An introduction to Shibboleth Federations

Table of Contents

Introduction

The implementation of Shibboleth technology requires the development of trust between organisations planning to share resources. This trust can be nurtured through the formation of a federation of interested organisations.

Federations are made up of a group of organisations, usually with a common purpose (e.g. research and education), who trust one another. Federations also need to gain the trust of suppliers or resource providers. Federations operate to a set of agreed rules, some of which will be common to all federations, others may be useful or necessary to be developed locally. Federations can have their own legal status as an organisation in their own right.

Federations commonly exchange information about their users in order to enable transactions and collaboration to occur. This will lead to a variety of legal issues, and the need to develop security and a privacy set of understandings between the participating institutions.

What is a Shibboleth Federation?

At its most basic, a Shibboleth Federation is an agreement between resource (service) providers and institutions (identity providers) wishing to access those resources or services. For sharing to occur, all

parties need to agree on a common set of acceptable authorisation attributes for their users, and a schema to describe them.

There is no technical need for federations to exist, however, federations should be useful in simplifying management decisions regarding the sharing of resources between partners. Both technical and policy decisions need to be made, and making these arrangements once to meet the many needs of a community scales better than relying on a series of two-party agreements.

What is a Shibboleth Federation supposed to provide?

A federation should act as an independent body, managing the trust relationship between the identity providers and the service providers.

In the Shibboleth model the service provider only sees the attributes of a user that allow the service provider to judge whether the user is authorised to access the service. The identity provider supplies the attributes for each user, but does not reveal the identity of individual users. Therefore the service provider has to trust the identity provider.

The federation can act to simplify the relationships between identity providers and service providers, as instead of requiring multiple agreements with each identity provider, the service provider should only need one agreement with the federation.

The attributes continue to be held by the identity providers, and they and the individual users can choose which attributes to release (obviously within the requirement that they release enough to ensure authentication and authorisation can be granted).

The federation would also be expected to:

- vet new members (in particular the service providers and identity providers);
- maintain a list of members;
- set policies that the federation members can agree to

Policies should ensure privacy and security for the federation members, such as saying which are the acceptable certification authorities.

Purpose of this document

The purpose of this document is to outline the existing information on University Federation structures and to suggest the best way forward for the development of UK University Federations wishing to share resources and services.

Principles for UK Shibboleth Federations

The Internet2 model[1] is one proposing a “cluster” of distinct federations within higher education, with each federation setting a set of independent standards, but subscribing as well to a cluster-wide set of agreements.

The assumption is that federations will correspond to national higher education networked communities, with one or more federations per nation. By participating in national federations, universities will be able to customise trust and privacy rules and establish particular sets of common attributes, entitlements and other services for distinctive national needs. By individual federations participating in the cluster of

[1] http://middleware.internet2.edu/foo/docs/internet2-mace-foo-shibboleth-based-federations-within-he-200306.html

higher education federations, interactions can be developed to operate across national borders and include global providers of digital content. The model also permits "limited-purpose" federations, for example Shibboleth research test beds, to coexist with "production" federation services (including ones that charge a fee for membership).

Trust

As Shibboleth has moved towards real-world deployments and production environments, it has become clear that there will be a need for several types of federations to support the evolution of sites as they engage with the community. It's clear that sites won't come prepared to interoperate at a high level of assurance, and in many cases, unclear about which sites they will interoperate with and in which manner.

Since Service Providers will see only user attributes, not identity, the Service Provider must trust the Identity Provider asserting the attribute. The Federation can simplify the trust framework, since the Service Provider only needs an agreement with the Federation and not with each Identity Provider.

Policies and practices

Within a Shibboleth-based federation, agreements have typically been established around the following issues:

- a list of the operational metadata for each of the sites in the federation (a signed sites.xml)
- a list of the trust values for each of the sites in the federation (a signed trust.xml)
- an agreement about the attributes and entitlements that will be exchanged (e.g. eduPerson)
- operational procedures and/or legal understandings, both at the identity and service providers and for the federation, to address security, privacy, and data integrity concerns.

