TRUST.

"assured reliance on the character, ability, strength, or truth of someone or something"

- Merriam-Webster

Trusted Relationships for Access Management: The InCommon Model

InCommon®

"The InCommon Federation is the U.S. education and research identity federation, providing a common framework for trusted shared management of access to online resources."

- InCommon Federation

Repository ID:	TI.3.2
Authors:	Jill Gemmill
	David Walker https://orcid.org/0000-0003-2540-0644
	Ann West
Sponsor:	Internet2
Superseded documents:	(none)
Proposed future review date:	December 1, 2018
Subject tags:	policy, service

TABLE OF CONTENTS

INTRODUCTION

THE INCOMMON FEDERATION WAS FORMED IN 2004 AS A WAY OF SCALING THE MANY ONLINE RELATIONSHIPS AN ORGANIZATION MAINTAINS WHEN OFFERING SERVICES TO ANOTHER OR ENABLING ACCESS FOR ITS USERS TO ANOTHER'S SERVICES.

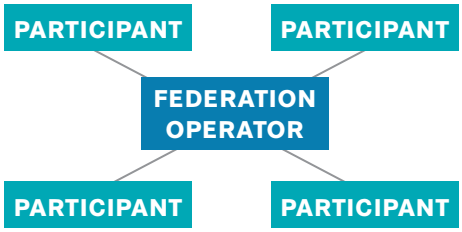
The federation provides a common, agreed-on framework for things like responsible parties, contacts, security model, change management process, and incident handling. The federation operator publishes these to the community so that each participating organization only sets up their processes and infrastructure once when it joins the federation and leverages that over and over with each participating partner.

Because of this, the federation is a great facilitator of collaboration use cases involving multiple institutions. Coupled with policy adherence tags like the Research and Scholarship Entity Category, it greatly reduces the burden on individuals to navigate their own way to resources hosted at other institutions.

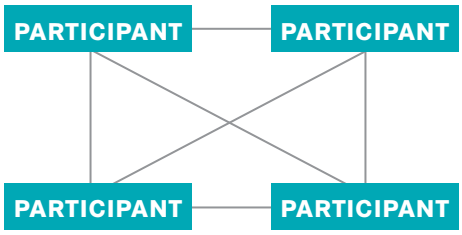
But what are the components of this trust? This document is a high-level introduction to the model for trusted relationships within the InCommon Federation. It is intended as a resource for executives and business managers who have responsibility for the policy, legal, and technical aspects of identity and access management at their institutions. It also is intended to serve as a guidepost for those involved in InCommon's planning for future strategic directions.

BASICS OF TRUST

At a very high level, InCommon's trust model is fairly simple. InCommon Participants rely on the InCommon Federation to introduce them to each other (by publishing a Trust Registry) in a "hub and spoke" configuration.



Once introduced, however, Participants rely on each other in a mesh configuration to exchange identity information in support of access control and personalization for their services.



The devil, of course, is in the details. Who are the "someones" and what are the "somethings" that we trust within InCommon? Why do we instill that trust; what are the "characters," "abilities," "strengths," and "truths" that we rely on?

WHAT DO WE MEAN BY "IDENTITY?"

According to the InCommon Identity Assurance Assessment Framework, "identity" refers to the set of information that pertains to a person. This information includes identifiers, memberships, eligibility, roles, names, characteristics, etc. Some of this information may uniquely identify that person, even sensitive Personally Identifiable Information (PII), but much of this information is not.

Note that this definition of "identity" is not the common English definition of the word[1], which implies unique association with a specific individual. In fact, in the practice of identity management, unique association is not required and, therefore, is disallowed to enhance privacy.

[1] "the distinguishing character or personality of an individual"

THE WHO, WHAT, AND WHY OF TRUST

Who Are the Actors We Trust?

There are two primary types of actors within the InCommon Federation:

Participant. An organization that has signed an agreement with a federation operator to cover the registration, verification and publication of information about its authentication or application services in the federation's Trust Registry (see below).

Federation Operator. The organization that operates and administers a federation on behalf of its Participants.

Individuals that use services in the Federation are also actors, though not explicitly part of InCommon's trust model. See Role of the Individual and PII.

What Do We Trust?

When one uses an online service, there are two primary actions associated with access:

1. Authentication verifies who you are and is the act of ensuring that the person with the credential (login id for example) is the same person that the organization has on file as having permission to use that credential. The verification is done using a password or some other mechanism.

2. Authorization is about what you can do and is the act of granting access to the authenticated individual based on role, grant number, license number, organizational affiliation and the like.

