

Identity and Access Management in the KAREN Community

A report on the development of identity and access management systems

Professor James Dalziel, Macquarie University, Workshop Leader

Neil James, University of Otago, KAREN IAM Workshops Project Manager

December, 2007

Introduction

REANNZ contracted the University of Otago to run national workshops on identity and access management (IAM) for KAREN member organisations. The aims of these workshops were to:

- Raise the awareness of the role of identity management in e-Research.
- Produce a platform of knowledge and understanding from which KAREN members can move forward with a common understanding of their ultimate destination with respect to identity management.
- Produce a stocktaking of all members' current position and intentions with respect to identity management.
- Produce sufficient technology transfer to New Zealand that KAREN members are able to plan for membership in an appropriate identity management trust federation.

Professor James Dalziel from Macquarie University, and leader of the Australian MAMS (Meta-Access Management Systems) project, was engaged to lead the main presentations at Workshops in Auckland and Christchurch on the 5th and 6th of November 2007 respectively.

Twenty two delegates attended the Workshop in Auckland and 25 in Christchurch. There were eight KAREN member organisations represented in Auckland and nine at the Christchurch Workshop. While at least one delegate from each KAREN member organisation had pre-registered to attend the Workshops it eventuated that only 17 of the 18 KAREN member organisations were represented. Enrolment from outside the actual KAREN member community included Ministry of Research Science and Technology, the Ministry of Education, the SuperLoop and the Nelson Loop, and REANNZ. A full list of attendees is included in Appendix 1.

The Workshop agenda, including a list of questions delegates were asked to report on, is included in Appendix 2.

Executive summary

It is clear that the IT staff from members of the KAREN community are generally well informed about IAM issues. While some organisations have made significant advances others have yet to initiate a programme or project to address IAM development. While the IT staff generally have a good understanding of the importance of IAM and trust federation there is evidence that in many cases top-level executives of organisations have yet to appreciate the significance of well managed IAM, and in consequence may not provide support for the necessary work.

There is a strong desire to continue to work closely with Australia through the Australian Access Federation (AAF) initiative, and KAREN member organisations have indicated they are comfortable with joining the emerging AAF trust federation.

Work done by New Zealand government departments, and the Ministry of Education in particular, is seen as complimentary to the directions that the KAREN community is pursuing, but there is a need to ensure close ongoing communication and continued interoperability testing between the parties.

This report concludes with a list of recommendations for action by various agencies. If New Zealand is to progress satisfactorily in this area it is important that there is an active ongoing programme of supporting activities. It is recognised that the greatest advantage from federations comes with the growth in the number of services provided by federation service providers, and growth in the number of identities available from identity providers within the federation.

Stock take

Methodology

As noted in the agenda one of activities at the Workshop was a discuss around the development in the IAM area at each member organisation. A set of questions were sent out before the Workshops and organisations were encouraged to respond briefly in writing before the Workshops. Twelve organisations did respond before the Workshops and subsequently 5 sent in some notes. The information gathered during the dialogue at the Workshops has been combined with the provided notes to give a good insight into the level of IAM maturity within KAREN member organisations.

Responsibility for identity management

Most organisations have several internal agencies responsible for identity management (IdM). The agencies include Human Resources, Finance, Information Systems, and for universities, Student Administration. However few have any governance body overseeing issue to do with IdM. This can be a cause for concern, especially in larger organisation where coordination of activities, and consistency of services, can be jeopardised by lack of cohesion.

IAM principles and policies

Few organisations reported having any agreed principles and policies for IAM development and deployment, but there was good evidence that organisations understood the need for clear principles and policies, and there was an indication that this will be addressed in many organisations in the near future.

Existence of a centralised directory service

The majority of organisations already have a centralised directory service, or are well advanced towards this aim. It is clear that there is a strong recognition across the membership of the importance of a robust central directory service.

Directory systems in use

Novell's eDirectory, and Microsoft's Active Directory are in wide-spread use, as is Open LDAP. Many reported using a meta-directory approach, to provide the effect of a single directory. The limited number of technologies being used across the KAREN community simplifies any downstream support requirements.

Provisioning services

There were a number of in-house developments for the provisioning of access management information, plus some use of Microsoft and Lotus notes solutions. Both commercial and open source developments in this area will offer new opportunities in the future for internal organisational development of provisioning.

