

**Table of Contents**

**Project Summary .....2**  
**Project Objectives .....2**  
**Considerations.....3**  
**Project Progress .....3**  
**Project Team .....4**  
**Project Deliverables.....5**  
**Steering Committee .....5**  
    Steering Committee Meeting..... 6

## Project Summary

The eSecurity Framework project is part of a larger effort from Australian Higher Education Sector with support from AusCERT, CAUDIT, the Australian government and other institutions to develop an environment in which Universities can collaborate with each other at low cost and low risk.

This project builds on the existing CAUDIT 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.

DEST has approved a project extension until June 2007.

## Project Objectives

The aim of this project is to develop and ultimately implement a PKI for CAUDIT universities (which include universities in Australia, New Zealand, Fiji and Papua New Guinea) and the CAUDIT research community. To achieve this goal the project team is working closely with other projects such as Meta Access Management System Project (MAMS) and Middleware Action Plan and Strategy (MAPS). A phased approach is being used in order to test interoperability and find out issues regarding PKI enabled applications prior to production implementation.

This project has four central objectives as detailed below:

- **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 was making significant progress in this field, its funding was only to develop standards and some trial implementations.

- **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 includes 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.

- **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.

- **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.

## Considerations

This project and its funding are aimed at continuing the work of the CAUDIT PKI Project with the view to building a production PKI infrastructure that could be deployed to support the Australian Higher Education Federation. In addition, further discussions will continue with various vendors so that once the production PKI environment is commissioned, the Root Certificate for this environment can be embedded into the browser. This work cannot be drawn to a conclusion during this project and must wait until a production environment is established.

Discussions with Microsoft and other vendors regarding the possibility of adding the Australian Higher Education Federation Root CA certificate to browser have taken place. Microsoft indicated that they support this approach. The only request made by Microsoft for the AHECAF certificate to be added to the browser and other applications is for the production infrastructure to undertake and pass a WebTrust audit. The WebTrust audit and infrastructure hardware and software are outside the scope of the eSecurity Framework project and we are seeking support from DEST to implement this infrastructure without costs to the Higher Education Sector.

Additionally for the AHECAF to bridge and/or cross certify with other Bridge Certification Authorities it must follow world wide acceptable best security practices and standards, which include an independent, world wide recognised, third-party audit. In addition, to maintain such bridge membership an annual audit similar to the initial audit must be carried on. The Federal Bridge Certification Authority (FBCA) in USA is an example of these requirements.

There is an interest from the Higher Education Bridge Certificate Authority (HEBCA) and the Federal Bridge Certificate Authority (FBCA) both in America to bridge with the Australian Higher Education Certificate Authority once its production PKI environment is commissioned.

It has been noted that there is a lack of standardization and agreement between the higher education institutions in Australia and globally on what type of information should be available in campus directories to facilitate the deployment of multi-institutional networked services and resources.

Investigation is required to determine whether the various eduPerson schema being developed around the world need to be extended to meet the unique needs of the Australian Higher Education and Research sector and if so in what directions.

## Project Progress

The project team is working on the first phase of this project listed below:

- Develop Capability study of CMSs.
- Conduct extensive testing and document test procedures and results.
- Develop interoperability test matrix.
- Develop and process an applications requirement survey for universities to respond and publish results to Higher education Sector.

## Progress so far includes:

- The esecurity.edu.au domain has been registered and a web site for this project has been developed and is available at: <http://www.esecurity.edu.au/>
- The Higher Education applications requirement survey was well received and supported by the sector, with 28 responses from institutions. A survey summary is available at: [http://www.esecurity.edu.au/docs/application\\_survey\\_summary.pdf](http://www.esecurity.edu.au/docs/application_survey_summary.pdf)
- A mailing list for the SC to discuss issues regarding this project has been created. To post messages please email [sc-esec@auscert.org.au](mailto:sc-esec@auscert.org.au), if you have any problem with posting to this list please inform Viviani at [viviani@auscert.org.au](mailto:viviani@auscert.org.au).
- Three new staff have been hired, two are located at The University of Queensland and one at Macquarie University in the MAMS team.
- The Management Committee (MC) has been meeting regularly.
- A PKI Test-Bed federation has been setup. This test-bed includes several universities and virtual organizations CAs. From this PKI we are issuing SAML certificate for use in the MAMS test-bed federation as well as user and server certificates.
- There has been agreement between the Australian Grid, PKI and Shibboleth communities to form a common alignment in their policies and practices, thus forming the Australian Higher Education and Research Trust Federation (AHERTF). A name to describe this federation has not been selected yet.
- A Shibbolised wiki has been developed as a vehicle to help disseminate information regarding PKI deployment. It will also allow the Australian Higher Education and Research community to collaborate and participate in the processes necessary to help define policy and practice for the AHERTF.

