InCommon Basics and Resources

September 9, 2016

InCommon Basics and Resources

What is InCommon?

InCommon is part of the trust and identity services provided by Internet2. InCommon offers trust services to higher education institutions, research organizations, and their sponsored corporate partners.[1] Services include the InCommon Federation, the InCommon Assurance Program, the InCommon Certificate Service, and the InCommon Multifactor Authentication Program. You can find out more about each of these services below.

Joining InCommon

The first step toward taking advantage of any of these services and programs is to join InCommon; you can then implement federated identity management or subscribe to one of our other services.[2]

InCommon participation is open to higher education (two- and four-year degree-granting accredited institutions) and research organizations, as well as their sponsored partners (such as companies and organizations that do business with or provide services to research and

[1] InCommon and MCNC (the North Carolina regional network) are also exploring a proof of concept, the Steward Program, to provide federation services to K-12 and community colleges.

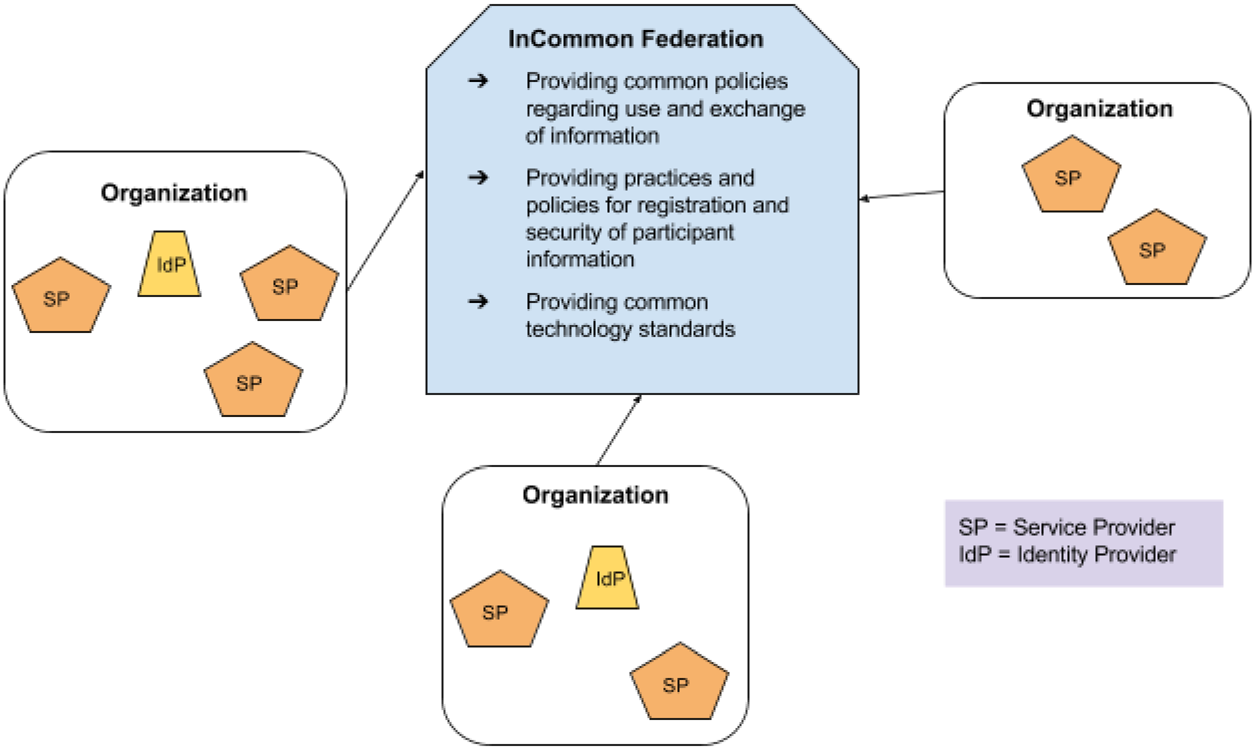
[2] Detailed information about the process for joining InCommon is at www.incommon.org/join.html. Joining is the first step in taking advantage of the InCommon Federation, the InCommon Certificate Service, and the InCommon Multifactor Authentication Program.

education). The process is straightforward; sign the participation agreement and pay the one-time registration fee and the annual fee. Sponsored partners also provide a sponsor letter from a current InCommon participant and a document showing annual revenues (the InCommon fee level is based on annual revenue).