Single Sign-on

Half of the member organisations reported deployment of single sign-on (SSO) solutions to some extent. However several noted their aim was towards reduced sign-on, rather than SSO. There is a recognition of the desire for stronger authentication for access to more security sensitive services. Balancing the strength of authentication against the desire for simplicity for the user continues to be a matter for discussion.

Federated access technologies

Most organisations reported that they had looked at Shibboleth or had done some research into deployment of Shibboleth. One organisation had already joined the MAMS Testbed at level 2 another at level 1. There was a good understanding in the majority of the organisations of the eventual requirement for federated access to services and resources. It is apparent the technology of choice is Shibboleth, and the next version is based on SAML2.

Existence of a formal development project in the IAM area

Three organisations reported that they had a formal project established for IAM development while several others were in the early planning stages for such a project. Others had development underway but not under a formal project structure.

Of those with projects, or planned project, most were being driven from the central IT section, in some cases with significant representation from outside of IT.

Collaboration with outside organisations

Half of the KAREN member organisations reported current IT collaboration with outside organisations, and there was a general understanding of the importance of making provision for IT trust federations to foster collaboration opportunities.

Summary of the main findings

Some positive indicators

1. A good understanding in the community of the issues around IAM

It was pleasing to note in discussion that the community members had a good level of awareness of identity and access management requirements, and their importance as a building block for collaboration via IT trust federated access.

2. Strong support for members of the KAREN community to join the AAF IT trust federation

There was strong desire expressed by several organisations to eventually join the AAF. The putative AAF members are seen as being those that the current KAREN community member would be most likely to collaborate with, and have the most in common with.

3. Good progress toward IT trust federation capability in some institutions.

Several organisations have already research and in some cases undertaken development work using Shibboleth and related IT federation software. There is already a growing community in New Zealand with some expertise, and a willingness to share skills an experience amongst the members.

4. The BeSTGRID project has been a significant driver in the development of capability.

There is ample evidence that the BeSTGRID project has spearheaded development in IAM and federated access. There was concern expressed that BeSTGRID must not be dropped, and an understanding that some form of continuation of the project must eventuate.

5. Liaison between the KAREN community and the Ministry of Education

There is ongoing liaison between universities (in their use of Shibboleth and the MAMS testbed federation) and the evolving Ministry of Education trust federation, including an initial technical interoperability demonstration. Further liaison and development of interoperability is planned for the future.

6. Working with Australia

Workshop participants were comfortable building on the work of the MAMS and AAF projects in Australia, and participating in these federations. For the short to medium term, it seems likely that research and education members of the KAREN community will continue to use these existing federations for sharing, although in the long term, it would be appropriate to review whether a separate New Zealand higher education and research federation is necessary (which could then peer with the AAF), or alternatively, to continue to participate in the AAF.

Observed shortcomings

1. Many institutions lack governance – both in structure and process.

It is clear that there is a general lack of governance over IAM development, and in many case IAM is seen as an IT project. This is of particular concern in that IAM in the current business environment is a fundamental infrastructural building block.

2. There is in many cases a lack of understanding, and hence support, from upper management.

This is despite IAM becoming a top issue with Directors of IT. While the rhetoric of collaboration in research is common linking this with the need to advance IT systems infrastructure to support easy inter-institutional IT operation is not always understood. When it comes to IT trust federation it is essential that the CEO understands the policy implications, as it is the CEO that will be required to sign federation agreements, and bilateral agreements that provide the legal underpinning for automated inter-organisational IT collaboration tools.

3. IAM is too often seen as an IT matter.

The IT people see the need and are the early movers to seek to create sound IAM systems, it is the organisation as a whole that needs to understand and support IAM development. Ideally an IAM project should be led by the 'business' managers as a whole.

4. Few KAREN member organisations have a specific project to tackle IAM issues.

Much of what is being done is managed by technical staff taking an initiative to develop what they can see as necessary, but without the explicit support a formal project would provide. In consequence IAM initiatives may struggle to get appropriate priority and resourcing.

5. Small institutions in particular are finding it difficult to see where resources would come from to mount a comprehensive IAM project.

Where IT is seen as a cost to be minimised, rather than an opportunity to better support the organisation's core functions, there will be continuing problems in achieving the necessary level of infrastructure.

