understanding-research-and-education-federation

***Who should read**: For those new to identity federations or to the research and education community; this primer provides important context to why InCommon works the way it does.*

Glossary

This Primer uses several terms that may be unfamiliar to you. This glossary provides a quick review of these terms within in the context of this Primer:

Identity provider - An identity provider (abbreviated **IdP** or **IDP**) is a system entity that creates, maintains, and manages identity information for principals and also provides authentication services to relying applications within a federation or distributed network.[wikipedia]

A **Service Provider** (abbreviated **SP**) is a network-accessible service that relies on an Identity Provider to perform user authentication and provide user information in order to make access decisions and/or personalizing the user's experience.

What is "Federation"?

Federation in identity management is a concept and set of technologies that allows for secured and standardized exchange of identity information across multiple domains or systems. Federation often refers to the act of using one organization's Single Sign-On (SSO) service (i.e., Identity Provider, or IdP) to sign into resources (i.e., Service Provider, or SP) offered by another organization. Another way to think about it is that "federation" refers to a collection of entities that have established trust: trust that the parties involved agree to adhere to an agreed-upon security, operational, and technical practices. This "trust" is often negotiated in a bilateral manner, on a case by case basis, between one identity provider and one service provider. For example, when a university subscribes to a SaaS platform and integrates its SSO with that platform, a trust is created via the terms and conditions of the procurement contract signed between the university and the SaaS provider.

On-Demand Scaling is Key in Research and Education

In academic collaborations, this one-at-a-time, bilateral negotiation doesn't scale well. Academic researchers and faculty are encouraged to work together and exchange ideas free from institutional control. Researchers don't depend on legal agreements between universities to share data and collaborate on projects. Collaborations happen spontaneously and quickly. University support infrastructures need to be tuned to facilitate these unique characteristics in research and education:

- **Collaboration across institutions happens spontaneously.** While there are many examples of formally created collaborations, such as instructional courses and grant funded research projects, most academic collaborations are *ad hoc*, created to meet an immediate, possibly short term, need. For example, a group of students might form a study group while they are taking a course, or a couple of researchers may find that they are working on the same problem and decide to join forces. The (international) academic societies keep their members abreast of current work, so collaborating researchers are likely to come from different institutions.
- **Research draws on resources from a wide range of disciplines.** Many of today's grand challenges cannot be solved within a single academic discipline. These collaborations must include participants with wide-ranging areas of expertise.
- **Trust occurs peer-to-peer between individuals, not among organizations.** Collaborations require trust among their participants. In academia, this trust is often established based on the participants' standings in their respective fields, not on formal agreements among the participants or their institutions. When there are formal trust relationships, the agreements generally address issues of the support infrastructure, such as access to funding or other resources.
- **Identity is for life, but roles and organizational affiliations change.** Learning is a life-long activity. A learner establishes a relationship with an institution as a student when they apply for admission; their relationship evolves and continues as an alumnus. A person may be simultaneously a student, a staff, a faculty, and a researcher. A faculty or researcher retain their digital identity as they take on different roles within their institution; their work, therefore access to resources and collaborations, may continue even when they move to another institutions.

What is the InCommon Federation?

On this page

Related content

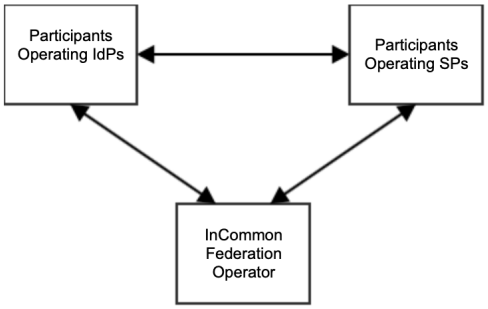
- Understanding Federation in Research and Education
- Putting things into Gear - Get Going with InCommon Federation
- Enable User Access to Federated Resources
- Register a Resource in InCommon
- Error Handling Service
- Federation Manager
- Metadata Service
- Discovery Service

Get help

Can't find what you are looking for?

help Ask the community

The InCommon Federation (InCommon) provides a trust framework enabling secure and scaled single sign-on (SSO) access to collaborations and resources across participating organizations. Specifically, InCommon's trust framework creates a multilateral trust among all participants, facilitated by the Federation Operator, to exchange identity information in a secure manner. Service Providers trust Identity Providers to provide accurate information, and Identity Providers trust Service Providers not to misuse the information they receive. Community Members trust both Identity Providers and Service Providers to respect their privacy, making use of their identity information only as needed, in accordance with legal and institutional policies.



This trust framework consists of commonly agreed-on operating practices and technical standards to enable seamless integration between an organization's single sign-on service (Identity Provider) and a resource outside that organization (Service Provider). These common practices and standards allow an InCommon Service Provider to trust an InCommon Identity Provider to perform sufficiently strong user authentication and provide accurate information to facilitate access to resources. An Identity Provider trusts a Service Provider to not misuse the information it receives as part of the single sign-on transaction. Individuals accessing resources in this manner trust all parties (Identity Providers and Service Providers) to respect their privacy, making use of their identity information only as needed, and only in accordance with legal and organizational policies. In addition to these practices and standards, a set of technical infrastructure (InCommon Metadata Service) exists to facailiate secure and scaled exchange of service registration information (metadata) among InCommon participants.

Since all InCommon participants already agree to adhere to the same practices and standards, it reduces, even eliminates, the delays often seen in bilateral integration negotiations. Scholars are able to access a wide array of global academic resources with little delay. Research centers and agencies significantly reduce their user account management overhead. Campus IAM teams can concentrate their efforts to secure one set of user credentials while improving user experience by not being a unnecessary blocker when a scholar needs to access a new (external) resource.

The InCommon LLC is charged by the InCommon Federation community to convene the United States research and education community to curate and to uphold this trust framework. The InCommon LLC is the InCommon Federation's Federation Operator. As the Federation Operator, InCommon LLC also operates the InCommon Metadata Service.

InCommon is also a part of a global research and education identity inter-federation called eduGAIN. Through eduGAIN, Participants have access to a global trust framework spanning 79 nations.

What am I agreeing to when I join the InCommon Federation?

When you join the InCommon Federation, you agree to adhere to a series of interoperability and data processing practices aimed at safeguarding user privacy and protecting resource security. You are also agreeing to publishing accurate service and contact information to facilitate incident response and user support matters involving federation participants.

Every service (and its operator) registered in the InCommon Federation must adhere to the InCommon Baseline Expectations for Trust in Federation (Baseline Expectations). Baseline Expectations holds each Participant accountable when interoperating with each other in InCommon, such that:

- an identity provider has the organizational authority and sufficient operating maturity to accurately authenticate and represent a user in a federated transaction;
- a service provider has controls in place to reasonably secure information and maintain user privacy;
- all parties maintain accurate, complete, and published metadata via the InCommon Metadata Service to ensure timely and secured exchange of service connection and contact information;
- all parties agree to follow common security incident response protocols to ensure speedy federation-related incident response coordination.

To ensure interoperability, InCommon-registered services are expected to conform to a set of technical standards when connecting to fellow services in InCommon. InCommon's primary federated access protocol is the Security Assertion Markup Language (SAML). Additional deployment profiles and data exchange standards further clarify interoperability gaps missing from SAML:

- Working with user data
- Communicating identity assurance: REFEDS Assurance Framework
- Communicating authentication assurance: REFEDS Assurance Profile
- SAML V2.0 Deployment Profile for Federation Interoperability

Further Reading

Trusted Relationships for Access Management: The InCommon Model provides a comprehensive introduction to this framework, including definitions of many of the terms used in this document.