Building a shared authentication infrastructure: a matter of trust

Peter Green
e-Learning Development Librarian
Curtin University of Technology
P.Green@Curtin.Edu.Au

Abstract:
The Western Australian Group of University Librarians (WAGUL) was successful in obtaining a substantial grant from the Commonwealth Development Pool (CDP) to fund a major authentication project. The resulting WAGUL Authentication Project will deliver a distributed authentication infrastructure for the five Western Australian Universities. This paper describes the motivations for the project, the expected benefits and the journey itself.

Motivations

In which we explore the role of libraries and why they drove the project.

The coming of the electronic age has caused a fundamental shift in the way university libraries view their collections and their patrons. In times past the collection was nurtured and grown, protected and sometimes weeded. Patrons were the people who came into the library and used the collection. Provided they were quiet, didn't eat hot food and didn't sleep on the floor they were tolerated. They were also predominantly engaged in study and physically located on campus for their studies. Unless they wanted to borrow something from the library their identities were irrelevant. The publishers of books and journals took little interest in those who wandered in from the cold and read their materials. This has all changed.

Patrons are now clients who may be earning while they're learning and learning while they're earning. Time is their scarcest resource and they expect value for money. They may spend little time on campus and do the bulk of their research while the library is closed. Their expectations of library service have been continually raised by the success of libraries in adapting to the information age and the complexities of library service provision has been increasingly masked from them.

In the online age collections are digital objects whose substance expands and contracts with each breath of the collective electronic heart. Collections ebb and flow with the tide of financial resources and the hum of publisher's scanners. Patrons can enter the library in a virtual, distant manner, eating hot meals and wearing their pyjamas at the same time. But their movements are noted and tracked and publishers are very interested in whom they are and what they are reading, and so are their information providers, the libraries.

This fundamental shift has crept up upon us over a number of years. In recent times the accelerated growth of online resources and the growth in flexible and online learning, coupled with the Internet revolution, has simply increased the rate of change. Libraries and publishers have responded to the pressures by finding new means of providing traditional sources of knowledge and inventing new ways to make money from the process. Regulatory changes have alternatively helped and hindered this process.

In this virtual age, identity is the linchpin upon which access is managed. The ability to prove that you are who you say you are opens the gateway to information. This access has been provided by libraries out of a stagnant budget and decreased purchasing power. Regulatory controls and the slowly increasing sophistication of publishers have increased the pressure on libraries to manage access to online resources while maintaining their traditional concerns for privacy and equality. Authentication and authorisation have become standard operating procedures for libraries in the information age.

Thoughts On The Nature Of Collaboration

Competition and cooperation make for interesting times.

In the small Western Australian higher education market place the five universities whose libraries collaborate under the auspices of WAGUL (Western Australian Group of University Librarians) are in fact competitors. The decreasing federal support of higher education has increased the competition for a piece of the educational marketplace. At the same time libraries have continued to work together for the overall benefit of students and the higher aims of Australian education. While there is a prevailing trend for policies to promote marketplace competition, other forces encourage efficiencies through cooperation and working together for the greater good of the Australian academic community. These conflicting forces make for an interesting educational environment on the local, national and international arenas.

The WAGUL Authentication project was born out of the desire for collaboration and efficiencies gained through collaboration but is situated against the backdrop of an educational marketplace. In some ways to attempt collaboration is to swim against the tide, though WAGUL has sought to struggle upstream for some years and has achieved some notable successes. The glue that binds this project together is that all WAGUL universities will benefit from the collaborative effort. The full extent of the benefit remains to be measured, but the promise is certainly there.

The need for collaboration doesn't cease when one enters the precincts of one's own castle and crosses the moat into friendly territory. Universities are loosely coupled collections of schools that form a united front more in the breech than the rule. In many cases there is more cooperation between universities than within them. This reality means that any assumptions of commonality must be tested against reality and collaboration starts at home. Trust has many facets and building trust is an essential part of the success of any authentication project.

Managing A Collaborative Project

The theory of project management meets reality.