The InCommon Federation

The InCommon Federation is the U.S. research and education identity federation, providing a framework for trusted shared management of access to resources (on-campus, off-campus, or in the cloud). InCommon allows higher education, research organizations, and their partners to give individuals single sign-on convenience to a wide variety of services in a secure and privacy-preserving way.

Here is a graphic demonstrating the trust model underpinning the InCommon Federation.


InCommon Federation
➔ Providing common policies regarding use and exchange of information
➔ Providing practices and policies for registration and security of participant information
➔ Providing common technology standards
Organization
SP
IdP
SP
SP
SP
Organization
SP
SP
Organization
SP
IdP
SP
SP = Service Provider
IdP = Identity Provider

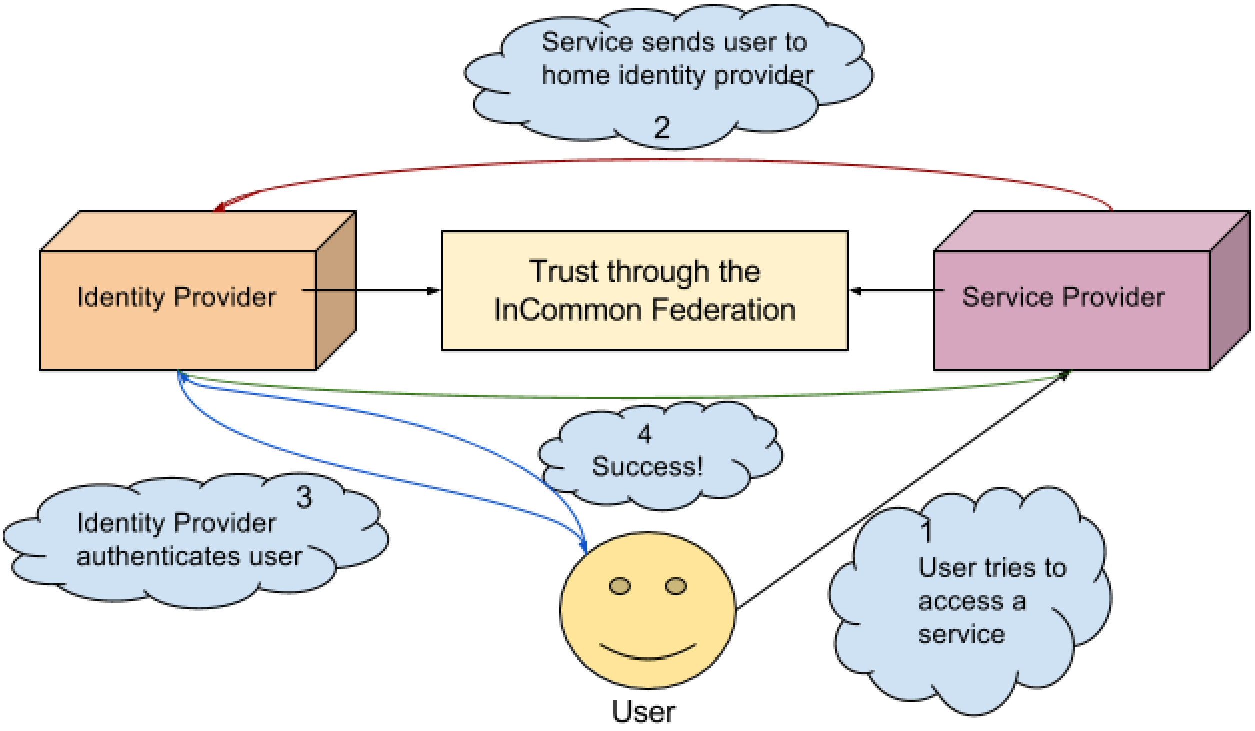
How Does it Work?

