CASE STUDY

November 2008

Cardiff University

Interviewed: Rhys Smith (Engineering Consultant Identity & Access Management)

The UK Access Management Federation FOR EDUCATION AND RESEARCH

BACKGROUND INFORMATION

Cardiff University has approximately 26,000 students and 6000 staff. In 2004 it merged with the University of Wales College of Medicine.

Cardiff is one of eight universities to have been using Shibboleth right from the start, having got funding for JISC's early adopter project. This project was to get the Shibboleth teething problems out of the way before it could be promoted to the higher education world at large. Until the project, Cardiff had been using classic ATHENS to manage access to its resources. AthensDA was considered as an alternative but the university switched straight to Shibboleth when the project came up.

A key player in the deployment project was Rhys Smith, Engineering Consultant Identity & Access Management at the university.

ACCESS MANAGEMENT

The ATHENS system at Cardiff had run into difficulties as the number of users piled up, many of whom were only technically or partially connected to the university. 'Identity management issues aren't always as clear cut as you might think,' says Rhys. 'Institution licenses always say 'members of the institution are allowed to access this,' but what is a member? Staff may leave or retire but stay on as consultants, so they are no longer members of staff but need access to resources.'

Deleting people from the system in a timely manner was a problem, and the situation was exacerbated by the merger with the University of Wales College of Medicine. 'We had NHS staff, paid by the NHS and working in a NHS hospital. They had no direct link to the university, but were teaching university students and so they needed access to resources.' The College also had a different approach to identity management that wasn't always compatible with the university's.

DRIVERS

Thus the need, as Rhys puts it, 'to tidy up our house' was a key driver behind the move to Shibboleth. It presented an opportunity to sort out the situation once and for all.

Another driver was cost. An OpenAthens subscription costs Cardiff in the region of £9000 a year. For a simple Shibboleth service, once the set-up has been paid for there is no further cost above its operating and maintenance costs. This may vary a little, Rhys says, if you are spending resources on activities such as Shibboleth-enabling VLEs and so on. Even so, Rhys says he has touched the Shibboleth servers 2-3 times at most in the last year or two. 'Once it's up and running, it's up and running.'

Cardiff requires 'two decent servers' to run its service and these are replaced every three years. The cost of these two servers is therefore spread over a three-year period. Power and maintenance go on top of that. The annual total is still far less than ATHENS's £9000.

Rhys points out that you also get your own control over a critical piece of infrastructure, rather than trusting it to an external organisation. 'You keep it in-house. This goes against the mantra of out-sourcing, but out-sourcing isn't all it's cracked up to be sometimes.'

On top of all that, however, Rhys says, 'In other parts of the world like the States web applications and VLEs are the driver; in the UK the driver is replacing ATHENS. Now Shibboleth is here people are thinking of exploiting other possibilities like VLEs and portals and cross-institution collaboration and wikis.'

DEPLOYMENT

Cardiff's deployment strategy was a phased approach. The university ran Shibboleth as a trial for a year alongside ATHENS, which remained the main identity management system. Then came a year-long changeover period during which first year students – about 8000 in total – weren't given ATHENS usernames and passwords at all; they were told to use Shibboleth. Thus out of the university's 29,000 students and 6000 staff there were 8000 potential Shibboleth users.

By the end of that year, only 2000 of those 8000 had used it – but there were 10,000 users in total. In other words, other students and staff members had migrated themselves. Shibboleth's technology had proved 'rock solid,' says Rhys, and it was spreading by word of mouth. 'This was a good indication users liked it ...' he agrees.

More formally, all users were e-mailed between September 2007 and January 2008 and told to switch over to Shibboleth.

'We e-mailed all users once a month for four or five months to encourage migration. Then for a couple of months we sent warnings about us turning off ATHENS, followed by a final declaration that we were turning it off tomorrow. In the course of that, most people migrated. Inevitably there were a few who hadn't migrated in time.'

Rhys says the university deleted its last ATHENS account in May 2008. At this point Shibboleth was getting in the region of 100,000 logins a month.

That said, by the end of July the university was still using OpenAthens, the Shibboleth/ATHENS gateway, as five key resources themselves are still ATHENS-only and haven't migrated to Shibboleth. 'We can't get rid of them without significant complaints,' Rhys says. Apart from them, of the 146 original ATHENS resources, 98 are native Shibboleth-compliant and about 40 more are not yet but can be accessed through EZproxy (a system that lets users IP authenticate on campus to gain access to restricted-access websites). The balance of resources are not yet Shibboleth-compliant but 'most say they will be.'

