InCommon and eduGAIN: Joining the International Federation Community

Executive Summary

Researchers, faculty, staff, graduate students and others involved in research, scholarship and education increasingly interact with international colleagues. Many projects and virtual organizations prefer to use federated identity management, allowing individuals to use their home credentials to gain access to collaboration tools. However, identity and access management federations align with national boundaries, creating barriers to international collaboration, with each country and federation maintaining their own policies, practices and legal constraints.

To aid with federation across national boundaries, InCommon will use eduGAIN, an international service run by GÉANT in the European Union. eduGAIN now includes 40 national research and education federations worldwide and can enable collaboration among 31 million individuals, 8 million of which are supported by InCommon.

InCommon will send connection information - otherwise known as metadata - about InCommon Identity Providers and Service Providers to eduGAIN for inclusion in their global service. (Metadata is the information exchanged among participants to make federation happen.) InCommon will make the necessary adjustments to its policy documents to align with eduGAIN policies and provide a review period for community comment. InCommon will strongly encourage Identity Providers and qualifying Service Providers to participate in the global R&S program to streamline access to services.

The balance of this document provides information about the changes needed for eduGAIN adoption -- both for the InCommon Federation and for InCommon participants. In addition, InCommon will provide a comprehensive series of communications about the implications of interfederation and about planning for deployment.

InCommon and eduGAIN: Joining the International Federation Community

Background - Strategic Direction

Many countries have established a national identity research and education federation similar to InCommon. This enables seamless access to services within each country, but not between countries. Interfederation takes place when a user from one federation accesses a service that is registered in another federation. This is important as research, teaching and learning increasingly cross international boundaries. The vision, like physical networking (and the creation of the Internet itself), is to interconnect federations so that a user in one country can seamlessly access a service in another country using his or her home credentials.

The international research and education trust and identity community have chosen to use the European-based global eduGAIN service, which provides a lightweight technical and policy infrastructure to enable interfederation.[1] eduGAIN now includes 40 national research and education federations worldwide and can enable collaboration among 31 million individuals, 8 million of which are supported by InCommon.

In 2013, the InCommon Technical Advisory Committee (TAC) appointed two working groups to explore the requirements for interfederation.[2] Based on these working group reports, and recommendations from the InCommon Steering Committee and the InCommon TAC, Internet2 joined eduGAIN in April 2014 to facilitate interfederation and enable international collaboration. InCommon has conducted a pilot to develop a proposed technical implementation process. The eduGAIN Policy and Community Working Group (PCWG), commissioned by the InCommon Steering Committee, has recommended legal and policy changes to accommodate this new functionality.[3] The New Entities Working Group, charged by the InCommon Technical Advisory Committee, has recommended policies and practices related to interfederation, specifically accommodating entities from other federations appearing in InCommon metadata.[4]

The PCWG explored InCommon's interfederation participation using these guiding principles:

- International interfederation is a cornerstone of InCommon's support for U.S. research and education, and global collaboration.
- Individual participant organizations will retain control over whether they interact with international organizations.

---

[1] http://services.geant.net/edugain/About_eduGAIN/Pages/Home.aspx
[2] See https://spaces.internet2.edu/display/incinterfed/Interfederation+TAC+Subgroup and https://spaces.internet2.edu/display/incinterfed/Final+Report+to+TAC
[3] A summary of the working group's charge and a list of members is at the end of this paper.
[4] The New Entities Working Group has published its recommendations at https://spaces.internet2.edu/display/NewEntities/Home