A user clicks on a resource -- perhaps a library database, a collaboration wiki, or a service supporting a business function (such as admissions or human resources). The user is sent to his or her Identity Provider for authentication. The Identity Provider then releases only the identity data necessary to allow the Service Provider to make an access decision.

Each individual has an associated set of attributes, such as role at the institution (e.g. student, faculty, staff), email address, name, and other more-detailed information like “med student.”[3] A service will ask for only the information needed to enable access. Identity providers manage user privacy and information exchange, and service providers no longer need to manage passwords, instead leveraging the identity provider’s identity system.

This eliminates the need for researchers, students, and educators to maintain multiple, password-protected accounts. The InCommon Federation supports user access to protected resources by allowing organizations to make access decisions to resources based on a user's status and privileges asserted by the user's home organization.

This graphic provides a simple overview of how InCommon works from the user perspective.


Service sends user to home identity provider
2
Identity Provider
Trust through the InCommon Federation
Service Provider
4
Success!
3
Identity Provider authenticates user
1
User tries to access a service
User

What is the InCommon Federation’s Role?

InCommon establishes the operating principles, technology standards, and data exchange schema that participants use in their interactions. By adopting these multilateral policies and procedures once, via the InCommon Participation Agreement, organizations do not need to negotiate such things with every other organization individually.

[3] The InCommon website has detailed information about supported attributes (https://spaces.internet2.edu/display/InCFederation/Supported+Attribute+Summary)

Here are examples of the types of policies and procedures:

- The InCommon Federation is based on SAML - the Security Assertion Markup Language. This provides the foundation for the technology and exchange of information.
- InCommon Federation participants agree to the eduPerson schema. Attributes - the key information exchanged - rely on eduPerson for their definitions and format.
- Organizations agree on the use of standards-based, SAML-compliant software to facilitate single sign-on. While the majority of participants use the Shibboleth software, there are other software packages (such as SimpleSAMLphp) available.[4]

Operationally, the key role for the InCommon Federation is to maintain and vouch for the integrity of the SAML metadata that has been submitted by its participants. InCommon updates the metadata file daily.

Each organization's Site Administrators manage that organization's metadata,[5] adding information about its identity providers and service providers, in machine-readable XML format. Included are such things as information about the entity, statements of support for the SAML protocol, and contact information for the people responsible for the entity.

InCommon also serves as the community convener for changes or enhancements of standards, and for the consideration of new services. At any given time, a number of working groups are forming, are underway, or have just concluded their work. Any member of the InCommon community is welcome to contribute to a working group. Recent working groups have studied ways to improve interoperability, the use of multifactor authentication, the use of external identities (also known as social identities) by groups of users, and how to improve and facilitate real-time user consent to the release of information during the single sign-on process.[6]

What is Shibboleth and How is it Related to InCommon?

There tends to be confusion about InCommon and Shibboleth and some mistakenly equate the two.

Shibboleth is open-source software that organizations use to enable single sign-on. Shibboleth is an implementation of SAML (Security Assertion Markup Language) Web Browser SSO. There are other software packages that do this (e.g. SimpleSAMLphp) but Shibboleth is the most prevalent.

[4] https://spaces.internet2.edu/display/InCFederation/Software+Guidelines

[5] InCommon metadata is the technical representation of trust and interoperability in the federation. Each identity provider and service provider submits its metadata, which includes all of the information needed for interoperability between deployments. Technical information about metadata is available on the wiki: https://spaces.internet2.edu/x/lwROAg

[6] A listing of working groups, and links to their wiki pages) is at https://spaces.internet2.edu/x/poNRBQ

The InCommon Federation wraps a framework around single sign-on software like Shibboleth. The federation defines the policy and technical standards and provides the platform that allows organizations to interact.

What is the POP and the FOPP?

These are the two foundational policy documents related to the InCommon Federation.