It is important to note that Federations are not involved in enforcing either the Identity Provider or the Service Provider to abide by the rules of the Federation. The role of the Federation is to indicate to Identity Provider members that they should be prepared to supply attribute information to the Service Provider members; and that Service Provider members should only make reasonable requests for the minimum amount of information required to authenticate users.

Membership

A UK Shibboleth Federation should aim to support research and education in higher and further education and research institutions by developing and maintaining an infrastructure for user authentication and authorisation.

The following organisations would be able to join the federation:

- higher and further education institutions
- publically funded research institutions
- university hospitals
- organisations supporting research and education (e.g. HE Academy)
- service aproviders

Technical Requirements

There is a fundamental and critical discussion ongoing to evaluate how multiple federations may interact and share various services they offer. There are several aspects of what federations do where it will be important to be able to group or bridge between them; among these are the signed representations of metadata enumerating and detailing individual federation members, the definition of the attributes and information exchanged between federation members, and provision of levels of assurance for different authentication methods. For further detail on these issues please refer to the IAMSECT documentation page.

Risk

An important aspect of the trust in a federation is a reasonable degree of comfort in the assertions passed around by other federation members. Two fundamental types of risk are commonly reported:

- informational: loss of value for the information the more broadly it is shared
- transactional: actual exchange of information and personal data

Federations may not cover risks well since one party needs to accept and trust data and assertions issued by another party with limited information. In the event of a problem, it could be difficult to find which party is culpable. In the case of Shibboleth Federations, a set of organisations will agree to share information with a common syntax and semantics.

Benefits

The benefits to UK academic institutions and service providers of federating can be summarised as being a member of a body which can:

- offer central services and facilitating mechanisms for linking Identity and Service Providers
- co-ordinate the response to technical developments
- represent the interests and needs of the Service Providers and Identity Providers to each other and to external agencies
- promote dialogue and communication between the members of the federation
- promote cross-regional collaborative research activity and sharing of resources
- operate to promote collaboration between institutions and users.

Towards a UK production federation

Practical and policy issues underpinning the formation of a single production Shibboleth federation in the UK HE and FE communities have been outlined in *Blueprint for a JISC Production Federation* (www.jisc.ac.uk/middleware_documents.html [http://www.jisc.ac.uk/middleware_documents.html]). An advisory board has also been set up to recommend the appropriate action to be taken by JISC to set up the federation following the conclusion of the consultation process.

How can I join?

The following consist of brief recommendations for joining a Shibboleth Federation. There is currently no production Federation in the UK that higher and further education institutions can join. However, there is a JISC "blueprint" for a Federation structure (see section 2.7).

Currently it is desirable that there are as few Federations as possible in the UK. One overarching HE Federation, with a set of basic policies could be set up. From this subsets of institutions or departments should be able to federate, operating within given parameters relevant to that groups, and potentially requiring a slightly different set of attributes for authentication and authorisation allowing access to resources relevant to that group. In this way the Shibboleth Federation should become a "network of networks".

Who can join?

The goal of the Shibboleth Federation should be to equip educational institutions and online resource and service providers with a credible platform for exchanging information in a highly secure and privacy-preserving manner while at the same time reducing the administrative burdens associated with setting up multiple accounts and managing user access. Therefore, in the UK any higher or further education insitutions would be able to join the Shibboleth Federation if they could guarantee to fulfill the minimum requirements (see section 3.3).

The other participants would need to be the resource and service providers, which could be the higher and further education institutions themselves, but would also include JISC-negotiated services, publishers and others offering suitable resources and, again, meeting the minimum requirements for membership (see section 3.3).

Who runs the federation?

The Federation could be run by an organisation (such as SwitchAAI or InCommon) or could be run as a consortium. In the former model each organisation that is a member of the Federation signs a bilateral agreement with the Federation Service. In the second scenario a consortium that is by definition an agreement, combination or group (as of companies) is formed to undertake an enterprise beyond the resources of any one member.

Whichever model is adopted for the Federation, it should be overseen by a steering committee who are elected from the membership. Committee members in existing Federations are commonly elected every two years and can be re-elected. In addition there are often sub-groups of the steering committee that work on relevant issues such as evaluation or communications. In the case of a Shibboleth Federation there would also need to be a technical sub-group.

