

# Identity and Access Management Survey 2005

James Sankar  
July 2005

## Acknowledgments

AARNet wish to express thanks to members of the Middleware Steering Group, CAUDIT, MAMS and Directors and staff of CAUDIT member organisations who responded to the survey. Without their support, the quality of the survey instrument and responses received would not have made this analysis possible.

## Executive Summary

The Identity and Access Management (IAM) survey 2005 revealed responses from a diverse range of Australian Universities. Many of these Universities are considering, piloting or using IAM systems to administer user accounts to access networks, applications and resources for staff, students (undergraduate and postgraduate), alumni, researchers and visitors. IAM systems are being used for at least 3-5 years and are based on a diverse range of platforms such as Microsoft, Sun, Novell and others. Many IAM systems have been deployed, maintained and supported in-house and are also quite adaptable with workarounds in place to ensure interoperability and integration with databases and Directory Services. These IAM systems support "agent", "push", "pull" and a combination of these authentication and authorisation processes.

LDAP appears to be the preferred Directory Service with a range of data extraction programmes written and developed in house using PERL, Visual Basic, JAVA, C++, or SQL languages to retrieve and process formatted data from various student and human resource databases. The use of standard schemas is high, however no organisations are currently using AU-eduperson and work is still needed to integrate various CAMPUS IAM system components together within organisations themselves.

The current use of IAM systems are to authenticate local and remote users using username/password combinations or IP authentication which seem to be sufficient for now. The use of usernames/passwords is not ideal as it requires users to remember a variety of credentials which is not user-friendly, however the development of same/single sign on environments may alleviate this problem some what. Another concern is that although some organisations transmit credentials through encrypted tunnels, others are not and are sending credentials unsecurely, which presents the opportunity for the unauthorised collection and use of someone else's credentials. Password aging is only used in 46% of organisations polled; wider spread use of such functionality should be encouraged.

Authorisation needs appear to be less well supported than authentication needs. This may be because there are no identifiable needs at the present time to develop fine grained

authorisation functions. Most common forms of authorisation are based on ezproxy or a proxy cache product. Authorisation may be tightly coupled to successful authentication where privileges are assigned to each user based on their assigned role (e.g. "student") for administration purposes. Where specific user requirements exist, these may most likely be administered in a manual way whilst requests remain low. Access to remote resources is supported by few organisations and may be limited for a number of reasons such as (1) the lack of available remote resources or (2) the lack of access to a collection of remote resources or (3) no federation policy and infrastructure to easily access remote resources in a secure, scalable and cost effective way.

The use of Public Key Infrastructures (PKI) and digital certificates has been limited, with only around 30% of organisations polled claiming their Directory Services support PKI. Some organisations are working on CAUDIT PKI initiatives, however widespread adoption of PKI is unlikely to occur until a national PKI is created, this is currently work in progress.

Many organisations are supporting visitor network access, in most cases the creation of accounts remains a manual process reliant on IT or Department staff to create accounts for http/https web or VPN access. Some organisations offer a wider range of access to applications including printing facilities though this is not widespread. A small number of organisations are using eduroam for automated visitor network access.

A key barrier to IAM system development is the lack of resources or funds available to cover time and effort to project manage, build, develop, test and deploy IAM systems, and the funds to cover the support, maintenance or iterative developments of these systems. Another barrier is the involvement of key stakeholders needed for systems to integrate and federate successfully. Such activities often are time consuming and require education and training in addition to agreed standards, policies and technical integration for the successful use of access controls to local and remote resources.

In addition, the use, access and maintenance of systems that create and store personal data and use critical business processes for staff and students to conduct their day-to-day activities mean that the risk and impact of development activities is high and could be costly. Any such IAM development may require additional support and guidance at political and technical levels to shape the direction of middleware so that IAM systems can align themselves to develop in a cost effective way with reduced risk. Access to relevant technical and support documentation and training should be encouraged.

## **Moving Forward**

If Australian developments follow similar paths to those overseas, the next major development phase after the creation of single sign on environments will be to create ways to access remote resources, services and applications and provide a range of collaborative tools to encourage organisations to work together on academic and research projects . Given the general use of fairly interoperable IAM systems and reliance on LDAP directory services, coupled with access to a high in house skills base, the opportunity exists to develop a framework to create one or more federations for access to remote services or collaborative tools. To do so requires a number of parallel activities

- To document a range of recommended Authentication and Authorisation methods and products that Identity Providers (e.g. Universities) can choose from.
- To engage with Service Providers to identify their authentication and authorisation and use requirements and develop middleware access controls that can lever from existing IAM systems so that users can be authenticated via their Identity Providers, possibly via a federation model.
- To develop a middleware framework that Identity and Service Providers can align themselves to that can deliver secure, scalable, cost effective and user friendly access to resources, ideally, enabling users to gain access when they are away from their usual physical location.

