Federation Soup

June 2-4, 2008
Seattle, Washington

Summary

In many countries, a single federation at the national level provides all R&E trust services. In other countries, notably the U.S., multiple federations have formed, along natural relationships, including a national higher education federation but also state university system federations, state-wide educational agencies and regional optical networks. Together, this soup of federations needs mechanisms to create a larger trust fabric, and that theme served as the backdrop for this meeting.

In some instances, particularly internationally, federations are beginning to overlap. Major service providers such as Elsevier and Microsoft, belong to multiple federations. Other approaches, for both Identity Providers (IdPs) and Service Providers (SPs), are being explored to find some other way to form partnerships between members of different federations. As a result, federations are considering interfederating – entering into agreements with one-another, allowing members to access resources from SPs or IdPs associated with either multiple federations.

Interfederation will only work if federations collaborate and cooperate in a number of areas, including:

- **Levels of Assurance** – Creating/negotiating common requirements for identity proofing, authentication, and delivery of credentials
- **Trust Relationship** – Developing methods for a federation to accept the trust established through another federation.
- **Attributes** – Agreeing on the use and meaning of attributes to successfully interfederate.
- **Privacy and Personally Identifiable Information (PII)** – working out when and how the PII rules in one federation can be met by a peering federation.

Each federation can enhance its ability to interfederate by keeping its legal and policy agreements as simple as possible while meeting member's expectations. In addition, at this early stage in our development, it is important for federations to emphasize core competencies, while being alert to new opportunities to add value for its members.

Interfederation would provide the next step toward coherent and widely trusted Internet identity, with users identity-proofed by some trusted organization that is in turn federated, and interacting with many resource providers in a variety of ways.

1. The Need for Interfederation

While federations typically follow national boundaries, the desire for collaboration and providing services crosses any boundary. Some Service Providers, for example, work with colleges and universities from more than one country. Such SPs often belong to multiple federations. These SPs tend to be technically sophisticated and have the budget and staff to manage all of the legal and policy considerations for each federation. Microsoft, for example, joined several federations as it leveraged access to its DreamSpark offer.

IdPs also see a need to join more than one federation or find some other way to interact with members of other federations. For example:

- Microsoft is not a member of the Texas federation, and some of the Texas IdPs are not members of the U.S. HE federation, InCommon. As such, members of the Texas federation did not have federated access to DreamSpark.

- Because of their research activity, some U.S. IdPs are being sought as potential members of the U.K. federation so that US campus researchers are permitted to access UK wikis, etc. Some university presses are considering joining the U.K. federation as SPs. These efforts are complicated by the differing privacy regulations between the U.S. and U.K. and the differences in the trust agreements used in the U.K. federation and in InCommon.

- Virtual organizations (VOs), involving researchers and others from different countries (and, hence, different federations), would like access to resources at a variety of VO sites. The VOs expect their campus credentials from one federation to be accepted by another, even though there may be inconsistent or incompatible methods for trust and identity proofing.

- In the U.S., online interaction among universities and federal agencies (such as NIH and NSF) has prompted some agencies to join InCommon. Interfederation between InCommon and the federal eAuth effort continues to be a possibility.

R&E interfederation efforts may also need to consider how users that are not affiliated with a traditional IdP (like a university) can gain access. In the U.S., for example, only those associated with higher education, and certain other related institutions, can benefit from the InCommon federation; individuals not associated with one of those organizations won't have credentials recognized by InCommon participants. Other use cases, including citizen-to-government interactions, are becoming increasingly popular, and may drive other interfederating within a country.

2. Interfederation Issues

Upon joining a federation, an SP or IdP agrees to the requisite trust and policy arrangements. While these agreements may be similar at different federations, they are not identical nor even structurally comparable. Federations must comply with relevant laws or regulations, such as those in the area of privacy, which differ from country to country.

Many of the barriers to interfederation have to do with policy and legal matters. In general, federations will need to exchange information about their governance and organizational approaches, understand one-another's business models, and understand legal and privacy issues that will differ from country to country.

Some of these issues include:

- **Levels of Assurance** – Creating/negotiating comparable requirements for identity proofing at different levels of assurance (such as NIST levels 1-4 and InCommon Bronze and Silver).
- **Trust Relationship** – The federation acts as the trusted third party for the organizations within its scope/community. Interfederation will require members of a federation to understand to what degree they accept the trust established through a user's own federation.
- **Attributes** –To be successful and useful, attribute definition must be a community activity within a federation. In turn, federations must agree on the use and meaning of common attributes to successfully interfederate.
- **Privacy and Personally Identifiable Information (PII)** – Privacy regulations and rules for handling personal information differ among countries and the European Union.
- **Business Models** – Federations may recover operating costs in different ways that could impact interfederation agreements. For example, one federation might have fees based on transactions and another doesn't or has different rates. A federation might contract for services on behalf of its members and find it difficult to convey this privilege to members of another federation.