In a federated transaction, the organization that manages authentication for the individual is not the one hosting the service that the person wants to access. One organization authenticates the individual (in many cases a college or lab), and one offers services (such as a cloud provider, research collaboration, federal agency) and grants access.

To enable this transaction to happen, the organization offering a service asks the individual to identify his/her home organization and then asks the home organization to make sure the person is authenticated. The home organization is then asked to respond to the service provider with the necessary information about the person to authorize access. Information is released only if (1) the person has been properly authenticated at the time of the request, and (2) the home organization has decided to release this information. The IdP has total control of which attributes are released. At minimum, the Identity Assertion indicates only that an anonymous member of the home organization's community has successfully authenticated. For example, a university library may have paid for a license to access an online journal; the journal SP only needs to know that the entity accessing the journal is indeed a member of that university community, but does not need to know the individual's name. Identity Providers and Service Providers can configure a customized exchange of additional information in a bilateral manner. For example, a textbook publisher may provide online homework and quizzes with results to be reported back to both the professor and the individual student. The R&S profile has been designed for IdPs to release a global identifier, Name, and email address to any R&S Service Provider without the need for one by one configurations.

In most cases this information, called an Identity Assertion, is tightly defined in a community standard[2]

What are we trusting in this relationship?

Identity Assertions. Participants operating Services rely on Identity Assertions provided by Participants operating Identity Providers to control access to their resources and for personalization. The Identity Assertions are requested by a Participant operating a Service on behalf of the individual currently requesting that service.

Use of Identity Assertions. Participants operating Identity Providers rely on Participants operating Service Providers to make proper use of the information in the Identity Assertions they provide.

Introductions of Participants (Trust Registry). Participants trust their respective Federation Operators to introduce them to each other by publishing a Trust Registry. The Trust Registry, often referred to as federation metadata, contains the following information for each Identity Provider and Service Provider:

- *Elements that enhance trust among Participants*
  - The Participant that is responsible for the entity. This is who is trusted for Identity Assertions and their use.
  - The Federation Operator that registered the Participant. This is who is trusted for the introductions of their participants both within their federation and to other federations.
  - Certifications that have been achieved for the entity (see below)
  - Digital certificates to enable authentication of Participants' IdPs and SPs

[2] See the eduPerson Schema at www.internet2.edu/products-services/trust-identity/eduperson-eduorg/

- *Other elements*
  - Technical information to enable interoperation among IdPs and SPs,
  - Other useful information, such as links to contact individuals, documentation, etc.
  - Cryptographic signatures to authenticate the Trust Registry

WHY DO WE TRUST THE INCOMMON FEDERATION?

Trust within the InCommon Federation is rooted in the InCommon Participation Agreement and the documents it references. The Participation Agreement is signed by all InCommon Participants and legally binds them to common responsibilities and practice standards for the creation, transmission, and use of Identity Assertions. The Participation Agreement and its companion, the InCommon Federation Operating Policies and Practices (FOPP), describe InCommon's responsibilities and practices for providing introductions of Participants, as well as its administration of certifications.

Specific requirements of the Participation Agreement for all Participants:

- Deployment of conformant software
- Use of common syntax and semantics for Identity Assertions
- Provision of accurate information for the Trust Registry
- Provision of accurate contact information
- Respect for intellectual property rights
- Respect for privacy of identity information

Specific requirements of the Federation Operating Policies and Practices for InCommon's Federation Operator include:

- Identify and authenticate eligible Participants and their trusted officers
- Process Participants' submissions to the Trust Registry, including the application of reasonableness checks to help the submitters in their requirement to provide accurate information
- Administer certification processes
- Administer the maintenance, storage, production, secure signing and distribution of the Trust Registry
- Oversee the operation of InCommon service platforms
- Administer dispute resolution, when disputes cannot be resolved directly between Participants

InCommon also provides facilitation for interorganizational issues among InCommon Participants. In particular, InCommon coordinates security incident response when those incidents span multiple Participants.

Only Participants of the InCommon Federation are bound by the Participation Agreement. The Participation Agreement and the FOPP describe the InCommon Federation Operator's responsibilities with respect to other federations under the overall requirements established by eduGAIN[3] in eduGAIN Policy Framework–Constitution. A notable eduGAIN requirement is that its participant federations must "primarily serve the interests of the education and research sector."

All Federation Operators that participate in eduGAIN are required to publish a Metadata Registration Practice Statement (MRPS). This, along with the eduGAIN Policy Framework–Constitution, are the basis of trust among those Federation Operators. InCommon's MRPS is available online.

Certifications

Certifications are associated with an entity's Trust Registry entry to indicate that the Participant responsible for that entity has complied with a formal set of requirements. The certification process may allow self-assertion of compliance by the organization receiving the certification, or it may require review by the Federation Operator or some other external entity, depending on the requirements of the certification. In all cases, though, the Federation Operator is responsible for ensuring that the certification process has been followed.

