Shibboleth – a strategic approach to school web content authentication and authorisation

Shibboleth is a trademark of Internet2 http://shibboleth.internet2.edu/

Contents

Executive summary

The work of Becta and its partners has shown that a unified authentication and authorisation infrastructure is needed to be able to meet the educational needs outlined by the DfES e-strategy.

Becta's research has shown that Shibboleth is the most suitable solution for securely accessing online content for the education sector and should be adopted as an integral component in the strategic approach to the future development of ICT in education, skills and children's services.

Shibboleth is an authentication system based on open source software developed by the Internet2[1] consortium members, with assistance from the National Science Foundation. Shibboleth is essentially a transport mechanism built on top of an institution's existing architecture that allows organisations to exchange information about their users in a secure and privacy-preserving manner. The purpose of the exchange is typically to determine if a person using a web browser has the permissions to access content or a service from a content provider based on information such as being a member of an institution or a particular class. The system preserves privacy in that it leads with this information, not with the identity of the user, and allows users (or their institution) to determine whether to provide extra information about themselves.

Becta's Shibboleth pilots have shown that Shibboleth-compliant technology will work within the complexity of the school sector and external evaluation has also stated that it is scalable for a national solution.

A Shibboleth authentication and authorisation infrastructure will underpin all of the e-strategy priorities. Specifically, Shibboleth will facilitate Priorities 1, 2, 3 and 6 by: enabling parents and pupils to have secure access to internet resources from anywhere and at anytime; allowing personalisation to occur in a privacy-preserving manner; and providing easier access to a wide range of content, while successfully meeting best value requirements by being open source, based on open standards and able to build upon existing infrastructure.

Recognising that Shibboleth is a viable solution for the school sector, Becta recommends that Shibboleth be adopted by RBCs and LEAs for all school online resource authentication and authorisation, and proposes the following actions:

- The commencement of an EU-compliant procurement process for a national school sector federation.
- The creation of a technical standards working group drawing representatives from industry, Becta, RBCs and LEAs to work within the federation to draw up the specifications and standards for a common framework and vocabularies.
- Consultation and briefing for industry partners [27 September 2005].
- Shibboleth national implementation road map to be published [October 2005].
- Engage with and disseminate road map to LEAs, RBCs, devolved administrations and JISC [November 2005].

[1] http://shibboleth.internet2.edu/

Strategic context – why a unified authentication and authorisation infrastructure matters

In setting out its vision for a 21st century education system, the DfES has identified five key aims:

- personalisation and choice
- flexibility and independence
- opening up services
- staff development
- partnerships.

Those key aims, delivered through strategies for reform across all sectors, are dependent for their successful delivery on the effective deployment and use of ICT. The DfES in its e-strategy identified the key system-wide contribution of ICT as:

- transforming teaching, learning and child development, enabling children and learners of all ages to meet their highest expectations
- connecting with hard-to-reach groups in new ways
- opening up education to partnerships with other organisations
- moving to a new level of efficiency and effectiveness in our delivery.

Overall, the ICT contribution is to be delivered through a series of sector-wide actions underpinned by system-wide priorities. The e-strategy identified six priorities, and we set out below the crucial contribution that a unified authentication, authorisation and accounting infrastructure will make to the delivery of four of those six priorities.

On the whole, however, the most important system-wide contribution that a unified authentication and authorisation infrastructure (AAI) system can make is by facilitating secure anywhere, anytime access to web resources and providing a more individualised learning approach by allowing authorisation to be at an individual level rather than school or LEA-wide. We estimate that AAI systems will be crucial to educational effectiveness.

Priority 1 – An integrated online information service for all citizens

A key milestone in the delivery of Priority 1 is that by 2007 parents and pupils are able to access online applications for places and support. Priority 1 also identifies the need for parents to be able to monitor and support children's learning online. For this to be effectively and meaningfully delivered, much of the core information required to populate these online systems will need to come, via open interoperability standards, directly from school MIS systems. Becta's *School Management Information Systems and Value for Money* report[2] states that one of the requirements for suppliers wishing to become accredited under Becta's proposed MIS Accreditation Scheme is to provide links to the Shibboleth authentication environment.

For parents and pupils to have secure access from anywhere, it is imperative that a reliable and trusted AAI framework is in place. Our work, therefore, has particular relevance for the delivery of Priority 1.

Priority 2 – Integrated online personal support for children and learners

Priority 2 identifies the need for integrated online personal support for learners, and envisages the provision for every learner of a personalised online learning space that can encompass a personal portfolio. It also envisages the development of better approaches to, and use of, e-assessment to improve assessment for learning, enabling learners to better self-manage their e-learning, and supporting learners' progression.

It is difficult to see how this priority could be successfully delivered other than through an authentication and authorisation framework allowing users secure access to their online learning

[2] http://www.becta.org.uk/corporate/press_out.cfm?id=4928

spaces from anywhere and at anytime, both inside and outside of school.

Additionally, by adopting an attribute-based framework, personalisation is facilitated in a privacy-preserving manner.

Priority 3 – Develop a collaborative approach to personalised learning activities

The personalisation agenda is further reinforced in Priority 3, together with an action to ensure wider use of existing resources. The implementation of a national AAI framework that supports and facilitates single sign-on will increase the use of online resources as pupils will no longer need to remember multiple usernames and passwords to access content that they are entitled to use. This benefit has already been seen in London, as following the LGfL pilot there has been a marked increase in the request for LGfL single sign-on usernames and passwords as more schools recognise the amount of content available to them and the ease with which it can now be accessed.

Priority 6 – Build a common digital infrastructure to support transformation and reform

Priority 6 focuses on the need for "robust and sustainable e-systems... based upon a common systems framework and technical standards for the software and systems needed to support the DfES e-strategy". As with Priorities 1, 2 and 3, the framework to support the e-strategy has to be underpinned by a secure means of authenticating and authorising users. Priority 6 also stipulates the need to deliver best value. The chosen method for school AAI presented in this document uses open source software, is based on open standards and builds upon existing infrastructure, thus successfully meeting best value requirements.

Becta and AAI

Becta's initial research into AAI began in May 2003 at a workshop held by the Regional Broadband Consortia (RBCs) with the support of the DfES and Becta to identify the key issues relating to AAI and their implications for the school sector. A subsequent meeting in June 2003 provided a mechanism for further progression of this important area of work, defining a mission statement and investigating possible authentication models. The workshops summarised the benefits of a unified AAI as:

- Ease of access – managing multiple usernames and associated passwords for different resources can be frustrating for the learner and educator, and lead to poor security. AAI should simplify the process by requiring a single username and password combination for each user to make it easier to access online resources.
- Reducing administrative burdens – administration can be reduced for content providers by eliminating the need to store users' personal information. Learning managers and users also benefit from a reduced requirement to store and provide multiple copies of user information.
- Anytime, anywhere access – single username authentication will enable learners and educators to access resources outside the school environment – from home or from a public library – subject to the validity of licences. This is particularly important in meeting the aim of the e-strategy of providing every learner over 14 with 'access to flexible, co-ordinated courses, with the opportunity to learn at home, in work, in college or in other community settings'.
- Personalisation – personalised learning requires learners to have access to individual resources and pathways, possibly suited to learning styles and delivered to the device of choice, in the place of choice and at the time of choice. Increasingly, the personalisation of portals, based on the identity and location of the user, will enable a more individualised presentation of information. Ongoing formative assessment should also be available at times and places to suit, with outcomes recorded and tracked and with high stakes assessment accessible on demand.
- Reduction in duplication (and cost) – a unified authorisation process would allow publishers to concentrate on protecting their assets rather than separately implementing registration and authentication procedures with each purchasing authority or user.

An authentication and authorisation infrastructure is fundamental to all activity within the learning environment. It controls access to resources and tools within an institution and up through the institution's connected hierarchy (school, LEA, RBC, National Education Network). Becta's investigation into defining a framework that will allow seamless delivery of network services to all end-users examined a number of possible approaches, and for such an infrastructure to work efficiently and securely, there are a number of requirements that are essential:

- There needs to be a trusted registration process to manage user access.
- Content delivery must respect Digital Rights Management (DRM).
- There should be flexibility to allow purchases at the school, LEA, RBC or national levels and potentially on a 'per individual' basis.
- Infrastructure should be location-independent to permit access from homes or libraries as well as institutions – subject to DRM issues.
- The user experience needs to be simple to encourage adoption among institutions and content providers.
- There will have to be 'trust' between users, providers and infrastructure managers. Content providers will have to trust the information that is provided to them and users will have to be assured that no more information is provided than is necessary and that they have given consent for the transaction.

Becta's research into AAI culminated in a report, *Towards a Unified Authentication, Authorisation and Accounting Infrastructure*[3], which outlines possible approaches and recommends using the Shibboleth-federated authentication system that meets all of the above requirements.

Shibboleth is increasingly being adopted in the higher education sector within a number of countries, including the USA, Finland, Switzerland and here in the UK. In the past two years, the Joint Information Systems Committee (JISC) has undertaken research into AAI solutions for the communities it serves. Facing similar problems to the school sector, the goal for JISC was to allow users to access internal and external resources seamlessly using a single, institutionally-controlled identity. This will substantially reduce issues surrounding the maintenance of multiple passwords for multiple resources in multiple domains. JISC investigated a number of different solutions for secure access management and in April 2005 announced its decision to adopt Shibboleth as the standards-based architecture for access management in the UK HE/FE sector[4].

Following this decision, UKERNA in conjunction with the University of Edinburgh is working to determine the feasibility of integrating Shibboleth with the JANET Video Conferencing Service system. A feasibility report has been published stating that Shibboleth offers significant benefits with only minimal re-engineering of the existing booking system[5].

[3] http://getconnected.ngfl.gov.uk/docs/aaa_version_1_3.doc
[4] http://www.jisc.ac.uk/uploaded_documents/JISC-BP-Shibboleth-v1-final.pdf
[5] http://www.ja.net/development/aa/shib/index.html

Shibboleth

Introduction

Learners and educators need access to a wide range of online resources to support their learning and teaching. In order to access online resources securely, but with minimal disruption for the user, an efficient authentication and authorisation system is necessary. Implementing a Shibboleth solution will:

- ensure no personal information is exposed unless necessary
- minimise the number of IDs and passwords a user needs to remember
- minimise the administrative burden imposed on institutions and on the commercial sector
- enable user tracking only for services that specifically require it, such as for e-assessment and e-portfolios
- be transparent to the user
- enable access from any location.

Shibboleth is an authentication system based on open source software developed by the Internet2[6] consortium members, with assistance from the National Science Foundation. Internet2 is a consortium of US universities working in partnership with industry and government to develop and deploy advanced network applications and technologies. Shibboleth is essentially a transport mechanism built on top of an institution's existing architecture that allows organisations to exchange information about their users in a secure and privacy-preserving manner. The purpose of the exchange is typically to determine if a person using a web browser has the permissions to access content or a service from a content provider based on information such as being a member of an institution or a particular class. The system preserves privacy in that it leads with this information, not with the identity of the user, and allows users (or their institution) to determine whether to provide extra information about themselves.

Shibboleth has been developed as an open architecture and as an open source implementation; it is standards-based so that information that is exchanged between organisations can interoperate with that from other solutions. Owing to the flexibility of the architecture, Shibboleth will typically be a progression from an RBC, LEA or school's existing supplier's solution and will not require a total rebuilding of their network authentication systems.

The Shibboleth system provides a standards-based link between existing authentication systems and resource providers of all kinds. For example, when a pupil requests access to a protected video clip, their home organisation (Identity Provider) requests authentication (if they have not done so already) and then passes on the information that the user is a 'Year 12 English student from Becta High School' to the site housing the video. The target site (Service Provider) uses the fact that the pupil is in a particular class to determine eligibility to access the video. It doesn't matter where this pupil is trying to access the video from – they could be at home, in school, or in an internet café anywhere in the world. As long as they are able to select their home organisation and successfully authenticate themselves with that organisation, they will be able to access the content to which they are entitled. Because only the attributes of a person requesting authentication are exchanged, the Shibboleth system allows institutions with different technology architectures and security systems to easily collaborate without using proxies or managing thousands of external or transitory accounts.