## **Recommended next steps**

- Develop guidelines for the use, transmission and storage of user credentials for authentication and authorisation purposes.
- Compile examples of best practice for current IAM systems and track/fund IAM system developments (MAMS have and continue to do good work in this area).
- Consider ways to develop and support same / single sign on environments for collaborative working environments.
- Develop a middleware framework that can deliver a secure, scalable, cost effective and user friendly method for users to remotely access resources by (1) engaging with service providers to aggregate provisions for access to content and (2) assessing middleware solutions and federation options to assist end users to access local and remote resources via their organisation's authentication and authorisation systems.
- Track CAUDIT PKI developments and where possible develop opportunities to make use of PKI to develop secure access to authentication/authorisation servers and service provider systems and content.

## **Analysis of the survey results**

### **Background**

AARNet, AARNet's middleware steering group, MAMS and CAUDIT developed a comprehensive survey of identity and access management (IAM) systems in Australian Higher education and research communities. The survey was circulated to CAUDIT members in May 2005 and responses were received during June 2005. The survey was designed to provide a snapshot of how "credential providers" currently operate and how user credentials are used to access resources, applications and services. The survey was also designed to assess the progress of campus identity and access management system developments to identify and recommend any actions resourcing, technical, political or other barriers to same or single sign on integration that need to be removed and to identify any opportunities to

- Promote campus infrastructure integration;
- Develop a federated authentication infrastructure;
- Develop authorisation components to specific services or applications.

This "user access to resources" scope is a critical component for middleware and integration / federation issues that may need to be addressed and/or suitably aligned with an Australian middleware framework for successful future deployment.

### **Details of organisations that responded to the survey**

50% of CAUDIT members responded to the survey, this average response rate may have been due to a number of factors; e.g. the short time to respond, the high number of questions or the need to involve a number of specialists within the organisation to complete the survey. All responses received were from Higher Education Community where six Universities were engaged in research activities. Responses were received from across Australia (ACT, NSW, QLD, SA, VIC, WA) and New Zealand. There was a range of main campus and off-site campuses that required support.

The number of users typically supported in each organisation was fairly evenly spread from >500 to 50,000+

On average 70.2% of these users were normally residing on the campus, 17.8% were remote users from home or work, whilst 7% were "mobile" users who accessed content from a number of locations.

## **Identity Management Infrastructure**

The current implementation status of IAM systems showed that a majority of sites have IAM systems in production, with 8 organisations planning to support staff in the future.

Not many users were part of a local directory; however most organisations had users who were part of a central directory with a unique, permanent identifier. There were more provisions in directories for students rather than staff, this may be due to the larger number of students and accounts to set up that can only realistically be managed and achieved via a directory service

Four organisations believed that they were not using IAM systems at the present time. These organisations created a unique ID, usercode, UPI or username to identify users. User authentication was based on Microsoft Active Directory, Novell NDS, Kerberos or “service based authentication” with two organisations relying on LDAP. The reasons why no IAM system had been deployed were

1. The organisation was still at an early stage of formulating objectives and project mandate.
2. Cost, complexity, immature technology, embedding and integration issues.
3. A home grown system exists.
4. A lack of integration coupled with the risk of third party integration tools and credential caching had delayed developments.

## **Identity Management Systems - Technical Aspects**

The key drivers to IAM system deployment were lower costs, enhanced security, user-friendliness, access to more resources/services and others (reliability, single sign on – access on demand).

Most IAM systems were deployed before and up to year 2000 with a small percentage deployed each year between 2001 and 2005. A quarter of all organisations did not provide an answer to this question. Anticipated future use of IAM systems showed a majority of responses estimate use of existing systems up to and in excess of 2-3 years. This shows that many systems are likely to be in use for at least 5 years altogether. The reluctance to change systems may be due to the inherent complexity of internal processes and use of critical credential provider systems that are required to enroll students and recruit staff and support critical business processes that generate revenue.

The type of CAMPUS IAM systems in use were a mix of Directory based systems, of which many were developed in-house. Systems in use included Yale CAS, Michigan Cosign, X509 certificates with Kerberos, eduroam, Kerberos 5 with Active Directory, SUN JES directory, SUN LDAP directory and Active Directory, open source with SUN and Novell NSure. There was a range of platforms that were predominantly SUN, Microsoft or Novell based.

Current IAM system utilisation remains high with local and remote user authentication in use by 80% of organisations polled and authorisation to local resources was used by 73% of organisations polled. Access to remote resources was lower at 54% of organisations polled and may be due to a lack of remote resources or a federation to access them easily.

IAM system integration appears high with 60% of organisations polled integrating their authentication, directory and user interface components. A lower percentage of organisations have also integrated authorisation components and network access. Meta data services were only integrated with 30% of organisations polled.