Examples of certifications include the following:

- **Being an InCommon Participant.** Signing the Participation Agreement also results in a certification. Most aspects of compliance are self-asserted, but the Federation Operator does verify the Participant's organizational identity and key contacts. This certification is allows Participants to know that the organization responsible for an entity acts in accordance with the terms required of InCommon Participants.

- **Research and Scholarship Entity Category (SP).** A certification that a Participant's SP's purpose is support for research and scholarship and that it meets specific privacy and technical requirements. External review by the Federation Operator is required. This certification allows Participants to know that an entity's purpose is to support research and scholarship, and that the organization responsible for it acts in accordance the best practices, as established by the research and scholarship community.

[3] eduGAIN is the service that interconnects research and education identity federations like InCommon around the world.

- **Research and Scholarship Entity Category (IdP).** A certification that an Participant's IdP will release specific information in Identity Assertions to Research and Scholarship SPs. External review is not required; compliance is self-asserted. This certification is used by Research and Scholarship SPs to target their services to IdPs that specifically support Research and Scholarship.

- **InCommon Bronze Assurance Profile.** A comprehensive set of specifications for authentication and identity management with less stringent requirements than InCommon Silver. External review is not required; compliance is self-asserted. This certification is most useful for IdPs that wish to interoperate with SPs that require Assurance Level 1, as defined in NIST Special Publication 800-63-2, Digital Authentication Guideline.

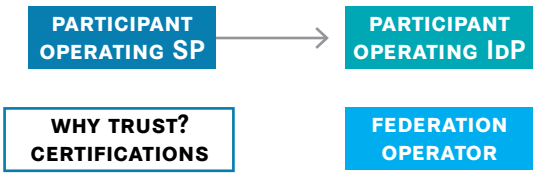
- **InCommon Silver Assurance Profile.** A comprehensive set of specifications for authentication of individuals and the identity management practices utilized to manage information about those individuals. Review of compliance by an independent auditor is required. This certification is most useful for IdPs that wish to interoperate with SPs that require Assurance Level 2, as defined in NIST Special Publication 800-63-2, Digital Authentication Guideline.

PUTTING IT ALL TOGETHER: The Trust Model

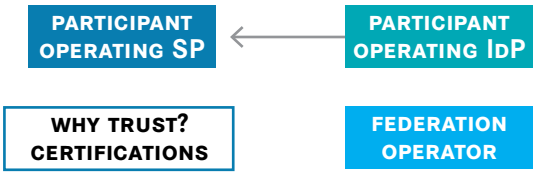
The following diagrams illustrate who is trusted for what, and why. The arrows point from a trusting actor to a trusted actor.

Provision of Identity Assertions

Release of information by and IdP occurs only when of that IdP's community members requests service from an SP. At that time, the SP requests an Identity Assertion from the IdP selected by the community member.

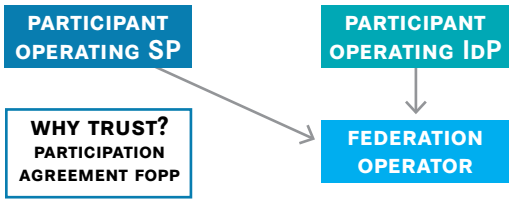


Participants operating SPs trust Participants operating IdPs to provide accurate Identity Assertions. The Federation Operator is not part of the transaction, although the Participants rely on the Federation Operator to introduce them (via the Federation Operator's Trust Registry) to each other correctly. Use of Identity Assertions.



Participants operating IdPs trust Participants operating SPs not to misuse the information in Identity Assertions and to protect the privacy of that information. The Federation Operator is not part of the transaction, although the Participants rely on the Federation Operator to introduce them to each other correctly.

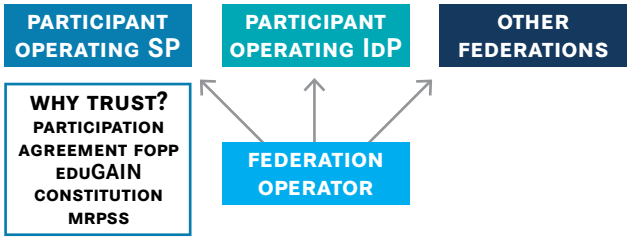
Introductions of Participants (the Trust Registry)



It is the Federation Operator's responsibility to maintain the integrity of its Trust Registry and distribute it to all of its Participants.