The Shibboleth model

Shibboleth forms a part of an organisation's single sign-on (SSO) environment for access to protected web resources. The Shibboleth component facilitates the exchange of authorisation and

[6] http://shibboleth.internet2.edu/

authentication information between organisations and resource providers. Shibboleth works in conjunction with an organisation's authentication system and user information databases and allows a resource provider to make authorisation decisions based on that information.

The Shibboleth architecture and protocols are made available publicly, with reference software for organisations and resource providers also available under open source licence.

Single sign-on

The purpose of a single sign-on (SSO) system is to allow the same username to be used to access many online resources and to allow the user to navigate from one resource to another without having to re-type their username and password within the same session. Many web-based applications have their own authentication system and each user of that application is issued with a username specifically for access to that system. Similarly, owners of protected websites issue usernames and passwords for access to their protected or subscribed resources.

As previously mentioned, one of the key drivers for investigating a unified authentication and authorisation system is the prospect of dispensing with pupils having to remember multiple usernames and passwords. Not only do multiple user IDs cause administrative and management burdens for institutions, but they also cause confusion for the user. These problems can be solved by the use of an SSO system.

It is important to note that the Shibboleth software does not provide an authentication system or the single sign-on system. The institution (or more specifically, the party responsible for the identity provision) is responsible for authenticating the user by whatever means it deems appropriate – typically a username and password combination, but could be, for example, via biometrics, X.509 certificates or other means.

Standards

Shibboleth uses the Security Assertion Mark-up Language (SAML), which is an open standard ratified by OASIS[7]. The adoption of an open standards solution is essential to facilitate the take-up of the Shibboleth architecture in as many resources as possible.

Attributes

Shibboleth is an attribute-based solution, with institutions responsible for providing attributes about each of its members, such as whether they are pupil or staff. The institution also provides an Attribute Release Policy so that administrators can choose which attributes are released to which online resources. The Shibboleth software provides an Attribute Authority that can be used to retrieve attributes from various sources, such as LDAP directories, databases and files.

Individual privacy

Shibboleth was developed in order to be a privacy-preserving solution and the architecture enforces this concept by providing users with a one-time session identifier and no persistent identity visible outside the organisation. Individual privacy is also enforced by the aforementioned Attribute Release Policy which allows the user (or their institution) to restrict the release of attributes to third parties.

Federation

A federation allows organisations and resources to work together within an agreed set of policies, governance and legal understandings. The federation also hosts the Where Are You From (WAYF) service that allows users wishing to access resources registered with the federation to navigate to their home organisation for authentication and the provision of authorisation information.

[7] http://www.oasis-open.org/

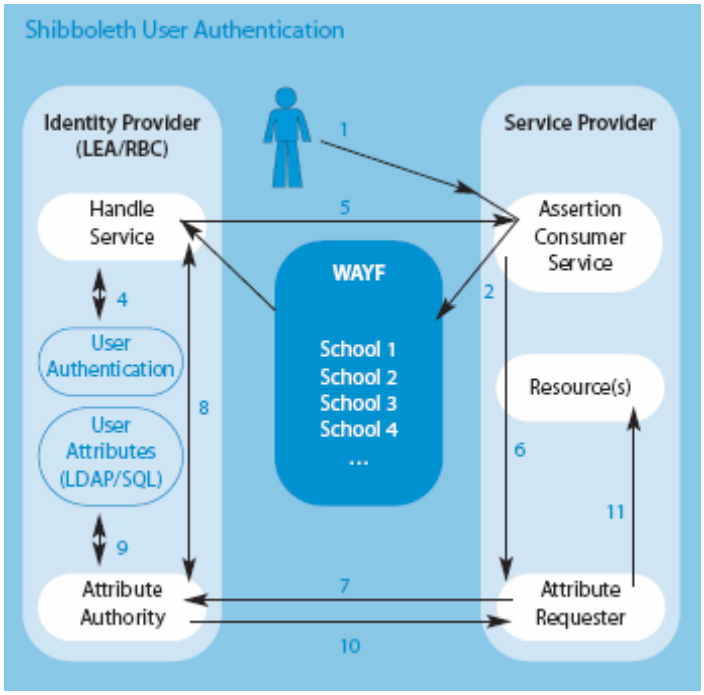
Service Provider

Using attribute information supplied by the user's home organisation, the online resource, or Service Provider (SP), determines whether a user is entitled to access the resource. The Service Provider is also responsible for publicising details of attributes required for access to each resource, enabling users to prepare themselves for access to the resource.

Identity Provider

The Identity Provider (IdP) – typically an RBC or LEA – will provide its own authentication and single sign-on system. The Identity Provider also manages the Attribute Authority linked to user attribute information.

The Shibboleth authentication and authorisation process



1	A pupil requests access to content at a Service Provider's portal.
2	The Service Provider transparently directs the pupil to a WAYF (Where Are You From service), where the pupil declares which school he/she attends or has an affiliation with, for example, 'Becta High School'.
3	The pupil is then redirected to a regional server (the 'origin' or 'Identity Provider') that locally authenticates him/her using any means of authentication available to it, for example, log-in application, digital certificate or hardware token.
4	Typically this will involve the pupil simply logging in with the same username and password that he or she uses to access the school network.
5	The Identity Provider then redirects back to the Service Provider with an opaque handle that pseudonymously identifies the pupil.
6	Now that the Service Provider knows it is dealing with a Becta High School pupil, it asks the Identity Provider for facts it requires in steps 7 to 10.
7 - 10	Is the user associated with that handle permitted to use the provided service? Depending on the attribute management policy that has been agreed between the institution and the Service Provider, this may be all the information that is required to be transferred; however, other attributes detailing the pupil's year or subject group, for example, may also be released at this time.
11	The pupil is then able to access the content or service that he/she is entitled to access.

The 11 steps above happen the first time content is accessed, with most steps hidden from the user.

The only steps that the user sees are the WAYF screen and the log-in screen.

If a subsequent request is made of the same Service Provider (at the same domain), the Service Provider will recognise that the user has an active session as it will have cached the session handle. The Attribute Requester will also have cached the user's attributes; therefore, the user is given access directly to the content they require.

If a subsequent request for content is made at a different domain within the same federation, the Service Provider will again recognise a valid session handle. However, the Attribute Requester will not know which attributes are associated with the user so will make a request to the Identity Provider's Attribute Authority. The Attribute Authority will return the new domain attributes, and based on these, the Service Provider will allow or deny access.

The benefits of Shibboleth

Implementing a Shibboleth solution will have many benefits for all stakeholders. Throughout the DfES e-Strategy document the concept of anytime, anywhere remote e-learning is highlighted. Currently, the only scalable, secure solution that is acceptable to all stakeholders is Shibboleth. Without Shibboleth underpinning a common digital infrastructure in education and children's services, the benefits of a strategic approach to ICT will not be realised.

Feedback from LEAs from both within and outside of Becta's pilots has been overwhelmingly positive, with many reiterating the fact that a national framework for AAI is required to prevent repetition of similar work by developing bespoke single sign-on solutions that will only work inside individual LEAs or RBCs.

Although Shibboleth has been designed primarily for secure access to web resources, work is ongoing to extend the framework for institutional authentication and authorisation. Additionally, Becta has stated in its *School Management Information Systems and Value for Money* report[8] that a requirement for suppliers wishing to become accredited under Becta's proposed MIS Accreditation Scheme is to provide links to the Shibboleth authentication environment.

A further extension is being investigated that combines Shibboleth authentication with a web proxy to enable user-based filtering.

User and institutional benefits

The fact that Shibboleth is attribute-based means that personalised learning can be easily achieved, with different learners being able to access targeted content and services using a granular authorisation process that does not unnecessarily share personal information. Shibboleth also removes the requirement on LEAs and RBCs to provide third party Service Providers with user details directly in the form of data files or user lists. This is very significant as in almost all circumstances where an LEA or RBC wants to procure access to third party online services, they have to engage directly with the Service Provider to agree the format of the user data exchange as well actually doing the extraction. This situation can be both time-consuming and problematic as the precise requirements and extraction methods differ in each particular situation.

Core benefits of Shibboleth adoption for users and institutions may be seen as:

- Each end-user will have a single ID linked to many resources so it will be easier for the end-user to access content.
- Managed attributes will allow appropriate content to be presented with minimal end-user intervention.

[8] http://www.becta.org.uk/corporate/press_out.cfm?id=4928

- Management of user accounts will be simplified for schools, LEAs, RBCs and other education providers.
- Schools, LEAs, RBCs and other education providers are no longer locked into sole-provider situations by the nature of the technical solution.
- Lower development costs for content producers should potentially lead to lower costs for schools.
- More flexible study – the learner has more choice about where, when and how they study as content providers can be confident that only authorised users are accessing content and do not have to restrict licences based on IP addresses, for example.
- Secure access to a personal online learning space – again this must be accessible from anywhere at anytime, which can be achieved by implementing Shibboleth.
- Adopting the same AAI solution as JISC will facilitate the sharing of information between sectors, especially in regards to the 14-19 agenda and e-portfolios.

Benefits for Service Providers

As a Federated Identity Management system, Shibboleth creates a clear demarcation between those bodies that should be responsible for managing a user's identity and those that should not. This is a critical point which has the potential to transform the way those bodies that manage identities work with third party Service Providers.

Previously, almost all third party online Service Providers in the UK education sector have provided their own authentication services. The result is that the personal details of individual students, teachers and other educationalists exist in different storage systems across the country and even abroad. In some cases, this data may be very limited, but in others much more detailed information is stored. This personal information is used to provide authentication into the services offered and in some instances provides differentiated access to personalised functionality. This situation has arisen out of the limitations imposed by the different technologies employed and the lack of a clear alternative.

By facilitating Federated Identity Management, Shibboleth provides the technical infrastructure, offering some very significant advantages for both the identity management bodies and those third parties offering online services to the UK education sector.

For those Service Providers who have traditionally been forced to maintain their own user data repositories in order to provide authentication into their services, Shibboleth removes the authentication requirement enabling the provider to concentrate on authorisation. This distinction is critical. Clearly, Service Providers need to ensure that a user is allowed to access the services they provide and traditionally this would be achieved by authenticating the user locally within the Service Provider's system. Typically, this would involve checking a username and password entered by the user against credentials stored in a database. With Shibboleth, the provider is able to ascertain whether a user has been authenticated at their Identity Provider. This means they do not necessarily have to store username and passwords and can forgo the worry of managing authentication services. Depending on the way the provider wishes to control access to their services, however, they may still need to store some details about the user – particularly if they make use of personalised service offerings.

Previously, content providers have needed to spend time and money developing and managing authentication and authorisation systems. The universal adoption of Shibboleth will dramatically lessen the resources required, yet still reassure providers that only those users that are entitled to access their content do so.

Shibboleth has the following benefits for Service Providers:

- No more customised support for authentication systems.
- No more maintenance of IP address tables.
- No more maintenance of user IDs and passwords.

- Lower helpdesk costs.
- Content producer costs reduced by not having to develop proprietary authentication systems.
- A level playing field for all content producers to provide accessible content for end-users, without having to worry about delivery through the mechanisms of other suppliers.

Becta's Shibboleth pilots

Given the recognised importance of a secure, resilient school authentication system, Becta embarked upon two pilot projects to deliver the basis and potential for a Shibboleth-compliant solution that is independent of vendor, RBC or other solution provider. The aim of these pilots was for schools and content suppliers to implement Shibboleth on their systems to allow universal single sign-on in order to verify that Shibboleth is a suitable solution for the school sector.