Value of the workshops themselves

In addition to achieving the require outcomes, the mounting of the workshops has already lifted the level of interest in IAM in general, and it is expected that further activities in this area will stimulate and accelerate development. It is important that an ongoing programme of activities is planned and supported, to help ensure optimal uptake of trust federation membership in the future.

Some potential action points

Development of the business case

There is a need to further build the business case for implementation of sound and comprehensive IAM infrastructure, leading to the potential to join IT trust federations. One mechanism for this is the development of strong uses cases that convey to senior executives and Board members the business needs in terms they will readily identify with.

Building capability and capacity in New Zealand to support IAM development and IT trust federations members

While there is the ongoing invitation to work with the Australian groups in AAF and in the MAMS project, it is important that the KAREN community develops its own capacity. There is a need for the establishment of a core group of New Zealand people with the knowledge and expertise to provide a national resource and a focus for the developments that are required as the KAREN member community work towards capability for IT trust federation membership. This is not just in the technical aspects, which are mentioned below, but is also in the international relationship building and in gaining experience and knowledge about what is necessary in policy development and establishment of agreements for trust federation.

Development of technical expertise

Most if not all KAREN member organisations will continue to develop IAM capability in-house, and use their own staff to achieve the capability to join IT trust federations. One key resource here may be – and indeed has already been for two New Zealand organisations – the MAMS hands-on federation workshops which are now being run in Australia – see Appendix 3. A general invitation has been made to the KAREN community to have staff attend these workshops, space permitting, as long as travel and accommodation costs are covered. This generous offer continues the strong collaboration on IT development in the research, education and library services across the Tasman. An earlier manifestation

of this cooperation was the formal establishment of AUSCert, where New Zealand universities were an early key supporter.

Support for smaller organisations

It is recognised that smaller organisations in particular find it difficult to identify resources that can be put toward infrastructural projects such as IAM development. There may be an opportunity to provide some outside support to help ensure that the whole KAREN community moves forward to IT trust federation capability. In the UK JISC¹ is currently giving consideration to a development whereby smaller organisations would receive a visit from a federation action team who would work with the organisation on a short-term basis. If such a direction is to be considered it is important not to overlook the need for the organisation’s top executive team to understand the policy implications of joining IT trust federations.

Opportunities for New Zealand to contribute to international IAM infrastructure development

It is recognised that New Zealand is benefiting, and will continue to benefit, from the work that has been done in the development of IAM and federation solutions in other countries, particularly including work done by MAMS in Australia, and by Internet2 in the US. There are however opportunities where New Zealand could provide its own contribution to the worldwide developments.

The Ministry of Education has worked closely with the MAMS project, and the higher education community are well informed about the AAF development. There is an opportunity to take a lead in the development of ‘account linking’, whereby the Ministry could provide identity information about perspective students as a starting point for identity creation in universities.

Also, again through the work already done by the Ministry of Education, New Zealand has an opportunity to bring the schools sector into it trust federation with the tertiary education sector. While work is progressing in this area in other countries, the small size of New Zealand, and the current level of development, does provide an opportunity for New Zealand to lead in this area.

Recommendations

Recommendation	Detail	Agencies responsible
1 Building capability and capacity in New Zealand to support IAM development and IT trust federations membership	Investigate the establishment of an IAM and trust federation working group supported by REANNZ. This group should include technical and organisational skills, and should provide the coordination for work in the area. It could also be responsible for the running of local workshops, perhaps in partnership with MAMS. One or more of this group should build and maintain international connections including attending international forums such as the Internet2 meetings, and participation in inter-federation policy and implementation discussions.	REANNZ Capability Build Advisory Panel
2 Create a support environment for those people involved in the development of IAM and trust federation	Form a mailing list for interested New Zealand people, and encourage discussion on implementation issues. Create a wiki for collation of useful support material, providing a forum for the interchange of technical information between the IAM	IAM Working Group