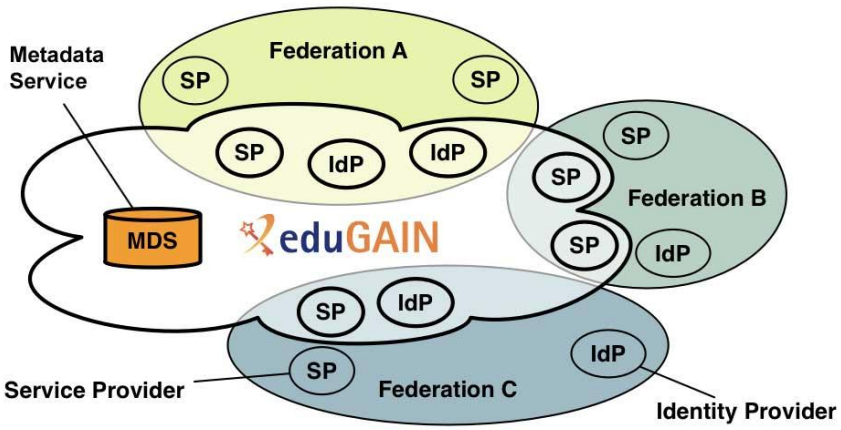
International Interfederation Service: eduGAIN

Operated by GÉANT, an organization that interconnects Europe's national research and education networks, eduGAIN now serves 40 national identity federations around the world, providing a common lightweight technical and policy infrastructure. Members of all of these federations have the potential to interact with one another. This ultimately allows a researcher to use credentials from his or her home organization and enjoy single sign-on convenience to resources offered through other national federations. Those InCommon Participants offering services via the federation (like a sponsored partner) can, if they choose, offer SSO convenience to international customers and colleagues.

eduGAIN enables the trustworthy exchange of identity information between federations. To join the service, each national federation must sign an unilateral declaration, be reviewed by its federation peers, and export all or part of its metadata information to eduGAIN (see the illustration below).[5] The eduGAIN service combines these files and republishes a signed aggregate file (following its technical and security procedures).

An eduGAIN member-federation imports the global metadata file, does any processing based on its policies and procedures, and publishes that metadata for the use of its members.[6]

The trust model of eduGAIN is simple: operators of IdPs or SPs must follow the policies, rules and legal structure of their home federations. Federations post their practices, in the form of a Metadata Registration Practice Statement, that others can review to determine eligibility, registration practices and other relevant details. It is important to note that not all eduGAIN



member federations register participant metadata in the same way as InCommon.

[5] A video overview of eduGAIN is also available: https://www.youtube.com/watch?v=x1YhuFPxMz8
[6] eduGAIN member federation registration practices: see: https://technical.edugain.org/status.php

InCommon in the Context of Interfederation

Interfederation will require changes for the InCommon Federation and may require changes for individual InCommon Participants. This section identifies and describes these changes and offers advice where appropriate.

Governance: InCommon has appointed a delegate and deputy to the eduGAIN Steering Group (eSG), which provides oversight and governance for the service. As part of the eSG, InCommon participates in discussions and adheres to decisions made on policy and technical matters, such as changes to the documents governing service capabilities, eligibility, technical requirements and dispute resolution. The service is stewarded by the eduGAIN Executive Committee (eEC), a group currently appointed by GÉANT.[7]

1. InCommon will report any relevant eduGAIN service changes to the InCommon Steering Committee, the Technical Advisory Committee and the Assurance Advisory Committee.
2. InCommon will also provide updates on interfederation to the community as necessary.

Transparency: Transparency is the basis for trust in eduGAIN, just as it is within the InCommon Federation. eduGAIN requires that federations post how they manage their metadata. InCommon publishes its Metadata Registration Practices Statement (MRPS) on its wiki and eduGAIN maintains a list of member federations and their respective MRPSs on its website.[8]

Policy Structure: InCommon Participants have signed the InCommon Participation Agreement and are bound by that document and its rules and practices (and the laws of the United States). Identity Providers and Service Providers from other countries are bound by the rules and practices of their home federations and laws of their countries.

3. InCommon will publish a list of questions that organizations should consider when making decisions relating to interfederating with international partners.[9]
4. Per the eduGAIN PCWG recommendation, InCommon will publish a policy outlining the data it collects about organizations participating in the federation and related identity provider and service provider contacts.
5. Interfederation with international partners required InCommon to revise the InCommon Participation Agreement. Participants should review these changes prior to February 11, 2016, when they take effect.