Levels of Assurance

Negotiating common identity proofing requirements for different levels of assurance (or assurance profiles) will help the interfederating process. Federations will need to agree on requirements for identity proofing at different assurance levels, as well as the types of audits that will be required of identity management systems. Fortunately, many federations have adopted the NIST guidelines and that produces rough compatibility. One gap is the lack of specification on federations operations (identity proofing its enterprise members, protecting the federation metadata signing key, etc.) that would be a part of any end-end trust mechanism.

Trust Relationship

Federation members form trust relationships based on agreements to appropriately manage and maintain identity management systems, including identity proofing and methods for authenticating users. Standardizing identity proofing procedures – the identification and registration of users – for each level of assurance will help improve the ability to interfederate.

Perhaps the most important issue for members of a federation is how a relationship signed by its federated operator with another federation binds the behavior of the member. An interfederation agreement might require, for example, that IdPs manage audit logs differently or seek user consent when visiting certain countries. This might

force changes in the IdP operations that were not part of the original agreement that the IdP signed for its federation membership.

IdP and IdM audits will be needed to underpin the trust relationship. IdPs with a central IdM have a greater level of control for managing access. In fact, it may be relatively easy for such IdPs to integrate identity proofing requirements with human resources processes.

Interfederation may start by creating interoperating agreements that have the lowest possible level of assurance (that is, an assurance profile with the minimum necessary identity proofing requirements). From there, interfederating agreements could gradually build out to higher levels of assurance.

As recommended below, a common template, perhaps done as an IETF RFC, for an federation agreement would certainly ease the challenges of interfederation.

In addition, some process for resolving issues across federations. These issues could take several forms: something doesn't work or is broken; some mis- or malfeasance has occurred and forensic information needs to be exchanged; reliability or performance is not adequate for some reason. All these require cooperation; some may require NDA exchange of information. One difficult aspect of this space may be international adjudication. Some process for managing change across federations will also need to be considered.

And, as always, there will need to be reconciliation between different models of managing risk, including liability, indemnification, etc.

Attributes

Agreeing on attributes may be one of the most critical issues involved in interfederating. To be successful and useful, attribute definition must be a community activity within a federation. In turn, federations must agree on the use and meaning of attributes to successfully interfederate.

Where there are shared schema in place, such as eduperson, the issues are understood, though there are always tensions for federations to expand the controlled vocabulary for the schema. (While this is not a good idea, there are many instances where the original eduperson vocabulary is not adequate for new requirements.) The worst situations are those where equivalent attributes are expressed differently in different federations; attribute mapping is not a viable option at this point.

There is another challenge, that of mapping the popular and generic use of a word into the precise controlled vocabulary. For example, when the National Institutes for Health needs to know a principal investigator's "organization," what does that mean? It could be a university, medical center, department, or cross-discipline research organization. It bears no known relationship to the eduOrg attribute. Every member of the federation, and the interfederated community, must know what attributes that will be passed related to the concept of "organization" for NIH.

Attributes may also specify roles, providing access to certain services or allow some action to be performed by the person in that role. Examples might include "registrar,"

"purchasing agent," or "research grant administrator." Successful interfederation will depend on defining these terms and agreeing on the process used to determine the appropriate attribute.

Privacy and Personally Identifiable Information (PII)

A main concern about privacy is the differing requirements worldwide. The European Union Article 29 privacy directive defines personally identifiable information (PII) and defines a user's privacy rights. The EU also has a default information release policy that requires consent. Users must be presented with that policy and provide consent, at least the first time the information is released. Successful interfederation will almost necessarily include methods for users to control the release of attributes that include PII.

There is an activity underway in the EU to track attributes and see which constitute PII. In the U.S., different laws are related to particular privacy domains, including FERPA in higher education and HIPAA in health care, but in general in the US, there is a dearth of federal law on privacy. States may have their own privacy laws as well. Capturing information about relevant laws, and tracking how they affect different attributes, will become necessary in order for interfederation to work.

Another challenge is to maintain privacy while enhancing the user experience. It is likely that the user experience of managing privacy will need to be similar across federations, even if the attributes and the release policies themselves vary. Federations may need to become proactive in this area. Another user educational experience is needed around attributes that are persistent but non-identifiable. Such attributes allow personalization without passing identifiable information to the SP.