When the Project Manager of the WAGUL Authentication project began in February 2001 one of his first tasks was to pull together a project team that would represent each university library as well as the IT sector of each university. The outcome was a broadly representative and very disparate team. The logistics of gathering the team together in one place for regular meetings was a challenge in itself. The exploration of the scope of the project was also a challenge but this would prove to be a dialogue that would eventuate in a shared vision.

The definition of a project is that it is a temporary activity with a start and an end. Principles of project management dictate that the scope of the project should be clearly stated and agreed to by the project participants. Scope in this sense means the work to be undertaken that will achieve the objectives of the project. In the life cycle of a project this can be the most significant phase. Failure to agree on the scope and objectives of the project will lead to inevitable confusion and uncertain outcomes. In this project over a month was taken to reach agreement on the scope. This was formally documented and agreed to by WAGUL. Changes to the scope would need consensus agreement and formal approval from WAGUL. This is a standard project management practise, but its importance in technical projects can't be understated. Once a project get underway in earnest members of the project team will

focus their energies on the road and not the eventual destination. The danger is that the project can become a very well functioning vehicle heading to the wrong town. Clearly stated and documented objective are a means of retaining control over the destination. Changes to the objectives and scope are then documented and agreed upon.

The Scope document can be viewed at
http://john.curtin.edu.au/walap/rfp/WALAP_Scope1.0.pdf

The project appeared to fall into three broad phases. The first phase of the project was coming to agreement on the nature of the problem, while the second phase could be described as the search for a solution. In this phase an extensive investigation was conducted into similar and related projects, worldwide, to ensure that we would be informed by their work and that we wouldn't be reinventing the wheel. As it transpired this particular wheel had not been invented, though some of the spokes had been put in place and some of the tools for wheel building had been created. The third phase would be implementing the solution.

Shared Authentication Infrastructure

Where we disentangle the words and come to the heart of the matter.

What is meant by a 'shared authentication infrastructure'?

In some ways the use of the word authentication is simply an invitation to muddy the waters, though it does provide a useful initial for creating acronyms. Authentication is usually defined as proving that you are who you say you are. There are various methods for doing this, some of which are considered stronger than others. For instance, having something and knowing something (CARD and PIN) is considered stronger than simply knowing something (username/password) though the latter is far more common. The project was not concerned about methods of authentication, except for enabling various methods to be used. The aspect of interest lay in having the authentication credentials available, whatever they might be. The hidden aspect, hidden by the sole use of the term authentication, is authorisation. This is usually defined as what you are permitted to access after you have proved who you are. To do this some profile information is required about the person beyond the authentication credentials. The bringing together of these two aspects is usually bundled together as 'authentication' for the sake of brevity and though clarity might suffer in the process.

'Shared' is liable to mean different things to different people and we began to use the alternate word 'distributed' in some contexts. We wanted to be able to authenticate members of one or more universities but didn't necessarily want to share the information upon which the authentication was based. To do this would require a level of trust that is generally beyond separate organisations and certainly universities. However if one or more university were sharing a resource, then they would want to share the authentication. Distributed is a better description in that the data is distributed but the authentication is shared.
Infrastructure can be taken to mean something that is a foundation upon which other structures can be built. In the context of authentication we came to understand that we were involved in the middleware part of the pipeline. Middleware is something that enables applications to fill their functions without having to get involved in the underlying structures. In this case we would allow an application to authenticate without having to connect directly to legacy systems. If underlying systems changed, this would not have an impact on applications that were dealing with the middleware layer. An example of this might be a

