
Victorious Project Pilot 5 Report

Exchange Students and Identity

Using Shibboleth to Manage Exchange Student Identity

Document Notes

Author	Jasper Tredgold
Date	27 February 2007
Version	1.0
Document Name	pilot5 report
Notes	

Summary

This report describes the work undertaken by the Victorious project's pilot 5: exploring the use of Shibboleth to maintain exchange student identities from home to host institutions. Besides providing background and details as to the demonstrator that was undertaken, it also considers some of the issues surrounding federated access management and student and teacher exchanges.

Contents

1 Pilot Rationale.....	3
1.1 Overview.....	3
1.2 Context.....	3
1.3 Participants.....	4
2 Activities.....	4
2.1 Use Case.....	4
2.2 Erasmus Federation.....	4
2.2.1 IdP and SP Participation Agreements.....	5
2.2.2 Certificate Authorities.....	5
2.2.3 Authentication Assurances.....	5
2.2.4 Attribute Use Assurances.....	6
2.2.5 Attribute Exchange.....	6
2.3 Pilot Federation.....	7
2.4 Demonstrator and On-line Guide.....	7

2.5 Related Work.....	8
2.6 Questions to Project Partners.....	8
3. Conclusions.....	9
4. References.....	9

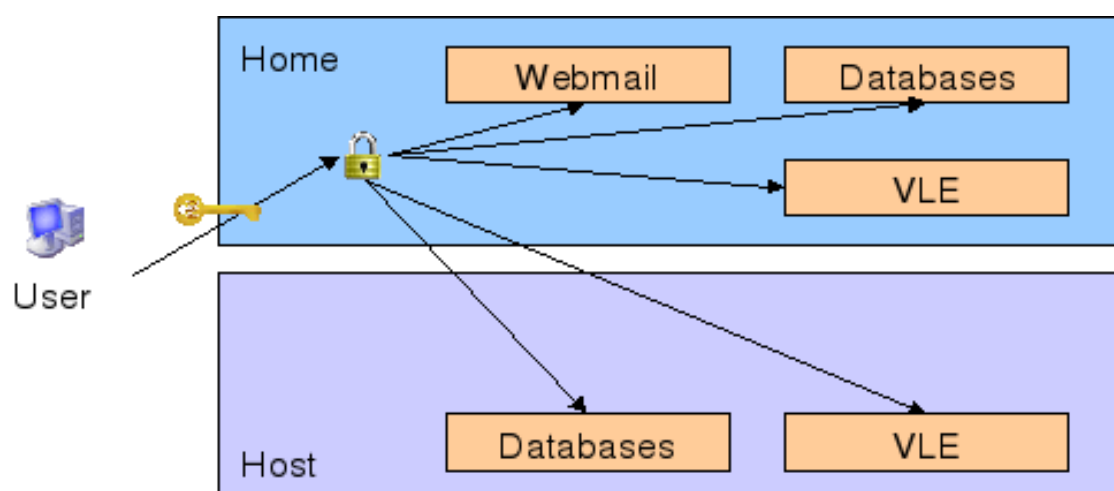
1 Pilot Rationale

1.1 Overview

This pilot sought to explore the issue of mobility with regards to digital identity. Staff and students at today's educational institutions almost always find that having a digital identity is an essential pre-requisite to managing their day-to-day studies. It will often be used in a variety of scenarios, for example, securing access to library facilities, logging in to a departmental Virtual Learning Environment (VLE), or reading email. In many cases students find that they have to manage several institutional digital identities, as well as often maintaining several others in the wider world.

For an exchange student this problem can multiply. They are still required to manage their home institutional identities, but in addition they are expected to maintain one or more new ones for their host institution. This can lead to an unmanageable set of identities, which in turn can lead to insecure practices, such as using the same password for all accounts. At the end of an exchange, upon leaving the host, a student can find that their rights of access to host-based resources have been revoked. This can present problems for a student attempting to complete their studies back at their home institution.

