

## **JISC, UCISA, UKERNA Access Management Conference**

**Trinity House, London, 6 November 2002**

The keynote address was given by Jean Sykes, Librarian and Director of Information Services at the London School of Economics. She began by proposing a vision for access management. Users want to be able to search multiple sources simply, and to have access to a range of resources – some local, others national or international, some commercial and others free. Sensitive data needs to be kept secure, and the privacy of individuals must be safeguarded. A national scheme for access will allow the spanning of boundaries between resource types as efficiently as possible. In order to provide such a system successfully, we need to recognise how our users now function. They are increasingly mobile, and want access on a 24/7 basis. eScience and the Research Grid has recently provided a new dimension to shared working on a vast scale – and this presents significant challenges. Another recent development is the closer operation of the HE and NHS sectors in the UK. Jean also mentioned the Research Support Libraries Group, whose report is due imminently. Its vision is likely to be one of much greater sharing of research resources.

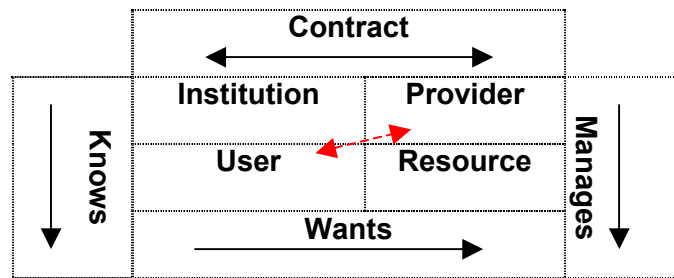
The components of the environment in which access management must be run are the many e-content services and digitised resources provided by JISC, Athens, and cross-catalogue services (M25, CAIRNS and Riding). These are often featured within portal and integration technology services which now proliferate, and which have brought into focus the access management deficiencies in our environment.

The recent growth of walk-in reference access library schemes and reciprocal library borrowing schemes has also highlighted the requirement on HE libraries to cater for members of the entire HE community irrespective of their 'home' university. UK Computing Plus is setting out to provide the same reciprocal access to PC facilities. Reciprocal access brings with it a fear of 'swamping', of course, which is normally unfounded. She also described 'kiosked' services, which are available to walk-in users. There are many more of these than might be thought. All services provided by JISC allow walk-in access, for example. The complexity of licence conditions presents difficulties to librarians which sometimes results in them taking the easy way out – and denying access. But this is poor service.

She went on to describe the JISC 06/02 Programme in Access Management. These cover 'the three As' – authentication, authorisation and accounting. She then discussed the successor system for Athens, currently the subject of an EU tender. A production service is sought for 3-5 years from August 2003. These tenders must address registration and identity management, authentication and authorisation, accounting and administration, and standards and service levels. The successor scheme, which must span HE and FE, must be simple to use – both for users and administrators. It must also be secure, and must guarantee privacy. It must permit an audit trail, and must include a means of avoiding any single point of failure. It must attract wide adoption by DSPs, be built on open standards and interoperate with existing HE and FE infrastructures. It must effectively separate authentication and authorisation. The national and institutional roles must be clearly delineated, but devolution of authentication is desirable. The scheme must cater for the complexity of user attributes, support minimum intrusiveness by DSPs, and scale to the full HE/FE community.

A question from the audience related to the scale of any new service asked whether it was appropriate for the scheme to be national, or international? Jean Sykes agreed that the international dimension was ultimately more desirable, but that a UK-wide scheme might integrate within it.

John Paschoud (JISC ANGEL and SECURE projects) then gave an overview of current technologies. He presented a 'four player' access management basic grid:



The fact that the institutions know who the users are distinguishes FE/HE from commercial applications of authentication/authorisation. E-commerce applications only consist of three players.

The user-provider relationship is undesirable and all-too-common. Our access management systems must work to prevent this relationship.

He reminded us that, before the three 'As', there is an 'R' – for registration, in which our institutions have already invested many business processes. John then described a number of relevant protocols – HTTP, Kerberos, LDAP, SMB, SOAP, SSL and X509.

He then focussed on five products which are of primary relevance to us as we contemplate the future.

*Shibboleth ('Shib')*: An Internet2 Middleware Initiative project. Shib consists of a technical architecture plus policies for federated administration, privacy, etc. It is based on open source software, and is designed for HE. Shib is now being piloted with peer access and vendors. They have explicitly taken on the library agenda, and are talking to Ebsco, Elsevier and other major library resource vendors, and have recently made a breakthrough with Ohio State University, which now has 'Shibbolised' access to Ebsco. The SAML standard (Secure Access Markup Language) which underlies Shib's method of describing users is now a recognised OASIS standard – and so that also lends weight to Shib's claim to be ahead of the alternative approaches. Shib does require a lot of effort to install. It separates authentication and authorisation.

In the Q&A session, Alan Robiette of JISC informed the meeting that WebCT had now 'climbed on board' Shib, and that a working demonstrator of 'Shibbolised WebCT' now exists. This is clearly a very interesting new development.