Research into Shibboleth – including successful laboratory environment demonstrations and the widespread adoption of Shibboleth in the HE/FE sector – led Becta to commission pilot projects with two Regional Broadband Consortia (RBCs) – London Grid for Learning (LGfL)[9] and WMnet[10]. Two pilots were commissioned due to the very different general approaches of each RBC – one with a highly centralised function in terms of management and administration and one with more of a co-ordinating approach. The aims of both pilots was to verify that Shibboleth as a technical solution is truly using open standards and can be 'bolted on' to different existing accounting database infrastructures in a way that is suitable for the school sector.

The outcomes, deliverables and experiences of all parties involved in the pilots have helped produce definitive best practice guidelines on how to implement Shibboleth in the school sector and have also assisted in formulating a project plan for moving the AAA Shibboleth solution from strategy into a national implementation phase. Details of both pilots can be found in Appendix A.

Both RBC-led pilots have proven that Shibboleth is a viable solution for authentication and authorisation of online resources in the school sector. Shibboleth has further been proven to meet the educational and administrative issues the project set out to solve while facilitating the anytime, anywhere learning agenda called for by the e-Strategy. It is the opinion of all those involved in the pilots that Shibboleth is currently the only secure method of achieving the strategic goals set out by the Government.

In order for Shibboleth to be successfully deployed throughout the school sector in the UK, there are a number of issues that need to be addressed. Where the pilots have made recommendations for moving forwards in various areas, these are noted below and discussion is encouraged from all stakeholders.

Of prime importance is that all Shibboleth implementations be compliant and meet the same standards.

- Shibboleth-conformant implementations must meet the criteria defined in [http://shibboleth.internet2.edu/docs/draft-mace-shibboleth-arch-conformance-latest.pdf].
- Implementations of the Shibboleth protocol must implement the protocol described at [http://shibboleth.internet2.edu/docs/draft-mace-shibboleth-arch-protocols-latest.pdf][11]

Issues and recommendations

The federation

It is clear from the work carried out thus far that the cornerstone of a successful Shibboleth implementation is the federation – a group of organisations that share a set of agreed policies and rules for access to online resources. These policies enable the members to establish trust and shared understanding of language or terminology and the structure and legal framework provided by the federation enables authentication and authorisation by Shibboleth across different organisations.

[9] http://www.lgfl.net/
[10] http://www.wmnet.org.uk/
[11] At the time of writing these documents are in draft. Final versions are expected in September 2005.

Investigation into existing federations revealed that outside the UK there is currently no active development of the use of Shibboleth for school sector authentication. Many countries are investigating or using Shibboleth for HE/FE and there has been great interest in the Becta pilots with a number of organisations likely to investigate the implementation of Shibboleth in the school sector following publication of Becta's work.

It should be noted that the major differentiator between the school sector and other sectors/countries is the presence of commercial providers throughout the system. This means that a school sector implementation of Shibboleth will face issues not yet experienced in existing deployments.

Both pilots highlighted the need for compliance between versions of Shibboleth. This is of particular relevance as version 1.3 of the Shibboleth code was released between the end of the pilots and the publication of this report. The WMnet implementation has v1.2 and v1.3 set-ups running side by side with no problems. The federation, however, will need to recommend a version for stakeholders to adopt and this should be to remain in line with the Internet2 development programme.

- Stakeholders should implement the most recent stable release of the Shibboleth software.

The federation is responsible for maintaining the trust fabric to which all members sign up to, so has to be a trusted entity itself. Any federation dominated by a commercial supplier, or even a consortium, is likely to fail to achieve the potential benefits, as other major commercial suppliers withhold key information or continue to seek to maximise their own products. Indeed, there is a very clear danger of a commercial model being implemented whereby all access to content is 'controlled and charged' by a single supplier through its 'tunnel' between authentication services and content services. The effect of this model could be to drive up the cost to education and throttle access to resources.

- The Shibboleth-compliant national solution should be provided by a vendor-neutral organisation.

The federation asks its members and Registration Bases to 'trust' that the Service Providers and Identity Providers can provide a Shibboleth-compliant service. The federation also asks Service Providers to 'trust' that the Identity Provider is capable of sending a set of attributes that is accurate and not malformed. In order to achieve this level of trust, the federation must accredit participating Identity Providers and Service Providers.

- The federation must accredit Identity Providers and Service Providers.

It is also imperative that all members can trust the services provided by the federation, in particular, the resilience of the WAYF. Should the WAYF fail, not only will different suppliers' Identity Providers and Service Providers be unavailable, the same supplier's Identity Provider and Service Provider will also be unable to communicate.

- The federation must provide a resilient and reliable WAYF service.
- The federation should establish a fault management procedure.

There are a number of stakeholders in a federation with their terminology differing between implementations. The LGfL pilot documents describe the stakeholders and the relationships between them. It is recommended that these descriptions be adopted by the national federation:

Federation members	Federation members will generally be drawn from the community of Regional Broadband Consortia, Local Education Authorities, or groups of schools with a formal constitution of their own federated arrangements. Exceptionally, non-profit-making educational organisations of significance would be eligible as members where their aims and objectives are broadly in line with those of the existing members. The members will represent organisations that act as Registration Bases.
Registration Bases	A Registration Base is an organisation to which end-users are registered. The term registered may be taken to mean 'being on the school roll', or, 'employees of a federation member'. The Registration Base should also include parents, school governors and other relevant users. The key factor

	here is that the existence of the end-user and their legitimate access to resources is verifiable and controllable by that organisation. This will include institutions and organisations, such as schools (state and independent), Pupil Referral Units, professional development centres, City Learning Centres, libraries, museums, LEAs and RBCs.
Federation partners	It is proposed that commercial organisations – whether content producers, Service Providers, Identity Providers or third party support providers to Registration Bases – will be federation partners. In broad terms, these federation partners will generally be commercial organisations that deliver Shibboleth-compliant services to federation members. These services may include content production, content delivery or authentication services. A commercial organisation that manages end-users on behalf of a Registration Base will also fall into this category.

- The federation should adopt the stakeholder descriptions as proposed by LGfL.

The key issue of interaction with other federations needs addressing. Discussions with JISC and others during the course of the pilots has revealed that there could be a single education federation, but that it is currently more practical to build separate schools' and HE/FE federations. There will be a need going forward for interoperability between national and international federations and Becta and the national federation will keep a watching brief on other organisations' work in this area with a view to benefiting from their experience.

- The federation should liaise and communicate with JISC and international federations.

From examination of the practicality of running pilot federations, it is recommended that Identity Providers should be established at RBC or LEA level, or if appropriate, by clusters of schools, as opposed to the individual school level. This provision may be by RBCs/LEAs/clusters themselves or by their commercial partners. Based on this scenario, the likely number of Identity Providers in a federation could be 150 or more, with each Identity Provider requiring relationships with multiple Service Providers. To be able to come to an agreement between all members, a coherent and scalable solution is for the federation to prescribe the rules, language and associated policy, and to publish fixed templates containing details of attributes to be shared. It is likely that assistance from the federation will be required by Identity and Service Providers when 'Shibbolising' their systems and joining the federation; therefore, the federation should be prepared for this.

- Identity provision should be at RBC or LEA level.
- The federation should provide support for UK school sector IdPs and SPs.

Attributes and schemas

Both pilots examined the existing eduPerson schema which is used as a basis for most Shibboleth implementations, and found that it doesn't cover all the attributes required in the school sector. From discussions with other federations, it was thought that most data sharing requirements could be met by using a core subset of attributes as follows:

Attribute	Description
eduPersonScopedAffiliation	Used for basic authorisation: does this school subscribe to the service in question?
eduPersonTargetedID	This is a persistent opaque identifier, which enables service personalisation (remembering data about a user over different log-in sessions) without the Service Provider knowing who the user is. It is unique between an IdP/SP pairing and typically consists of a long hexadecimal value.
eduPersonPrincipalName	The 'NetID' of the user, for example, user@school.lea.sch.uk. This is useful when you want to have a known identifier.
eduPersonEntitlement	A random string with a specific meaning between IdP and SP. This is a privacy-preserving attribute that negates having to do attribute algebra (the process of combining two or more personal attributes, such as date of birth and gender).

It is likely that these four attributes can still cope with most situations; however, LGfL found that five extra attributes were required. The reasons for these are shown below:

Attribute	Reason
bectaGender	To allow population of Digitalbrain account
bectaDoB	To allow population of Digitalbrain account
bectaIntake	To allow population of Digitalbrain account
bectaMIS	To allow population of Digitalbrain account
bectaIdPgroup	To allow a geographically dispersed Identity Provider group to be recognised by a Service Provider

However, as the project progressed, the importance of the eduPersonTargetedID attribute in being able to link an authentication account to a content account without the release of bectaGender and bectaDoB may well lead to these being seen as obsolete attributes.

The WMnet pilot discovered a need for extra attributes, too. Information in these attributes is currently used by existing content/Service Providers in the West Midlands RBC. These differed from those above:

Data item	Description
Unique Identifier	Some unique ID, which will be used by services such as email and assessment, which identifies each and every user.
User Type	The general user type of the user such as pupil or teacher. The distinction is not limited to that scope with other types including classroom support, LEA staff, school management, school administrative staff and other not so obvious groupings.
Key Stage	For pupils and teaching staff including classroom support, an identifier to determine the key stage of the user.
School Year	Possibly for restriction of resources and services that require membership of a certain year group. Possibility that commercial content providers may start to sell per user charged content to smaller groups with schools.
School Phase	The school phase of the pupil being served such as nursery, primary or secondary.
Subjects	Not only curriculum subjects, but could also include other areas for staff such as management or finance.
Classes	Teachers, pupils and classroom support for such services as assessment and reporting.
Departments	Usually maps to National Curriculum subject areas, but could include others, such as for LEA staff.
School (Primary Organisation)	Schools and other organisations, such as CLCs and libraries
LEA (Secondary Organisation)	Local Education Authority area.
RBC (Tertiary Organisation)	Regional Broadband Consortia area.

Although these data items are currently required by commercial organisations, it should be possible to reduce these extra attributes by judicious use of the four core eduPerson attributes. However, it is clear that ongoing research and consultation needs to happen in this area. This should be led by the federation, as agreement between members is an important consideration.

- The federation should consult with all stakeholders on a minimum attribute set.
- The federation should provide a standard attribute schema.
- The federation should act as a clearing house for additions to the attribute schema.

Every Shibboleth attribute should have its own Object ID (OID)[12], containing a Private Enterprise

[12] http://www.alvestrand.no//objectid

Number of the organisation that invents said attribute. For example, the eduPersonTargetedID has an OID of 1.3.6.1.4.1.5923.1.1.1.10, with the 5923 representing Internet2. In preparation of the need to invent extra attributes for the school federation that are not currently in an available schema, Becta has registered a Private Enterprise Number with IANA and has been allocated 23476. This should be used by the federation when inventing new attributes.

- The federation should provide OIDs for any new attributes invented by the federation.

For a national implementation to be successful, a consistent approach is required across all LEAs and multiple suppliers. Part of this implementation is the need to define a specification for 'user identity', for example, whether all user names should be unique across the UK, or just unique for a given LEA. The approach taken by both pilots is the latter, with WMnet's solution being hierarchical in that uniqueness is only necessary at the school level. This issue may be discussed further, but the current recommendation is that a national unique ID scheme is not required for Shibboleth.

- User identities should be unique at least at LEA level.

The WMnet pilot looked at extracting data from school MIS or LEA EMS and the practicality of using the Common Basic Data Set as a Shibboleth data schema. Given that it is judicious to build on existing effort, further work should be undertaken on the use of existing data stores to populate attributes.

- The federation should assess the practical implications of using the CDBS and other data schemas.

During the testing within the LGfL project, it was discovered that Shibboleth's default configuration leads to two attributes sent by the Identity Provider being mapped to unexpected HTTP headers by the Service Provider, resulting in values that do not conform to specifications. It is important to note that any transmission of attributes should be tested to ensure a) the attribute name is mapped to an appropriate HTTP header, and b) the transmitted value of the attribute is in the correct form.

