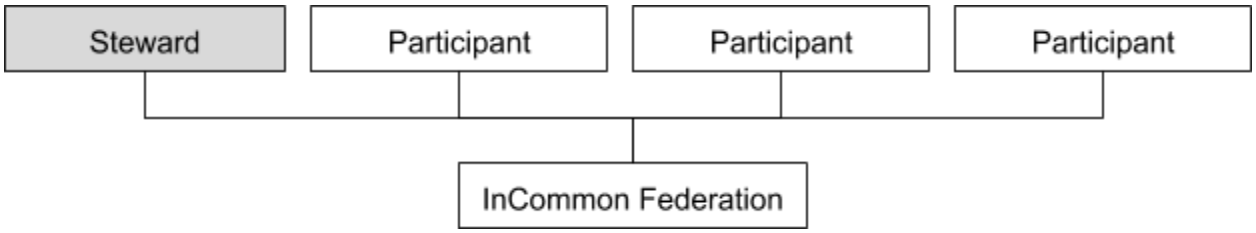
The following descriptions and diagrams illustrate the information flows and responsibility assignments that support trust within InCommon, comparing current procedures and those that will be in place with the Steward Program.

Organizational Vetting

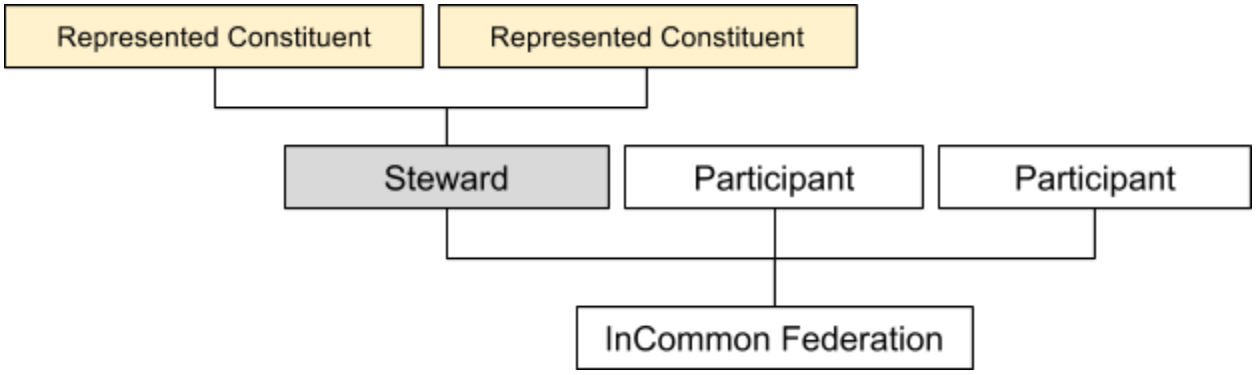
When an organization joins InCommon, the InCommon Registration Authority staff verifies the identity of the organization and the trusted officials authorized to act on behalf of the organization (the InCommon Executive and the InCommon Site Administrators).



Under the Steward Model, the Steward is the InCommon Participant, and InCommon will vet the Steward, just as any other participant.