¹ Joint Information Systems Committee

	Working Group recommended in 1 above and members of the KAREN community. The actions for this recommendation could be initiated and maintained by the IAM Working Group recommended in 1 above.	
3 Develop a briefing paper on IAM and IT trust federation for senior management	This could be actioned through seeking expressions of interest from KAREN member organisations, or other appropriate bodies, to contract for the development of a briefing for senior management, and the mounting of a series of meetings with senior executives (CEO, Vice-Chancellor, Deputy VC) of KAREN member organisations. This briefing would need to have compelling 'use cases' that senior executive can intuitively understand and identify with.	REANNZ Capability Build Advisory Panel to develop expression of interest documentation for an appropriate agreement or contract
4 Identify key services for federated access	Conduct a review and document strategic services that would drive federation adoption, prepare a plan for bringing these services into federations. This action could become part of the contract for the development of the senior management briefing.	Briefing Contractor
5 Encourage prioritisation of SSO and local directory development within institutions to help them prepare for joining the trust federation	Members of the KAREN community need to investigate and develop appropriate internal programmes to support IAM development. Organisations should be encouraged to send staff to MAMS workshops where appropriate. To encourage this further the capability travel fund could support attendance at such workshops, and the availability of the workshops and the potential travel support should be widely advertise in the KAREN member community.	Members of the KAREN community. REANNZ Capability Build Advisory Panel and REANNZ
6 Liaison with government departments	Continue liaison with government Ministries and in particular the Ministry of Education on trust federation, and continue technical interoperability trials.	REANNZ Capability Build Advisory Panel and REANNZ
7 Direct financial support of IAM and federation initiatives	Consideration should be given to the establishment of a mini-grant scheme such as that operated by the AAF. See Appendix 4.	REANNZ Capability Build Advisory Panel
8 Explore the opportunity to lead in the	Within the liaison activity between the universities and the Ministry of Education there should be consideration of the establishment of	REANNZ Capability Build Advisory Panel and the Ministry of Education

development of account linking technology	a specific project to develop open source identity management account linking policy and technology	
--	---	--

References and links

MAMS – <http://www.melcoe.mq.edu.au/projects/MAMS/>
AAF – Australian Access Federation – <http://www.aaf.edu.au/>
BeSTGRID – <http://www.bestgrid.org/>
KAREN – <http://www.karen.net.nz/>
JISC – <http://www.jisc.ac.uk/>

Appendix 1 – Workshop attendees

The Workshops were Chaired by Neil James, the IAM Project manager. Professor James Dalziel lead the presentations. Vladimir Mencl and Yifan (Eric) Jiang from the BeSTGRID project gave presentations at both Workshops.

Auckland

Art Brown	AUT
Brian Green	AUT
Calum MacLeod	AUT
Iain Matcham	GNS
John McMaster	HortResearch
David Dyer	HortResearch
Andrew Hartnell	Massey University
Graeme Fox	Massey University
Anton Gerdelan	Massey University
Jenni Harrison	MoRST
Lockie Stewart	National Library
Bill Choquette	REANNZ
Sharon Fafeita	SCION
Leonie Hayes	University of Auckland
Yin Yin Latt	University of Auckland
Matthew Cocker	University of Auckland
Nick Jones	University of Auckland
Paul Bonnington	University of Auckland
Yifan (Eric) Jiang	University of Auckland
Vladimir Mencl	University of Canterbury
Pieter Le Roux	University of Waikato
Mike Vallabh	University of Waikato

Christchurch

Phillip Lindsay	AgResearch
Stuart Dillon-Roberts	AgResearch
Dean Patfield	Crop&Food
Terry Broad	Crop&Food
Mark Phegan	IRL
Chris Jordan	IRL
Flo Weingartner	LandcareResearch
Marcus Holland	Lincoln University
Royston Boot	Lincoln University
Mike O'Connor	Ministry of Education
Danny Hill	Nelson Loop
Anthony Cole	NIWA
Julie Watson	REANNZ
Derek Wenmoth	SuperLoop
Yifan (Eric) Jiang	University of Auckland
Robin Harrington	University of Canterbury
David Whale	University of Canterbury
Peter Kennedy	University of Canterbury
Vladimir Mencl	University of Canterbury
Ivan Mason	University of Otago
Mark Borrie	University of Otago
John Hine	Victoria University
Sam Searle	Victoria University
Andrew Beaumont	Victoria University
Caleb Ling	Victoria University

Appendix 2 – Agenda

Identity and Access Management Workshops

5 November 2007, Council Room (210), Clock Tower, 22 Princes Street, Auckland

6 November 2007, Coppertop Room, Level 2, Commerce Building, Christchurch

The Workshops will be led by Professor James Dalziel. The IAM Workshop Project Manager, Neil James, will Chair the proceedings.