The increasing adoption of Single Sign On (SSO) solutions across education establishments has gone some way to alleviating this problem by allowing the user seamless access to the range of an institution's resources using just one digital identity. This pilot looked at how this approach could be extended to interoperate between home and host institutions. This complimentary approach could for example enable an exchange student, using their usual home credentials, to access the host's secure on-line materials both whilst they were on exchange and once they had returned. Illustration 1 shows the possible scenario.



Acknowledgement: thanks to SWITCH AAI

Illustration 1: Possible future access scenario

This pilot aimed to demonstrate this by use of Shibboleth technologies, using Shibboleth installations and expertise already existing at the pilot participants' institutions.

1.2 Context

Shibboleth is an open, standards-based implementation of a federated authentication and authorisation architecture. It is not a replacement for existing campus identity and access management infrastructures, rather it builds on these systems to enable organisations to securely exchange information about their users. This allows an individual to maintain one set of identity credentials, managed by their home institution, which is able to pass enough information about a user to a resource provider to enable it to make an informed authorisation decision.

Education institutions across Europe are adopting Shibboleth as a solution to the problem of multiple-identity management and the scalability issues around single central identity repositories. Shibboleth's federated architecture of identity and service providers, knitted together in trust relationships, is flexible and scalable.

European adopters in production or in development include:

- Switzerland: SWITCHaai [SWITCH]
- United Kingdom: UK Access Management Federation for Education and Research [UKFED]
- Finland: HAKA [HAKA]

1.3 Participants

Unfortunately, the exploration of the technical details that a Shibboleth installation would require was beyond the scope and resources of this Victorious project pilot. Therefore the pilot was confined to those partners that were already involved in Shibboleth-related work under the auspices of other projects. The pilot utilised both these institutions' existing installations (in production or development) and their experience for its demonstration.

The partners who agreed to participate were:

- University of Bristol (lead)
- K. U. Leuven
- University of Edinburgh

2 Activities

2.1 Use Case

To illustrate the potential utility of digital identity mobility the pilot drew up a use case scenario:

A student from the University of Bristol is enrolled in a virtual exchange course at K. U. Leuven. They are taking a semester-long economics module. As part of their studies they must make use the e-Learning tools made available to them, for example, to submit essays and participate in discussions with fellow students. One such application is named Toledo, K. U. Leuven's VLE. As they are enrolled as an exchange student they have not been issued with a K. U. Leuven digital identity, but rather are able to continue to use their single University of Bristol identity. Logging on to Toledo from their home in Bristol, the student is asked to prove their identity to the University of Bristol's secure login pages. Once they have done so they are able to access Toledo, which presents them with their work as it was left from their previous session.

The pilot then aimed to produce a proof of concept federated access management demonstrator that could facilitate the tasks and aims captured in this use case scenario.

2.2 Erasmus Federation

One of the key tasks in a Shibboleth-based access management framework is the establishment of a trust fabric between participating entities. The component that can effectively manage the trust amongst a group of entities (Identity Providers (IdPs) and Service Providers (SPs)) is the *federation*. This allows the many entities to communicate with each other without having to establish a multitude of bi-lateral agreements. The federation provides a level of assurance to all participants as to the identity of the other participants, allowing them to exchange sensitive information about users during

the authentication and authorization process. Each participant only has to join the federation. The level of assurance the federation can offer is dependant on the nature of the agreements it enters into with its participants.

The model for this pilot is to join together an SP at an exchange student's host institution with the IdP at their home institution. This allows the student's home digital identity to follow them to their host institution where it can be used to allow them access to services local to the host. In addition, upon return to their home institution, the student can still be allowed access to materials they may have stored at their host, for a period determined by the policies adopted by the institutions within the federation.

This model would require the host SP to trust the home IdP so that they could communicate and so that it would believe any authentication assertions emanating from it (e.g. we assert that this user is student A from the University of Bristol). In addition it may want more information about this user in order to make a fine-grained access decision. It needs to communicate with the IdP to retrieve this (e.g. this user is currently on exchange at K. U. Leuven). As discussed above, the trust fabric that allows this communication to take place is a federation.