Dispute Resolution: If organizations from different federations have a dispute that they can't resolve, eduGAIN requires that the sites engage their national federations to manage the interactions. In this global dispute resolution process, InCommon will use best efforts to work with its participants, eduGAIN and other federations.

[7] The eduGAIN constitution is here: http://services.geant.net/edugain/Resources/Pages/Home.aspx
[8] InCommon's MRPS is at https://spaces.internet2.edu/x/nwvkAg. The list of eduGAIN federations and their MRPS are available at https://technical.edugain.org/status.php.
[9] https://www.incommon.org/eduGAIN

6. An InCommon Participant that has a dispute with an organization in another federation will follow the published InCommon dispute resolution process, outlined in the Federation Operating Policies and Practices (FOPP).[10]

Metadata Sharing: InCommon has always published its metadata aggregate publicly, as have many other research and education federations.[11] This metadata includes information required for interoperability, security, privacy and troubleshooting, such as identity and service provider URLs, organizational contacts, and public keys. Joining eduGAIN does not change this; it merely provides a common international clearinghouse and sharing mechanism for this information.[12]

InCommon will conform to the eduGAIN Metadata Profile, which defines rules for submitting metadata to the eduGAIN Metadata Service.[13]

7. InCommon will communicate how it will import and export metadata to and from eduGAIN.
8. Just as with current policy, organizations retain the ability to decide whether or not they will interact with partners.
9. InCommon strongly recommends that all identity providers and global service providers participate in international federation service. However, organizations can request not to do so.
10. InCommon will publish guidelines for implementing these local decisions.

Attribute Schema: The eduGAIN Attribute Profile recommends the user information to be included in attribute exchange.[14]

11. Like InCommon, eduGAIN uses the eduPerson schema. No further attribute schemas need to be supported.

Research and Scholarship Service Category: The Research and Scholarship (R&S) Service Category[15] includes Service Providers that support research and scholarship collaboration. Identity Providers can release a small set of attributes to the entire category of services. As additional services meet the qualifications of the category, researchers from campuses

[10]The InCommon dispute resolution process is described in section 8 of the FOPP (Federation Operating Policies and Practices), as referenced in section 5 of the InCommon Bylaws. Links to both documents, as well as the candidate drafts are at http://www.incommon.org/policies.html.
[11] https://www.incommon.org/federation/metadata.html
[12] To view the global services and identity providers that will be added to the InCommon metadata once interfederation is in production, see https://incommon.org/federation/info/all-entities-mdq-beta.html
[13] http://services.geant.net/edugain/Resources/Pages/Home.aspx
[14] http://services.geant.net/edugain/Resources/Pages/Home.aspx
[15] http://refeds.org/category/research-and-scholarship

supporting R&S can automatically access these new services. Through eduGAIN, InCommon Participants will have this same convenience of interaction with international R&S services.[16]

12. InCommon strongly encourages Identity Providers and qualifying Service Providers to participate in the global R&S program to streamline access to services.[17]

Other Categories and Services: InCommon will collaborate with other international federations in the creation of categories and services that benefit InCommon Participants and the global research and education community.

13. Any proposed new international categories or federation-level services will be reviewed by the InCommon community before implementation.

Implementation Approach and Timeline

Given the strategic nature of interfederation, the PCWG recommends that InCommon support the following approach:

14. By default, all InCommon Identity Providers will be included in the metadata exported to eduGAIN. Identity Provider operators will have the opportunity, through the Federation Manager, to choose *not* to include their metadata in the export.
15. By default, all InCommon Service Providers will *not* be included in the metadata exported to eduGAIN. Service Provider operators will have the opportunity, through the Federation Manager, to choose to include their metadata in the export.

Organizations still determine with whom they federate, and those that wish to restrict their federation partners to InCommon Participants can do so in their local configuration.

General Timeline and Transition Period

InCommon plans to complete the transition to full interfederation in the spring of 2016.