- The transmission of attributes should be tested to ensure correct mapping and formatting.

Each Service Provider will generally want to receive the same set of attributes for each Registration Base to which it has sold licences or is prepared to give access and each Identity Provider will be requested to release different sets of attributes to different Service Providers. Therefore, each Identity Provider will have a pairing with several different Service Providers. In these pairings, although an attribute, say eduPersonTargetedID, gets passed to each Service Provider, its value should be different. Other attribute values should remain the same for that end-user, for example, surname, irrespective of the Service Provider that is entitled to see it.

- Only the end-user should be able to tunnel to their personal content across multiple content providers.
- The Identity Provider will need to hold many eduPersonTargetedID attribute values; an end-user will be uniquely identified to a Service Provider by the combination of this attribute and the name of the Identity Provider or the Identity Provider group.
- The Identity Provider will need to provide adequate back-up procedures to prevent loss of persistent values.

Federation membership will provide a guarantee to Service Providers that users have been authenticated at their Identity Provider, but it does not guarantee that the Identity Provider will assert the attributes required by the provider, or that in those circumstances where extra information is required that a protocol exists to begin this process. Much of this can be achieved through negotiation, where on subscribing to a particular Service Provider a dialogue begins in which the

requirements for transactions to occur are discussed. However, the terms of reference for this type of process must be defined to ease management of the Identity Provider's attribute store.

- The federation should publish a protocol defining a Service Provider's requirements and the level of attribute release an Identity Provider supports.
- Only the Registration Base should be able to decide on the attributes that are to be released. This should be achieved using an Attribute Release Policy (ARP).

The Service Provider has to determine the minimal set of attributes they would want to receive so as to control access to their content and to be able to offer its base functionality. This does not mean they will arbitrarily get these attributes, as the Registration Base has the ultimate sanction on what attributes their Identity Provider may release to the different Service Providers. The attribute set should be minimal; however, there is nothing to stop extra attributes being released to assist the Service Provider, so long as all parties are in agreement. To resolve any potential issues concerning the release of attributes, the federation will manage what is known as an Attribute Control Authority (ACA). The role of the ACA will be to act as a brokering and clearing house service for Registration Bases and providers, and will include the following:

- The ACA database should contain details of Registration Bases, accredited Identity Providers, Attribute Release Policies and their related attribute sets, accredited Service Providers and their related Attribute Acceptance Policies.
- The ACA should negotiate an appropriate attribute set required by an individual content provider.
- The ACA should produce exemplar Attribute Release Policies and manage these on behalf of Registration Bases.
- The ACA should approve and manage appropriate Attribute Acceptance Policies between Identity Providers and content providers.
- The ACA should manage the attributes formally approved by the federation, those agreed locally between different pairs of suppliers, and those agreed between different federations.

Once the end-user has been authorised to access the Service Provider's content, the privacy protection offered by Shibboleth-compliant AAI is minimal if the Service Provider decides to present screens to the end-user that invite them to enter personal details. There is a danger that the Shibboleth-compliant system (with its minimal attribute set) will cause Service Providers to seek to get the end-user to enter even more information about themselves than pre-Shibboleth AAI. It is the end-user, or the Registration Base's policy (a policy not connected with Shibboleth-compliance, but instead covering what information the end-user is allowed to enter into the content screens), that will determine whether the requested information should be entered, or even requested in the first place.

- Registration Bases should ensure their users are not unnecessarily invited to input personal data into Service Provider screens.

Namespaces

Each Identity Provider and Service Provider must have a unique name known as a 'providerID'. Each 'providerID' exists within a Uniform Resource Namespace (URN) that will need to be operated by the federation. The Internet2 Middleware Architecture Committee for Education (MACE) defines directory attributes and controlled vocabularies for the values of some of those attributes and the URN represents global, distributed, persistent, location-independent names for these resources.

Within both pilot projects it was decided to use 'local', informal URNs to achieve unique identifiers for both Identity and Service Providers. The URN currently in use by LGfL is *urn:mace:becta* while the WMnet pilot used a URN provided by JISC's SDSS Federation: *urn:mace:ac.uk:sdss.ac.uk*.

All major Shibboleth-compliant developments are registered with MACE, so in order to achieve international compliance, Becta has subsequently registered the namespace *urn:mace:sch.uk*. This means that all providers' servers built before the MACE registration will need to be updated with this value before joining the national federation.

- All providers in the federation should use the namespace *urn:mace:sch.uk*.

Data

An issue to do with Data Protection Act (DPA) compliance of Attribute Release Policies has been raised following the LGfL pilot. This subject is being investigated by the Information Commissioner's Office and any result from this will be disseminated as necessary. The current view is that in placing on the data processor an obligation to process data in compliance with the DPA, and in detailing how that should be done, the federation contracts are likely to fulfil all the major criteria of a data controller/data processor contract.

The Information Commissioner also takes the view that a fair processing statement should be in place. This would require that parents be notified what data it is proposed to process, how and by whom the processing will be carried out, and details of any disclosures which may be made. There should also be an "opt out" clause for those parents who do not wish their children to participate in such a scheme.

This may seem unwieldy, but once a fair processing statement has been issued schools could then reissue this on a regular basis, perhaps yearly or at the beginning of each term, in a standard format along with any other information usually released at this time. This would ensure that all parents were aware of the scheme and of their ability to withdraw their children should they see fit.

Schools currently process personal data so are regarded under the DPA as data controllers. When data is obtained from data subjects, the data controller must ensure, so far as is practicable, that the data subjects have, or are provided with, or have readily available to them, the following information, referred to as the 'fair processing information': details of the data that they hold on them; the purposes for which they hold the data; and any third parties to whom the information may be passed.

Schools should, therefore, have an existing fair processing statement that pupils or their parents have agreed to and this should be updated to reflect any changes that may occur due to the implementation of Shibboleth.

In order for the federation to protect itself from an end-user claiming not to have realised the data protection implications of using its service, albeit via screens provided by others, there will be a requirement on Service Providers to display a DPA requirements clause within the provider's entry screen.

By implementing Shibboleth it is also likely that many LEAs will be better able to meet DPA requirements as it will enable LEAs to establish a manageable data store and Shibboleth provides the tools to protect a user's privacy.

- The federation should ensure processes comply with the DPA.
- Schools should put in place a fair processing information statement.
- Service Providers should display a DPA requirements clause within the provider's entry screen.

The way data is collected, managed and used is a key issue for all LEAs and RBCs considering Shibboleth. It is very difficult to provide detailed guidance on these issues because each LEA or RBC – while possibly sharing some basic characteristics, such as the existence of an educational management system at the LEA – will have its own unique set of circumstances which will affect its ability to extract and manage user data. The ideal situation is one where accurate user data can be electronically collected, checked and used to populate the authentication/attribute store.

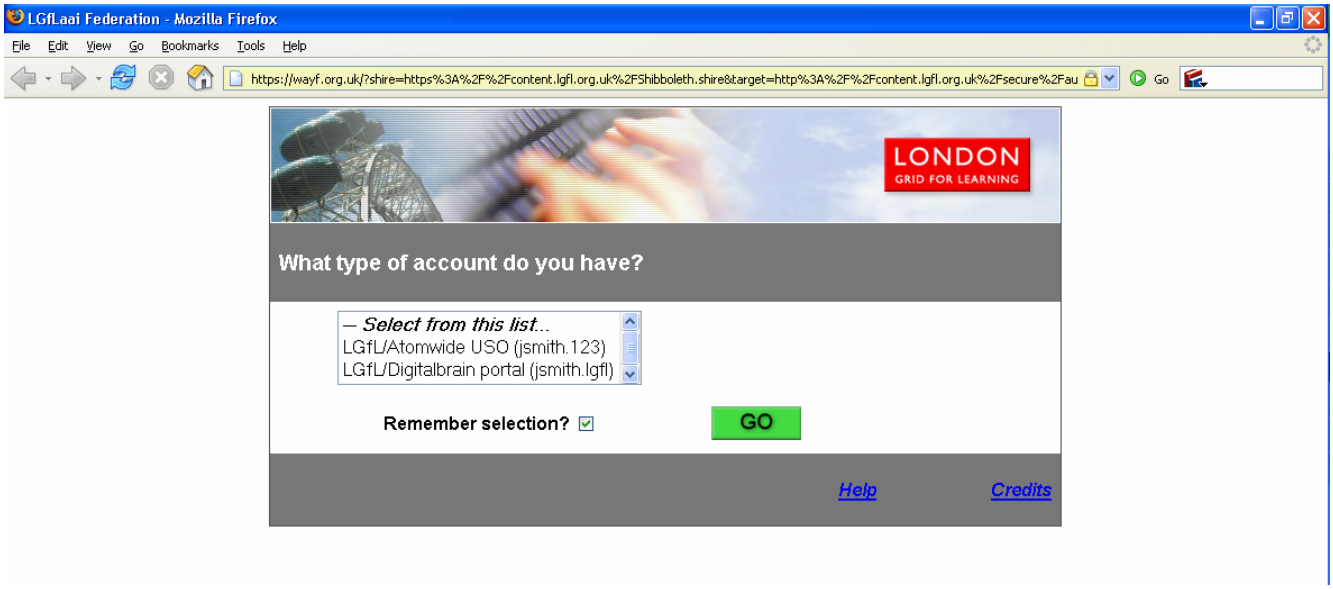
The WMnet pilot explored the following methods with varying success: extracting from school MIS; extracting from EMS; and converting existing data. An issue with extracting user data from the school's MIS is that, although the kind of information required to populate the attribute store is readily available and there are fairly well-defined extraction methods, there are concerns over the quality and consistency of this data. It was not clear from the pilot whether extracting EMS would be able to supply all the required data for the attribute store and again there were concerns over the accuracy as some LEAs wait for the PLASC returns before the EMS can be updated. Converting existing data is usually only possible where a limited set of attributes are required, as existing user data stores, such as those used in LEA or RBC portals, do not contain all the required attributes identified in the pilot.

However, as a starting point this may be the most straightforward method.

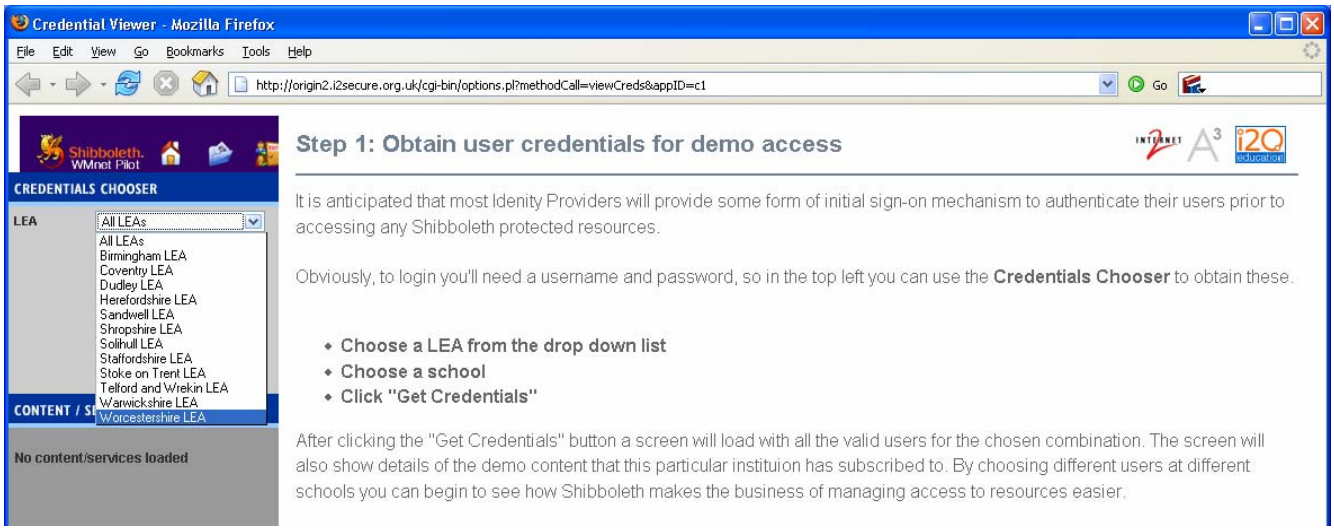
- Data stores used for attributes must be accurate and consistent.