As mentioned above, federations already exist within many European countries, facilitating federated access management amongst institutions and services within those countries. However in the Erasmus scenario being considered here the trust fabric has to be extended across national boundaries. For the purposes of the pilot the issues around the establishment of a separate Erasmus federation were considered, and are discussed below. In practice a more scalable approach would need to be taken.

Any federation requires some level of agreement between the participants over various issues.

- Assurance on authentication standards
- Assurance on attribute use
- Attribute exchange
- Technical interoperability

An organisation usually indicates their acceptance of the federation policies on these matters by the signing of a federation participation agreement (appropriate to the level of participation) upon joining.

2.2.1 IdP and SP Participation Agreements

In a production environment there would be a need for a federation infrastructure similar to what has been set up for K. U. Leuven, HAKA or SWITCHaai, i.e. a comprehensive legal framework that sets out the rights and responsibilities that fall on the various federation participants, whether IdPs or SPs (or both).

However, for the successful running of our pilot, a much lower barrier of entry could be used. The UK-based Athens test federation uses two agreements, one each for IdP and SP participants, and these were the basis for the draft pilot agreements. These agreements served both as a definition of the participant's details, and as an acceptance of the pilot federation's terms and conditions. They are available from the project website [VIC].

2.2.2 Certificate Authorities

In a production setting a federation would have to recognise a set of established Certificate Authorities (CAs). In this case, where the security requirements were not so high, the pilot federation could take a more pragmatic approach. Where IdPs and SPs already had certificates signed by established CAs the federation included the CAs root certificate. IdPs or SPs that required a certificate could submit a request to Leuven's CA, which the federation recognised.

2.2.3 Authentication Assurances

Again, in a production environment, IdPs would need to guarantee that their user authentication practices (assignment of digital IDs, password integrity, etc.) were of a standard acceptable to the

federation. This could well entail an internal audit of their practices, combined with an official organisational signature on a federation-provided declaration.

In our pilot however, this requirement could be safely ignored, given the clauses included in the agreements.

2.2.4 Attribute Use Assurances

In production, SPs would need to guarantee that their use of user attributes received via Shibboleth was appropriate. An SP's organisation would in all likelihood have to sign a federation-supplied declaration to formalise its intended use of attributes provided to it by IdPs within the federation.

As above, in our pilot federation this level of assurance was not required. The pilot agreement included a clause that proved sufficient for our purposes.

2.2.5 Attribute Exchange

Production federations generally require a minimum set of attributes that IdPs must make available. Of course, IdPs and SPs can agree additional attribute exchanges, but the federation minimum is a requirement of federation membership.

In the case of the pilot, it seemed appropriate to only mandate a small set of attributes for exchange. This set should be enough to make the pilot demonstration use case work. The set that was proposed, with some comments, is below (the namespace component `urn:mace:dir:attribute-def:` has been left out for convenience):

<i>Attribute Name</i>	<i>Comment</i>
<code>eduPersonPrincipalName</code>	<code>userID@domain</code> . Globally unique persistent user identifier.
<code>eduPersonTargetedID</code>	Opaque persistent user identifier. Allows SPs to maintain per-user state between sessions but provides no linkage to user's IdP identity.
<code>eduPersonAffiliation</code>	User's role at IdP.
<code>eduPersonScopedAffiliation</code>	<code>affiliation@domain</code> . User's role within domain.
<code>eduPersonEntitlement</code>	Allows inclusion of federation-, or SP-, specific authorization values.

Table 1: EduPerson federation attributes

This list represents a not-uncommon set of attributes found in production federations. However, in the specific case of the pilot, the list could probably be reduced to just `eduPersonTargetedID` (or `eduPersonPrincipalName`) and `eduPersonEntitlement`.

However, further information would be required. When an exchange student presents himself or herself to a host institution SP, having logged in at their home IdP, all the SP can initially determine is that the user is recognised by an IdP that they trust. However that is not enough, in this case, to gain access. Only students from that home institution who are (or have been recently) on exchange at the host institution are allowed access to the SP in question.

