

# PROPOSAL FOR SII FUNDING

## TITLE PAGE

### **Production PKI and PKI/Shibboleth alignment project**

#### **Summary of Project**

This project builds on the existing PKI and MAMS projects to establish a production Public Key Infrastructure (PKI) for the University and Research Sector, based on the standards developed in the existing project, and to develop a pilot federation which leverages the PKI infrastructure in aligning the trust arrangements between institutions to support the implementation of Shibboleth across the sector. It also seeks to lower the barriers of entry to PKI using open source software. The project outcomes would be to enable the secure sharing of resources and research infrastructure across the domestic sector and with international partners.

**Funding Requested**                      **\$ 649,000**

**Lead Institution (recipient of Grant)**    The University of Queensland

#### **Supported by**

Macquarie University, Council of Australian University Directors of Information Technology (CAUDIT), Australian Partnership for Advanced Computing (APAC), and AARNet Pty Ltd

#### **Team Leader**

**Nick Tate**                      (07) 3365 3521 (phone) (07) 3365 9069 (FAX)  
[N.Tate@uq.edu.au](mailto:N.Tate@uq.edu.au) (Email)

#### **Contact Officer**

**Nick Tate**                      (07) 3365 3521 (phone) (07) 3365 9069 (FAX)  
[N.Tate@uq.edu.au](mailto:N.Tate@uq.edu.au) (Email)

**BUDGET PAGE**

Item	2005	2006
Cost of steering committee meetings (travel and accommodation) at \$8,000 each	\$16,000	\$32,000
Estimated cost of teleconferences	\$ 2,000	\$4,000
Cost of 3 FTE analysts (2 AusCert, 1 MAMS)	\$115,000	\$330,000
Technical services for APAC "GridShib" implementation	\$5,000	\$15,000
Estimated Cost of legal advice	\$35,000	\$25,000
Cost of travel for liaison with HEKPI, CREN and UK e-science centre	\$8,000	\$17,000
Cost of travel for the project team	\$5,000	\$10,000
Estimated cost of 5 "capital city" workshops to provide a conceptual overview and hands-on technical experience in deploying project technologies.	\$15,000	\$15,000
<b>TOTAL</b>	<b>\$206,000</b>	<b>\$443,000</b>

It is proposed that this project would only provide funding for those activities which are best undertaken once for the sector. In order to participate in a production PKI, each institution will need to provide at least the computer hardware to run the appropriate certificate management services and devote resources to supporting and managing it. The capital cost to institutions is estimated at between \$5,000 and \$15,000 per institution, with an annual staffing cost of between \$10,000 and \$20,000 per year. This cost is an investment that each institution would need to make in order to participate and is, in effect therefore, a co-payment by each institution.

## Authentication, PKI and Pilot Federation project

### Background and Context

One of the main priorities for E-Research in Australia is increasing the effectiveness of researchers through rapid access to data, software systems and research outcomes (such as e-journals). Seamless, rapid access requires sophisticated systems for authentication and authorisation, and these systems need to work not only in local contexts, but also at a national and international level.

To enhance national research effectiveness, it is essential that a robust, reliable and well-managed set of identity and access management technologies is readily available. The provision of these technologies will assist in achieving the goals for E-Research set out by Hon Brendan Nelson MP, Minister for Education, Science and Training, in his address to the National Press Club on 8 March 2005; and more specifically, the four themes outlined in the current Call for Proposals, particularly theme 1 “Maximising access to digital resources in Australian universities, especially regional universities” and theme 4 “Providing effective linkages between sets of research information to enable seamless access by researchers”.

In terms of the national research priorities, effective access and identity infrastructure is central to all four key areas of research. In particular, strong authentication methods such as PKI are important for Safeguarding Australia via their role in E-Security; and federation infrastructure provides exciting new approaches in Frontier Technologies/innovation.

Access and identity management for E-Research covers a wide range of technologies and approaches. In particular, the requirements for authentication and authorisation vary according to the research discipline and the type of access required. In some cases, such as Grid Computing, strong authentication methods such as PKI are essential to ensure high levels of certainty before providing access to powerful compute resources. The nature of these resources requires a high degree of certainty that only appropriate researchers are able to gain access. Further, many of these resources exist in an international context where Australian researchers would be disadvantaged in international collaboration if they were unable to use the required PKI methods.