Timetable

- Commence at 10am (with tea/coffee/juice/water etc. from 9:30am)
- Lunch at 12 noon
- Afternoon break with drinks at 2:45
- Close at 4pm

Agenda

	<i>Approximate timing</i>
Introduction by the Chair	[10 minutes]
<ul style="list-style-type: none">▪ What to expect during the day▪ What are the desired outcomes?	
IAM – what is it all about?	[20 minutes]
Identity management within the organisation.	[15 minutes]
IT trust federation.	[15 minutes]
<ul style="list-style-type: none">▪ A brief introduction to federation.▪ Shibboleth and other tools	
Where do PKI certificates fit?	[10 minutes]
OpenId and ‘Identity 2.0’ – what is it and where does it fit?	[10 minutes]
AAF	[30 minutes]
<ul style="list-style-type: none">▪ Projects underway▪ What has been achieved? Examples of use	
LUNCH	[30 minutes]
A roundtable discussion to elicit information about each organisations capabilities in IAM. At least one person from each KAREN member organisation should prepare for this <i>before</i> the Workshop this using the attached questions (also circulated before the meeting) as a guide.	[120 minutes]
The big picture for KAREN members – membership of AAF in relation to the New Zealand Ministry of Education initiatives	[15 minutes]
AFTERNOON BREAK	[15 minutes]
Case Studies	[30 minutes]
<ul style="list-style-type: none">▪ An example from Australia▪ BeSTGRID IAM developments in New Zealand (Vladimir Mencl and Yifan (Eric) Jiang)	
The next steps	[15 minutes]
A round table discussion on what attendees would find useful to support their work in IAM and IT Trust Federation preparations.	

Preparing for the Identity and Access Management Workshop

One of the activities at the Identity and Access Management Workshops will be a round-table discussion aimed at determining the state of IAM development across the KAREN member community. To facilitate this discussion it is important that at least one person from each KAREN member organisation attending is prepared to respond to the questions below. Information gained from this exercise will help the Advanced Network Capability Build Advisory Panel determine where additional support should be provided in the future as the KAREN community moves toward general capability for membership of IT trust federations. It would also be appreciated if you could provide some brief written responses before the Workshop to <mailto:neil.james@otago.ac.nz>

A. State of identity and access management in the member organisation

- Who is responsible for user identities in your organisation?
 - Is there more than one part of the organization that manages user identities independent of other parts?
 - Is there a high-level governance body that oversees the development of IAM?
- Are there established clear policies covering the whole organisation for IAM?
 - Guiding principles
 - Business process rules
 - Technical standards
- What technologies are currently in use for IAM?
 - Do you have a centralised directory system?
 - What directory system(s) are you using?
 - What solution are deployed for provisioning/access management?
 - Do you employ single sign on technologies?
- Is there a strategy for using a central directory & SSO mechanism for access to organisational systems and services?
 - In terms of users having a single account for access to all relevant systems, which of the following best describes your current status:
 1. Already implemented
 2. Implemented in part, moving to full implementation over time
 3. Currently implementing central directory/SSO, plan to implement unified access to systems/services after this
 4. Yet to implement, but project planning is underway
 5. Yet to develop a project if this kind
- Is there any development work on Shibboleth or other federated access technologies?

B. Is there a project planned or underway to address any outstanding IAM issues?

If so how is it structured?

- Who are the participants?
- What involvement is there from the high-level executive team of the organisation?
- How is the activity funded?
- Does the project only focus on technical activities, or is there involvement of managers who control existing identity information?

C. Level of collaboration with other (external) organisations

- Are you currently sharing access to data sources with other organisations?
- Are you providing or gaining access to IT based services for or in other organisations?
- How do you currently provide security of access in these collaborations?

Appendix 3 – AAF workshop example

AAF Workshop – August 2007

When: 27-29 August 2007

Where: Macquarie University, Sydney, Yerbury & Whitely room – SAM Building (C10A)

RSVP: before 22 August to Bruc Liong (bruc.liong@melcoe.mq.edu.au)

AAF Website: <http://www.aaf.edu.au>

Meals: Morning/Afternoon Tea and Lunch will be provided

AAF (MAMS and AusCERT/UQ) will host a free 3-day Federation Workshop at Macquarie University in Sydney. The Workshop will provide preparation for transition to the Australian Access Federation and technical information and guidance for participants to join the Shibboleth-based MAMS Testbed Federation and a Public Key Infrastructure (PKI) hands-on component.