3. Federation Operations and Core Services

There was an array of possible business opportunities shared among the workshop attendees, attached as an appendix below. While there was a strong awareness of the broad impact of federated identity, it was widely agreed that for now federations need to concentrate on their core skills and stay close to the provisioning of basic trust services, rather than the new businesses federation enables.

Simplicity

When federations keep policies and legal agreements as simple as possible, interfederation becomes easier. Suggestions include:

- Legal requirements and agreements need to protect the federation and its members, but not become onerous or prohibitive for interfederating.
- A successful federation will evolve, from the simple to the more complex, starting with the basics and making changes to the environment only when required.
- Stay as agile as possible in adding partners. Both the technologies and the policies should be aligned to be flexible at this early stage in development.
-

Core Skills

Federations should focus on their basic skills. There is a danger, in offering additional services, of losing focus, becoming too complex, or driving up member costs. When considering additional services, it would be wise to begin by determining the need, the value that members might attach to the service and, ultimately, what members would pay for such services.

The core competencies include:

- Federal agency interactions. The NIH, NSF and research.gov services are deploying federated approaches and it represents a real win-win-win for user, institution and agency.
- A number of scientific organizations, including the Laser Interferometer Gravitational Wave Observatory (LIGO), the Ocean Observatories Initiative (OOI), the Worldwide Universities Network (WUN) and Project MUSE (scholarly journals online) continue to find new ways to collaborate, providing an opportunity for federations.
- Studentness. There is an increasing number of SPs looking to provide services to students. Microsoft Dreamspark, Apple iTunes, student travel services, and others want access to that broad filter.

Just above these basics lie a number of interesting business opportunities, and some federations are beginning to explore offerings in this space:

- A number of collaboration tools are now replumbing to make use of federated identity. Taken individually, such as a web conferencing tool, in a product suite (Sharepoint) or in an integration (e.g. COmanage), there is value for a federation in offering collaboration services for communities among its members. Statewide roaming wireless access for federated members is another example of a value-added service.
- There is a demand for higher levels of assurance, providing additional security and perhaps addressing privacy concerns.
- Entering into agreements for access to content on behalf of its members is of growing interest. Some state federations have video distribution as an explicit mandate, while popular and public sector content distributors such as the BBC are looking for cost-effective distribution.

Federation and Personal Credentials

Enterprise, institutional and other IdP oriented activities get a powerful leverage from federations and their scope and impact grows again from the externalities of interfederation. The results of interfederation may well be Internet-scale.

Moreover, students have already shown a propensity to use their university credentials for unrelated services, including social networking sites like MySpace and Facebook, blogs, and other such communities. Will identity providers and federations take the next step and promote the opportunity to use credentials for a wide range of unrelated services?

The rise of other possible Internet-scale identity schemes has led to a trend toward “user-centric” technology. Federations need to understand how they make use of user-

centric interfaces to improve the user experience. Attention to the user experience will provide the key to success in this area. Important considerations include simplicity in the interface, getting the defaults right and an ability for the power user to control attribute release and be assured that, to the extent they wish, they can be in control of their identity and privacy.

4. Next Steps

There were a number of topics proposed for next steps after the Federation Soup meeting.

Next Step Commitments

- InCommon and/or Internet2 will create an affinity group of state education system federations (including the University of California, California State University, the University of North Carolina, and the University of Texas) to discuss issues of common interest and challenges.
- InCommon will pursue bilateral agreements with JISC (the U.K federation) and edupass.ca (the Canadian federation)
- The R&E community would promote a plan that creates two related interfederation efforts. The first would address the broad issues of interfederation, working on the complex of mechanisms needed by any two or more federations. This effort would be conducted, if possible, as a Liberty Alliance Special Interest group and draw participants from sectors as diverse as health care and financial services. The second, likely continuing to operate under the REfeds process, would address R&E specific interfederation issues, such as attribute mapping, dynamic metadata, and virtual organization support.

Other Potential Next Steps

- Further development of data developed by JISC (the U.K. federation), which looked at member agreements from nine different federations and found them to be very similar. JISC is optimistic that these agreements could be standardized to allow for easier interfederation. The idea was offered to create an IETF RFC that captures the recommended format of a member agreement.
- Development of a federation roadmap. There was interest in providing a document that would assist new federations in their formation, taking into account all of the issues discussed (such as assurance, attributes and privacy).
- Understanding and addressing EU privacy compliance. As information becomes available about final EU privacy guidelines, it should be widely circulated among the soup participants.
- PII normalization – this is a topic of interest and it was suggested that Internet2 contact NACUA (National Association of College and University Attorneys) to determine if there might be a working group in this area
- Emphasizing/positioning InCommon as a focus point for interfederation in the US

Appendix – Federation Roundup

Canada (edupass.ca) – Canada is a recent entrant to federation and middleware under the auspices of the Canadian University Council of Chief Information Officers (CUCIO). The federation is working on automating trust among institutions and is rolling out a Shibboleth service. They are also rolling out eduroam, a federated wireless access service among institutions. The CUCIO is also interested in related areas, like disaster recovery, and are looking to be the national body to negotiate content agreements.