WAYF

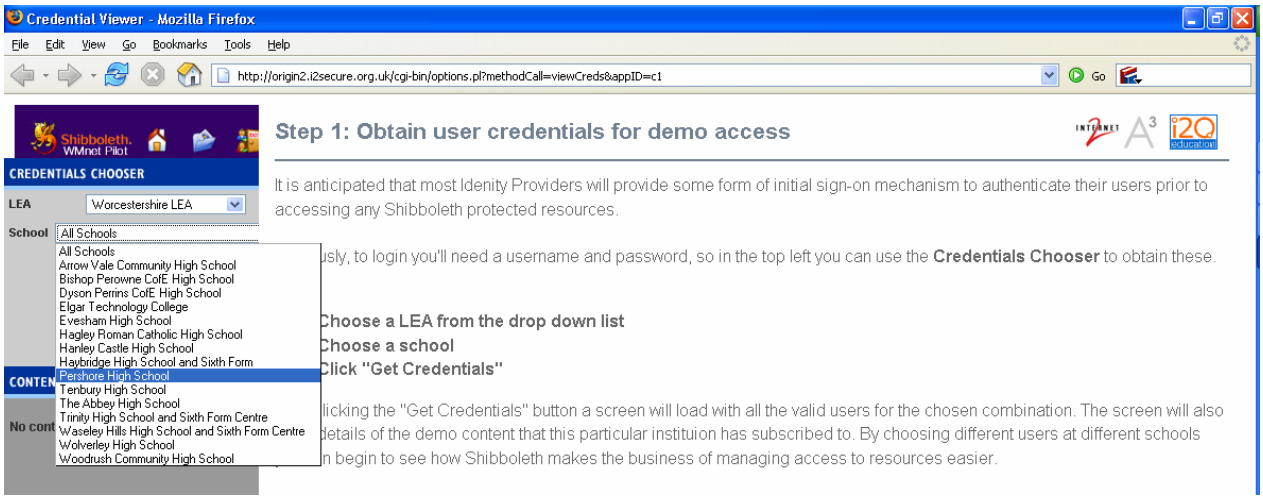
An important issue for further discussion is the design of the WAYF screen. Both LGfL and WMnet have designed different screens for their users, with LGfL's based on users selecting from a drop-down list depending on the type of account they have: LGfL/Atomwide USO (jsmith.123) or LGfL/Digitalbrain portal (jsmith.lgfl).



WMnet has chosen to display a drop-down list of LEAs. Unless accessing via the LEA's portal, a user must first select their LEA from a drop-down list, for example, Worcestershire.



The choice of LEA then determines the list of schools to be displayed. For example, if Worcestershire LEA is selected, then a list of schools in Worcestershire is displayed, allowing a user to then select their school, for example, Pershore High School.



Other design options have been discussed over the course of both pilots, but it is clear that further work in this area is necessary, particularly to take into account usability and accessibility issues. It should also be noted that a WAYF screen can be bypassed or simplified by the use of cookies.

- The federation should investigate WAYF screen usability.

Political issues

During the time an end-user's account resides with an Identity Provider in the school federation, assuming inter-federation operation is possible, students would theoretically be able to continue using their school accounts when they move to HE/FE. However, Identity Providers within the school federation would most likely only deal with Registration Bases in primary and secondary education. Conversely, Identity Providers in HE/FE would only deal with institutions in that sector. Consequently, it is important to note that an account with a school Identity Provider is not an account for life, and the end-user would be expected to move to a new account on a different Identity Provider within an HE/FE federation upon moving to that phase of education. This has important implications if one wanted learning platforms or an e-portfolio to be accessible across the sectors with, by definition, the end-user still having access to their personal content.

- Cross-sector federation issues should be investigated.

If Becta runs or manages the school federation, the implication of the Freedom of Information Act for the federation will be the same as that for Becta, even if the former is provided as an arms-length operation as information "…is held on behalf of the originating public authority by a third party".

Under the Code of Practice on Access to Government Information (1998), Becta is committed to extending access to official information and responding to reasonable requests for data. The Freedom of Information Act (2000) extends this commitment to a culture of openness in government. The Act establishes a right of access from January 2005 to all types of 'recorded' information, including electronic documents, held by public authorities. It imposes obligations on public authorities to disclose information, subject to a range of exemptions.

Individuals already have the right to access their own information held on computer, and in some paper files, under the Data Protection Act 1998. This is known as the 'subject access right'. The Freedom of Information Act will extend these rights to allow access to all the types of information Becta holds, whether personal or non-personal. However, Becta will not be required to release information to which any of the exemptions in the Act applies.

- Becta will need to decide into which of the seven Information Classes the school federation should be placed or whether a new Information Class is required to cover direct service supply.
- Becta will need to consider whether any of the exemptions (qualified or absolute) apply to the information held by the school federation.

Security issues

Although being addressed in Shibboleth 2.0, currently, the end-user browser session, once authentication via Shibboleth has occurred, will not 'log out' of accessed resources until the browser session has closed. A message concerning this situation should be placed in prominent positions on any log-out screen. This will generally be an issue for the Service Provider, but education of end-users by Identity Providers will assist in reducing the possibility of occurrence.

- Instructions must be given to users of the need to close browsers down after accessing content via Shibboleth.

A primary Shibboleth design consideration was to require very little or no modification to client machines. The only requirement is that a browser is used that supports cookies, redirection and SSL. Browser users will have to perform an extra click to submit the authentication assertion if JavaScript is not functional.

- For an end-user to be able to access Shibboleth-protected content, the browser's cookie settings must be set to allow cookies.

Within Shibboleth, certificates are deployed to protect traffic against eavesdroppers and to guarantee the identity of the sender and integrity of the message. It is important that certificates in use are from a recognised Certificate Authority.

- Certificates must be issued by a trusted Certificate Authority recognised by the federation.
- The federation should provide an infrastructure for the distribution of certificates between its members.

Limitations

Shibboleth is a federated solution which allows a user to authenticate with multiple external systems. On its own, it does not provide a single user identity for a teacher and student that will allow them to access external systems and internal school systems at the same time – in its current release, it only functions for web resources. This is internationally recognised as a limitation and is expected to be addressed in Shibboleth 2.0 in mid-2006. This version will use SAML 2.0[13] and will allow the extension of Shibboleth-compliant solutions to beyond the web-based limitation. This will, however, require a change in the way the Handle Service works.

Another limitation to be solved in Shibboleth 2.0 is that of single sign-off. In the current versions, it is necessary for the user to close their browser window following their session as logging off from one application will not log the user out of all the services they may have accessed in that session.

From research and from within the projects, the following important caveats about Shibboleth-compliant solutions have also emerged:

- Not all systems and applications can be made to be Shibboleth-compliant.
- Not all systems, applications and products that could be Shibboleth-compliant may be ready to convert.
- Registration bases may not be ready or prepared to use Shibboleth-compliant services.

From this it can be deduced:

- End-users may still need more than one username/password.
- A Service Provider's application/product set may include a mix of Shibboleth-compliant and non-Shibboleth-compliant applications, which will necessitate the end-user re-authenticating.
- Interfaces between Shibboleth-compliant and legacy systems may be required.

[13] SAML - Security Assertion Markup Language – http://www.oasis-open.org/specs/index.php

Advice for LEAs and RBCs

It is recommended that Shibboleth is implemented at an RBC level in order for aggregation and to lessen administrative issues at the federation. Where this is not possible or local decision deem it to be undesirable, then implementation at LEA level will suffice. It is possible, though unlikely, for large schools or clusters of schools to establish their own Identity Provision.

In moving towards Shibboleth as the system for implementing AAI, each RBC/LEA would be required to set up an Identity Provider platform. It would need to integrate this platform into whatever is currently deployed for authentication or, in some cases, implement a compatible authentication system. Whether this is better achieved as a regional or an LEA activity will depend upon the topology of the regional network. Typically, if the regional network is the sole Internet Access Provider for its member authorities, then the Identity Provider should live at this level.

While the hardware/software costs for implementing an Identity Provider are not high, the data management and maintenance costs would need investigating. As the costs involved will vary depending on many factors, it is not possible to estimate accurately what these would be; however, the information provided here and in the individual reports from the pilots will aid authorities and RBCs in the evaluation process.

By definition, Shibboleth is middleware – it is meant to sit between existing systems – so it should be possible to integrate Shibboleth into most existing set-ups. However, there are certain key requirements that any Shibboleth system must have, so potential Identity Providers will have to evaluate their current set-up before beginning the integration process. A summary of the key requirements for an Identity Provider set-up are:

- an attribute source
- mechanism for web-based authentication of users
- the full DNS name of the server on which Shibboleth will be installed
- firewall configurations
- relevant software depending on the platform on which it is to be deployed
- SSL certificates for Handle Service and Attribute Authority.

As part of the Identity Provider development, the Identity Provider will need to join the national school federation; instructions on how to do this will be provided as soon as the federation is established. The LEA/RBC will then be able to begin the process of establishing Attribute Release Policies (ARPs) with content providers for RBC/LEA-wide content and assist their Registration Bases with local ARPs.

Identity Providers will also need to supply a suitable name for entry into the WAYF screen, a list of the Registration Bases that have selected this partner as the principal Identity Provider and the ARPs in place or required. The details of how to supply these details and what form they should be in will be determined by the federation when it is established.

An LEA or RBC that is a resource provider to its own community of users should also establish its own Service Provider infrastructure. This would have the advantage of allowing users from other RBCs or LEAs to access resources in a controlled manner and allow its own users to easily and securely access resources from off site where access is through a commercial ISP via the internet.

Advice for industry partners

Resource providers would be required to establish the infrastructure of a Service Provider's site within the Shibboleth system. The work required to authorise access to the resources is not onerous and would not involve significant cost. Content providers already protect their resources in a variety of ways, and moving to a common approach should not present them with problems. It would be relatively simple to continue with current authorisation techniques while migrating to the Shibboleth approach.

Service Providers will be expected to integrate their content or authorisation services within the federation's infrastructure and operational policies. They will be allowed to use those AAI services sufficient to meet the needs of the members and this will include being able to replicate the activities of a Registration Base for testing and administration purposes.

To ensure the contractual relationship, Service Providers, as a federation partner, will be expected to enter into agreements that detail their responsibilities and rights, including contractual arrangements for being a federation partner. They will also need to supply a list of attributes they wish to receive (and the relevant Registration Bases that will be affected) to the federation to enable adequate checks that the attributes requested are not excessive in order to identify the range of resources appropriate to the end-user or their membership of certain groups, and to ensure the Registration Base's Identity Provider Attribute Release Policy is linked to the Service Provider's Attribute Acceptance Policy and content licence.

Where a Service Provider also operates Identity Provider services, they are, in effect, two different entities; in order to achieve full Shibboleth-compliance, they must provide two services that communicate with each other through the same mechanisms as if they were different suppliers. If the Service Provider chooses to 'front-end' authenticate their content in a different fashion, they are not providing a Shibboleth-compliant service to their own content.

Appendix A – Becta's Shibboleth pilots

LGfL project scope and deliverables

Officially launched in November 2004, the LGfL pilot aimed to investigate the viability of implementing Shibboleth across the UK school sector as a viable means for authentication and authorisation. Based upon Becta's initial research and laboratory demonstration, the aims of the pilot were to:

- Examine the Shibboleth model in further depth in a 'real world' environment.
- Provide additional evidence of the validity of the Shibboleth model.
- Identify issues arising out of this further examination.

The project's scope encompassed activities by LGfL, Atomwide, PenCompass and IBIS with assistance from DigitalBrain and Equinox Converged Solutions to deliver a working production environment that implements the architecture for the following Shibboleth entities: Identity Provider (Origin), Service Provider (Target) and WAYF.