Objectives of this hands-on workshop:

- participants will be able to Shibbolize service providers by themselves;
- participants will be able to setup and manage their Identity Provider;
- participants will be able to setup and manage a certification authority and issue certificates.

The intended audience, therefore, are technical architects and developers at HE and research institutions. If you know a colleague that would like to attend to, forward him this message and ask him to register (first come, first go).

The workshop consists of two parts, the first 2 days (27 and 28 August) will be full discussion on Shibboleth and the last day (29 August) will be a Public Key Infrastructure (PKI) hands-on workshop.

The Program:

- Introduction to the Australian Access Federation (what it is, what are the benefits, how can you join)
- Introduction to Shibboleth federations (what it is, what it can do for you)
- How to setup an Identity Provider (IdP)
- How to setup a Service Provider (SP)
- How to "Shibbolize" an application
- LDAP resolver back-end
- Attribute exchange between IdP and SP
- Attribute Release Policies (ARP) and Attribute Acceptance Policies (AAP)
- ShARPE & Autograph (including Service Description File, Attribute Mapping)
- Log file explanation; SAML assertions examination
- Certificates, Synchronizing time
- Introduction to IAMSuite (Identity & Access Management suite for Virtual Organizations)
- Advanced topics reserved for 2nd half of 28th August (send me email if you'd like some topics to be discussed)
- Introduction to the technical foundations of PKI
- Introduction to the PKI features of the AAF
- How to set up the PKI components: Certification Authority and Registration Authority, including the processes involved (a hands-on workshop installing and using OpenCA software)
- How to issue and manage certificates
- Work through example certificate use cases
- Discussions on certificate profiles under the AAF

- Discussions on PKI best practices within the AAF

Requirements:

Participants will bring their own laptops, which require:

- Hardware:

- Wireless network with 802.11G (eduroam will be enabled too).
- No wired Ethernet will be provided.
- *Optional:* If they want a copy of their vmware images, they also need to have approx 8GB free on their HD.
- Optical drive capable of reading DVDs (for PKI workshop)
- A USB flash drive (for PKI workshop)

- Software:

- SSH Client + X windows (on windows you can install cygwin + X)
- Web browser
- *Optional:* VMware Workstation or Server suggested for the PKI workshop, if delegate wants to run their own VM.

Appendix 4 – AAF mini-grant programme example

From the AAF Web site in November:

Mini Grant applications due 30 Nov 2007

In order to promote uptake of the AAF within the Australian higher education (HE) sector, the AAF Project will conduct an AAF Shibboleth Mini-Grant Program to assist institutions join the AAF as an identity provider (IdP) or service provider (SP). In particular, the Mini-Grant Program will target valuable, Federation-wide services which will provide value to IdPs and attract the majority of Australian HE institutions to join the Federation as IdPs.

An invitation is therefore extended to Australian HE institutions and related government research organisations to apply for an AAF Shibboleth Mini-Grant to assist in the technical work required to join the Federation as an IdP and/or SP.

Further information is provided in the Application Package document.

Program Name:	AAF Shibboleth Mini-Grant Program
Mini-Grant Value:	Funding up to AUD\$40,000 (ex GST):
	25% prior to commencement of implementation
	50% upon commencing operation as an SP and/or IdP in the Federation
	25% upon presentation of a Federation activity report due within 3 months of commencing operation in the Federation
Applications Due:	Friday 30th November 2007; Notification by 7th December 2007
Selection Criteria:	<ul style="list-style-type: none"> • Value of the service (for SP) and/or user-base (for IdP) in terms of promoting uptake of the AAF • Relevance to AAF goals • Technical excellence of the proposal • Relevant experience of the proposed project team • Relevant project management experience • Involvement with the AAF and/or MAMS Projects to date • Commitment to continue to contribute to the AAF as an SP and/or IdP until at least the end of 2008. • Proposal does not duplicate work already expected from funding received • Proposal is from an Australian university or related Australian government research agency