The Federation Operator, however, is dependent on its Participants, as well as other Federation Operators, to provide correct information for later distribution, as described below. The Trust Registry includes signed metadata describing the IdP, as well as that IdP's digital certificate public key. Public/private key pairs are used to validate Identity Assertions and the IdPs that send them.

Creation and Submission of Information to the Trust Registry

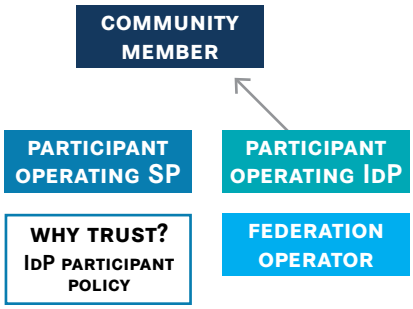


The Federation Operator trusts its Participants and other Federation Operators to create and submit correct information. The Federation Operator does, however, provide tools and review services to help InCommon Participants do this successfully; this enhances the trust that InCommon's Participants and Participants of other federations place in the Trust Registry information they receive from InCommon.

ROLE OF THE INDIVIDUAL AND PII

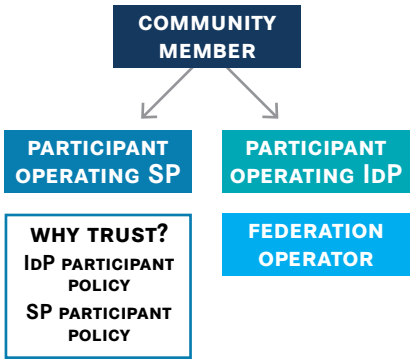
The InCommon trust model is explicitly among its Participants and the Participants of interfederated federations. Participants operating Identity Providers, however, represent communities of individuals, and those individuals both trust and are trusted. This section discusses trust relationships that involve individual community members and how that trust is impacted when Personally Identifiable Information (PII) is involved.

Protection of Authentication Secrets and Tokens



Participants operating IdPs trust their community members not to share the passwords, authentication tokens, secrets, etc., with others in ways that would cause them to issue false Identity Assertions.

Use of Identity Information



Community members trust Participants operating IdPs to release only appropriate information to authorized Participants' SPs. They also trust Participants operating SPs not to misuse information they receive. Note that what constitutes "appropriate information" may be subject to explicit consent by the community member.

Identity Assertions will not usually contain protected PII. When they do, however, community members' trust is enhanced by the legal provisions, such as FERPA, HIPAA, and state-specific laws, that Participants must obey. FERPA, for example, requires Participants operating IdPs to implement an opt-out mechanism for students accessing SPs that are not required for operation of their university. Also, use of protected PII in Identity Assertions will generally require specific contractual agreements between Participants covering allowable use and protection of the information exchanged.

GLOSSARY

Community Member. A person who is represented by a Participant that operates an IdP. For university Participants, Community Members may include students, staff, faculty, and other persons who have some affiliation with the university or its programs.

Digital Certificate. An electronic document that can be used to verify the authenticity of information (e.g., within a Trust Registry) that has been signed using public key cryptography. Digital Certificates have other uses, such as data encryption, that are not discussed in this document.

Entity. An Identity Provider or a Service Provider.

Federation Operator. The organization that operates and administers a federation on behalf of its Participants.

Identity. In contrast to its usual English meaning, "identity" in the context of the practice of identity management refers to the set of information that pertains to a person. This information includes identifiers, memberships, eligibility, roles, names, characteristics, etc. Some of this information may uniquely identify that person, even sensitive Personally Identifiable Information (PII), but much of this information is not.

Identity Provider (IdP). A network-accessible service that authenticates users and provides information about those users to Service Providers in Identity Assertions.

Identity Assertion. Information about a Service Provider's current user that is sent from an Identity Provider to the Service Provider for the purpose of making access decisions and/or personalizing the user's experience with the service. Examples of such information include identifiers, name, email, phone, address, group membership, and permissions. Note that an Identity Assertion may or may not uniquely identify an individual, depending on what information it contains.

Participant. This document defines the term Participant to as an organization that has signed an agreement with a federation operator to cover the registration, verification and publication of information about its IdPs and SPs in the federation's Trust Registry. This and other terms have been used in the following documents in potentially confusing ways.

InCommon Participation Agreement. The term Participant is used to indicate what this document calls a Participant, but only those that have signed an agreement with the InCommon Federation.

eduGAIN Policy Framework–Constitution. The term Member is used to indicate what this document calls a Participant.

Service Provider (SP). A network-accessible service that relies on Identity Assertions for the purpose of making access decisions and/or personalizing the user's experience.

Trust Registry. A registry of all Entities known to the federation. Also known as federation "metadata."