CASE STUDY

September 2009

Worcestershire LA

Part of Worcestershire County Council

The UK Access Management Federation
FOR EDUCATION AND RESEARCH

Interviewed: Dave Thomson, Education Improvement Adviser, Learning Technologies
Rob Jervis, Broadband Support Officer

BACKGROUND

Worcestershire County Council manages the role of Local Authority (LA) within the county, with over 96,000 students and 11,000 staff spread over a wide geographical area. 80,000 of these have now migrated to Global Identities, a single sign-on service developed by the LA that uses Federated Access Management to give access to resources from the LA and other providers. Global Identities builds on a pre-existing single sign-on system that the LA had already developed a few years previously, originally based on OpenLDAP.[1]

The LA covers a fairly rural area. Population centres like Redditch, Kidderminster and Worcester are surrounded by over 600 square miles of countryside. The LA's Children's Services Directorate caters for approximately 240 schools of all types: high, middle, primary and special needs. The variety and the geographical spread make it difficult to provide for some schools, and so looking at alternative technologies that will help has always been a priority. Dave Thomson, Education Improvement Adviser, Learning Technologies says that "our high schools were connected to a broadband infrastructure a year or two before national broadband developments were really being promoted." Having this infrastructure in place helped when it came to developing Global Identities.

AHEAD OF ITS TIME

Global Identities is based on Shibboleth but Worcestershire had actually developed a single sign-on system for managing its educational resources before Shibboleth emerged. The driver for this was a DfES strategy called Curriculum Online, which made funding available for digital materials used in schools. Dave Thomson's concern was that "we could end up just buying CDs and the odd bit of online content." A few years ago, therefore, Children's Services began to look at how it could aggregate access to online content.

The result was an internally developed concept called Content Stream which was then converted into a working service by one of the LA's commercial partners. Dave recalls: "We needed to be able to provide, through a single username and password, access to multiple content repositories. These were mostly commercial: for instance Learn Premium, Proquest and other sellers of digital materials that were eligible under government grant funding. We met with about ten of them and asked what they needed us to have in place for this to work. One memorable answer was: to know that the people who used their content were the appropriate users, i.e. they had paid for it!"

Because of the existing broadband model, the LA was able to incorporate an OpenLDAP directory service within its infrastructure which authenticated users' e-mail addresses. This then provided authentication for Content Stream and, with the agreement of the suppliers, access to the content was enabled through a single username and password. In addition, the XML manifest that described the content was brought into the online repositories, enabling cross-repository searches. "So," Dave says, "we had a federated access model without knowing there was such a thing as Federated Access Management."

[1] Lightweight Directory Access Protocol

SHIBBOLETH

Always on the lookout for improvements to the system, Dave says they began to hear of the emergence of Shibboleth and SIF.[2]

"We wanted to move forward into the Shibboleth world but not to throw away the good things we had achieved in the past. We wanted certain services to remain and we knew the people who developed Content Stream could probably redevelop its authentication as a Shibboleth resource, along with other content services and products that would be available in the future."

The challenge in developing Global Identities was to create unique IDs for over 102,000 people that would transfer seamlessly as the pupils moved between Key Stages and/or schools, and which would integrate with existing and future systems. Of key importance was local control of passwords and retention of the existing school e-mail addresses.

Other pre-existing commercial products seemed better designed for large corporations like banks rather than schools, and they were also considerably more expensive. Dave says they would have been very difficult to integrate with what Children's Services was already doing, and also there would be no way of fully costing the process before starting. So, alternatives had to be looked at.

"We had no pre-conceived knowledge of products. We wanted a blend of technologies, open source and otherwise – we wanted a system that's fit for purpose and best of breed.

"Another problem with alternative models was that they only authenticated 'into a content pot': there was no cross search aggregation using XML descriptors of the content. In a learning environment you want the maximum amount of learning resources available to you, but also to be able to locate what you need."

IMPLEMENTATION

All the LA's infrastructure is Linux-based, says Rob Jervis, Broadband Support Officer, and very reliable.

As well as the existing OpenLDAP, Worcestershire had also started using Microsoft SharePoint, a solution for collaborative web environments, and so had an Active Directory installed. Rob says that it seemed sensible to use the existing OpenLDAP infrastructure as the Shibboleth authentication mechanism but also to provision Active Directory from the same system too. "That way we could use the data that was already available through the identities that we knew existed in schools, to flow through, populate and provide access to Shibboleth protected services.