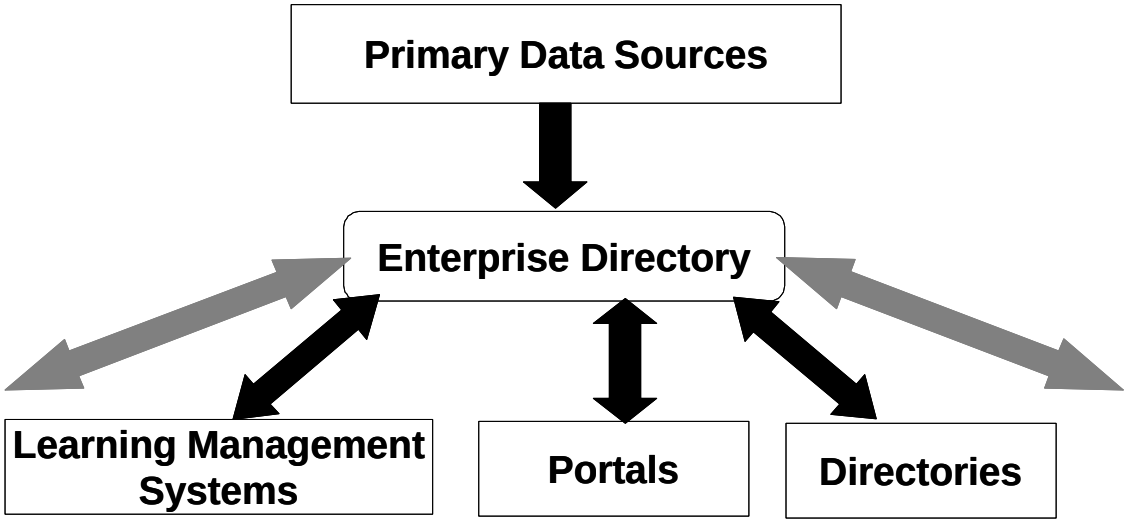
portal application. A portal is usually described as a web application that integrates authenticated access to various resources, while allowing the user to customise the interface. A portal will thus need to know authentication information for more than one system, and also hold profile information on that person. In other words the portal application needs to authenticate users and know some of their profile data. This data might have originated in a student system and been transferred to the directory. The portal doesn't need to know any of this. If the student system were migrated to a different system the portal application wouldn't need to know as long as the middleware continues to be fed the student data. In the project scenario there might be 5 different student systems (not to mention HR systems) that contribute data to the middleware layer. This complexity is hidden from the end user applications and from the eventual users.

Thus a shared authentication infrastructure means providing a method for applications to authenticate members of more than one university in a way that doesn't require the sharing of data and hides the complexity of the underlying sources of data.

Enterprise Directory Services

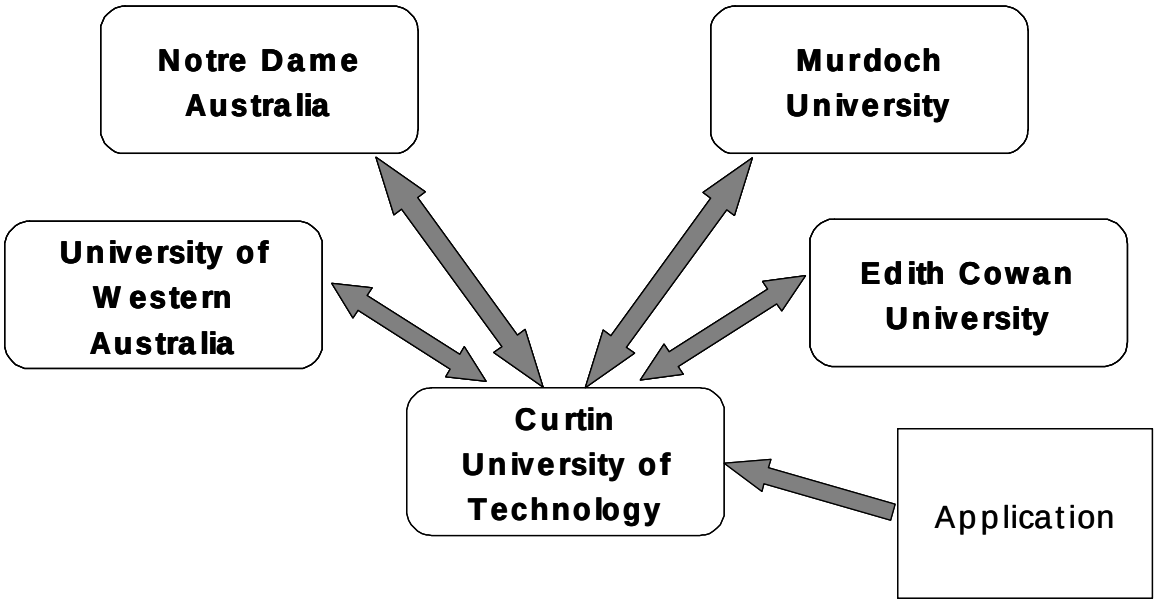
Capturing the beating heart of the university.