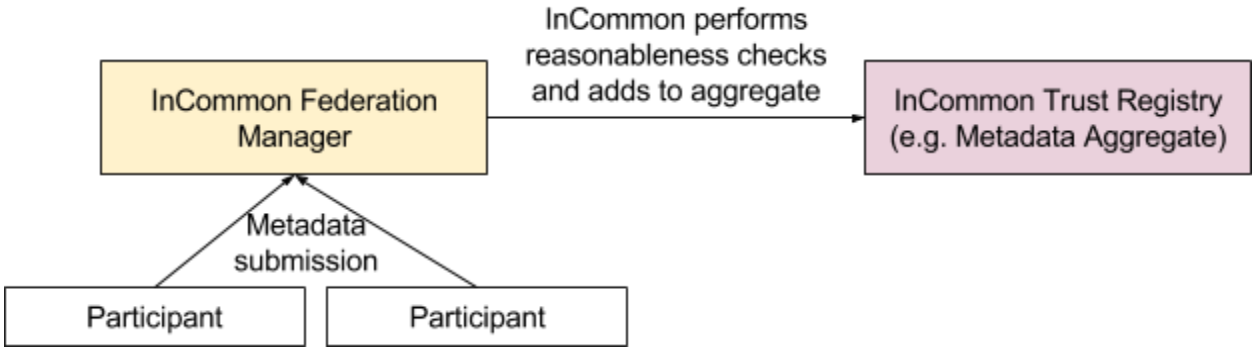


The Steward assumes responsibility for the organizational vetting of its Represented Constituents. InCommon trains the Steward on its documented process for organizational vetting. The Steward performs these functions with its Represented Constituents and InCommon will periodically audit the Steward's processes to ensure compliance.

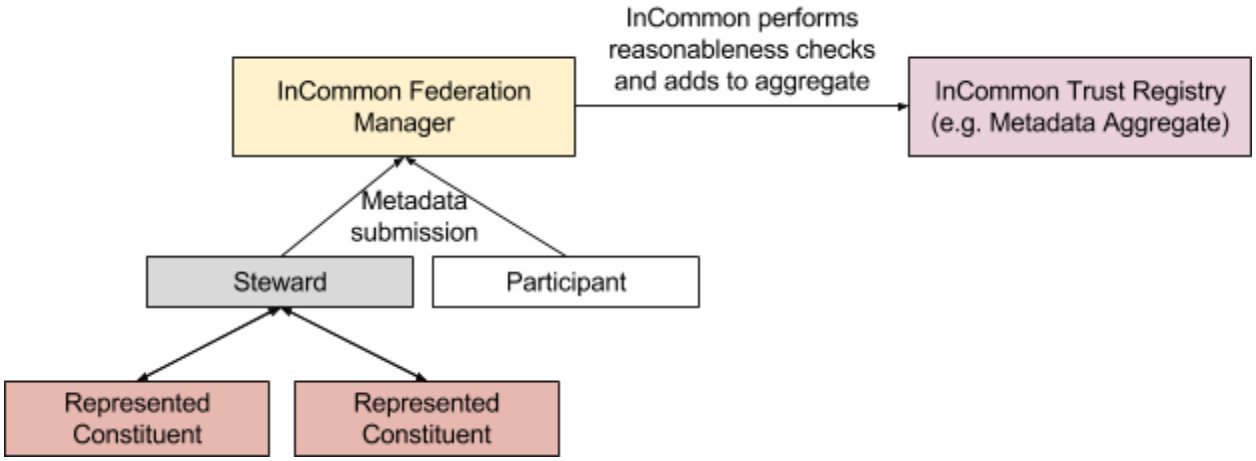


Trust Registry Submissions and Updates

Once an organization and its trusted officials are vetted, that organization can submit information to the trust registry for its entities (identity providers and service providers). InCommon Participants submit this information via a web portal, and InCommon staff performs validity checks on the submission and, assuming validity, this information is then included in the trust registry (e.g. metadata aggregate). Participants must manage the operation of the IdPs and SPs for which they submit metadata.



This process is the same with the Steward Program, except that the Steward manages the operation of IdPs and SPs and submits their metadata on behalf of its Represented Constituents (RC).



In both scenarios, InCommon Participants now have access to the IdPs and SPs submitted by all Participants, including Stewards (and the Steward metadata includes that of its Represented Constituents).

Review of Information in the Trust Registry

InCommon performs specific reasonableness checks on submitted trust registry information (e.g. metadata) to look for common errors (such as formatting problems), but the Participant has the ultimate responsibility for correct submissions.

Under the Steward Program, InCommon delegates to the Steward the responsibility to perform these reasonableness checks on the Represented Constituent information. Stewards are obligated contractually to perform the same checks as InCommon. The Steward is also required to separate the duties of submitting the information, on the one hand, and performing these checks on the other.