"To do this, we took into consideration the existing infrastructure and set about working with our external consultants,[3] who had developed the existing broadband and accounts infrastructure, to work on our central user database. We updated the system to pull all the information we wanted to be available in Shibboleth and then provisioned OpenLDAP, Active Directory and Shibboleth from the same data source."

A Shibboleth IdP4 based on SimpleSAMLphp (a framework which provides web browser-based single sign-on) was implemented in partnership with the external consultants and Worcestershire began to work with external content suppliers. Rob says, "We are now working with over 30 suppliers who have implemented a Service Provider[5] or are working to do so. It is now a procurement requirement for a supplier to be compatible with the LA's infrastructure as a Shibboleth Service Provider."

[2] Schools Interoperability Framework, a data sharing specification for educational organisations.

[3] Ateb Ltd: www.ateb.co.uk

[4] Identity Provider

[5] i.e. become a provider of information or resources.

USER AND DATA MANAGEMENT

Dave was adamant that they didn't want a centralised helpdesk administering passwords for 102,000+ users. The solution to this issue is what makes Global Identities truly federated.

The infrastructure contains approximately 250 sites. Each site has an appliance server with a user management feature and a LDAP directory for local users on that server. Meanwhile the central directory held by the LA has a list of every single user attached to it: every pupil, member of staff and governor. "This is a system that we have been able to build on over a number of years and is an ideal base for Federated Access Management and Shibboleth."

To migrate to Global Identities, an educational establishment can match local users on their local database up with their corresponding entries on the central database. Management responsibility for accounts is devolved to the school, which handles things such as password administration, user status management (enable/disable) and e-mail accounts. Meanwhile, the LA can still guarantee that users are authenticated: for the school to manage their accounts, they still have to pre-exist on the central database and be assigned to that school. For the same reason, schools can't just add unauthorised users at random.

The central user database is populated from existing data on students and teachers, and the system is fully automated, *apart from* migrating user accounts to Global Identities. This is intentional, to allow schools to opt in at their own discretion. The database contains all the data that suppliers are likely to want, but this does not mean all the data is automatically supplied – just what is required. For example, all the attributes that the UK federation requires as a minimum are available to all suppliers: meanwhile some suppliers, but not others, may want user first names or e-mail addresses so that users can be sent messages or alerts.

A key strategy for Children's Services is to make the single sign-on concept available to every user, regardless of their needs. For this reason the LA has worked in partnership with its contractors to develop the idea of picture passwords to cater for pupils with specialist education needs. At the stage of the sign-on process where a password must be selected, instead of typing out a password of their choice the user is presented with sets of pictures to choose from. For instance, the first character of the password can be drawn from a set of 10 animal pictures; the second from 10 different colours; the third from a series of caricatured job types like an astronaut, cowboy or fireman and so on. The cartoon-type characters were specially commissioned from designers for this task.

The picture password system went live in September 2009 and is proving to be very successful. This is a key area where the usage of Open Source technologies has benefited the rollout and adoption of Federated Access Management. Children's Services is now considering the development of picture usernames to complement the passwords system.

SELLING THE SERVICE

As with any new service, some schools have resisted changing to Global Identities. They understandably want to keep doing what they are currently doing, which seems to work for them perfectly well to date. Dave therefore says that migration is "done *with* rather than done *to*."

"A Big Bang switchover to Global Identities would be a nightmare. We try to give as much control as possible to organisations and let them migrate users on the basis of value, as and when they are ready – one user, two users, a group of users, all users, in any combination they want. The migration process is wizard-driven to make it all as easy as possible. We can even do it remotely on behalf of schools if necessary, at the school's request."

An important feature to put doubters' minds at ease is that they can retain familiar things like their pre-migration e-mail addresses. Migration is simply an upgrade so that they can have a federation identity to login to other services.

"What you need," Rob adds, "is for the IdP to be implemented along with a set number of services – about five, in our case – before users can see the benefit of not having to login to each one separately. Once they have e-mail, their website, and two or three content packages, they can really see why they need to use the system. It would be much harder to sell the concept of Federated Access Management to schools without these because it can be hard to visualise it in action."

Users are not the only ones who have to be sold on the idea, however: before anything can be done the process will need approving within the organisation itself. Dave did not find this a problem.

"If you have a strategy and a budget and the right checks and balances, you can drive it forward. Any ICT implementation needs to be driven by someone who has listened to the educational arguments and business requirements and drives ICT to deliver it. An independent project manager might be able to deliver the identity management solutions but then have to draw on a lot of other people. It must be clearly driven from a senior position within the organisation."