In other cases, such as access to e-journals, more modest authentication methods are sufficient, such as the use of names and passwords. In these cases, scalability may be more important than strong authentication. The ability to leverage existing organizational Directories (including existing names and passwords) via federation infrastructure such as that provided by the Internet 2 “Shibboleth” project allows for rapid widespread deployment at a level of authentication strength appropriate to requirements in this context.

Further, in a small but growing number of cases, the combination of strong authentication (PKI) and Shibboleth federation infrastructure is opening new approaches to distributed authentication and authorisation, such as the new “GridShib” work in the US. This area provides some initial indications of how different approaches to authentication and authorisation can be complementary, based on the different requirements of different categories of users. The MAMS project has also provided initial demonstrations of how PKI-based authentication methods can be combined with attribute-based federation approaches that include “authentication strength” as one of the attributes available to federation Service Providers. The growing collaboration and complementary approaches between PKI and Shibboleth approaches is a key area for further development.

## **The Objectives of the Project**

This proposal builds on the existing CAUDIT PKI standards project, funded by Grangenet with support from DCITA; the MAMS project being undertaken by MELCOE at Macquarie University and work that has been undertaken by APAC. Much of the work undertaken on the PKI project is being undertaken by AusCERT (The Australian Computer Emergency Response Team), which is based at the University of Queensland and participants in the pilot phase of this project include The University of Queensland, Monash University, The University of Melbourne, Queensland University of Technology, Griffith University, Victoria University, University of Technology, Sydney, The Victorian Partnership for Advanced Computing (VPAC) and Victoria University of Wellington in New Zealand.

This Proposal has four central objectives as detailed below:

### **(a) Putting PKI into Production**

A project to build upon the existing Public Key Infrastructure (PKI) standards project and move PKI into production for the Higher Education and Research Sector. While the CAUDIT PKI project is making significant progress in this field, its existing remit and funding is only to develop standards and some trial implementations. The proposal here is to build on this existing work, and then take it to production implementation across the Higher Education and Research Sector

### **(b) Establishing PKI/Shibboleth alignment**

A project to build upon the existing PKI and MAMS projects and the Production PKI project identified earlier to develop models and pilot implementations of a common trust federation which would support both PKI and Shibboleth and therefore support a common approach to authentication and authorisation across the sector. This could include the development of a unified model for federation and trust which aligns PKI and Shibboleth approaches, including pilot demonstrations. This unified model, once complete, could form the basis for a future production Federation service across the Higher Education and Research Sector, aligned with the production PKI service outlined above.

### **(c) Reducing the Systems Cost barriers to entry for PKI**

This project aims to reduce the barriers for entry to PKI for all universities and research institutions by providing cost effective access to a free or low cost Certificate Management System for the sector (including access to the source code). This will require the development of training, documentation and a support mechanism. There is a reasonable possibility that SUN may provide their system to the sector via AusCERT.

### **(d) Integrating Grid technologies with PKI/Shibboleth**

This project will investigate the requirements and develop appropriate technologies to allow the APAC Grid infrastructure to become properly Shibboleth aware. It will provide opportunities for research activities in high-performance computing and large-scale data initiatives to test the functionality and scalability of the Shibboleth authentication architecture and associated authorisation architectures being developed by groups such as PERMIS. It will work directly with the NMI "Grid-Shib" initiative as appropriate.

## Governance

The existing PKI project has a steering committee which is directed by CAUDIT with very wide representation from the sector. The committee includes representatives of Grangenet, AARNet, the Council of Australian University Librarians (CAUL), the Australian Vice-Chancellor's Committee (AVCC), the Australian Research Council (ARC), the Australian Partnership for Advanced Computing (APAC), the Commonwealth Department of Education, Science and Training (DEST), the Commonwealth Department of Communications, Information Technology and the Arts (DCITA), the Australian Computer Emergency Response Team (AusCERT), MELCOE at Macquarie University as well as representatives from a number of CAUDIT members. CAUDIT member universities with representatives on the committee include, The University of Queensland, Monash University, University of Western Sydney, Griffith University, Queensland University of Technology and Waikato University in New Zealand. It is proposed that this existing steering committee would oversee the project in this proposal.

This bid is made primarily under the headings "*Maximising access to digital resources in Australian universities, especially regional universities*" and "*Providing effective linkages between sets of research information to enable seamless access by researchers*", as part of ARIIC's Second Stage – New Project Requirements.

