

The PKI Certification Authority for the AAF

Viviani Paz¹, Rodney McDuff²

¹ AusCERT

² The University of Queensland

Abstract

The eSecurity Framework project results will provide input into the Australian Access Federation (AAF) Project.

This project is part of a larger effort from Australian Higher Education Sector with support from AusCERT, CAUDIT, the University of Queensland, the Department of Education, Science and Training and other universities to develop an environment in which Universities can collaborate and interoperate with each other at low cost and low risk.

This project builds on previous CAUDIT PKI and MAMS projects to establish a production Public Key Infrastructure (PKI) for the Higher Education and Research Sector, based on the standards developed in the previous 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. The aim of this project is to develop and ultimately implement a PKI for the Australian Higher Education and Research Sector together with the CAUDIT members outside Australia such as universities in New Zealand, Fiji and Papua New Guinea. 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. The University of Queensland has been awarded with further funding from DEST to ultimately develop and implement the Australian Access Federation, which incorporates a governance body, PKI and Shibboleth trust environments.

The eSecurity Framework 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 aid the APAC Grid infrastructure uptake of Shibboleth technology. 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 authorization architectures being developed by groups such as PERMIS. It will work directly with the NMI "Grid-Shib" initiative as appropriate.

This paper will describe the trust fabric and trust model proposed to implement the PKI Certification Authority for the Australian Access Federation and will provide an update on the eSecurity Framework and Australian Access Federation project progress.