One possible way of passing this information would be to specify additional attributes for the exchange federation. Examples of attribute names that might serve this purpose are shown in Table 2. Namespaces have been left out for readability.

Data passed within these fields from the user's home IdP to the host SPs would allow the applications to make authorization decisions based on the student's Erasmus status with respect to the host institution.

<i>Attribute Name</i>	<i>Comment</i>
erasmusHostId	Unique identifier for the host institution.
erasmusHostIdStartDate	Start date of student's exchange. Includes host ID to allow correct association in the case of multiple concurrent virtual exchanges.
erasmusHostIdEndDate	End date of student's exchange.

Table 2: Possible additional federation attributes

Note that this places the onus for authorization management onto the *home* institution. If, for example, the `erasmusHostIdEndDate` value held at the IdP is incorrect the host services will still allow access when they should be denying.

Although this model of effectively transferring the management of attributes used for authorization from the service to the identity provider is often used (for a commercial service with many clients it may be the most scalable and economical option) it may not be acceptable in this setting.

An alternative would be for the metadata required to make the authorization decisions to be held locally to the service at the host, but keyed on an id passed from the user's IdP. Confirmation of the user's identity would still be required from their home institution, but management of their Erasmus status at the host would be maintained locally.

2.3 Pilot Federation

Although some discussion about the requirements for an Erasmus federation was undertaken within the pilot, for the purposes of actual testing, and for proving the concept, a simpler pilot federation was created. This was a pragmatic decision based on available time and resources. The main distinction between this approach and the Erasmus federation discussion above was the set of attributes exchanged.

K. U. Leuven managed the pilot federation metadata and it contained the following entities:

- An application based at K. U. Leuven (Toledo, an installation of the VLE application Blackboard)
- K. U. Leuven's identity provider
- University of Bristol's identity provider

This metadata was installed at each of the federation members.

Its requirements regarding attributes were minimal, and followed K. U. Leuven's: in order to access the test application, Toledo, the user's IdP needed to present the following two attribute/value pairs:

```
urn:mace:dir:attribute-def:eduPersonEntitlement =
urn:mace:kuleuven.be:entitlement:toledo
```

```
urn:mace:kuleuven.be:dir:attribute-def:uidToledo = <Toledo User ID>
```

The Toledo User ID passed had to be registered with the Toledo application in advance.

Once this infrastructure had been established the scenario detailed in the use case above could be demonstrated: a user could login to the K. U. Leuven Toledo application by using their University of Bristol credentials.

2.4 Demonstrator and On-line Guide

Although the pilot federation was demonstrably working for those within the federation it was not possible to demonstrate it publicly. Inherent in the federation's set-up is the restriction of access to

only those users who can authenticate at one of the included identity providers. It may well have been possible to include an open identity provider in the federation, such as openidp.org [OPEN-IDP], but this was not considered a high-enough priority to justify the work involved.

Rather, a walk-through of the use case being demonstrated was created. This is available on-line from the project website [VIC].

2.5 Related Work

There is much ongoing work regarding the federated approach to access management. As has been mentioned, the Shibboleth architecture is a key area of present development, especially within public sector networks, for example those of Higher Education. Examples of production federations based on Shibboleth have been mentioned above [HAKA, UKFED, SWITCH]. In addition there are other well-established federated access management technologies, for example eduroam [EDUROAM], which provides an academic institution's visitors network access using their home institution credentials, and A-select [A-SELECT], which is in wide use in the Netherlands. There is also work considering the interoperability of these approaches, for instance in the DAME [DAME] project.

2.6 Questions to Project Partners

As part of the context-setting research around this pilot the project participants were asked to respond to two questions regarding the state of federated access management within their own institution and within their country's education sector:

1. Is your institution working with or considering working with federated access management solutions?

- If so, what is the status of that work?

2. Are you aware of federated access management developments elsewhere in your country's Higher Education sector?

- If so, what are they?