*Passport*: This is the Microsoft offering. It is quite pervasive already in e-commerce environments. It is cookie-based, does not use X.509 digital certificate technology, and works by storing user credentials centrally. It is currently used by around 90 vendors. It is included in the Windows software present already on the majority of user desktops.

*Liberty Alliance*: This is the non-Microsoft approach, led by Sun, consisting of 120 corporate members. It deploys a federated architecture. Again, it is primarily intended as an e-commerce application, but may be shaped for the four-element needs of HE/FE.

*PAPI*: This is an open source package, which –like Shib – is non-trivial to install. It is also cookie-based. Its architecture is not particularly scalable to a large number of resources. PAPI and Shibboleth are now in dialogue, which may take it in an interesting direction.

*WS-Security (Web Services Security)*: Microsoft is also involved here, and are hedging their bets with it. It is being developed by Microsoft, IBM and Verisign. It employs SOAP. It is mainly aimed at e-commerce, and wide adoption seems likely.

John finished by describing the SECURe Project. This is based at the LSE, and will look at institution-wide deployment of Shibboleth and PKI. In response to a question from the floor, he said that LSE were considering the use of both smart cards and USB devices as potential ways to 'carry' certificates.

Simon Bains, Electronic Information Services Librarian at the University of Edinburgh, then spoke about the access management issues in the daily lives of Athens administrators. He described his talk as really being about 'life at the coalface'. He began by talking about his previous job at City University, where manual registration was used. All registration was done on paper, because of worries about legal obligations. They also deliberately avoided advertising the ability of users to access Athens resources off-campus. He admitted that this now seems bizarre, but it illustrated how worried administrators can become about their legal position. At Edinburgh, they use Athens self-registration. It allows for prefixes which identify group usage. It does not need Computing Service support, and it promotes self-sufficiency. Edinburgh does not bulk-upload, because the user data was not in any straightforward state for migration (but it now might be possible because the databases concerned are both Oracle). The fact that the Library and Computing Service are not converged also meant that it was problematic to consider bulk-uploading. He then presented the benefits and disadvantages of the self-registration method. He showed how many accounts were expired when annual re-registration was introduced in November 2001 (over 17,000).

Edinburgh now believes that bulk-uploads may soon be possible (or at least, offline account creation, which is similar). They think they can run an LDAP service (though the student records are not currently on it), but he admitted that no one in the Library understands certificates well enough to want to use them. He finally made a plea for better user information from the system. Edinburgh wants to know which groups of users use which resources, in support of funding decisions.

The second part of the 'Athens Administrator' double-act was then given by Neil Smyth from the Library of the University of Wales Swansea. Swansea used to run both access accounts and personal accounts, which were created by library staff for users. This became increasingly burdensome. Swansea rejected self-registration, but opted for bulk-upload which led to a large reduction in administrative overhead on the Library. The Voyager system at Swansea already received registry data, and the bulk-upload for Athens was then based on the records from Voyager. A 'converged' project team was created – something more easily done at Swansea where the Library and IT Services are organisationally converged.

Swansea's bulk-upload runs daily, and incorporates expiry date processing. Administratively, it is a very simple system to run. Introducing bulk-upload led to an uplift of approximately 10,000 accounts over the number of personal accounts which had been created, because the system became so much simpler for users as well. He then went on to describe the confusion created for new students by the plethora of accounts they require in order to use the Library's e-services and the university network.

Both Simon and Neil mentioned that their libraries were considering use of EZProxy. John Paschoud reckoned that the EZProxy would not scale to the the number of resources libraries will soon be making available. Neil felt that the answer would lie in a greater number of Athens-compliant resources. Lyn Norris of Athens said they were working on this. John Paschoud reminded us that the UK's Athens users represented only a proportion of 1% of global DSP business, and that therefore the future lies in a mixed economy, rather than a centralisation upon Athens.

After lunch, Lyn Norris of EduServ gave a presentation on the future of Athens. Athens now serves 270 FE institutions, 247 HEIs, 206 NHS sites and a number of users in Ireland, Scandinavia etc. She made it clear that EduServ has international ambitions. There are now

over 2 million Athens accounts. Services supporting Athens now include ScienceDirect, Wiley InterScience, SwetsWise, Oxford Reference Online and ExLibris Metalib. Roughly 50% of all Athens services are now SSO ('Single Sign-On').

There are currently (only) 10 users of the Devolved Authentication service, which can be based on LDAP, Kerberos or digital certificates. Athens sees itself as becoming less of a central repository and more of a channel to other technologies.

Shib features in the future of Athens. It is a protocol for passing authorisation information, based on user attributes. Athens wants to build the 'Athens Shib' club ('Atholeth') to enable Athens sites to access Shib-protected resources. Athens will then provide an authentication service, an attribute authority (i.e. a namespace) and a WAYF (Where Are You From) capability. Athens sees itself as both a competitor of and a collaborator with Shib, and boasts of the fact that it is not a project: it is here and it works.

Another new Athens direction is in learning environments. They have been working with the University of Ulster in their deployment of WebCT, using Athens SSO. Lyn demonstrated the service. At Ulster, the student database is LDAP. The project embeds links from the WebCT course to resources in the library portal, via Athens SSO.

