

Interfederation Use Cases

- [LIGO](#)
- [NIH](#)
- [K-12](#)
- [University federations](#)
- [InCommon Member Publishing Journal with Intl Subscriptions](#)
- [State Agencies](#)
- [Federated Wireless](#)
- [TERENA Service Provider Proxy](#)
- [Internet2 Spaces Wiki](#)
- [Shibboleth Project Services](#)

The [Interfederation TAC Subgroup](#) is using this page to document use cases for interfederation. All are welcome to contribute.

LIGO

[LIGO](#) (an InCommon Federation member) seeks to enable federated access to LIGO operated service providers including wikis, document catalogs, event databases, and data investigation tools for LIGO collaborators from across five continents, including collaborators from interferometric gravitational wave experiments and organizations including the European Gravitational Observatory ([EGO](#)), responsible for the computing and networking for the Virgo (French and Italian) interferometer experiment, and KAGRA (Japan). Today the federations that either intersect directly with LIGO membership or with existing and possible LIGO collaborators includes:

- Australian Access Federation (AAF)
- Canadian Access Federation (CAF)
- DFN-AAI (Germany)
- Fédération Éducation-Recherche (France)
- eduID.hu (Hungary)
- IDEM (Italy)
- GakuNin (Japan)
- SURFnet (Netherlands)
- UK Access Management Federation for Education and Research
- INFED (India)

NIH

Here's a summary from Christopher Whalen, International Program Manager at the Office of CyberInfrastructure and Computational Biology, National Institute of Allergy and Infectious Diseases, NIH:

The institution that we work with is the National Institute for Research in Tuberculosis in Chennai. They have about 200 users though we work with about 50 of them on the International Center for Excellence in Research (ICER) and through that collaboration support their Active Directory infrastructure. We would like to move to the federated approach for managing this instead of creating accounts for them here at the NIH when they need to access resources (like SharePoint) here. In addition, like the ICERs in Uganda and Mali, we are also helping them build their own portals for collaboration there which will leverage the federated relationships for broader data sharing and collaboration for projects involving multiple sponsors and collaborators.

In the case of India we thought that it would be best for us to use a domestic federating group instead of the approach we used in Mali and Uganda. Mostly because these are collaborative relationships and we want to use whatever domestic resources are available. In sub-Saharan Africa that means not much, but in India we expected to be able to partner with an institution to provide this functionality.

K-12

Use case is the use of Regionals (REN/RON providers) to extend Federation Services to their constituents - in this case K-12. One of the options would be to interfederate, another might be to use the Metadata Aggregator for local federation entities and following a model similar to eduGAIN sending a subset of metadata upstream to InCommon.

Biggest concern is the scaling of federation to K-12, Community College systems, other Community Anchor Institutions (CAIs) like healthcare, libraries, public safety, etc. Looking for a better federation model to handle metadata.

A specific use case is the Virginia Tech summer camps.

University federations

University systems may establish their own federations that then need to inter-operate with InCommon (examples: [UT System](#), [UCTrust](#)). What are the pros and cons to establishing a separate federation versus using InCommon directly?

InCommon Member Publishing Journal with Intl Subscriptions

This use case doesn't require subscriber identities, just license info ("entitlement", "unscoped-affiliation" and "affiliation") per the [COUNTER Code of Practice](#). Example (<http://www.ciaonet.org/>) provided by Alan Crosswell (Columbia). Encountering obstacles due to EU personal data protection.

State Agencies

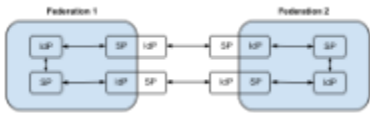
From Feb 22 2013 InCommon TAC update:
Marc Jones: interfederation with state agencies
Scott Cantor: and more broadly just other verticals in general, but my guess is we'll hit profound trust model differences moving beyond higher ed

Federated Wireless

eduroam is a powerful example of federation deployed internationally for a single application (wireless network roaming). The [eduroam Configuration Assistant Tool](#) is a SAML SP in eduGAIN that allows eduroam administrators to log in and configure custom installers for their local eduroam users.

TERENA Service Provider Proxy

The [TERENA SP Proxy](#) is an SP registered with InCommon and many other federations for international access to TERENA services including the [REFEDS wiki](#). See the InCommon's info page for the [TERENA Secretariat](#).



This use case shows that proxies or gateways can be used to expose services in one federation to users in another federation (and vice versa). In fact, TERENA has joined numerous federations and set up its SP Proxy at the border of each. The most onerous byproduct of this approach is having to separately manage metadata in each federation. If TERENA could manage one set of metadata centrally (say, in the [REFEDS PEER instance](#)), that would be a huge win.

Internet2 Spaces Wiki

The Internet2 Spaces Wiki (i.e., spaces.at.internet2.edu - where this page is located) is another example of an SP registered separately in many federations to support international collaboration. We can learn from that experience.

Shibboleth Project Services

The [Shibboleth Project Services](#) (wiki, issue tracking) are registered in multiple federations to support international authentication. The project's goal is to offer as widespread a set of options as we can, given our technical and legal constraints.

Like with many smaller projects, it's simply infeasible to execute the legal machinery required to register in every federation out there. As a technical matter, the disparate ways metadata is managed is definitely a barrier. The lack of uniformity is a bigger problem to me than the manual effort. And lastly, we need federations to stop requiring custom certificates if they're going to seriously claim they support the well-known key trust model.

The assurance goals of the project services are very modest, but we feel the need to take certain steps to ensure that the identities of the core project team can't be faked. To that end, we need identifiers with some kind of well-understood namespace management binding them to IdPs, and the ability to filter that (so scope filtering is crucial). We might even feel the need to go so far as to manually apply filtering rules that limit the scopes of project participants to their "known" IdPs. I can probably be safe in assuming that osu.edu would never show up in any federation's metadata, but I don't know if it's worth taking the chance.

We do support eduPersonTargetedID, but I would not make that choice again for services like we offer. Public attribution is the main reason we need logins at all.

We also prevent, where possible, the updating of display name fields in our applications by IdPs known to provide self-asserted values in those attributes. I think we'd be interested in exploring a way to automate that, so I suppose that's an attribute assurance use case. This is where 800-63 is too heavy, but "nothing" is too light. There's a big gap between nothing, and the typical practices at most organizations.

I highlight these issues as relevant to interfederation, because the expanded set of IdPs and different practices one encounters becomes a bigger consideration as you scale up and out.

File	Modified
PNG File The_TERENA_Use_Case.png	Jan 30, 2013 by trscavo@internet2.edu