What are the minimum requirements?

The following are the indicated minimum requirements following the SDSS demonstrator model:

At their most simple, the Identity Provider requirements are:

- the operation of an authentication system for local accounts
- the operation of a user directory which supports, as a minimum, the manadatory attribute set (unique ID, surname, given name, home organisation type, affiliation).

In the UK it has been estimated by the SDSS project that some institutions would be nable to satisfy these requirements directly.

For the Service providers the requirements are

- the resource owner must be either a Federation member (for institutions) or Partner (for commerical resources)
- the resource owner must qualify to become a holder of a server certificate.

In more detail, the following requirements should be met:

- Institutions must install the Shibboleth target software as described in the deployment guide at http://shibboleth.internet2.edu/guides/deploy-guide-target1.2.1.html;
- An X.509 certificate from GlobalSign must be obtained; the same certificate may be used for both an identity provider and a service provider;
- Compliance with UK Data Protection and EU directives regarding Data Protection must be ensured;
- A schema should be adopted for transferring attribute data to the federation; identity providers must be able to populate at least the mandatory elements of the schema;
- Identity Providers must take due care to ensure that personal data is correct and up to date before release to the Service Providers;
- Identity Providers need to assign a unique identifier to each user; the eduPerson schema could be a useful model in this context:
    - eduPersonPrincipalName (EPPN) attribute should be used as the unique identifier of a user;
    - the domain part of the EPPN attribute should be the only domain of the identity provider;
    - Service Providers should be aware that one person may have more than one EPPN, either because they have two different roles or because they are members of two institutions. The User will have to assess which identity to use with which Service;
    - the EPPN of a user should not change unless for specific reasons (such as a family name change if the EPPN contains that field); Service Providers should be informed of such changes so that a User's profile is not lost
    - revoked EPPNs should not be reassigned unless the user has not used the EPPN for a period of more than 2 years; Service Provider's should ensure that the user profile is deleted if the user has not logged in to the service for a period of more than 2 years
- Data Protection law states that logs of use of personal data should be kept for three years; both the Identity Provider and the Service Provider need to keep logs containing the user's Shibboleth use; Identity Providers also need to keep a log of the User's Unique Identifiers.
- The Identity Provider should maintain a description of its identity management and collection procedures which can be provided to End Users, as well as other Identity and Service Providers.

Legal Issues

Legal understanding for federations includes the establishment of rules for local authentication, which define shared attributes, use of received attributes, security, privacy and data integrity concerns. Other issues to be considered include trust across federations and rules for subsets of federations.

Data Protection

A UK Shibboleth Federation will be composed of organisations which need to handle personal data about individuals in order to carry out their work and fulfil their obligations to members of staff and students. The law governing the way in which such data should be used or processed is set out in the Data Protection Act 1998, which came into effect on 1 March 2000.

Personal data can be collected from individuals and processed provided there is compliance with the eight data protection principles. The first principle states that personal data must be processed fairly and lawfully. In order to fulfil this principle, the Act sets out that lawful processing will be achieved when either consent is received or one of the other condition of schedule 2 of the Act are fulfilled; these include where it is in the legitimate interest of a data controller (identity provider) to fulfil a contractual requirement such as that between a university and its staff and students. Therefore, although written consent is not necessary to comply with the Act, it is the easiest way. It is best to get it at the point of data collection, and can be obtained through acceptance of a privacy statement of some kind. In the absence of consent the University will need to ensure that it can fulfil one of the other conditions.

The other data protection principles[2] are that personal data must be:

- collected for a specified and lawful purpose and process in accordance with that purpose;
- adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
- accurate and, where necessary, kept up to date;
- kept for no longer than necessary;
- processed in accordance with the rights of the data subject;
- have appropriate technical and organisational measures taken to protect it against unauthorised or unlawful processing and accidental loss, destruction of, or damage; and
- only transferred outside the European Economic Area in restricted circumstances, and if the country or territory guarantees an adequate level of protection for the rights and freedoms of data subjects.

In the case of a Shibboleth Federation, the data controller specified in the act will normally be the Identity Provider. Processing covers anything that can be done with personal data.