When asked what organisations would do differently if they were given the chance, the following emerged: better standards and in-house training rated highly, a range of other responses also emerged followed by diversify/consolidate vendor products, better unique identifier and finally go open source. Other responses included higher security/functionality, automation, flexibility, a rigorous assessment beforehand, more resources, better end-to-end aspects, the adoption of a client focused approach, a common identifier and streamlined systems.

In terms of deployment and support experience with IAM systems most organisations found the experience average (as expected) or difficult, the remainder of responses found the experience either very difficult or did not answer. No-one found the experience easy or impossible

Almost 60% of organisations polled believed their IAM system was partly interoperable requiring workarounds, 19% were highly interoperable, whilst 23% did not answer.

In all cases the IAM system was supported and maintained in-house, in a small number of cases this also included vendor support.

The next set of major IT projects scheduled for development were portals, single sign on, account self-service and CAUDIT PKI initiatives. Same sign-on and PKI related work with web, staff, and student certificates ranged between 5 – 15% of organisations polled.

The major hurdles to centralised or federated authentication were highlighted as political (62%), technical (42%), security (35%), training (15%) and legal (15%) barriers.

Half of the organisations polled used a combination of agent, push or pull authentication and authorisation processes. 15% used only “pull” processes (where the user requests a service where the service itself interacts with an authentication server), 8% used “agent” process (where the user sends a request to a service provider’s authentication server which in turn interacts with the service provider) and 4% used a “push” process (where the user requests and receives a ticket/certificate from an authorisation server to access the service). 23% did not answer this question.

Current user interfaces to enable a user to login to authenticate were by Portal, Proxy or VPN in more than half of the organisations polled. The use of .htaccess or 802.1x

accounted for approximately 30% of organisations polled. Acceptable user credentials were username/passwords (88%) and IP based authentication (46%), only one organisation used digital certificates, this may be due to no national PKI being currently in place. 85% of all organisations polled made use of a directory based service to verify authentication requests, a range of SUN, Microsoft, Novell, RADIUS, Kerberos and Oracle products were in use as primary, secondary or tertiary Directory Services. Only 31% believed their directories had a provision for storing PKI certificates or keys.

Primary data sources for directory services were Student Databases (88%), Human Resource Databases (77%) and Other Sources (42%). In most cases, data is migrated from these sources to a Directory Service using a variety of in house developed solutions written in code based on code such as PERL, Visual Basic, JAVA, C++, or SQL to process formatted data into Directories.

Many organisations provide an Identifier to staff, students, visitors, alumni and others. Unique identifiers tend to be assigned to staff and students. Standard metadata schemas for configuring user profiles are either LDAP based and/or locally developed. Almost 20% use eduperson, one organisation uses X500. No sites used AU\_eduperson. A range of eleven metadata fields are currently in use

Role based authorisation is supported by 61.5% of organisations polled; the most supported roles were staff (65%), postgraduate and undergraduate students (54%) and alumni & researchers (15%).

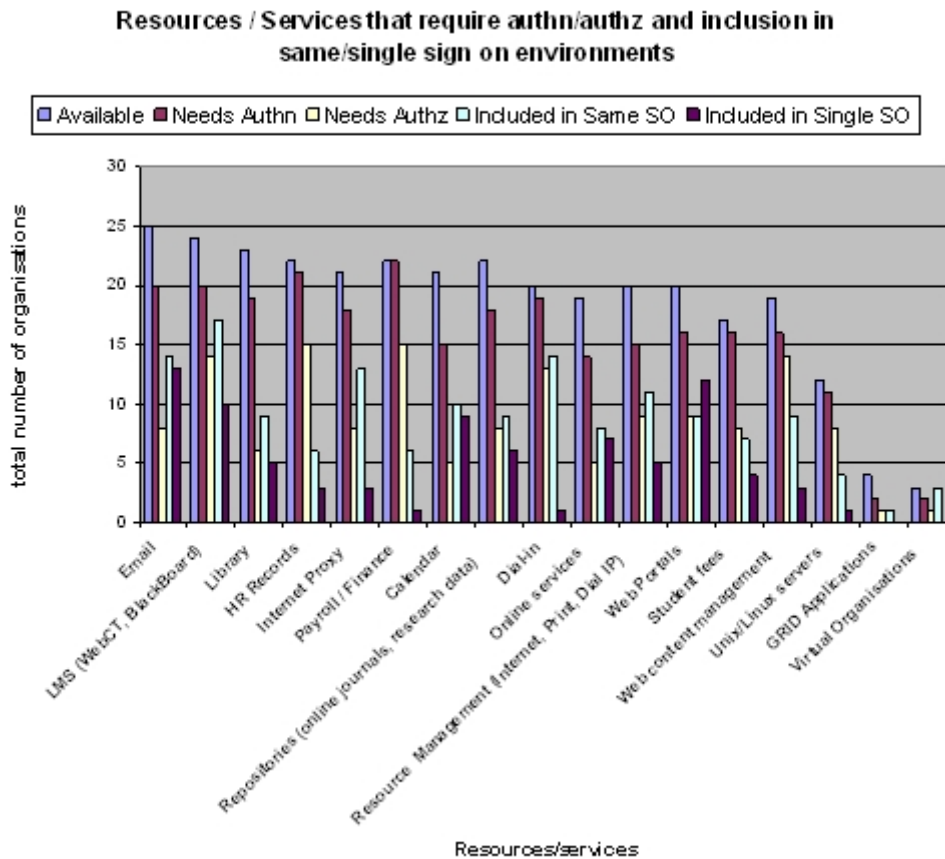
In terms of visitor access, 76.5% of organisations polled provide temporary accounts to visitors; these accounts are administered by IT staff (53.8%), by Department (19.2%) or by other means (IT service desks, secretariat or central management). Visitors can access http/https web browsing (65.4%) or VPN access (38.5%), Others (42.3%) included access to printing facilities, email and a range of applications.