The Proposal is led by the University of Queensland, which is the university where AusCERT is based, and is supported by Macquarie University, The Australian Partnership for Advanced Computing (APAC), CAUDIT and AARNet

## What will be done in the Project/Intended Outcomes of Project

### (a) Project - Putting PKI into Production

The existing CAUDIT PKI project is delivering the following outcomes:

- A definition of different levels of trust for Australian universities
- A common PKI architecture for the sector, using AusCERT as the trust "anchor" to facilitate interoperability
- Common standards for X509 certificates to support and underpin collaboration
- The requirements for a sector wide root certificate signed by AusCERT
- Identified options for a common sector wide approach to obtaining a "browser friendly" certificate
- The implementation of prototype PKI systems, using these common standards, among a small number of universities and research groups.
- Wide dissemination of the standards, definitions and architecture

These outcomes take PKI to the point at which standards have been developed and information about these projects has been widely disseminated. The aim of the proposal here is to take the outcomes of the existing PKI project and support the introduction of a production PKI across the Australian (and if possible New Zealand) University and Research sector.

The activities which will be needed to support this move to production are:

- The development and implementation of appropriate policies and practice statements
- The development of appropriate extensions to the existing AusCERT agreements with CAUDIT institutions which would require members to abide by the agreed policies and practices. {Note – AusCERT already has a contractual relationship with virtually all CAUDIT members}
- The development and implementation of an auditing framework which would allow compliance to be regularly audited
- The development of appropriate training courses for both technical and policy issues.
- The development of agreement for cross trust with other federations {e.g. the US HEBCA, the UK e-science Certificate authority }
- The establishment of a single national certificate authority for the Higher Ed and Research sector at AusCERT
- The sustainable establishment of services for certificate issuance, verification and revocation at the national authority
- Developing, promulgating and supporting common identity standards, {eg. Australian eduperson }

The outcomes and benefits of this project would be:

- A scalable production PKI architecture for the sector which would support strong authentication, encryption and digital signatures
- Interoperability between Australian (and possibly New Zealand) universities and research institutions
- Interoperability with overseas Certificate authorities using Australian issued certificates
- A common approach across the sector to providing secure access to major research infrastructure
- An agreed trust fabric between Australian (and possibly) New Zealand institutions

Work on this project would be undertaken by AusCERT and MAMS

### **(b) Project - Establishing PKI/Shibboleth alignment**

PKI is one part of the requirement for a common sector wide approach to both authentication and authorisation, which tends to be used most where strong authentication or encryption is required. The other main part is the Internet 2 system, “Shibboleth”, which is currently being analysed and implemented as part of the existing MAMS project at Macquarie University.

It is both possible and desirable for PKI and Shibboleth to operate together so as to provide a common approach to authentication and authorisation across the sector. Furthermore, both require an agreed trust fabric between universities and research institutions if they are to be fully effective. Establishing such a fabric is difficult and expensive to set up and there is considerable reason to believe that the trust agreements, which will need to be put in place to support production PKI could be expanded to form the basis of a federation. Development of a unified approach that aligns PKI and Shibboleth would be not unlike the "In Common" federation in the USA but with the existing PKI steering committee setting policy, MAMS providing technical support and federation development/implementation and AusCERT acting

as the potential operational agency.

This is a project to align policy, management, governance and trust models between PKI and Shibboleth, including establishment of pilot implementations of such a federation. It will build substantially on the existing PKI and MAMS projects, the interest in GridShib approaches from APAC, the experiences of other federations, the specialised skill sets within AusCERT, MELCOE, AARNet and Grangenet and the availability of the new high speed AARNet3 network between institutions. The outcome of this project will be to create a unified policy approach to PKI and Shibboleth, together with collaboration with MAMS on a pilot federation which allows sharing of resources using an aligned PKI/Shibboleth approach.

Work on this project would be undertaken by MAMS and AusCERT.

### **(c) Project - Reducing the Systems Cost barriers to entry for PKI**

Having standards, a common architecture, a trust framework and training, one of the remaining barriers to entry for many institutions may be a suitable Certificate Management System (CMS). Whilst there are some existing Open Source Systems which will be investigated, a number of institutions are already using the Sun ONE Certificate Management system, whose heritage is the Netscape Certificate Management System. Although this is a highly functional system, Sun have announced that they will no longer be selling it and that they will cease support.

