Introduction

The purpose of this report is to facilitate a decision by the InCommon Steering Committee to understand the value, risks, and responsibilities of joining the international community in the eduGAIN service.

What is eduGAIN?

EduGAIN is a service based in the EU that allows participating R&E federations to exchange metadata of IdPs and SPs to ease the cost and increase the interoperability among common partners and collaborations. European national R&E federations founded eduGAIN through the GÉANT consortium, where its governance continues to reside.

Additional introductory materials include:

- A brief, four minute YouTube video:
- The eduGAIN website:

The eduGAIN service is governed by an Executive Committee, today synonymous with the project's original sponsor, the GÉANT Executive Board. Together with a Steering Group comprising representatives from the federations who have signed the eduGAIN Declaration, maintain, a framework of policies comprising the **eduGAIN Policy Framework**, which consists of three required and three optional documents**:**

1. Declaration (required)
2. Constitution (required)
3. Metadata Profile (required)
4. Attribute Profile (optional)
5. GÉANT Data Protection Code of Conduct (optional)
6. SAML 2.0 WebSSO Profile (optional)

There are no fees to participate in eduGAIN. Member federations unilaterally sign a copy of the Declaration and comply with the requirements listed in the Constitution and Metadata Profile prior to exchanging metadata.

Why should InCommon join?

In order to support international collaborations in research and education that are critical to its participant institutions, InCommon seeks a scalable, trusted means to interfederate with its peer R&E federations. Today, if an organization wishes to federate across national boundaries, it must join every national federation in which its partner organizations reside. This is not practical at scale and is particularly difficult for virtual scientific collaborations without the resources to navigate each nation's diverse legal, technical, and policy idiosyncrasies.

Of the various alternatives, interfederating by joining eduGAIN is, today, the most scalable and expedient method to serve our InCommon participant community. By exchanging metadata about our participants' identity provider and service provider systems, InCommon will facilitate a more scalable approach to federation, eliminating the need for a given organization to join all of the nationally based R&E federations through which it has active partnerships.

It is also consistent with our mission as written in the InCommon charter:

> to facilitate collaboration through the sharing of protected network-accessible resources by means of an agreed upon trust fabric;

The International Community

If eduGAIN can be considered the service organization of interfederation, REFEDs – the Research and Education Federation consortium – is the community gathering place for discussing shared goals of R&E federations worldwide. InCommon is already an active participant in REFEDs discussions and work plans. The two organizations are complementary to our progress: eduGAIN the service and REFEDs the meeting place to share and develop common practice and policy.

Decisions

It may be overly simplistic to generalize the many complex policy and technical decisions into three categories, but for the sake of making measurable progress on this complex undertaking, three general decision areas can be proposed for Steering's consideration:

1. Should InCommon sign the eduGAIN declaration, signaling our intent to exchange metadata?
2. What are our responsibilities, risks and rules for *importing and exporting* eduGAIN metadata into InCommon?
3. Do we need to make modifications to our Participation Agreement and FOPP prior to signing the Declaration or after signing? Which Steering advisory or subcommittee should take on this task?

InCommon Community Reviews eduGAIN

InCommon participants and staff have been discussing these questions actively for a little over a year.

Community Process

We began discussions and a pilot in earnest through an open TAC subcommittee chaired by TAC member Jim Basney of the National Center for Supercomputing Applications (NCSA) at UIUC. The subcommittee released its Phase 1 recommendations to the TAC and Participants at the end of June 2013.

The Phase 1 group successfully piloted interfederation for LIGO partnerships between the US and EU, with a set of recommendations, chief among them, to pursue joining eduGAIN as the primary means of international interfederation. Final Phase 1 Recommendations: https://spaces.internet2.edu/x/Dw9OAg

Issues discussed included the working pilot, the size of a combined metadata aggregate, metadata aggregation tools, opt in versus opt out participation, the EU code of conduct for services receiving personally identifiable information, and federation registration and trust practices.

At the TAC's request, a new interfederation subcommittee took up the Phase 1 Recommendations, chaired by Warren Anderson of LIGO. The working group reviewed the declaration, constitution, and metadata profile from eduGAIN, as did Internet2's legal office. The working group recommends that InCommon sign the eduGAIN declaration. After some discussion, the TAC approved accepting the report and its recommendations; it asked the TAC chair to send the report to Steering accompanied by its strong support for signing the eduGAIN declaration.
This final report is available attached as an appendix and on the working group's website < https://spaces.internet2.edu/x/NYPPAg>.

Legal Review

Signing the Declaration

Signing the declaration is the first step to interfederating through eduGAIN.