Alan Robiette then spoke about the 06/02 Programme (the JISC 'Authentication and Authorisation Programme'). Alan said he regarded authentication as 'a solved problem'. Digital certificates offer 'strong authentication'. The Grid's eScience community insists upon digital certificates, and the NHS is likely to require them. eGovernment is another arena in which they will be used.

Authorisation is a much more complex problem. The 06/02 programme sets out to test the working of digital certificates in real institutions, and to examine the possibility of a common authorisation solution. There are 11 projects in all, including four on authentication and four on authorisation. Leeds has a project to develop tools for certificate management. On the authorisation side, the ULL is looking at PAPI; Manchester Computing is using Akenti with Zetoc; Salford is looking at Akenti with Permis; and Warwick is examining roles and institutional memberships. A couple of the projects also involve Athens.

The next speaker was Sally Chambers of the ULL, who described their 06/02 Project 'GLAM' – 'Global Access Management'. This is a partnership between the Library and the University of London External Programme. The authorisation software in use is PAPI. They are looking explicitly at the work required of the 'PAPI Administrator', to see how it compares with the work of Athens Administrators. ULL has a large number of off-campus distance learning students, including many who may never visit the campus at all. When users log in, they are delivered a list of the resources they may access 'on the fly'. The project will look at compatibility of PAPI with the University's LDAP authentication, and at its value in delivering useful statistical information. The project will also examine speed of response.

Michael Fraser of Oxford University Computing Services then spoke about their 06/02 project, which is looking at institutional deployment of digital certificates in a complex environment. He cited a proposal someone had made facetiously, to speed up the development of standardisation in this industry by giving every citizen of the UK, or of Europe, a certificate to grant them access to government services, and leaving the market to sort it out. He suggested that this might be the position of UK HE and FE in a couple of years' time, when the Athens successor system is due to come on stream.

The Oxford project is not simply technical. It is looking also at the administrative culture required by a system like this. Oxford hosts a regional eScience centre, and, since the Grid access management system requires certificates, the Library at Oxford is managing the

distribution of these. He also mentioned the fact that Oxford receives many visitors each year, and so has a large 'walk-in' population to manage. Partners include EduServ, MIMAS (Zetoc) and the RAL e-Science centre.

The question of alternative uses of digital certificates was raised in the Q&A. They can be used to sign digital documents or indeed email. Alan Robiette felt that the use of certificates for these other purposes (i.e. non-repudiation) introduced complexities which required a lot more thought on the part of the institution in respect of legal requirements. The possibility of using them for document delivery signatures compliant with copyright legislation was raised, and John Paschoud said that LSE had examined this and his understanding was that this was a valid use. Alan Robiette supported this provided that a contractual agreement existed, which was analogous to the use of cheque-signing machines. Jean Sykes described the way by which LSE implements this in practice. After signing an agreement at matriculation, a window pops onto the screen every time an article is supplied reminding the user that they have signed a contract permitting the facility.

In the final Q&A, Mike Fraser asked about authentication and authorisation within a portal environment. Could JISC become involved in the business relationships shown in the 'four players' diagram? John Paschoud thought not, because the business relationship does not involve JISC. Alan Robiette said he felt that the only way of doing authentication properly in the portal context is by means of short-lived public keys, which 'die' after the user has finished their session.

There was a question about what will happen 'after Athens'. Alan Robiette could not say much because the details are sub-judice at present, with an outstanding tender exercise in progress to procure a successor system. Lyn Norris commented that 'Athens would not be going away', since it has other customers besides JISC. The tender call requires that the successful supplier support the migration from Athens, if EduServ is not successful.

Maureen Wade asked whether any of the panellists would 'back a particular horse' in respect of an authorisation system which would emerge as the one we were all using in a few years' time. John Paschoud went for Shib, as did Alan Robiette, though he preferred to point to SAML as the underpinning standard, which Shib uses (and Athens is likely to). Alex Reid of the University of Western Australia asked the panel if they were wise to dismiss Microsoft and Passport. Brian Gilmore – referring back to John Paschoud's 'four player' diagram - said that the main reason for doing so was that Microsoft's system was designed to permit a relationship between the user and the provider: it does not cater for the institutional role.

In response to a question about preservation of privacy of the individual, Alan said that Shib does this by issuing a once-only opaque string to identify users for each session. A question was asked about library portal systems, like Metalib. Why should we wait for HE information environment solutions to emerge, when vendors are already marketing products to do this job? Jean Sykes replied that these are limited to bibliographic data (which is not in fact the case in products like ENCompass, for example). The limitation is surely in the authentication/authorisation solutions they deploy, which are certainly not any further advanced than work going on experimentally in HE.

Alan was asked about the needs of the Grid, and whether the authorisation system in use for Grid researchers might be different from that which will win out in the world of library resources. The resources for Grid users are different, and controllers of them may not be willing to tolerate the 'leakage' which DSPs in the library area tend to accept. He suggested that Akenti may be a better system in that instance, though Brian Gilmore hoped that the authentication system at least might be common to both domains.

*John MacColl. 7 November 2002.*