






Document Title: Formalizing the Role of Federation Proxies within the InCommon Federation

Document Repository ID: TI.169.1

DOI: 10.26869/TI.169.1

Persistent URL: <http://doi.org/10.26869/TI.169.1>

Authors:

- Tom Barton, independent consultant,  <https://orcid.org/0000-0003-1878-3448>
- Ken Klingenstein, Internet2,  <https://orcid.org/0000-0003-3182-4566>
- Mark Rank, Cirrus Identity,  <https://orcid.org/0000-0001-8930-9247>
- David Walker, independent consultant,  <https://orcid.org/0000-0003-2540-0644>
- Albert Wu, Internet2  <https://orcid.org/0000-0001-7570-0923>

Publication Date: June 2023

Sponsor: InCommon Technical Advisory Committee

Formalizing the Role of Federation Proxies within the InCommon Federation

(June 2, 2023)

Introduction

In early 2022, the InCommon Technical Advisory Committee (TAC) considered a collection of opportunities and threats related to identity federation in research and education for deeper study. Of these, the topic of federation proxies (FPs)¹ rose to the top, primarily when used for the benefit of service providers (SPs)², and an *ad hoc* group of community members was convened to study the issue. Other issues that were considered included pending changes to web browser behavior, alternative federation technologies (e.g., OIDC, Verifiable Credentials), campus IT challenges, the impact of sub-optimal software deployments, etc. FPs were chosen for the initial study, as they provide great benefits but also have potential challenges.

The group's early work has already been described in "Framing a Discussion to Foster SP Middlething Deployments"³. In this final report of the *ad hoc* group, we provide a synopsis of what we have learned, followed by a short list of proposed actions for InCommon to enhance its service offerings, as well as to modify its governing policies and cost recovery model.

This is an issue that is growing in importance and should be addressed within the medium term as part of InCommon's planning horizon.

What We Have Learned

The past 15+ years of R&E federation have revealed use cases for FPs that benefit research service providers⁴, exemplified by CILogon⁵ in the US and multiple other academic FPs worldwide. As has been observed in "Federated Identity Management for Research Collaborations version 2"⁶ (FIM4R) and "Academic Interfederation into the 2030s,"⁷ FPs have succeeded by relieving service providers of some of the burdens of federation participation, thereby greatly expanding the reach of federation. In particular, FPs facilitate the integration of service providers into the federation by mediating the

¹ Federation Proxy. A component that acts as a logical RP to a set of IdPs and a logical IdP to a set of RPs, bridging the two systems with a single component. These are sometimes referred to as "brokers." [NIST SP 800-63-4 ipd, *Digital Identity Guidelines - Initial Public Draft*, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-4.ipd.pdf>, p. 51]

² Called *Relying Parties (RPs)* in NIST SP 800-63-4.

³ See [Appendix: Earlier Work](#) in this document.

⁴ There are also benefits to identity providers, but our charge is focused on service providers.

⁵ <https://www.cilogon.org>

⁶ <http://doi.org/10.5281/zenodo.1296031>

⁷ <https://doi.org/10.5281/zenodo.6584586>

exchange of identity information between their *mediated service providers*⁸ and federation identity providers (IdPs) to offer:

- protocol normalization and translation to achieve interoperability,
- enhanced user information for use within collaborations and communities of interest,
- management of access and other policies, and
- integration of multiple service providers into a single meta-service, avoiding the need to federate each service.

FPs also present potential challenges, as they are middlethings between IdPs and their mediated SPs, creating a new trust relationship between IdP and mediated SP. This is potentially concerning when the FP does not share the academic community's mission. These potential concerns include:

- creation of an operational relationship outside of established federation trust agreements,
- lack of transparency of the handling of user attributes by FPs,
- lack of transparency of the nature and number of mediated SPs,
- misalignment among InCommon Participants⁹ (including FP operators), which have agreed to federation policies and processes, and mediated SPs that may not have agreed to them,
- impacts on user experience,
- shifts in support responsibilities among IdPs, mediated SPs, FPs, and the federation operator, and
- potential undermining of the federation's business model.

FPs that may warrant attention will have one or more of the following properties:

- They onboard mediated SPs that otherwise would need their own membership agreement with InCommon.
- They enable a mission not entirely aligned with that of the Academy¹⁰.
- They profit monetarily by selling their service.
- Their mediated SPs do not share the same requirements for identity attributes and thus data minimization may not be realized.
- They do not provide transparency of the mediated SPs available to current and prospective InCommon Participants.

SPs that invoke 3rd party services as part of their own service offering would not generally be considered to be FPs. For example, a service that embeds YouTube to display visualizations of climate change would not be considered a FP.

⁸ Mediated service providers are service providers that utilize a FP.

⁹ An InCommon Federation member institution is called a Participant. All Participants have executed the [InCommon Participation Agreement](#).

¹⁰ By "Academy," we mean the extended community of institutions of higher education and research.