Based on the following provisions, our legal review advised that signing the Declaration would create no new legal obligations or rights (section 9), nor is there any financial consideration (section 12) that creates a binding contract. Each federation is simply signing a one-sided declaration that is not countersigned by another party, but is submitted to eduGAIN as evidence. From the Declaration:

> 9. Neither the existence of this declaration, nor the exchange of information enabled by it, shall create any new legal obligations or rights between Members or operators of any federation. Members and operators remain bound only by their own respective laws and jurisdictions.
>
> 10. In particular this declaration creates no rights of membership, nor of access to services, between Members of any federation.
>
> 12. No financial consideration will be expected between the Federation and other Participating Federations as federation operators and any financial consideration between Members or Members and operators is outside the scope of this declaration.

Since there is no bi-lateral agreement and no consideration, there is little concern in signing the Declaration from the perspective of contract law.

Next Step: Putting Import and Export Into Practice

The more significant issues arise when looking at the limits of our own Participation Agreement related to international data transfer beyond InCommon participants.

To put the risk in context, eduGAIN provides no guarantees about communication, timeliness, or the veracity of other federations' metadata. It is up to individual federations to police their members' accurate metadata – and no common standard for verifying metadata yet exists. If something bad happens, InCommon is protected from external organizations by some measure, in the eduGAIN Declaration:

> 8. In particular any complaint about a Member shall be made to the operator of its Participating Federation and dealt with between that Member and that operator according to the rules of that Participating Federation and subject only to that Participating Federation's governing law and jurisdiction.

However, while there are some protections from international organizations coming after InCommon as a result of a problem related to sharing metadata, our own InCommon participants might have take issue with us sharing their IdP or SP metadata with non-InCommon organizations.

Two sections of the InCommon Participation Agreement may imply constraints on international metadata exchange. First, section 7.b. may imply that InCommon only provides *Participant* metadata and does not import any non-Participant metadata that has not been "registered" with InCommon. Second, sections 7.b. and 9 also may imply that we share participant metadata only with other InCommon participants, even though InCommon metadata has always been publicly available.

> ***Section 7.b. Participant Metadata***
> *InCommon will use reasonable efforts to* ***provide*** *periodically to Participant composite metadata describing all Higher Education systems and Sponsored Partner systems that have been* ***registered with InCommon.*** *THIS METADATA IS PROVIDED ON A BEST EFFORT BASIS AND IS NOT WARRANTED NOR GUARANTEED TO BE COMPLETE, CORRECT, OR FIT FOR ANY PARTICULAR PURPOSE. PARTICIPANT CONSENTS TO INCOMMON* ***SHARING*** *PARTICIPANT'S METADATA* ***WITH OTHER INCOMMON PARTICIPANTS.***
>
> ***Section 9. Respect for Privacy of Identity Information***
> *Participant agrees to respect the privacy of and any other constraints placed on identity information that it might receive from other InCommon Participants as agreed upon between Participant and the InCommon Participant(s). In particular, Participant understands that it may not permanently store nor share or disclose or use for any purpose other than its intended purpose any identity information that it receives from another InCommon Participant without express written permission of the other InCommon Participant.* ***Participant understands that the storing and sharing of resources is between the Participant and the InCommon Participant(s)*** *and is not the responsibility of InCommon.*

We could choose to augment the provisions in the legal agreement to be crystal clear about how we share metadata and provide metadata to our participants. A modification to each agreement requires permission, *unless* a policy by the Steering Committee necessitates the change:

> ***Section 17. Modification***
> *This Agreement may be modified only by written consent of the Parties; provided, however, that* ***InCommon retains the right to amend this Agreement unilaterally to conform to any modifications made by InCommon to its policies if so approved by the InCommon Steering Committee.*** *Any such unilateral changes shall be presented to Participant at least ninety (90) days before they are to take effect, and InCommon will work in good faith with Participant to negotiate and resolve any issues raised by such changes that may be of concern to Participant. Each participant's continued participation in InCommon after the change takes effect will constitute its continuing agreement to this Agreement as so modified. Each participant, including Participant, has the right to terminate this Agreement if it is modified in any way that is not acceptable to the Participant.*

We have initial feedback from our attorneys – separate from this document – as to recommended modifications in the FOPP and PA. Modifications to these documents can be worked through with Steering before or after the signing of the Declaration.