An Identity Provider will collect a wide range of personal data relating to staff and students for its own purposes, and to meet external obligations. This information may eventually be transferred to third parties such as a Service Provider. All transfers of personal data which are made must comply with the Data Protection Principles given above. Express consent for transfer of personal data to a third party is only needed for sensitive personal data. Otherwise it must be made clear and unambiguous when the data is collected how it will be used, including that data transfer to third parties involved in provision of services may occur.

It is worth noting that, in the case of a Shibboleth connection, no sensitive personal data which is covered by the Act should be passed to a third party. Shibboleth also gives the user privacy control on release of personal attributes. An Identity Provider would contract with the Federation that it will release data as necessary for authentication and authorisation processes; Service Providers will be contracted to only request necessary data about individuals. In many cases all data will be relatively anonymous, e.g. in the case of an institutional subscription, the only data needed to authenticate individuals is "affiliation to university x".

[2] Additional guidance on the Data Protection Act and other legal issues surrounding the use of information is available from The Information Commissioners Office: http://www.informationcommissioner.gov.uk/eventual.aspx?id=34

The JISC Data Protection Code of Practice for the HE and FE Sectors provides guidance on best practice concerning the retention of records containing personal data (version 2 is available at: http://www.jisc.ac.uk/pub_dpacop_0101.html).

Intellectual Property Rights

Ownership of intellectual property (IP) usually rests with the employing institution. In common with existing library and institutional use policies, end users at institutions must respect the copyright on any content accessed, including that accessed through participation in the Federation. End-users and institutions also have to abide by the terms of any copyrights applicable to the use of software, documentation or other materials developed by the Federation or other federation participants.

All works are automatically copyrighted, which can in fact prevent use when the authors and other rights holders would prefer the reuse was possible[3]. To overcome this organisations such as Creative Commons[4]

have created a small set of standardised licenses that can be associated with content. Licenses are a mechanism for copyright holders to grant rights to others under specific conditions without relinquishing control. For example, the license associated with this paper allows anyone to copy and distribute it provided that proper attribution is given.

The JISC have also commissioned work in this area. Casey (2004) presents an overview[5].

It is unclear exactly how developments in the management of rights in the digital environment will alter the availability and use of digital works. The increasing enclosure of digital works by publishers, supported by changes in the legal environment that favour rights-holders over public access, has seen innovative responses from those who wish to maintain the free flow of information, in the form of creative copyright licensing (open source licensing, the Creative Commons[6] model), new publication models (pre-print publishing e.g. SSRN[7], open access publishing) and greater co-operation and collaboration between interest groups, such as educational institutions, which is part of the approach taken by existing federations.

Digital Rights Management

Digital Rights Management (DRM) is necessary to support digital library collections, code and software development , distance education, and networked collaboration. Intellectual Property (IP) needs to be protected from misuse, and open publishing requires DRM strategies that emphasise multiple subscription models, fair use[8] and include paid and unpaid access. It is desirable to support local and inter-institutional sharing of resources in a discretionary, secure and private manner, but a balance between the rights of the owner and the rights of the user needs to be maintained. According to Dalziel and Vullings (2004)[9] , digital rights management has two meanings:

- management of intellectual property creation and related rights
- enforcement of rights to use digital intellectual property

[3]Collier, C., Muramatsu, B., Robson, R. (2004). The Reusable Learning Project. Site). Retrieved from http://www.reusablelearning.org/
[4]Creative Commons. (2004). The Creative Commons. Retrieved http://www.creativecommons.org/
[5]Casey, J, 2004, Intellectual Property Rights in Networked e-Learning: A Beginner's Guide for Content Developers, http://www.jisclegal.ac.uk/pdfs/johncasey_word_version.rtf
[6]http://creativecommons.org/
[7]http://www.ssrn.com/
[8]In the USA, "fair use" is a commonly used legal exception enabling users to make "reasonable" use of copyrighted work without requesting permission based on factors outlined in section 107 of the Copyright Act 1976, including: the character of use (commercial vs educational/ non-profit); the nature of the copyrighted work; the amount of work used; and the effect of the use on the market for the work.
[9]Dalziel, J. and Vullings, E. (2004). Federations in Action. Presentation

Digital rights expression languages (XrML or ODRL) are commonly used to encode rights. The key to fulfilling requirements in this area may not be to do with expressing all rights via a rights expression language but instead in automating access control - i.e. how, what, who. In most cases trusted access control via the web or desktop encryption would be sufficient.