This environment enables USO (Unified Sign-On) end-users to access Shibboleth-enabled applications situated within their own RBC infrastructures (LGfL, WMnet and other RBCs) from a school base as well as from outside their institution.

Public demonstrations of the working of this architecture were presented at the BETT 2005 show and NAACE conference, both occasions representing staging points of the work in progress.

The main deliverable of this project is a set of documents evaluating the environment, highlighting issues that have arisen from the project and guidelines for the preparation and implementation phases of a national roll-out of an AAA system based upon Shibboleth architecture. These documents consist of the following outputs:

- build specifications for three key entities: Identity Provider, Service Provider and WAYF
- security requirements
- interoperability requirements
- contractual agreements
- acceptance tests
- evaluation
- national strategy.

Build specifications

The Identity Provider and Service Provider build specifications will allow technically competent third parties to build Shibboleth-compliant entities that will function fully within the federation.

The WAYF build specification identifies the technical requirements of the central WAYF service. Within the architecture of the federation, there will be only one WAYF, but its specification has been produced for completeness, and to enable examination by others to ensure full compliance with Shibboleth.

All the LGfL build specifications use Shibboleth v1.2 and each supplier (Atomwide and Digitalbrain) has provided an Identity Provider that has inbuilt redundancy and resilience. However, this has been achieved by different solutions: Atomwide's solution is based on MS Windows server 2003 SE while Digitalbrain's solution runs on Ubuntu Linux.

Connectivity, physical environment and security (both physical and systems) are also described. The client requirements for Shibboleth are confirmed as consisting solely of the end-user's browser, a number of which were tested on Windows, Linux and Apple machines with no issues. It is important for security permissions in the browser to be set to accept cookies for Shibboleth to work. It is also important to note that the end-user's browser session, once authentication via Shibboleth has occurred, will not 'log out' of accessed resources until the browser session has closed, therefore a message concerning this situation should be placed in prominent positions on any log-out screen.

This will generally be an issue for the Service Provider, but education of end-users by Identity Providers will assist in reducing the possibility of occurrence.

Identity Provider build specification

The Identity Provider specification describes the hardware used and the application software, as well as a review of the certificates used. Both suppliers installed and used certificates from GlobalSign – as used by JISC's SDSS Federation[14].

Within the project, certificates are deployed for two purposes:

i) HTTPS communications – to protect traffic against eavesdroppers.
ii) The signing of messages that are carried as part of HTTP communications – to guarantee the identity of the sender and integrity of the message. This second situation is referred to below as TLS (Transport Layer Security).

Most importantly, the specifications describe the configuration process where it deviates from the standard process as defined within the original Internet2 Shibboleth documentation.

Federation interface requirements are covered, describing that an Identity Provider is the authentication side of Shibboleth-compliant systems. The Identity Provider service is where the end-user's attributes are stored for the purpose of authenticating who they are, and what roles and rights they have. Identity Providers will therefore need to know what they can legitimately send to the Service Provider, and will wish to be protected from Service Providers attempting to gain extra attributes. To prevent this from happening, it is proposed that there will be two legally binding agreements in place: an Attribute Release Policy and an Attribute Acceptance Policy.

- **Attribute Release Policy (ARP)** – This will take the form of an agreement, drawn up and managed by the Attribute Control Authority (ACA), between the individual Registration Base and the Identity Provider. The agreement would list the attributes that the Registration Base will permit to be released by that Identity Provider to a specific Service Provider. The Identity Provider will be legally prohibited from releasing other attributes without a variation being formally agreed by the Registration Base.
- **Attribute Acceptance Policy (AAP)** – This will take the form of an agreement, drawn up and managed by the ACA, between the Service Provider and the Identity Provider as a back-to-back agreement to the ARP, possibly as a co-signed page of the ARP. The agreement will list the attributes that are controlled in the ARP and which the Identity Provider will be permitted to release to the Service Provider. Although, technically, the Service Provider cannot engineer the release of other attributes, they will be legally prohibited from entering into an arrangement with an Identity Provider for the unapproved release of attributes.

In addition to the two agreements above, the Identity Provider will be expected to enter into agreements that detail their responsibilities and rights as a commercial organisation operating with federation members.

Service Provider build specification

This document describes the issues surrounding the building of a Shibboleth-compliant Service Provider. It gives the details for two very different environments in which the Service Provider server and services may be located and should contain sufficient detail for a technically competent organisation – whether school, LEA, RBC or commercial provider – to provide an authorisation service that is Shibboleth-compliant and which will function with other Shibboleth-compliant entities.

As with the Identity Provider build specification, the Atomwide and Digitalbrain solutions are based respectively on MS Windows Server 2003 and Ubuntu Warty Linux. However, it was found that the Shibboleth Service Provider did not run correctly under 64-bit Linux and so it had to be run in a 32-bit environment. Full details of the hardware, load balancing, software, connectivity, physical attributes, environment security and certificate usage are described in this document.

[14] http://www.sdss.ac.uk/

Installation and configuration guidance is given where it differs from the original Internet2 documentation.

Federation interface requirements

A detailed discussion of the federation interface requirements is given, containing information about the use of ARPs, AAPs and content licences. It must be noted that the Service Provider service is the content or resource provider side of Shibboleth-compliant systems, it does not provide authentication. The Service Provider service is concerned that the content is only ever accessed by those who are authorised do to so in order to protect their intellectual property rights and copyrights.

A Service Provider does not necessarily need to know 'who' an end-user is – for example, Jane Smith – but 'what' the end-user is – for example, Wallington Girls School, Year 10, geography. For many Service Providers, this is acceptable as all they wish to know is that an end-user belongs to a licensed institution. There are, however, content providers who will wish to direct an end-user to the same set of resources, possibly their own document area, each and every time they return to this service. Instinctively, the reaction is that the Service Provider has to create an authentication service to manage this. With a Shibboleth-compliant system, this is totally unnecessary, and actually runs counter to the underlying philosophy. Details of how this can be achieved using special attributes can be found in the *Issues and recommendations* section above.

In addition to the Attribute Release Policy and Attribute Acceptance Policy, Service Providers will need to agree content licences with the Registration Base that agree with the ARP and AAP. The Service Provider will also be expected to enter into agreements that detail their responsibilities and rights as a commercial organisation operating with federation members.

Clock synchronisation is another important issue for Service Provider servers. An NTP/SNTP client must be configured to operate against a reliable and accurate time source as a difference of more than three minutes between the Service Provider and Identity Provider will cause authorisation to fail.

WAYF specification

The purpose of this document is to specify a standard build for WAYF servers and associated services, along with install, configure and management requirements. It should be noted that it is not envisaged for the WAYF service to be managed and delivered by more than one organisation. However, as the failure of the WAYF service means all Shibboleth-dependent services fail, it is important for all organisations (Identity Providers, Service Providers and users) to be assured of the resilience, robustness and redundancy factored into the WAYF solution, which is why the architectural design and specification has been documented.

The document includes the following:

- References to the integration of WAYF servers and services into the overall design of a national Shibboleth-based AAA service.
- Identification of the physical and administrative locations required within the possible overall national Shibboleth-based AAA service designed to address issues of resilience and redundancy.
- An expansion of the technical specifications for the WAYF as shown in the existing demonstration/proof of concept model.
- The specification and information on:
    - operating platform
    - hardware
    - application software
    - certificates
    - connectivity
    - physical attributes
    - power and climate
    - security – physical and systems
    - accommodation
    - management – remote/local

- installation
- configuration
- support
- interface requirements
- client configurations.

The role of the WAYF is crucial to the operation of a Shibboleth-compliant system and is a 'simple' mechanism by which the end-user, Service Provider and Identity Provider entities are linked. The WAYF service has to be reliable and resilient; if it is not, then the end-user cannot access the content as the Identity Provider cannot be reached for Shibboleth-compliant authentication and, thus, the Service Provider cannot receive the set of attributes upon which to base authorisation checks.

Of relevance here, and a less well-considered aspect of a Shibboleth-compliant system, is that where a Service Provider also operates Identity Provider services, they are, in effect, two different entities. This means that for full Shibboleth-compliance they must provide two services that communicate with each other through the same mechanisms as if they were different suppliers. If the Service Provider chooses to 'front-end' authenticate their content in a different fashion, they are not providing a Shibboleth-compliant service to their own content.

This situation was identified and resolved within the project with each commercial organisation creating both Identity Provider and Service Provider services which were used to authenticate/authorise each other and each other's content.

Should the WAYF fail, not only will different suppliers' Identity Providers and Service Providers be 'off the air', but the same supplier's Identity Provider and Service Provider will also be unable to communicate. This has serious implications for its design, delivery and management.

In terms of other WAYF functions, although all the end-user will typically see is a simple screen from which they select their Registration Base, there is much that lies underneath this in terms of interoperability and service terms.

Of significance are:

- The WAYF service is underpinned by a database.
- The database has the details of Registration Bases; these details are provided from the EduBase[15]. service and require periodic updating and maintenance. The back-end link between each Registration Base and its primary Identity Provider also requires population and maintenance.
- The underlying database will need to store details of accredited Identity Providers.

Security requirements

This output considered all the security issues surrounding the implementation of a national service, including a description of the requirements for physical and logical security. The area of physical security includes references to 'soft' issues, such as vetting of staff, while logical security includes issues surrounding software, SSL/TLS, HTTPS, certificate procurement and certificate distribution.

Where possible, reference is made to the developments underway in the US by the Internet2 group in providing the InCommon Federation and those undertaken in Switzerland by the Swiss Education and Research Network (SWITCH) in providing the SWITCHaai Federation.

It quite clearly states that the school federation must operate in a tightly regulated environment to ensure the security of its systems, processes and stakeholders, the most important of which are the children who will be using the services safeguarded by the Shibboleth-compliant infrastructure. To achieve this level of regulation will require organisation and processes sufficient to manage, accredit, evaluate and enforce those matters highlighted.

[15] http://www.edubase.gov.uk/

Interoperability requirements

This document examines the various interoperability issues that the federation will face or have to address and contains recommendations on the essential requirements for that service. Key among these recommendations is the structure of the federation and the interrelationship with, and between, the various stakeholders.

Interoperability is taken to include the requirements for the operation and interaction between Shibboleth-compliant systems, federations and non-Shibboleth-compliant systems, including components, people, organisations and systems.

Contractual agreements

Building upon the *Interoperability requirements* document, this output contains descriptions and a significant number of the model documents for the legal relationships and agreements, including service descriptions, service-level agreements and ESCROW. Generic issues include compliance with the Data Protection Act, limitation of liability, Acceptable User Policies, terms of use, IPR, accreditation and service agreements.

A key issue arising from analysis of the above is that all participants in a Shibboleth-compliant world have to 'trust' each other. In order to enjoy the appropriate level of 'trust', there will need to be a number of supporting documents, including:

- WAYF service description – This lays out in detail what the WAYF service will deliver, containing such information as contact details, hours of operation, pre-requisites, performance metrics, fault-reporting arrangements, escalation procedures, and so on.
- WAYF service contract: Identity Provider – This consists of a contract between the federation, as the WAYF service deliverer, and the Identity Provider detailing the rights and responsibilities of each party. This would not be the same contract as for the Service Provider, as items such as registration and naming permissions would be different.
- WAYF service contract: Service Provider – This is a contract between the federation, as the WAYF service deliverer, and the Service Provider detailing the rights and responsibilities of each party.

Acceptance tests

The acceptance testing undertaken on the production environment was structured to determine whether different commercial providers could access the Shibboleth-compliant solution – using the WAYF environment proposed for the national service – without loss of service under a range of realistic conditions. This detailed document covers acceptance testing to determine:

- Compliance with the architectural design and other documentation
- Readiness for deployment
- Any remediation or enhancements that may be required in subsequent releases.