## **End User Support**

End users typically register for the first time to obtain an identity and password for network, application and resource access. Method for first time registration currently used are by receipt of a letter (as part of the registration/enrolment process) (65%), via the helpdesk (46%), online registration (19%) or others methods (on/off campus online service, via IT faculty staff (for staff) or by an account automatically created for students based on their personal information).

54% of organisations polled do not use password aging, of the 46% that do use it, the password time limits are 60 days (19%), 90 days (15%) 120 days (8%) and 180 days (4%).

A number of resources/services require authentication, authorisation, same or single sign on integration (see below).



The low response to GRID and Virtual Organisation applications/resources may be due to the fact that only six Higher Education Universities polled are involved in Research community activities. In addition no replies were received from the research community. The graph above shows that in all cases authentication needs are generally higher than authorisation. Human Resource and Payroll and Finance systems show a high level of both authentication and authorisation which is understandable given the sensitive data stored and accessed. The same is true for access to Unix/Linux servers which require higher levels of access control to ensure both standard and critical systems remain secure. Same and single sign on integration appears more erratic in support of the range of applications or services listed. 77% of organisations rely on Virtual Private Networks to securely transport user authentication data (username/password) securely, whilst almost half of all organisations that responded use either ezproxy or a proxy cache to authorise on campus users, webiso was used by 12% of organisations

Information released such as user attributes to authorise access was in most cases based on a cookie or token, whilst 19% of organisations used a username/password, unix membership username, user attributes or LDAP attributes.

Where user roles and attributes are assigned and managed in groups, the Microsoft platform was in most use (45%) whilst SUN, Novell and other methods (in-house, oracle, or LDAP based) accounted for 30% of all organisations polled for each platform.

Support for users with multiple affiliations was highest for staff and visitors with many organisations included support within their same or single sign on environments.

Differences that exist within authentication and authorisation infrastructures to support users who are not on campus to gain access to resources/services tended to be in the way authentication credentials are securely transported this is because off campus users have to pass their credentials across multiple administrative domains. Access to resources and services may also be affected if access is based on IP based authentication (which in most cases relies on the user accessing resources when physically located on the campus in line with digital rights licence conditions for example).

### **Same / Single Sign On**

38% of organisations polled have deployed same sign on environments for staff or students. A slightly higher proportion of organisations polled have deployed single sign on support for students (46%) than for staff (38%). Organisations polled were either not using single sign on but would like to, were piloting single sign on or using it “in production” . Overall there appeared to be a positive approach towards developing systems to support single sign on environments for end users.

Only 23% of organisations polled currently collaborate with others in some way, therefore the scope or opportunity to develop same or single sign on environments that can support inter-organisational collaboration may be quite small.

### **In house skills set**

The answers to previous questions seem to show that most organisations polled have developed their IAM systems and system integration aspects with other components in-house. Most also manage and support their systems in-house. This approach may be the result of integrating legacy systems or simply the complex nature of system integration in this area where IAM systems have evolved to become critical business processes over time. This reasoning is based on answers in previous questions combined with the relatively high scores for in-house skills that are in on average either rated as average or above. Lower scores appear in AU-eduperson (that no-one who responded to the survey seems to be using at the moment) and same or single sign on deployment that many sites have yet to deploy or are in the process of doing so

## **Profile/Awareness**

The highest average score was in Senior Management Awareness of IAM systems, followed closely by Senior Management understanding of core middleware technologies and Management available to support development and maintenance activities. Areas of possible improvement were in the allocation of time/resources to identification and implementation activities of IAM systems, receipt of funding and commitments to IAM system development, and the availability of resourcing and stakeholder involvement.