In a given context, authorisation should therefore be granted on the basis of an agreement on common attributes and common policies, and an expression of both in generic languages so that other combinations are possible in future as the community/ federation and its understanding grows.

In a presentation at a recent European conference, Andrew Charlesworth[10], from the University of Bristol Centre for IT and Law, states, "Educational institutions in the UK (and indeed elsewhere) are now faced with a digital environment where ownership of rights in works, the ability to exert ownership control over those works, and the ability to secure access to works at a reasonable cost are of key importance. It is thus an environment where effective rights management is becoming increasingly important, and rightsholders are becoming ever more efficient at identifying and pursuing infringements, supported by changes in the law which provide rightsholders with far greater rights and powers than were previously available to them".

DRM in Federations

Acquisition and distribution of learning resources are likely to increasingly take place between federations of repositories that share metadata and provide their uses with access to each other's content. These federations (such as the NSDL[11] or coalitions of academic institutions) will have or will develop membership criteria and policies and allow users to simultaneously search and acquire content from all members of a federation.

Existing University Federations

There are three existing 'production' University Federations worldwide; SWITCHaai Federation, a group of Swiss academic organisations; the HAKA Federation in Finland; and InCommon Federation in the USA. There is also a transitional service in the US called InQueue, for organisations which have not identified a suitable Federation to join, but wish to participate in the use of Shibboleth (this is available to institutions in countries which have not established a national Federation, or cannot comply with the trust and privacy regulations of existing Federations).

SWITCHaai Federation[12]

The SWITCHaai Federation is a group of organisations (universities, hospitals, libraries, etc.) that have agreed to cooperate regarding inter-organisational authentication and authorisation and, for this purpose, operate a Shibboleth-based authentication and authorisation infrastructure (AAI).

Policies and Practices

The organisations agree to abide by a common set of policies and practices such as:

- business rules governing registration of users and exchange and use of user attributes

[10]Charlesworth, A. (2005) Copyright Strategies in the Networked Environment.TERENA Networking Conference 2005 - Networking within the Law - Extended Abstract, 6-9 June 2005
[11]NSDL (2004). National Science Digital Library. Retrieved from http://www.nsdl.org/
[12]Detail taken from SWITCHaai Federation - Organization and Processes documentation: http://www.switch.ch/aai/documents.html

- a set of rules governing the development of the Federation
- best practice on associated technical issues, involving attribute management and security

Membership

SWITCH defined two categories of membership for participation in the Federation:

- Education and Research institutions; i.e. all universities, Swiss Federal Institutes of Technology, research institutes in the FIT sector, universities of applied sciences, public research institutes and teaching hospitals. It comprises all organisations which, pursuant to Swiss Law, are supported by public subsidies. It also includes organisations engaging predominantly in pre-competitive research.
- Supporting Organisations; comprising public institutions with which the Education and Research organisations collaborate by way of practice and support of their activities (e.g. libraries, Swiss National Science Foundation, Swiss University Conference, SWITCH)

SWITCH also acts as a service provider, supplying the central AAI Services and operating a resource registry. SWITCH has also allowed for Federation Partners, who would offer services and resources to the Federation members, but would not act as Home Organisations, as they do not represent communities of users. However, to date no such Partner organisation has been found to act within the SWITCHaai Federation, so there is no formal service agreement covering this category of member.

Legal Framework

The legal framework for the SWITCHaai Federation has been based on existing Swiss Data Protection Law outlining the legal basis for handling personal data and existing University rules governing liability issues among participating organisations. A new legal framework[13] had to be devised for the SWITCHaai Federation since there was no existing service agreement structure in Switzerland. This complies with data protection laws, but there appear to be gaps which would need to be filled for compliance with the UK Data Protection Act; for example, it does not make it clear who is responsible for challenging which attributes Service Providers request, and does not clearly require that the Identity Provider must ask for consent from its users before releasing attributes to third parties.