- InCommon will provide a series of communications and training sessions for both managers and implementers about the ramifications of interfederation and about planning for deployment.
- Once approved by InCommon Steering, InCommon will release the revised InCommon Participation Agreement and Federation Operator Policies and Practices, both of which go into effect 90 days after Steering approval. InCommon will conduct an extensive community outreach effort around the changes, answer questions, and take feedback.

[16] An overview of the InCommon R&S category is at https://spaces.internet2.edu/x/TYDwAg. For more detail, see https://spaces.internet2.edu/x/QIVHBQ
[17] To find out which InCommon Participants support global R&S, see https://incommon.org/federation/info/all-entity-categories.htm

Conclusion

The InCommon Federation was established to support scholarship, teaching and learning, and research. As these activities have evolved to transcend national boundaries, InCommon will become the national springboard to international partners to support these functions and to ease the friction of access for users. While federation and interfederation delivery will evolve over time, the first step towards this vision is to become full participating partners in eduGAIN.

Using this service places a number of requirements on InCommon and InCommon Participants. InCommon Steering and Technical Advisory Committees commissioned two community groups, the eduGAIN Policy and Community Working Group and the New Entities Working Group, to determine the policy and technical ramifications of this change. These two groups developed a set of recommendations that support this international vision while still enabling InCommon Participants to choose with whom to federate.

To help the community understand the impact on their organizations, InCommon will host calls, webinars and training sessions to help participants understand what they need to do to best support their organization and make a decision about interfederation.

Appendix A InCommon Working Groups and eduGAIN

Several working groups contributed to the recommendations in this draft, including two interfederation working groups led by Jim Basney (National Center for Supercomputing Applications) and Warren Anderson (LIGO). Many thanks for their time and attention.

eduGAIN Policy and Community Working Group

The InCommon Steering Committee chartered the eduGAIN Policy and Community Working Group (PCWG) to recommend a direction for InCommon's eduGAIN deployment and to review InCommon's key policy documents and identify changes needed to align with eduGAIN structure. The PCWG met during the first quarter of 2015 to discuss the trust model and key policy documents underlying the InCommon policy and technical infrastructure (the InCommon Participation Agreement and the Federation Operating Practices and Principles). The PCWG met during the first quarter of 2015 to discuss the trust model and key policy documents underlying the InCommon policy and technical infrastructure (the InCommon Participation Agreement and the Federation Operating Practices and Principles).

Working Group members:

Warren Anderson, LIGO
Donald Beck, Davidson County Community College
Susan Blair, University of Florida
Steven Carmody, Brown University and InCommon Technical Advisory Committee
Chris Holmes, Baylor University and InCommon Steering
Craig Jackson, Indiana University
John Krienke, Internet2
Tracy Mitrano, Cornell University
Theresa Semmens, Chair, North Dakota State University
Von Welch, Center for Applied Security Research
Ann West, Internet2
Bill Yock, University of Washington and InCommon Steering

New Entities Working Group

Up until now, the InCommon metadata file contains only Identity Providers and Service Providers (entities) owned and managed by, either directly or indirectly, an InCommon participant. The InCommon Technical Advisory Committee chartered the New Entities Working Group to review how the Federation should include international metadata and other identity and service providers with unusual requirements. The appearance of these new types of entities within the InCommon metadata file will create new risk scenarios for current InCommon members. The mission of this Working Group was to identify what an IdP or SP operator would need to know about policies or practices associated with such entities. The Working Group met during late 2014 and the first part of 2015 to complete its work.

Working Group members:

Jim Jokl, Chair, University of Virginia
Warren Anderson, LIGO
Steve Carmody, Brown University and InCommon TAC
Steve Devoti, University of Wisconsin-Madison
Tom Golson, Texas A&M University
Eric Goodman, University of California Office of the President
Ken Gray, University of Michigan
Michael Hodges, University of Hawaii
Scott Koranda, LIGO
Steve Olshansky, The Internet Society
Tom Scavo, Internet2
Mark Scheible, MCNC
David Walker, Internet2
Keith Wessel, University of Illinois