The InCommon POP (Participant Operational Practices) provides key contact information for your identity management operation and describes your practices as they relate to the federation. For identity providers, that means providing information about your identity management and credentialing processes, and your risk management measures. For service providers, it means demonstrating the appropriate use of attribute assertions received from an identity provider and protecting that information from non-related uses. The InCommon website has both a Word version and an HTML version of the POP, which you can complete and post on your organization's website.[7]

The InCommon FOPP (Federation Operating Policies and Practices) describes the activities and systems of the InCommon Federation.

Your Identity Management System

Identity management includes the policy, administrative processes, and technical systems involved in online identity services and access management. An identity management system ensures that the right people access the right services. Efficient and effective use of the InCommon Federation assumes an organization has the fundamentals of an identity management system in place.

In the past, each system or service came with its own identity infrastructure. Managing these duplicate identity stores and the associated security issues quickly becomes burdensome. The solution is to use the same identity information service for all applications. Identity information about a person is collected from authoritative sources such as the human resources, payroll, student information, and other systems of record and is securely maintained in a registry. This information is then used to grant, change or rescind access to services based on a person's roles or affiliations with the institution.[8]

[7] The Policies and Practices page on the InCommon website has links to the Word and HTML versions of the POP, as well as the FOPP, the InCommon Privacy Policy, and other documents. www.incommon.org/policies.html

[8] Thanks to the authors of the AACRAO IdM Brief #0708. While written with registrars in mind, it provides a good overview of identity management. https://spaces.internet2.edu/download/attachments/5259/IDM%2BBriefs-3.pdf).

The single sign-on federating software then draws the necessary information from that registry (that's where attributes come in) and provides the technology for making the authentication and authorization decisions.

Evaluating Your Identity Management System

A number of community members, over several years, have developed and refined a self-assessment tool[9] that may be useful in determining the maturity level of your IdM system and your readiness for federation.

The tool includes several items, each describing an aspect of identity and access management and provides four choices that roughly equate to the maturity level for that process or function. At the end, the assessment will give you a number that you can compare to the total possible points and get a rough idea of where you stand. The real benefit, though, is to help you identify the maturity of your IdM processes and infrastructure. The tool defines the characteristics of each maturity level in order to help you develop your IdM program with federation as the goal.[10]

What is TIER and its Relationship to InCommon?

Internet2 created the TIER (Trust and Identity in Education and Research) program to develop and integrate existing open-source identity and access management software, fill the gaps by providing a set of integrated components, and develop community standards and practices in the area of identity and access management that are compatible with InCommon participation. TIER currently includes Shibboleth (single sign-on and federating software), Grouper (enterprise access management software) and the COmanage registry. By focusing on both software integration and community policies and practices, the planned result is a comprehensive set of tools and improved interoperability with common practices.

Help with Identity Management and Federation

InCommon Education and Outreach

InCommon offers a number of education and training programs to help participants get started:

1. The annual Internet2 Technology Exchange has an extensive Trust and Identity track, which includes campus case study presentations, discussions of community successes and challenges, and specialized workshops (such as "Base CAMP" for those new to federation).[11]

[9] https://internet2.box.com/v/IAM-Assessment. This self-assessment tool also includes a handy glossary of identity management terms.

[10] Another document that may be useful is "Federated Identity Management Checklist," which includes policy, business, and technical steps to implement federated identity, or to serve as a guide for implementation readiness. https://spaces.internet2.edu/download/attachments/16548332/Federated_IdM_Checklist.pdf

[11] For information about the Technology Exchange, see www.internet2.edu/news-events/events/

2. The monthly IAM Online webinar series offers presentations on topics of general interest in identity management, campus case studies, and a look forward at features and programs under consideration.[12]
3. InCommon Shibboleth Installation Workshops provide face-to-face training on the installation and basic configuration of the Shibboleth software.[13]

Corporate Consulting and Support

Not every institution has the staff and resources to deploy and manage all of the aspects of identity management and federated identity management. A number of companies provide consulting, support, and cloud-based services related to IdM and federation. InCommon maintains a web page with a list of such companies that are also part of the Internet2 Industry Program (thus showing their interest in being part of the community).[14]

Community Support

InCommon operates a number of email lists, both for general information and help, as well as lists for specific topics and collaboration groups.[15]

InCommon Assurance Program

Some service providers offer services that carry a higher risk, should there be a compromise. Services with financial and other such sensitive information are one example. Higher education and research organizations can become certified[16] by demonstrating that their practices for providing credentials meet a prescribed standard.[17] These practices determine the confidence in the accuracy of a user's electronic identity and help mitigate risk for the Service Provider.