United Kingdom (JISC – Joint Information Systems Committee) – JISC is centrally funded and covers all levels of education in the U.K., from primary schools through higher education. The federation is technology-neutral and serves education and research, but may be adding health care as the next big community. There is also a move in the U.K. to a government gateway. The U.K. is interested in recruiting SPs in the U.S. and is interested in the knowing the barriers to joining (for example, U.K. laws) and whether an interfederation approach might be better.

Sweden – Sweden is in the early days of building a federation for the academic institutions (SWAMID), with the support of the government.

Norway – Norway's UNINETT, owned by the Ministry of Education and Research, operates a federation for its national research network and universities. The government now wants to roll out the federation to K-12 schools. The challenges include the small size of some of the schools, the differences in how they are organized, and their different interests (much more interested in purchasing issues, for example). The federation's biggest challenge currently is to increase the number of federated services available.

Kalmar Union (Nordic countries) – The Kalmar Union is the interfederating method for interconnecting the Identity Providers in Denmark, Finland, Norway and Sweden.

ELSIVIER – From the aspect of an SP, the main challenge in a federated world is collaborating with multiple federations. While ELSIVIER is large enough to have the resources to do so, there is a limit; and smaller SPs would reach that limit sooner. Attempting to interact with multiple U.S. federations could tax ELSIVIER's resources. The user experience is the most important element for ELSIVIER.

InCommon (U.S.) – InCommon is the U.S. federation wholly owned by Internet2. InCommon is governed by a steering committee that is representative of IdPs and SPs. After starting with primarily large research universities, and their partners, as members, InCommon has recently started to see smaller universities and colleges join. LoA is becoming a bigger issue, particularly as the federation moves to adopt its Silver Level, which requires a greater identity assurance. Another growing priority is helping state and regional organizations build their federations on top of InCommon.

U.S. State-Level Federations

UCTrust – UCTrust is a federation of University of California campuses, intended to enable sharing of applications – such as travel, training, employee self-service – within the entire UC system. UCTrust is built on top of InCommon.

North Carolina – North Carolina has 16 campuses and one high school and is developing an effort similar to UCTrust. The application that spurred this was an interest in consolidating all UNC online courses into one website, so that any student at any UNC campus could take any of the courses. The UNC Federation will roll out over the summer. The federation is also looking at initiatives to either include K-12 in the federation or develop a K-12 federation.

Texas – The University of Texas System federation has operated since 2006. Since the University of Texas is not, legally, one single entity, the federation has a membership agreement with each institution. The membership agreement allows the federation to set all policies, to prevent small institutions from being left behind. There are about 30 applications, system-wide. There is also some interest in either joining or federating with InCommon.

Other Federation Activity

U.S. Department of Energy – ESNet (Energy Sciences Network), hosted at the Lawrence Berkeley lab, is in the process of joining InCommon as an SP. ESNet issues certificates to partners and has begun to accredit European federations. The network serves as a CA independent of an individual institution.

Great Plains Network – The Great Plains Network is one of the early GigaPOPs in Internet2 and now provides collaboration among institutions in an organized and controlled way.

Southeastern Universities Research Association (SURA) – SURA is a community-driven project and relies on existing infrastructures. There is interest in providing access for member universities to the SURA-Grid.

U.S. Government – The eAuth effort has about 190 applications, but has had a hard time gaining traction among IdPs. Discussions to interfederate eAuth and InCommon have not gained traction, either. There is now an effort to bring together three federal initiatives under one umbrella called FIAM (Federal Identity and Access Management). The National Institutes of Health (NIH) has joined InCommon and is ready to federate a number of applications, beginning with SharePoint.

Themes that emerged from the roundup:

- Interfederation
- K-12
- Attributes – want to normalize and manage
- End-user experience

Appendix – Potential Federation Services

Some of the services discussed (in no particular order) include:

- Name-mapping service
- Guest IdP – home for the homeless
- Statistical services (aggregated)
- User-consent service –Danish federation does this.
- Helping to construct attribute acceptance policies and release policies
- Affiliation management
- Registries – for library licenses
- A federation should advocate on behalf of its participants, such as finding ways for members to access government services
- Check to make sure IdP meet data integrity requirements
- Help users diagnose problems – refer users to appropriate application – coordinate help desks
- Security token translation services
- Help SPs that have joined the federation to make their presence known to IdPs and to users