Insights

Our work provided us with valuable insights:

1. The above concerns of FPs are not related to technology. They focus on alignment of the mission enabled by a FP with that of the Academy. Science proxies, such as CILogon, are well aligned with InCommon's academic mission, but we are starting to see more commercially-aligned FPs which may warrant the creation of policies, processes, or guidance outside of the current form of agreements InCommon has with its registered SPs and IdPs.
2. FPs have become a common architectural paradigm for the integration of mediated SPs used by research projects and other consortia into the federation, particularly in the sciences. "Federated Identity Management for Research Collaborations version 2"¹¹ (FIM4R) assessed the needs of this paradigm. The Authentication and Authorisation for Research Collaborations project¹² (AARC) established general policies and technical architecture (the AARC Blueprint) for the use of such FPs.
3. The EU research community has considerable experience with FPs for science. There are funded projects to further develop their architecture and define standards to enable consistent implementations. There are multiple mature deployments. CILogon is an AARC Blueprint implementation.
4. Greater awareness of the academic value of specific mediated SPs would help many current and prospective InCommon IdP operators justify continued support for R&E federation.

Recommended Actions

FPs are not new. The FIM4R group described elements of what makes up an FP in its first paper in 2012. These needs were further refined and expanded in FIM4R's second paper in 2018. The European Commission has funded the AARC project for years.

The existing guidance is primarily technological, however. It is time for InCommon to provide guidance on policy issues to foster trust and support access controls. For example, many FPs add and/or modify attributes; good practice suggestions about the use of attributes, groups, entitlements, useful schema, *etc.* are needed.

This will likely require communications strategies that reach beyond InCommon's common focus of central IT organizations to researchers, libraries, and other academic functions and disciplines. Also, government funding agencies, as well as non-government funders, such as Mellon and Sloan, are often unfamiliar with the issues surrounding FPs. Nurturing an ongoing relationship between InCommon and these cohorts would benefit all.

Our specific recommendations follow.

¹¹ <http://doi.org/10.5281/zenodo.1296031>

¹² <http://aarc-project.eu/>

The Federation should enhance its policies and agreements to address specific concerns that attach to FPs.

The current federation trust model assumes direct, secure communication between an IdP and an SP. An FP's purpose is to mediate; it translates, transforms, and/or enhances the assertions forwarded from IdPs to mediated SPs. Therefore, there cannot be direct communication between IdPs and mediated SPs. For this reason, agreements and guidelines should be enhanced or established for these mediators. These should include the following:

- protection of the federation's values, its Participants, and the federation itself,
- operation of the FP with sufficient due care (confidentiality, integrity, availability, and privacy),
- appropriate use of identity information,
- responsibilities for incident response and other operational issues
- transparency of the specific functions performed as part of its mediation of assertions (as appropriate),
- transparency of existence of the FP's mediated SPs (as appropriate), and
- transparency of the organization(s) responsible for administering the proxy and its mediated SPs.

When formulating these policies, the following issues should be considered:

- An FP's purpose matters. Policies, and enforcement of policies, should avoid constraining an FP's operation when its purpose aligns with the federation's purpose to support research and education.
- When an FP's mediated service providers are part of the same management domain as the FP, have joined the federation, or have otherwise agreed to the federation's policies, we believe no additional policy language is required. When this is not the case, we believe the creation of a new type of entity, FP, is warranted to describe its dual role as an IdP facing its mediated SPs and an SP facing the rest of the federation.
- Transparency items may require deployment of a mechanism for documenting federated services. A current example is the list of Science Gateways¹³ maintained by the Science Gateways Community Institute. This mechanism will need to accommodate the reality that some mediated services are proxied in a self-serve fashion and their proxy operators are not aware.
- Consideration and respect for the international scale of operation of some FPs.

InCommon should expand its documentation of best practices for IdPs and SPs to include FPs.

Advice for IdPs and SPs, of course, already applies to FPs, but there are nuances in the area of operational handoffs, user experience, *etc.* that should be documented. This will require adoption of more precise vocabulary for articulating major concepts, components, and interactions. If we don't have the words to describe an issue, it's hard to address that issue.

¹³ <https://catalog.sciencegateways.org/>

InCommon should consider a modified fee structure for cost-sharing with FPs.

An FP has the potential to impact InCommon's business model by acting as an aggregator enabling a significant number of its clients, as mediated service providers, to benefit from being a part of InCommon without joining InCommon directly. This can negatively impact InCommon revenue and should be mitigated in InCommon's fee structure.

Appendix: Earlier Work

The study group's first goal was to frame and facilitate a discussion of FPs during a session at the December, 2022 Internet2 Technology Exchange. We started this process by examining some case studies with which the group members had some familiarity. We also interviewed Jim Basney, the person behind CILogon, the preeminent federation proxy supporting research in the US.

The result of that work has been reported in "Framing a Discussion to Foster SP Middlething Deployments"¹⁴. It was distributed in advance of the Technology Exchange session to frame that discussion. It described the use cases we had examined:

- EDUCAUSE's federated login platform,
- CILogon,
- academic journal publishing platforms (e.g., Elsevier, Highwire Press, SilverChair), and
- domain-specific research gateways,

as well as the potential challenges mentioned above. The document then raised a number of questions, both general and in the following specific areas:

- federation trust,
- effort required for participation and operation,
- user experience, and
- implementation guidance.

¹⁴ <http://doi.org/10.26869/TL.168.1>