Near Term Issues to Work Through

Steering may recommend that InCommon staff work with a group such as the TAC or a subcommittee of Steering on each of the following:

- Will we need to make modifications to the Participant Agreement and policy FOPP prior to implementation? How will we involve or give notice to participants? Steering approves material changes to these official documents.
- Will we export all entity metadata or some subset, and if a subset, what will the rules for the filtering be? Will we use opt-in, or opt-out?
- Will we import only a subset of eduGAIN metadata?
- Will we aggregate eduGAIN metadata into our own InCommon metadata aggregate, or will we create a second aggregate that is combination of InCommon and eduGAIN metadata?
- How will we encourage InCommon SPs to comply with the EU Code of Conduct, to allow EU IdPs to release attributes? How will we encode this compliance to make it technically feasible to determine at run time?
- EU Data Privacy laws define PII much more narrowly. For example, anything that can be reasonably linked to an individual and used to identify an individual is defined as PII. The VIN number for a car would be deemed PII under the EU directive because it can be reasonably linked to the name of a resident in their home location. InCommon metadata contains contact information for technical, administrative, or support contacts at organizations. We recommend the use of group email aliases, but there remain individuals' names and emails in the metadata aggregate. Our attorney consulted with EU colleagues and reported that as long as the

export of this name and email information is necessary to fulfill and facilitate the data transaction, it's acceptable.
- From a US standpoint there are no problems with PII related to EU metadata and US import laws.
- Communicating the caveat emptor to our participants about what we are and aren't providing via eduGAIN.
- Creating the technical means by which to import other metadata aggregates into some combined InCommon/eduGAIN set, and to filter and export a metadata aggregate to eduGAIN.

Some recommendations for the above points have already been discussed by the Interfederation subcommittees.

Longer Term Issues

- Governance evolution from GÉANT alone to a more internationally representative body.
- Continued alignment on metadata security and trust practices, levels of identity assurance, tagging of entity metadata, etc.
- Piloting other techniques than aggregation for the scalability of metadata exchange.
- Other?

Final Report of the Interfederation Working Group

This iteration of the Interfederation Working Group spanned approximately six months time, from the end of October 2013 through the end of March 2014.

Executive Summary

The Interfederation Working Group makes the following specific recommendations to TAC:

1. InCommon should sign the eduGAIN Declaration as soon as possible
2. TAC should work with Ops to operationalize eduGAIN over the next six months
3. TAC should instantiate a new working group with a charter based on the Future Work items listed below

Work Summary

We began our work with the following set of deliverables, derived from the recommendations of the first iteration of this working group:

1. Review international interfederation agreements with eduGAIN and UK federation.
2. Document trust practices and policies for entity registration and publishing.
3. Review and adopt the US-EU Code of Conduct to address privacy and attribute release.
4. Review and assist in the implementation of improvements and new capabilities for metadata management/publication/aggregation/tagging.
5. Establish practices and policies for domestic interfederation.

We made the following progress toward these deliverables:

1. Review international interfederation agreements with eduGAIN and UK federation.
   - Reviewed eduGAIN Policy Framework to better understand the implications of InCommon joining eduGAIN.
   - The outcomes of that review are documented at eduGAIN Policy Framework notes.
   - Provided specific recommendation to the TAC regarding the signing of eduGAIN Declaration.
2. Document trust practices and policies for entity registration and publishing.
   - Some general discussion of trust practices and policies for entity registration and publishing are found in our notes on eduGAIN Policy Framework notes. However, there is still considerable work to be done here. Foremost is the creation of a Metadata Registration Practice Statement, which is required for active participation in eduGAIN.

3. Review and adopt the US-EU Code of Conduct to address privacy and attribute release.
    - We note that the international version of the EU Code of Conduct is not finalized at this time, so progress was limited.
    - However, we did discuss some technical aspects of the proposed EU Code of Conduct, as indicated in the document CoC FedOp Perspective.
    - Further review and discussion will be needed when the Code of Conduct is finalized.
4. Review and assist in the implementation of improvements and new capabilities for metadata management/publication/aggregation/tagging.
    - In the context of interfederation, this is essentially the operationalization of the trust practices and policies outlined in item b. This is an area for follow-on work.
5. Establish practices and policies for domestic interfederation.
    - Pilot projects for domestic interfederation are still in the works, so limited progress was made.
    - While it falls short of establishing practices and policies, the committee did provide a forum to inform regional providers looking to interfederate with InCommon (IdP and Metadata Best Practices) through a series of two telecons devoted to that subject.

Future Work

The Interfederation Working Group hereby recommends to the TAC that there be another iteration of the working group with the following charter:

1. Aid in the production of an InCommon Metadata Registration Practice Statement that will suitably satisfy the requirements of eduGAIN.
2. Provide options and recommendations for aligning current practices with eduGAIN requirements.
3. Assist in operationalizing eduGAIN requirements in metadata registration/aggregation/tagging practices.
4. Monitor progress of regional federation and The Quilt/InCommon pilot programs in preparation to assist in regional interfederation.
5. Monitor progress of International EU Code of Conduct in order to provide feedback to InCommon on its policy and operational ramifications.

We recommend the charter again span a six-month time period.