Evaluation

IBIS Business Consultants Ltd was engaged to provide an independent assessment of the implementation within LGfL of an authentication and authorisation infrastructure using the Shibboleth package designed and developed by the Internet2 consortium.

The purpose of the evaluation was to verify that the solution complies with the Shibboleth standard, and to assess the solution's scalability.

The evaluation was carried out by scrutiny of the specification documents listed in the AAAI – Document Set and by visiting the two companies (Atomwide and Digitalbrain) retained by the London Grid for Learning Trust to carry out the implementation.

Scrutiny of the specification documents, system demonstrations and interviews with the technical staff all indicated that the solution now in place is fully Shibboleth-compliant.

On the basis of the work of the LGfL Shibboleth project, the following may be stated:

- Shibboleth-compliant technology, within the complexity of the school sector, will work at a technical level.
- The scalability of the system is considered appropriate for purpose.
- The business benefits will be, in the main, realised.
- For effectiveness, the national strategy requires the creation of mechanisms that:
    - deliver various services
    - manage standards for and of all parties
    - minimise the administrative burden for all parties
    - allow for further development of the AAI solution.

National strategy

This document lays out the strategy for implementing a national solution to provide an authentication and authorisation infrastructure based on a Shibboleth-compliant model. Reference is made within the documentation to the third area of AAA, that is, accounting, but the actual provision of this service is left for further development within the remit of the federation.

The strategy looks at the creation and provision of a federation managed by Becta, the Becta AAI Federation, in delivering appropriate services to its members. The term 'member' (and their Registration Bases) is defined elsewhere, but it is important to stress that principally this will apply to LEAs, schools, RBCs and, exceptionally, other organisations with similar aims and objectives. The role and remit of partner organisations responsible for the delivery of authentication and content services are fully covered within this strategy.

Becta now has sufficient evidence and experience from the various projects to proceed to the implementation of a national Shibboleth-compliant AAA infrastructure.

In broad terms, the achievement of this requires the following stages:

- statement of strategic direction
- creation of the Becta AAI Federation as an entity
- sourcing of sufficient resources to guarantee delivery
- creation of the underlying services
- creation of various legal documents
- establishment of procedures
- recruitment of stakeholders
- entering into contractual agreements by various parties
- ongoing development of the federation's services
- interaction with national and international bodies
- provision of the operational aspects of the federation.

LGfL project conclusion

External evaluation has proven that Shibboleth works with multiple vendors and will scale to a national level. As part of an extension to its involvement in the AAA Shibboleth project, LGfL has implemented a regionally-based, Shibboleth-compliant federation. This decision was taken on the grounds of educational validity of the Shibboleth-compliant model. The LGfLaai Federation has all the characteristics, procedures and agreements described in the AAA Shibboleth document set.

The LGfLaai Federation officially went live in July 2005 with the management tasks being undertaken by existing LGfL staff. The matrix of schedules, procedures and contracts in place during the pilot are so far working as expected in the live regional federation.

WMnet project scope and deliverables

The WMnet Shibboleth pilot began in February 2005 with i2Q Ltd working with three WMnet LEAs: Birmingham, Shropshire and Worcestershire. The original intention was to establish a number of demonstration Shibboleth Identity and Service Provider sites, and to provide useful guidance for future users in the UK education sector. In a number of ways, the original focus of the WMnet pilot shifted as set-up and configuration issues required further investigation.

The main deliverable of the WMnet pilot is a project website [http://origin2.i2secure.org.uk/] consisting of a working demonstration of Shibboleth and a set of documents including IdP and SP set-up, configuration guides, discussions of Initial Sign On solutions, unique identifiers and attribute usage, as well as national issues that need resolving concerning federations, metadata and extending common attribute schemas.

Specifically, the pilot deliverables are:

- General documents:
    - *Executive Summary* – This short summary outlines the purpose of the pilot and the main findings.
    - *Pilot Findings* – This guide provides a short overview of the pilot findings.
    - *Next Steps* – This guide suggests some of the obvious next steps for Shibboleth in the UK school sector.
- Pilot details:
    - *Pilot Introduction* – This guide provides steps for setting up and running the Shibboleth Service Provider 1.2 software.
    - *Pilot LEAs* – Summarising the original goals for each of the three pilot LEAs.
- Identity Provider documents:
    - *Identity Provider Set-up Guide* – This is a step-by-step guide for setting up and running the Shibboleth Identity Provider 1.2 software.
    - *Identity Provider Configuration Guide* – This guide provides an annotated configuration guide for the main Identity Provider configuration file.
    - *User Data and Local Authentication* – This guide summarises the user data and local authentication requirements for Shibboleth presenting a number of alternative solutions.
    - *Authentication and Authorisation* – This guide looks at the general issues surrounding authentication and authorisation.
    - *Alternative Local Authentication Solutions* – This guide takes a very brief look at alternative local authentication solutions.
    - *Self-Registration and Unique Identifiers* – This guide presents a possible solution for generating unique identifiers for use with Shibboleth by a process of self-registration.
    - *Attribute Usage* – This guide summarises a variety of approaches to attribute usage including brief notes on using LDAP as an attribute store and how to configure the Identity Provider to use LDAP.
    - *Minimum and Default Attributes* – This guide summarises some of the current thinking on the minimum and default attributes required for Shibboleth.
    - *SSL Requirements Guide* – This guide gives an overview of the SSL certificate requirements for running Shibboleth including notes on how to generate the certificate signing request.
    - *Apache 2 Bug* – This guide provides a workaround for using Shibboleth 1.2 with Apache 2.
- Service Provider documents:
    - *Service Provider Set-up Guide* – This is a step-by-step guide for setting up and running the Shibboleth Service Provider 1.2 software.
    - *Service Provider Configuration Guide* – This guide provides an annotated configuration guide for the main Identity Provider configuration file.
    - *Protecting Resources with Shibboleth* – This guide provides an overview of how to protect resources using Shibboleth, including detailed notes on how to set up Apache and the specific configuration requirements.

- Pilot demonstration:
    - *Introduction* – This guide provides a brief overview of the pilot demonstration.
    - *Demonstration Notes* – This guide provides notes on the way the pilot demonstration works and a user guide with simple steps and screenshots.
    - *Demonstration Configuration Guide* – This guide provides details on how both the Identity and Service Provider components were set up to function within a test federation. It also provides brief notes on how to protect resources using Shibboleth and basic settings for attribute retrieval from LDAP.
- National issues:
    - *Federations* – This guide provides a brief overview of Shibboleth federations.
    - *Metadata* – This guide provides a brief overview of the use of metadata within Shibboleth, including sample metadata files.
    - *EduPerson Schema* – This guide provides a detailed exploration of an alternative to the EduPerson schema.
    - *Cost Estimations* – This guide provides details of the costs involved in setting up Shibboleth for potential Identity and Service Providers. The information here is based on the findings of the Swiss Shibboleth Project SWITCH.

Pilot details

Originally, data collection was seen as the key issue and in Worcestershire LEA the focus was solely on the methods of extracting data for use within Shibboleth. However, as the investigations continued, it became clear that obtaining and managing user data, though a significant issue, had to be considered in the context of the overall portal and user management architecture in place. As many RBCs and LEAs already have a portal of some kind and will have considered, and in many cases solved, the issues relating to the collection and management of user data, the question for the pilot became one of how to integrate the Shibboleth identity management system more generally.

This focus shift led to two crucial outcomes: first, an investigation and implementation of a flexible Web-based Initial Sign On (WebISO) mechanism that allows the Shibboleth Identity Provider software to integrate with an existing portal authentication system; the second involved the investigation and implementation of an LDAP schema to facilitate the storage of user data in a hierarchical structure that would reduce the burden of managing user's unique identifiers.

In Birmingham, the focus was originally intended to explore the issues surrounding Shibboleth's use of attributes. This investigation quickly showed that although the management of such attributes is an important issue, the first and most serious issue concerned the practical steps that would need to be in place for any kind of attribute exchange to occur between Identity and Service Providers in the first place. This led to a further investigation into the way Shibboleth enabled sites to interoperate in a federation and how the metadata issued by the federation would ultimately determine the type of attributes available. To this end, a test federation was set up in order to fully explore the role of metadata. All the servers in the demonstration are part of this test federation.

In the final participating LEA, Shropshire, the focus was specifically on how a Service Provider uses Shibboleth to protect its resources. This investigation has led to a fully working demonstration of a Service Provider Shibboleth set-up with extra non-Shibboleth components to simplify the management of protected resources. While a basic Shibboleth Provider set-up that protects a single resource is relatively straightforward, a significantly greater degree of configuration and management is required to protect multiple resources; therefore, the investigation focused on the extra configuration required and on various methods of simplifying the long-term management of such configurations. This has resulted in the development of a Service Provider that can host any number of protected resources, each with the option to have specific attribute policies, and which are all handled through one HTTP server set-up.

Identity Provider documents

As part of the Identity Provider set of deliverables, a detailed guide to installing and configuring the Shibboleth Identity Provider software on the Red Hat Linux platform has been provided. Aimed at

system administrators who will be responsible for establishing Shibboleth services in their organisation, this guide outlines the software used in the pilot and instructs how to install the required software.

The documentation includes details of setting up test certificates and SSL keys for testing purposes; however, it should be noted that the decision on which production certificates to use will be decided and supported by the national federation (see *Issues and recommendations* section).

The user data requirements for Shibboleth Identity Providers is discussed, covering the issues of user privacy, local authentication, minimum data requirements and a high-level overview of setting up a user data store.

The *Authentication and Authorisation Guide* describes how to establish a local authentication system that integrates with an Identity Provider, including a detailed description of the required configuration required. This section is of particular interest to potential IdPs that do not currently have a WebISO mechanism.

The *Unique Identifiers Guide* concentrates discussion on the issues surrounding the creation and management of unique identifiers, including a solution for obtaining unique identifiers through user self-registration. This method is based on a process developed by Worcestershire LEA in the roll-out of its Virtual Workspace Project[16], but will need further debate and investigation before it can be widely recommended.

The *Attribute Usage Guide* covers the issues surrounding attribute availability and release, including a discussion of a potential solution for extracting attributes from an LDAP directory. An important development from this pilot is the investigation of a solution developed by the University of Washington into a web interface to allow the release of attributes to be permitted or denied.

The *Minimum and Default Attribute Sets* document discusses the issues surrounding the use of attributes within a Shibboleth system, including a discussion on the emerging minimum attribute set. This was discussed in the Issues and recommendations section.

The *SSL Requirements Guide* outlines the basic steps required to obtain SSL certificates and how they are referenced by Shibboleth. It should be noted that the federation will be responsible for managing the Certificate Authority.

Service Provider documents

The *Service Provider Set-up Guide* provides a detailed guide to installing and configuring the Shibboleth Service Provider software on the Red Hat Linux platform. The guide expands upon the Internet2 installation guide and illustrates how to build the software on a single host for testing and then extends these instructions to cover installation across two or more hosts.

The *Service Provider Configuration Guide* provides an annotated guide to the SP configuration file which also explores joining a genuine federation and advanced set-up issues such as metadata management and data population.

The *Protecting Resources Guide* is a reference that provides information on how to protect resources using Shibboleth, including a discussion of configuring separate applications in the SP configuration file.

Pilot demonstration

To demonstrate that Shibboleth is a transparent and seamless aspect of the information architecture, and to help explain the key concepts involved, a demonstration has been developed to guide the user through each step in a Shibboleth transaction and present some of the key information that is exchanged between Identity and Service Providers.

[16] http://www.worcestershire.gov.uk/home/edu-index/edu-virtual-workspace.htm

The demonstration embodies many of the pilot findings. For example, when logging into the demonstration the details the user enters are authenticated against an LDAP directory in what is effectively a WebISO. This initial sign-on is not strictly part of Shibboleth, but as part of the pilot it became clear that as many LEAs and RBCs would want their users to log into their portals first, a WebISO component was required. Subsequent Shibboleth-based transactions integrate with the WebISO architecture in order to confirm that a user is authenticated before a Service Provider makes its authorisation decisions.