The investigative phase of the project led us to believe that the shared authentication infrastructure would revolve around having at each university a repository of identity information that was authoritative, reliable and current and a method for shared access for authentication purposes to a certain portion of these repositories. The software that fills this function is generally known as a directory service. Such directories are not unknown in the university environment. In fact there are usually a great many of them holding overlapping information of various degrees of currency and correctness and being used for a variety of purposes. The type of directory that was envisaged to meet this need is commonly referred to as an enterprise directory. This type of directory would stand at the pinnacle of directories within an organisation and other directories would take their data from that directory. Applications would also be able to authenticate directly against such a directory. The diagram below illustrates such a scenario.



In practise, in a large organisation, there will remain a number of directories filling different purposes but synchronised with the enterprise directory. The enterprise directory would typically be synchronised with the sources of primary data. In a university setting these would include the student and HR systems. This aspect of the solution would not be innovative; though establishing such a directory was likely to be somewhat of a challenge in the university environment.

The innovative aspect of the solution would be linking these 'peak' directories in such a way that authentication could be shared between the WAGUL universities. However sharing authentication doesn't necessarily mean sharing directories or sharing data. There are many political and practical reasons why universities would be reluctant to have their identity data either shared or physically loaded on another university's hardware. This is the delicate balancing act that requires a degree of trust but acknowledges the necessary distrust required by concerns over privacy and sovereignty. The solution proposed would also need to recognise the shifting nature of collaboration. The diagram below illustrates a distributed authentication scenario build on the interconnection of local directories. An application seeking authentication for a user could direct its request at the local directory and have the request filled by the directory that actually holds the information for that user, regardless of the home university. This is the essence of distributed authentication.



It is entirely possible that one or more universities in the WAGUL group might want to discontinue a shared arrangement at some future time and even more likely that they will want to establish an arrangement with a third party. The university sector has a number of overlapping groups and these serve different purposes at different time and for different ends. The solution must take these factors into account and provide a degree of flexibility for the future.

Creating an infrastructure base that would provide a platform for future development would also require a commitment to using standards-based solutions. Standards in this area have reached some degree of maturity and their use would be an expected part of the solution. It was considered that the following Open Standards were important:

Authentication Protocols (e.g. Kerberos, Radius)
Directory Services (e.g. X.500, LDAP)
Public Key Infrastructure (e.g. X.509)
Other communications protocols such as TCP/IP

Come To My Party

Exposing ourselves in the market place.

Having decided the scope of the problem and having an understanding of the shape of the solution, it was decided that a Request for Proposal (RFP) would be written. The project team felt that we had advanced further than a Request for Information but given the innovative nature of aspects of the solution we were unable to do a Request for Tender. The RFP would describe the problem and set certain boundaries around the solution. This would allow Respondents to propose one or more solutions that would meet the needs of the project. Writing the RFP and coming to consensus between all parties took some time. It was advertised nationally on the 20th August 2001 with a six-week response period.

The RFP can be viewed at http://john.curtin.edu.au/walap/rfp/RFP_v1.1.pdf.