Of the respondents:

- Only one was at an institution with no current or planned federated access management developments.
- Two were already participating in fully functioning Shibboleth-based federations.
- Two more had definite plans to join their new national access management federation.
- One was considering working with A-Select [A-SELECT], which now has Shibboleth support [AS-SHIB].
- The majority were functioning eduroam [EDUROAM] members.

3. Conclusions

The pilot successfully managed to produce a demonstrator, internal to the project, showing the proof-of-concept solution in action. This demonstration illustrated a student gaining access to a secure resource at the host institution by authenticating with their home institution credentials. The publicly available on-line walk-through [VIC] shows the steps of the process from the user's point of view.

The approach adopted by the demonstrator was largely driven by pragmatic considerations and achieved its goal by utilising existing infrastructures. Though it offers no model for a scalable implementation it succeeded in demonstrating the use case in practice using existing active institutional Shibboleth components.

As well as this, the pilot surveyed the project partners to help gauge the current standing of federated access management approaches within European Higher Education institutions. Their responses, combined with a broad knowledge of current developments in this area, show clearly that forms of federation are being both researched and implemented as a way of devolving and making scalable the management of authentication and authorization with an increasingly mobile (both physically and virtually) European student and educator population.

Given this, and the EC's stated aim of the expansion of the Erasmus programme, it seems highly likely that the federation of access management will impact on the process of Erasmus exchanges within the mid-term future. Any sort of federated solution would require the establishment and management of trust between multiple entities across Europe.

When considering the general feasibility of the Erasmus federation approach it is clear that there are some general problematic issues with it:

- A home IdP might have to manage additional data for all its students on exchange. If the host institution expected bespoke per-application attributes to be available this would soon become unmanageable.
- The current deployment of the infrastructure components (SPs and IdPs) that would support this approach is, while increasing, still very low.
- A flat pan-European federation would require significant resource to manage, and the participant institutions and services would all have to maintain membership of this federation in addition to others (e.g. national ones).
- Maintenance of a federation on this scale may well be too great without some hierarchical federation structure, such that national federations could be used as the building blocks of a European federation. The technology for this in relation to Shibboleth is undeveloped at present.

Overall, at present, the state of adoption of these technologies is not at a stage where an Erasmus solution could be achieved without considerable effort. The potential benefits for end-users and administrators are unlikely to be considered large enough to justify the associated expense. A more plausible route for adoption will be to leverage the federated access management institutional and national developments that seem likely to occur within the mid-term future. These developments will provide much of the infrastructure upon which an Erasmus federation, or equivalent trust network, could be built.

4. References

- [A-SELECT] A-Select Authentication System website. WWW document. URL: <http://a-select.surfnet.nl/> [as at 10 January, 2007]
- [AS-SHIB] A-Select 1.5 release notes. WWW document. URL: <http://a-select.surfnet.nl/version/1.5/aselectchangelog.txt> [as at 13 February, 2007]
- [DAME] Deploying Authorization Mechanisms for Federated Services in the eduroam Architecture. WWW document. URL: <http://dame.inf.um.es/> [as at 13 February, 2007]

- [EDUROAM] Education roaming website. WWW document. URL: <http://www.eduroam.org/> [as at 10 January, 2007]
- [HAKA] Finnish IT centre for science: HAKA federation website. WWW document. URL: <http://www.csc.fi/suomi/funet/middleware/english/> [as at January 10, 2007]
- [OPEN-IDP] openidp.org website. WWW document. URL: <http://openidp.org/> [as at February 13, 2007]
- [SWITCH] Swiss Education & Research Network: Authentication and Authorization Infrastructure website. WWW document. URL: <http://www.switch.ch/aai/> [as at January 10, 2007]
- [UKFED] UK Access Management Federation for Education and Research website. WWW document. URL: <http://www.ukfederation.org.uk/> [as at January 10, 2007]
- [VIC] Victorious website. WWW document. URL: <http://www.victorious-project.org/> [as at February 13, 2007]