Rhys has the main technical responsibility for Shibboleth at the university and was the one who did most of the technical work, though he says he works closely with the university's Directory Services team. 'Two or three members of the team have been trained on the basics and management of the server, and they keep abreast of what is happening, but they don't have much to do with it day to day. Having just one person who knows the stuff is not a good idea. This is a critical piece of infrastructure and if the Shibboleth service goes down for even five minutes then we start getting phone calls. All the university's research work would be affected.'

(Rhys also notes that the Shibboleth service has only been down when the network has had issues – it has 100% uptime in its own right.)

To tackle identity management issues such as those mentioned above, with users not falling into an obvious scoped affiliation category, the university decided to set up a Membership Categories Entitlements Group. This was an official university project rather than the domain of IT Services, headed by the University Board, though IT Services did do the legwork. After many months the Group had a list of about 60 categories of users, including those linked from the NHS, with different entitlements – e-mail accounts, network access, filestore, the right to borrow library books. The situation is much tidier than it was before.

'We now have a defined list of permitted users of resources,' Rhys says. 'If a publisher wants to audit usage, we can say 'these are all the people allowed to access it.''

These access rights can be enforced with Shibboleth: attribute management lets access to resources by users be allowed and disallowed. 'Users who are ''members'' of the university have been designated as such by the Vice Chancellor and the entire board. We have a much better legal compliance with license restrictions than we had before.'

CHALLENGES

Getting the necessary identity management work in place was an obstacle to overcome, but not a great one. 'We have a very good Directory team,' Rhys recalls. 'Other places may not have such an experience.'

Aside from that there were the inevitable technical challenges of being an early adopter: 'no documentation of how it works,' Rhys remembers, 'and the install guides were awful back then. It's much better now for those new to the area with things like the JANET helpdesk and training courses. These challenges don't exist any more.'

With those out of the way, the remaining challenges were more of perception and understanding than anything technical.

'People think it's hard to do,' Rhys comments. 'It's not at all. It's not hard, it's complex, and there is a difference. There is a stack of software that needs to work together, and that is complex, but no more than any new technology that any techie will have to come to grasps with. Thinking it's hard is a misconception.'

Even with that mental block dealt with, there was the matter of getting users to understand how to use it and to migrate from the old system. Hence the policy of giving new users Shibboleth passwords only. Rhys also made sure that the library staff were trained to handle queries. 'They are the front line for this kind of thing. We didn't train them in technical details, just what it was, how it worked; what they needed to know.'

'Generally, it has not been too much of a challenge because it's easier to use than the old system it's replacing. It's a lot easier to say 'log in with your existing username and password' than 'go to the library, get a new user name and password, remember it, do this, do that.''

DO DIFFERENTLY?

Is there anything Rhys would do differently if he had to do it all over again?

'We would do it faster! The phased approach was absolutely right for the time but now we know the technology is reliable. New organisations implementing Shibboleth nowadays don't need to follow suit – they can just do it.'

BENEFITS

Using the experience gained from deploying Shibboleth and the infrastructure now in place, Cardiff has Shibboleth-enabled a couple of internal applications, potentially allowing members of other organisations to log in to them to enable collaboration in a way that is easy to manage.

'We've enabled Shibboleth authentication to our EZproxy service,' says Rhys, 'which gives us the nice advantage that if our users want to access resources, be it through native Shibboleth, via the OpenAthens gateway, or via EZproxy, there is one authentication mechanism – Shibboleth. Nice and consistent.'

Cardiff also runs a couple of commercial services, European Sources Online and Procureweb, which are either already available on the UK federation or will be shortly. The advantage of doing this for

Cardiff is to make these services more easily accessible to potential customers, and to reduce the overhead of administration work.

Rhys is clear on the benefits that Shibboleth has brought.

'The library systems management team get far fewer queries – staff don't have to deal with things like password management. It has taken time off the shoulders of people who have better things to do than reset people's passwords.'

'In short, it's cheaper for us, better for the users, and easier to maintain with a lot less effort involved.'

Our thanks to Rhys Smith for agreeing to be interviewed for this case study.