Components and operation

The core functionality of the Switch AAI is to couple together the three basic interactions between a user, his or her home institution and a resource during the authentication and authorisation process. These three basic interactions are: user authentication, which is always carried out by the user's home institution; access request; and delivery of authorisation attributes from the home institution to the resource.

Figure 1. Figure 1: Generic functional model for SWITCHaai

The system and interface specification for SWITCHaai is given in their online documentation: http://www.switch.ch/aai/documents.html

InCommon™[14]

[13] For more detail see http://www.switch.ch/aai/agreement/
[14] Summary information taken from: http://www.incommonfederation.org/

"InCommon is a formal federation of organisations focused on creating a common framework for trust in support of research and education".

By using Shibboleth authentication and authorisation technology, InCommon intends to make sharing of protected resources easier, enabling collaboration between InCommon participants which protects privacy. Access decisions to protected resources are based on user attributes contributed by the user's home institution. InCommon became operational on 5 April 2005.

InCommon development was based on a temporary members Federation called InQueue. This was set up in 2004 to test basic services, processes and policies needed for a Shibboleth Federation. Member organisations in InQueue are able to trial membership in a Shibboleth Federation, and learn about Shibboleth Software. However, it did not have sufficient security to operate as a production-level federation, and organisations were discouraged from making sensitive resources available via the federation.

Policies and practices

One goal of the Federation is to develop, over time, community standards for such cooperating organisations to ensure that shared attribute assertions are sufficiently robust and trustworthy to manage access to important protected resources. As the community of trust evolves, the Federation expects that participants eventually should be able to trust each other's identity management systems and resource access management systems as they trust their own.

In October 2004, the InCommon Federation published[15] the following documents outlining their planned policies and practices:

- Overview of the InCommon Federation
- InCommon Federation: Federation Operating Practices and Procedures
- InCommon Federation: Participant Agreement
- InCommon Federation: Common Identity Attributes
- InCommon Federation: Participant Operating Practices

Participants in the Federation place a certain amount of trust in the Federation Organisation to perform correctly and reliably the support functions that it provides. Participants also need place a great deal of trust in each other as the source of attribute information or a repository of subject information. InCommon has also developed a risk assessment, and operations which will be undertaken within the federation to mitigate those risks.

Given that the primary mission of InCommon is to build trust between participants, institutions must agree at an executive level to adhere to the terms and conditions of federation participation. InCommon requires that participants make available to other participants certain basic information about how they verify identity, distribute user accounts, and manage information on their campus.

Membership

Organisations applying to join InCommon must agree at an executive level of their organisation to the terms and conditions of federation participation, which include documenting the practices and procedures used to grant and manage user accounts. Being accepted into InCommon has been set up as a two-step process:

[15] http://www.incommonfederation.org/policies.cfm

- completion of the InCommon application: this identifies the person who will act as the liaison to InCommon; the application is reviewed by the InCommon Steering Committee, and the liaison person is vetted;

- by invitation, the administrative contact for the organisation can submit metadata to InCommon, after which InCommon will issue certificates to the organisation.

All information submitted to InCommon will be verified to check that it is correct.

Participation in InCommon is open to all two- and four-year, degree granting higher-education academic institutions that are regionally accredited by agencies on the U.S. Department of Education's list of Recognised Accrediting Agencies. Academic institutions join InCommon primarily as Higher Education Institutions that act as Credential Providers (or Identity Providers), supporting an identity management system for its community, though they may also choose to offer resources as well.

Regarding service providers, to join InCommon a Sponsored Partner must be an organisation providing resources (information or services) to the academic community and as such, must be sponsored by an InCommon Higher Education participant.

Legal Framework

InCommon has been set up as a Limited Liability Company (LLC); the Limited Liability Company Agreement outlines the purpose, membership, and structure of InCommon. The InCommon steering committee, representing the founder university members of the federation make up the directors of the LLC. No fees are paid to them, but their expenses in running the federation are covered. There is also an "operations manager", who is appointed by the Steering Committee from Internet2 staff and acts as the Chief Executive officer.