## Project Team

Three new staff have been hired, two are located at The University of Queensland and one at Macquarie University (MAMS).

The following are working in this project:

**Project Manager:** Mr. Nick Tate, Chair of the Committee and CAUDIT

Phone: (07) 3365 3521      Email: [n.tate@its.uq.edu.au](mailto:n.tate@its.uq.edu.au)

**Project Officer, Policy Designer:** Ms Viviani Paz, AusCERT.

Phone: (07) 3365 4290      Email: [v.paz@auscert.org.au](mailto:v.paz@auscert.org.au)

**Project Architect:** Dr. Rodney McDuff

Phone: (07) 3365 8220      Email: [r.mcduff@its.uq.edu.au](mailto:r.mcduff@its.uq.edu.au)

### Technical Team:

John Zornig

Phone: (07) 3365 4288

Email: [j.zornig@uq.edu.au](mailto:j.zornig@uq.edu.au)

James Lever

Phone: (07) 3365 7342

Email : [j.lever@uq.edu.au](mailto:j.lever@uq.edu.au)

Michael Yi Lin

Phone: (02) 9850-9077

Email: [ylin@melcoe.mq.edu.au](mailto:ylin@melcoe.mq.edu.au)

## Project Deliverables

The following deliverables have been identified from the eSecurity project framework proposal submitted and approved by DEST.

Description	Responsibility	
	AusCERT	Others
- Production AusCERT Root CA	√	
- Production AusCERT Sub CAs	√	
- Production AusCERT RA	√	
- Production University example CAs	√	
- Production University example RAs	√	
- Documentation including		
o AusCERT Root CA Certification Practice Statement	√	
o AusCERT Root CA Certificate Policy	√	
o AusCERT Root CA support policies	√	
o AusCERT Sub CAs Certification Practice Statement	√	
o AusCERT Sub CAs Certificate Policy	√	
o AusCERT Sub CAs support policies.	√	
o Higher Education CP/CPS draft template	√	
o CMS installation guidelines for Higher Education Sector PKI adoption	√	
- Integrate Grid Community technical requirements into PKI production	√	VPAC
- Integrate Shibboleth technology into PKI Federation	√	MAMS

## Steering Committee

The Steering Committee for the CAUDIT PKI project became the Steering Committee for this project. The Steering Committee is as follows:

Ms Maxine Brodie, Council of Australian University Librarians  
 Mr Bruce Callow, Griffith University  
 Mr Jack Chorowicz, Monash University  
 Mr Phil County, Victoria University  
 Professor James Dalziel, Macquarie University (MELCOE)  
 Mr Paul Davis, GrangeNet  
 Mr Darren Geddes, University of Western Sydney  
 Mr Peter Nicholson, DEST  
 Dr Rodney McDuff, The University of Queensland  
 Mr Richard Northam, CAUDIT Senior Project Officer  
 Prof John O'Callaghan, Australian Partnership for Advanced Computing  
 Ms Viviani Paz, AusCERT

Robin Harrington, NZ Vice Chancellors Standing Committee on IT  
Prof Alex Reid, AARNet  
Prof Chris Marlin, Australian Vice-Chancellors Committee  
Mr Keith Besgrove, DCITA  
Mr Nick Tate, Chair of the Committee and CAUDIT  
Dr Joe Young, Queensland University of Technology

A Management Committee (MC) has been created to provide additional close direction for this project. MSC members include:

Prof James Dalziel, Macquarie University (MELCOE)  
Markus Buchhorn, The Australian National University, APAC  
Prof Alex Reid, AARNet  
Mr Nick Tate, Chair of the Committee and CAUDIT

It is expected that the Project Officer will also attend MSC Meetings and that the CAUDIT Senior Project Manager may do so.

MSC is working closely with the project team developing and implementing this project and meets regularly.

## **Steering Committee Meeting**

The inaugural meeting is scheduled for 8<sup>th</sup> September 2006.