The RFP generated considerable interest from various players in the market place, as shown by the number at the industry briefing session conducted shortly after the RFP was advertised. Written requests for clarification and further information were received and responses were posted on the website for all interested parties to be informed. Companies grappled with the nature of the problem, and built partnerships to deliver a solution. Finally the final hour for submission of Proposals drew near. An RFP process can have two undesirable outcomes, a flood of responses or none. We attempted to mitigate these undesirable outcomes by raising the bar to a height that would discourage speculative proposals but not scare off the serious contenders. In the end we received seven Proposals. They all arrived in the last hour before the deadline, but were of good quality. The first hurdle had been leapt successfully. The next hurdle would be evaluating the proposals.

Herding Cats

The real work begins.

The project team was rather too large for running the evaluation process so a smaller team of five was selected from the larger team. This would enable each university to be represented, but create a small enough group that could function effectively. The project manager would act as non-voting chair. The evaluation had to be consultative, thus other members of the project team were to have input and there would also need to be consultation within the universities, thus gathering input from a wider range of technical and administrative staff. This process was facilitated by the distribution of multiple copies of each proposal. However the eventual success of the project would depend on the solution being embedded within each university and thus the consultation would need to be broadly based while remaining within the bounds of commercial confidentiality. This would be a delicate balancing act.

The quality of the proposals was a blessing and a curse. The ability of most of the Respondents to deliver a solution meant that we were unable to create a short short-list and had to request presentations and further information from six respondents. After the presentations and written response to additional questions and an analysis of the cost estimates provided, we were able to reduce the list to two, though we didn't eliminate any of the six, simply choosing our preferred two and investigating further. This initial process took three weeks. Further investigations involved speaking with reference sites and reviewing the software solutions and examining the cost estimates in more detail. This process took a further three weeks.

Despite the complexity of the evaluation process an eventual decision was made that had consensus agreement and high expectations that the diverse needs of the five universities had been balanced against the desire for a shared authentication infrastructure. The evaluation team concluded that any of the six short-listed Respondents could deliver a solution to meet the project requirements but selected one Respondent whose Proposal was considered to best meet the criteria, including the ability to implement and provide value for money. While there is much work to be done, achieving a consensus view bodes well for the successful implementation of a shared authentication infrastructure.

A Work in Progress

The canvas has been stretched and the paint pots readied

At the time of writing this paper a final recommendation has been made with regard to the recommended supplier. Contract negotiations have begin are expected to be concluded by December 2001. Implementation will be started in January 2002 and it is expected that implementation will be concluded by the middle of 2002.

The presentation of this paper at VALA2002 will include a detailed state of play, including information that has been withheld from this paper because of the current state of contract negotiations and a requirement for confidentiality in that regard.

Bibliography

Authentication and authorization: a guide – GLOSSARY. Hp. 2000. Online. Candle-Athens Integration Project. Available: http://litc.sbu.ac.uk/candleathens/glossary.html 22 November 2001

Australia. Department of Education, Training and Youth Affairs. DETYA - Education - Higher education report for the 2001 to 2003 triennium. 2001. Online. Available: http://www.detya.gov.au/highered/he_report/2001_2003/html/4_4.htm 22 November 2001

CAUDIT/CAUL Authentication System Project. Hp. 1998. Online. Available: http://www.gu.edu.au:81/uls/sso/ 22 November 2001

Identifiers, Authentication, and Directories: Best Practices for Higher Education. HP. 2000. Online. Internet2 Middleware Initiative's Early Harvest workshop. Available: http://middleware.internet2.edu/internet2-mi-best-practices-00.html 22 November 2001

McLean, N. 2000, 'Matching people and information sources: authentication, authorisation and access management experiences at Macquarie University, Sydney', *Program*, vol. 34, no. 3, pp. 239-255

Reed, A. 2000, *Implementing Directory Services*, McGraw-Hill, New York, NY

WALAP Project Scope. 2001. Online. WAGUL Authentication Project. Available: http://john.curtin.edu.au/walap/rfp/WALAP_Scope1.0.pdf 22 November 2001

WALAP Request for Proposal. 2001. Online. WAGUL Authentication Project. Available: http://john.curtin.edu.au/walap/rfp/RFP_v1.1.pdf 22 November 2001.