A series of brochures and briefing sessions were also prepared to help spread the word and promote the idea.

Of the 102,000 accounts in the system, about 80,000 so far have migrated to Global Identities. Dave points out however that, "just because there are 80,000 users, this doesn't mean they are using it *well*. Where we are heading is now making sure they know what to do with it."

BENEFITS

The fact that 80,000 users can access a wide variety of types of service and content through just one username and password speaks for itself. As well as Content Stream, the LA's pre-existing but now Shibbolised content portal, current and planned e-services for staff and pupils include the EduLink portal,[6] external learning platforms, national federated services such as the BBC Motion Gallery and the National Archives, e-mail services such as Horde Groupware,[7] instant messaging and live communication tools, and targeted information for specific individual users within schools.

Furthermore, it is not just the users who benefit. Dave says that a lot of providers found Content Stream a route to market and Shibboleth could well provide the same opportunity – they can securely put up demo materials and provide short-term access to their service so that schools can evaluate it and then make a decision to buy. Meanwhile the LA does centrally managed procurement rounds twice a year to market these products to schools, meaning that schools get cost breaks.

Rob adds that integrating Shibboleth and SharePoint required extra code that was not available in SimpleSAMLphp. The code that was developed to support this integration with ADFS has been developed and released to the wider Open Source community, and is part of the main SimpleSAMLphp source.

FUTURE PLANS

One of the reasons for adopting Shibboleth was that it was not only suitable for what Children's Services wanted to accomplish in the near future, but also seemed to allow for the department's more long-term plans.

For the time being, Dave says, this is period of consolidation: "consolidate the user base and increase usability." However, he also happily admits: "We have all sorts of ideas for the future: linking to learner profiles, usage patterns, Amazon-type models ('other people interested in topic X are also using service Y'). Shibboleth also presents an opportunity to go beyond the limitations of content and into the applications. We could use single sign-on for, say, videoconferencing.

[6] https://www.edulink.networcs.net
[7] www.horde.org/groupware/

"We would like to federate more widely with other things, for example access to repositories like MERLOT.[8] We did some work with DCSF on federated repositories a few years ago to explore the possibilities.

"Similar to YouTube's 'embed' command, we can foresee the ability to paste buttons from a Shibboleth catalogue gateway service, which we already have,[9] into a school's learning platform. These buttons can lead to content, tools or applications and be placed so that content can be accessed from wherever you want.

"A big issue at the moment is that Global Identities only provides individual logons while primary schools want class logons. A class of 30 five-year-olds all logging on individually for one teacher is quite a challenge. We are now looking at how best to resolve this issue. We could group them all into a single entity, say: we are looking at whether it's acceptable at the federation level to authenticate several users in one 'container'.

"Also, integration with the desktop is not there yet. Not all authorities have single Active Directories for the whole organisation, which is what is generally used. We are keen to hear from anyone who has actually done this without having everyone and every computer in the same Active Directory."

LESSONS LEARNT

"You need a very clear idea of your direction of travel," says Dave. "We needed to know on Day 1 what was to be done within the envelope of the single sign-on process. With that, you avoid falling over yourself later on when you find something else is needed."

Implementation came within the department's budget, so budgetary concerns were not a problem given the direction that Children's Services took. The infrastructure was already in place and much of the time the implementation built on previous investments rather than throwing away legacy equipment and services and starting completely afresh.

Budget *would* have been a problem, Dave agrees, if they had used a proprietary system: there would have been consultancy costs, licensing, configuration, integration with other services and hardware to worry about. "You can't be proprietary *and* cheap," he advises, "and a proprietary system probably wouldn't be able to supply or embed such a range of services at a cost we could have afforded."

Lack of knowledge of Shibboleth in the commercial sector has slowed down take-up, he thinks, though this too is changing. Several big suppliers were not even looking at Shibboleth until they had talked to Children's Services: now, they are looking to take it to market with other local authorities. Some Shibboleth-compliant services are now approaching the LA themselves, having talked to other suppliers.

Above all, Dave has no doubt that this was the right decision to make. "I certainly would not do it differently! But taking a hard, fast look at what you've got is still vital."

Thanks to Dave Thomson and Rob Jervis for agreeing to be interviewed for this case study.

[8] www.merlot.org
[9] www.networcs.net