On 18 April 2005 a set of "bylaws" for operating the InCommon LLC were published online, defining the operations of the company, and the responsibilities of the members of the Steering Committee in more detail

Since InCommon has been set up as an LLC it forms a legal entity and therefore is governed by the laws of the State of Delaware and any other state in which the company conducts business, as well as US Federal Law. The participant contract includes clauses covering adherence to Governing Law, and that the "Participant agrees not to participate in the Federation in a manner that violates federal, state or local laws and rules, or in a manner that interferes or could interfere with services provided to others".

Participants must agree to respect the copyright on any content accessed. Clause 8 in the participant agreement refers to respect for intellectual property (covering usage of copyrighted materials) and Clause 9 of the agreement outlines Respect for Privacy of Identity Information

Components and operation

There are technical requirements to becoming an InCommon member; Shibboleth v1.1 or higher must be installed, to support InCommon's federated authentication model. Otherwise the technical framework is outlined in documentation on the InCommon website: http://www.incommonfederation.org/technical.cfm

HAKA Federation Finland

The HAKA Federation in Finland entered its production phase in late 2004. The Federation was set up in 2003, currently including 2 (of 20) universities and 1 (of 29) polytechnics as Identity Providers, and 4 service providers, including the National Library Portal (Nelli). In Finland[16], the libraries in higher education traditionally co-operate widely in licensing electronic journals. The Finnish Electronic Library

consortium is the centralised organisation negotiating the licence agreements with publishers. Furthermore, the consortium has recently deployed a portal (Metalib, a product of Ex Libris Ltd) that constitutes a common interface to the dozens of publishers the libraries have licence agreements with. The portal uses services of the Haka federation to authenticate the user and provide her with customised services.

Policies and practices

The organisation of the HAKA Federation has been based on the SWITCHaai model[17]. Development of the Federation has been closely coupled to the IT department developments in the HEIs involved. From the start special attention was paid to the quality of data held and collected by institutional identity management systems and directories. The Federation is hosted by the Finnish IT Centre for Science (CSC), which also maintains the national research network (FUNET), however, identity management rests with each of the higher education institutions. The HAKA federating infrastructure service will be provided by CSC and based on an agreement between CSC and each Federation member.

Membership

One of the HAKA Federation rules states that only institutions with up to date user data are welcome to join. HAKA have also defined minimum requirements for an institution intending to join the Federation[18].

Legal Framework

The SWITCHaai service agreement is the basis for the legal framework for HAKA. The Finnish Personal Data act needed to be considered in setting up a legal framework for the Federation. The Swiss agreement was considered to be "unnecessarily detailed and complex". A shorter more generic framework has been written for HAKA. This considers three main principles:

- the purpose of the federation "to support research and education in higher education and research institutions".
- responsibilities for challenging the necessity of attributes
- asking for user consent before attributes are released and for the end user to be able to study a privacy policy

The HAKA Federation believes that Shibboleth technology fits well with Finnish Data Protection requirements, and there is no conflict of interest for the user between use of resources through Shibboleth and personal privacy.

Components and operation

The HAKA Federation has the same components and operation as the SWITCHaai Federation (see 2.1.4).

Like in SWITCHaai, the Haka federation has two categories for federation participants; federation members and partners. Higher education and research institutions may join the federation as members and become both Identity Providers and Service Providers. Federation partners, such as library content providers, may only become Service Providers. As the service agreement of the Haka federation is signed between the federation operator and the participant, from the federation participants' point of view, the federation is a service provided by the operator and the other federation participants are subcontractors for the operator. In the agreement, it is made explicit that the contents of the service agreements are

[16]Linden, M (2005) Organising Federated Identity in Finnish Higher Education. Trans-European Research and Education Networking Association Conference, 6-9 June 2005, Conference Paper. http://www.terena.nl/conferences/tnc2005/programme/presentations/show.php?pres_id=77
[17]http://www.csc.fi/suomi/funet/middleware/english/haka_organisation.pdf
[18]http://www.csc.fi/suomi/funet/middleware/english/haka_requirements.phtml

equal for each federation member.