InCommon offers two assurance profiles (that is, sets of practices):

- Bronze has a security level that slightly exceeds the confidence associated with a common Internet identity. It verifies that the same person is accessing a service, but not the identity of that person
- Silver has a security level appropriate for services requiring identity, such as financial transactions. Because of the identity proofing and more strict technical requirements, Silver provides some confidence about the identity of the individual using the service

[12] www.incommon.org/iamonline

[13] www.incommon.org/shibtraining

[14] www.incommon.org/affiliates/

[15] A list of available email lists is at lists.incommon.org/sympa/lists

[16] See the IdPs certified as Bronze or Silver: incommon.org/federation/info/all-idps-certified.html

[17] A list of the components of the Assurance Program, including links to a number of support documents, is available at www.incommon.org/assurance/components.html

Some campuses use these profiles as a way to evaluate their identity practices against a set list of criteria.[18]

The InCommon Certificate Service

The InCommon Certificate Service offers subscribers unlimited certificates for one fixed annual fee, including SSL, extended validation, client (personal), code signing, and IGTF-approved certificates. For those interested, private certificate authorities are also available.

The service is available to any higher education institution accredited in the United States (and qualifying for a primary domain name in .edu), as well as not-for-profit regional RENs (Research and Education Networks) in the U.S. All of the domains your college or university owns are eligible, be they .edu, .net., .org, .com, or any other.

Subscribers report cost savings into the tens of thousands of dollars (your mileage will vary, depending on the size of your campus) and cite key benefits as centralized control of the certificates (and purchasing), as well as being able to use "real" certs for development purposes. The service features robust delegation capabilities, allowing you to delegate certificate administration to departments, where appropriate.

Certificates are provided through a contract with Comodo, a leading international certificate provider. InCommon registers and identity-proofs your campus RAOs (Registration Authority Officers) and Comodo maintains a knowledge base and email and telephone support. In addition, InCommon maintains an email list as a place for community members to share experiences, discuss possible system enhancements, and see how other campuses handle various issues and tasks.

Interested subscribers must first join InCommon, as the agreement for using the Certificate Service is an addendum to the InCommon Participation agreement.[19] The service also requires a three-year commitment. Please note that, while subscribers join InCommon, you do not have to participate in federated identity management services in order to take advantage of the Certificate Service.[20]

InCommon Multifactor Authentication Service

InCommon and Duo Security offer a phone-based multifactor authentication service for eligible higher education InCommon participants. It is a site license with a choice between Duo Security's

[18] The profiles and associated criteria are explained in detail in this document: www.incommon.org/docs/assurance/IAP.pdf

[19] For details about subscribing: www.incommon.org/certificates/subscribe.html

[20] There is a very detailed FAQ available on the InCommon wiki: https://spaces.internet2.edu/x/7wBvAQ

Enterprise and Platform editions.[21] You can choose to use the Duo site license for faculty and staff, or you can add students for an additional fee. If you have an associated hospital or medical center, there is an additional cost as well.[22]

About InCommon

InCommon is operated by Internet2, with staff members responsible for the business, policy implementation, technical operations, identity verification, and support for InCommon and its participants. The InCommon Steering Committee, consisting of leaders from the research and education trust and identity community, provides direction and determines policy. The InCommon Technical Advisory Committee (TAC) is a group of community members that provide recommendations related to the operation and management of InCommon with respect to technical issues. The InCommon Assurance Advisory Committee, also consisting of community members, is the oversight body for the InCommon Identity Assurance Program.[23]

[21] See Duo's website for the differences and features of Enterprise and Platform: https://duo.com/pricing

[22] For information about the hospital/medical center pricing, please email admin@incommon.org

[23] Information and links to details about the roles and responsibilities of these committees is at www.incommon.org/about.html