Sun have been approached about the possibility of licencing this software, including source code to the university and research sector, via AusCERT, so that all institutions could avail themselves of this system without any licencing cost. These approaches have been positively received and are awaiting some agreements from SUN HQ in California.

The goal of this project is to take the SUN software and develop sufficient training, documentation and support mechanisms to allow universities and research institutions to be able to access a Certificate Management System at minimal cost. If it is ultimately not possible to use the Sun software for this purpose, then it is intended that the best available open source CMS is identified as a substitute.

Work on this project would be undertaken by AusCERT and MAMS.

### **(d) Project - Integrating Grid technologies with PKI/Shibboleth**

The APAC Grid infrastructure currently being developed is based in part around a Certificate Authority (CA) hosted by VPAC and the Globus GSI model. While this works to some degree for a small pool of compute resources, it is proving difficult to scale to suit the needs of the APAC application area projects. Large scale projects have attracted large scale user communities, many of them with external collaborators (outside of APAC, and outside of Australia).

In the Information Infrastructure ("Data Grids") program the APAC projects are managing many Terabytes of data for communities with global reach, and in many cases the data access control mechanisms require very rich and complex authentication and authorisation semantics. In many cases this goes well beyond the typical yes/no decision to allow access to a file or a supercomputer based on group membership.

This project will integrate the above PKI and Shibboleth efforts with the APAC grid infrastructure, will examine richer virtual-organisation management systems, and trial authorisation systems that meet the richest needs of many Australian e-research communities, especially those who work in global collaborations.

The work in this project will be undertaken by APAC and MAMS.

## **Usefulness of the project for other higher education institutions and the community at large**

Authentication and authorisation infrastructure are crucial middleware components needed to assist E-Research across the higher education sector; and their successful deployment in higher education can provide a reference model for deployment in other parts of the education sector, and throughout other parts of government through liaison with AGIMO, etc.

This project provides important missing components for the next stage of middleware development, that is: production PKI services; alignment of PKI and Shibboleth approaches; and provision of Certificate Management Services software. A failure to support the activities outlined in this proposal runs the risk of Australia having divergent authentication/authorisation infrastructures, which will hamper attempts to improve rapid access to data, services and research outcomes such as e-journals.

## **How information will be disseminated to other institutions**

The existing CAUDIT Steering Committee has wide representation of key players from throughout the sector, including links to major communities such as CAUDIT, CAUL, APAC, etc. In addition to dissemination through the committee, presentations and demonstrations at relevant national conference (such as the December Middleware Forum) can be expected.

A key dissemination mechanism will be two sets of 5 capital city workshops to provide a conceptual overview and hands-on technical experience in deploying project technologies.

A comprehensive project website, including background information, implementation advice and relevant standard and software will be provided to accompany the project.

## **Implementation timetable**

Phase 1: July-December 2005

- Project start-up
- Allocation of tasks across project partners, including recruitment of technical staff where required
- Initial project website development
- Preparation for presentation at December Middleware conference
- Site visits and extended collaboration between AusCert and MAMS
- Initial scoping of GridShib implementation (APAC and MAMS)
- Planning for production PKI rollout

- Continued negotiation on Certificate Management Software
- Initial scoping of alignment between PKI and Shibboleth trust approaches

#### Phase 2: January-June 2006

- Further development of project website
- Rollout of production PKI
- Continued site visits/collaboration between AusCert and MAMS
- Acquisition and implementation of Certificate Management Software
- Further development of alignment between PKI and Shibboleth approaches, including exploration of level of trust, legal agreements, scalability, etc
- Initial pilot implementation of PKI and Shibboleth test federation
- Pilot implementation of GridShib approach (APAC and MAMS)

#### Phase 3: July-December 2006

- Finalisation of project website, and planning for maintenance/sustainability by CAUDIT partner for 2007 and beyond
- Continued rollout of production PKI
- Continued site visits/collaboration between AusCert and MAMS
- Further implementation of Certificate Management Software
- Finalise unified approach to alignment between PKI and Shibboleth approaches, including exploration of level of trust, legal agreements, scalability; and including recommendations for rollout of a production Federation in 2007
- Further pilot implementation of PKI and Shibboleth test federation
- Further pilot implementation of GridShib approach (APAC and MAMS)
- Project evaluation, review and wrap-up