Other key pilot findings implemented in this demonstration are:

- LDAP schema which provides a set of attributes useful to the UK school sector
- hierarchical LDAP tree structure to facilitate institution-wide unique identifiers
- SSL-protected Attribute Authority and Handle Service using Apache 2
- custom-built Java data connectors for use in Attribute Resolve component
- scoped and non-scoped Attribute Release
- optional Attribute Release Policy editor
- multiple applications hosting on single Service Provider
- opaque Persistent Identifier
- membership of test federation with valid metadata
- NTP (Network Time Protocol) implementation.

Information on accessing and using the demonstration can be found at http://origin2.i2secure.org.uk/demo_rbc_notes.html, where screenshots and detailed guidance are provided.

The demonstration provides a good overview of the Shibboleth transaction in progress; however, it also raises a number of key questions which the UK schools' technical community will need to consider. These issues are discussed below.

The demonstration also provides an Attribute Release Policy editor to illustrate how changes to the Attribute Release Policy govern the way that information is released to Service Providers.

This section additionally includes a *Configuration Guide*, detailing how the demonstration was set up as a study of how an LEA might implement Shibboleth, providing details of how both the Identity and Service Provider components were set up to function within a test federation.

For the purposes of the demonstration, user data was extracted from the school MIS using the standard data extraction facility and then securely uploaded for processing. This is then made available to an LDAP server to provide authentication for the WebISO and to act as an attribute store for the Shibboleth attribute request/release process. In lieu of an LEA-wide unique username system, the demonstration uses a concept of Realm-based authentication where a username only has to be unique within an institution.

National issues

The pilot has raised a number of issues that affect or influence the national implementation of Shibboleth in the school sector. These are outlined here, but were discussed in detail in the Issues and recommendations section.

The *Federations Guide* provides a brief overview of the issues surrounding Shibboleth federations, including a discussion of how they operate and how to become a member. The *Metadata Guide* describes the use of metadata within Shibboleth, including sample metadata files – these files specify the identities of all Identity and Service Providers, including details of the exact locations of such components as Attribute Authorities, Handle Services and Assertion Consumer Services as well as providing the raw, encrypted values from various Certificate Authorities. These files are signed by the federation to guarantee their authenticity and are retrieved by the federation's Identity and Service Providers on a regular basis.

The eduPerson schema guide is a useful discussion of the issues surrounding the eduPerson LDAP schema – the attribute store chosen by most current Shibboleth organisations. This guide explains how it was found to be necessary to extend the schema in order to provide the relevant attributes for school sector authorisation.

The final deliverable from the WMnet pilot is a brief look at the possible costs associated with setting up Shibboleth. The cost estimations presented here have been converted from the work undertaken by the Swiss Shibboleth project SWITCH. The SWITCH work was aimed at an HE federation with a different infrastructure and scale to the proposed UK schools' federation, so the costs cannot be taken as being comparable; however, the type of work and purchases required are similar, which is why this section is included.

WMnet pilot conclusion

Although the pilot's initial focus was a set of very specific investigations that directly involved the participating LEAs, it developed to become a much broader investigation. The resulting pilot has provided a greater understanding of the whole picture. It is now possible to see clearly how Shibboleth can work effectively in the UK school sector.

Appendix B – possible federation model

This appendix contains details of a proposed federation model for further discussion and should not be assumed that this model will be adopted. An EU-compliant tender process for the setting up and running of a national federation will be launched towards the end of 2005.

Full details of the proposed model can be found in "Becta AAI - Organisation and Structure.doc", but a summary is presented here.

The LGfL pilot has developed a possible federation model for the national school federation – what they have termed the Becta AAI Federation. The Becta AAI Federation builds on LGfL's existing regional federation – LGfLaai – and has characteristic differences from other federations in Europe, the USA and from others in the UK due to the different nature of the school sector. The key difference relates to the significant presence of commercial organisations that are delivering services which in other federations are delivered by members or the Registration Base. This difference is reflected in the proposed constitution of the federation members and partners.

The main functions of the Becta AAI Federation will be as follows:

- infrastructure – design, delivery and maintenance
- contractual agreements
- Attribute Release Policies
- WAYF service
- accreditation service
- support services
- management.

Service provision

The provision of AAAI services is through the Becta AAI Federation acting on behalf of Becta. Some of these services will be delivered directly from the Federation's service team and others may be through a third-party service delivery provider. Where a third party delivers services to the Becta AAI Federation, the agreement will be with Becta.

Becta will be responsible for the provision of the Becta AAI Federation service as it is defined in the Schedule for the Service Description of the basic service, and any extra and optional services made available from time to time. All relevant agreements with the appropriate stakeholders and other federations will be with the Becta AAI Federation acting on behalf of Becta.

The Becta AAI Federation will manage and lead a Federation Partners' Forum on behalf of Becta. This Forum will be held once a year.

Federation members

Federation members will be drawn from the community of RBCs, LEAs, or groups of schools with a formal constitution of their own federated arrangements. Exceptionally, non-profit-making educational organisations may be accepted as members where their aims and objectives are broadly in line with those of the existing members. The members will represent organisations that act as Registration Bases. Where a federation member additionally offers services equivalent to that of a federation partner, they will have to additionally adhere to the same regime of regulations as if they were a partner.

Registration Bases

A Registration Base is an organisation to which end-users are registered. The term 'registered' may be taken to mean, in the formal sense, of 'being on the school roll', or, in a less formal sense, employees of a federation member. A Registration Base will be required to:

- Formally confirm that their registration processes meet the federation's standards and that their authentication processes are auditable.

- Operate, directly or indirectly, a helpdesk, or equivalent, which is capable of addressing AAI-related issues.
- Maintain an up-to-date Attribute Release Policy, and associated licence agreements, for all content and resources which the Registration Base and its end-users are entitled to access.
- Ensure all security requirements are adhered to including safeguarding user IDs and passwords, and use of certificates from Becta AAI-approved Certificate Authorities.
- Ensure full compliance with the Data Protection and Computer Misuse Acts.
- Maintain sufficient records to assist in any investigation of wrongdoing by the Becta AAI and relevant authorities.

A Registration Base cannot delegate its role within the federation to a federation partner.

Federation partners

Federation partners will generally be commercial organisations that deliver AAI-compliant services to federation members and Registration Bases. These services may include content production, content delivery or authentication services. A commercial organisation that manages end-users on behalf of a Registration Base also falls into this category.

Federation partners will be expected to integrate their content or authentication services within the federation's infrastructure and operational policies. They will be allowed to use those AAI services sufficient to meet the needs of the members.

Federation partners cannot be regarded as Registration Bases as they do not represent, or have the same legal responsibilities for, the end-user communities.

A federation partner will be required to:

- Enter into the defined contractual arrangements for being a federation partner.
- For Service Providers, supply a list of attributes they wish to receive, and the relevant Registration Bases that will be affected, to the Becta AAI. The reasons for this are to:
    - enable adequate checks that the attributes are not excessive in order to identify the range of resources appropriate to the end-user or their membership of certain groups
    - ensure the Registration Base's Identity Provider Attribute Release Policy is linked to the Service Provider's Attribute Acceptance Policy and content licence.

The federation will give written approval to the partner and maintain records of the Attribute Acceptance Policies and the Registration Bases to which they apply.

- For Identity Providers, supply a suitable name for entry into the WAYF screen, and a list of the Registration Bases that have selected this partner as the principal Identity Provider and the Attribute Release Policies in place or required.

The federation will give written approval to the partner and maintain records of the approved name, principal Identity Provider relationships and the Attribute Release Policies.

- For all Service Providers and Identity Providers, the partner must supply and use certificates that are Shibboleth-compliant and come from a Certificate Authority that has been approved by the Becta AAI.
- Ensure full compliance with the Data Protection and Computer Misuse Acts.
- Maintain sufficient records to meet legal obligations, for example, the Data Protection Act.
- Maintain sufficient records to assist in any investigation of wrongdoing by the Becta AAI, relevant authorities, federation members and Registration Bases.
- Ensure metadata is up to date and meets the requirements as defined by Becta and the UK Government standards[17]. This will include files (such as sites.xml) which are published by the federation on a regular basis for download and installation by all partners.

[17] http://www.govtalk.gov.uk/schemasstandards/metadata_document.asp?docnum=872

Operations Manager

The Becta AAI Operations Manager will be responsible for:

- ensuring the Becta AAI range of services performs to the appropriate specifications and outputs on a day-to-day basis
- identifying best practice on technical, operational and security issues
- operational aspects of contractual matters
- ensuring Attribute Release Policies are rigorously enforced
- change management and control
- line management for the Becta AAI Federation Service Team.

Federation Service Team

The Federation Service Team is responsible for the day-to-day operation of the Becta AAI services and will support the following functions:

- infrastructure integration
- WAYF service
- Attribute Control Authority service
- accreditation service
- support services
- management
- contractual agreements.

Federation Steering Group

The Federation Steering Group will represent the Federation's members and Becta. Acting in an advisory capacity, it will consider and make recommendations to Becta on the development of the service(s) and the long-term strategy for the Becta AAI Federation.

The Steering Group's remit will cover the following areas:

- creation and overall control of AAI projects
- budgetary responsibility
- Federation matters such as membership, inter-federation relationships
- AAI strategy
- policies and procedures
- business continuity
- service development
- accreditation and approval of federation partners.

It is proposed that the Steering Group's composition will initially consist of the Becta AAI Operations Manager and representatives from the RBC Technical Group, an LEA representative, an LGfL representative, a school representative and representation from DfES/Becta.

Costs

It must be understood that accurate estimations of the cost involved in 'Shibbolising' an LEA is not possible without a detailed analysis of the LEA's existing infrastructure. The greatest cost involved will be ensuring that the correct data is available, up to date and accessible.

The LGfL pilot has come up with a detailed breakdown of the purchases and work involved, but not all of these will be required for every LEA. It is also likely that most running costs are already being experienced by LEAs in their existing data management and authentication systems.

For a national model with a staff of six using web-based administration tools to run a federation covering 26,000 schools and at least 170 providers (RBC, LEA and main SPs), the central federation costs have been estimated at £831,448 for initial costs and £506,546 in running costs. The initial costs are broken down into salaries (for setting the standards, legal and contractual work, federation

resourcing, communications and strategy management), services (insurance, connectivity, certificates, WAYF, legal and ESCROW), programme management, 10 per cent contingency and VAT.

Running costs are broken down into salaries (for running the federation), premises (rent/lease, rack space, new services – air conditioning, electrics, connectivity, etc), equipment, services (maintenance, helpdesk, connectivity, WAYF, attribute clearing house, certificates), ESCROW, programme management, 10 per cent contingency and VAT.

There will be an initial outlay for LEAs to establish or procure Identity Provision for their Registration Bases and to ensure user data is in a usable state. This may involve the purchase of additional hardware, software and certificates, programming costs for installing the Shibboleth software and integrating it with existing or new authentication systems and user directories, and the addition of new attributes and conversion into correct data formats. There may also be extra costs required for project management, education and documentation. Running costs for LEAs will be maintenance fees and hardware upgrades, support costs, software upgrades, security audits, Attribute Release Policy configuration and continuing education costs.

Where an LEA already has an up-to-date user database and has methods in place for managing the user data, it obviously makes sense to use this data for Shibboleth. If, for example, the user data exists in an SQL database, against which checks are made when a user logs into a portal, it should be possible to integrate a Shibboleth Identity Provider without too much effort or cost. Where an LEA does not have a relevant data store, productivity savings can be achieved by establishing a data repository that can be used in a Shibboleth implementation and for all other data processes.

Ideally, further work is needed to determine the costs, but this may not be possible or advisable without actually implementing Shibboleth itself. The important consideration to bear in mind is that the figures should not be seen in isolation. The educational benefits that are gained by a national implementation of Shibboleth are vast and any return on investment calculations should not be judged purely in monetary terms.