



**eSecurity Framework**

# **Project Report**

Draft Version 3

30 July 2007



**An Australian Government Initiative**  
**Backing Australia's Ability**



## Table of Contents

EXECUTIVE SUMMARY.....	3
PROJECT OVERVIEW.....	4
PROJECT SUMMARY .....	6
ABBREVIATIONS.....	7
PROJECT OUTCOMES .....	8
<i>Disseminating eSecurity Framework Information</i> .....	8
<i>Working Groups</i> .....	9
<i>PKI-enabled Application Survey</i> .....	10
<i>Development of Trust Federation</i> .....	11
<i>Including the AusCERT Root in Browsers</i> .....	12
<i>Documentation</i> .....	12
RECOMMENDATIONS' SUMMARY .....	13
PROJECT EXTENSION PROPOSAL .....	15
APPENDIX A: AAF PKI MODEL .....	16
APPENDIX B: GRID WG PROPOSED PROJECTS .....	17
APPENDIX C: FEDERATED DIRECTORY SERVICE .....	22



## eSecurity Framework

### Project Report

### **Executive Summary**

This document provides an overview of progress towards completing the proposed eSecurity Framework project outcomes as well as proposing additional project tasks highlighted during the intensive research and development activities undertaken during the project.



## Project Overview

The eSecurity Framework project is part of a larger effort of the Australian Higher Education Sector that aims for Universities to collaborate at low cost and low risk. This project is also supported by AusCERT, CAUDIT, the Australian government and other institutions.

The eSecurity Framework project builds on existing CAUDIT PKI and MAMS projects to

- Develop a production Public Key Infrastructure (PKI) for the University and Research Sector based on standards developed in the predecessor project; and
- Develop a pilot federation that leverages the PKI infrastructure to align trust arrangements between institutions to support Shibboleth implementation across the sector while improving integration with Grid technologies.

The eSecurity Framework project also seeks to lower the PKI entry barriers by using open source software. The project outcomes are to research secure sharing of resources and research infrastructure across the domestic sector and with international partners.

The eSecurity Framework Project is funded by the Australian Government Department of Education, Science and Training (DEST) through the Systemic Infrastructure Initiative as part of Backing Australia's Ability – Building Our Future Through Science and Innovation. This project is part of the Managed Environment for Research repository Infrastructure (MERRI) program of projects.

The eSecurity Framework Project is led by The University of Queensland, in association with partners AusCERT, Macquarie University (MELCOE/MAMS), CAUDIT, Australian Partnership for Advanced Computing (APAC), and AARNet.

This report was produced by AusCERT on behalf of the eSecurity Framework Project Steering Committee that comprises the following members:

Mr Keith Besgrove, DCITA

Ms Maxine Brodie, Council of Australian University Librarians

Mr Bruce Callow, Griffith University

Mr Jack Chorowicz, Monash University

Mr Phil County, Victoria University

James Dalziel, Macquarie University

Mr Paul Davis, Victorian eResearch Strategic Initiative (VeRSI)

Mr Michael Dupe, AGIMO

Mr Darren Geddes, University of Western Sydney

Mr Robin Harrington, NZ Vice Chancellors Standing Committee on Information Technology

Prof Chris Marlin, Australian Vice-Chancellors Committee

Dr Rodney McDuff, The University of Queensland

Mr Peter Nicholson, Department of Education Science and Training

Mr Richard Northam, CAUDIT

Prof John O'Callaghan, Australian Partnership for Advanced Computing

Ms Viviani Paz, AusCERT

Prof Alex Reid, AARNet

Mr Nick Tate, Chair of the Committee and The University of Queensland

Dr Joe Young, Queensland University of Technology



## eSecurity Framework

### Project Report

A Management Steering Committee (MSC) was created to provide additional project direction. MSC members include:

Markus Buchhorn, The Australian National University, APAC

Prof James Dalziel, Macquarie University (MELCOE)

Prof Alex Reid, AARNet

Mr Nick Tate, Chair of the Committee, The University of Queensland



### Project Summary

The eSecurity Framework project is tasked with developing a PKI framework for CAUDIT universities (including universities in Australia, New Zealand, Fiji and Papua New Guinea) and the CAUDIT research community.

To achieve this goal the project team works closely with other projects including the Meta Access Management System Project (MAMS) and Middleware Action Plan and Strategy (MAPS). This project uses a phased approach to test interoperability and identify issues regarding PKI-enabled applications prior to a production implementation phase.

This project has four central objectives:

- **Objective 1 - Developing a PKI for the Sector**

This project builds on the existing CAUDIT Public Key Infrastructure (PKI) standards project to facilitate the deployment of a PKI production for the Higher Education and Research Sector. The CAUDIT PKI project was making significant progress in this field; however its funding was only to develop standards and specific trial implementations.

- **Objective 2 - Establishing PKI/Shibboleth alignment**

This project builds on the existing PKI and MAMS projects and the PKI project identified earlier to develop models and pilot implementations for a common trust federation that supports both PKI and Shibboleth and provides a common approach to authentication and authorisation across the sector.

This includes developing a unified model for federation and trust that aligns the PKI and Shibboleth approaches (including pilot demonstrations). When complete, this unified model could form the basis for a future production Federation service across the Higher Education and Research Sector, aligned with the development of the production PKI service outlined above.

- **Objective 3 - Reducing the Systems Cost barriers to entry for PKI**

This project aims to reduce the PKI entry barriers for all universities and research institutions by providing cost effective access to a free or low-cost Certificate Management System for the sector (including source code access). This requires the development of training, documentation and an associated support mechanism.

- **Objective 4 - 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 and will work directly with the NMI "Grid-Shib" initiative as appropriate.



### Abbreviations

This document uses the following terms:

<b>Term</b>	<b>Definition</b>
<b>AAF</b>	Australian Access Federation
<b>AARNet</b>	Australia's Academic and Research Network
<b>APAC</b>	Australian Partnership for Advanced Computing
<b>AusCERT</b>	Australian Computer Emergency Response Team
<b>BeSTGRID</b>	Broadband enabled Science and Technology GRID
<b>CA</b>	Certification Authority
<b>CAUDIT</b>	Council of Australian University Directors of IT
<b>CAUL</b>	Council of Australian University Librarians
<b>DEST</b>	Department of Education, Science and Training
<b>IGTF</b>	International Grid Trust Federation
<b>JISC</b>	Joint Information Systems Committee
<b>MAMS</b>	Meta-Access Management System
<b>MAPS</b>	Middleware Action Plan and Strategy Project
<b>NCRIS</b>	National Collaborative Research Infrastructure Strategy
<b>PKI</b>	Public Key Infrastructure
<b>RA</b>	Registration Authority
<b>SCIT</b>	Standing Committee on Information Technology
<b>SII</b>	Systemic Infrastructure Initiative
<b>TERENA</b>	Trans-European Research and Education Networking Association
<b>VeRSI</b>	Victorian eResearch Strategic Initiative
<b>VPAC</b>	Victorian Partnership for Advanced Computing
<b>WALAP</b>	WA Libraries Authentication Project



## Project Outcomes

This section details the project achievements for all four project objectives:

- Developing a PKI for the Sector;
- Establishing PKI/Shibboleth alignment;
- Reducing the Systems Cost barriers to entry for PKI; and
- Integrating Grid technologies with PKI/Shibboleth.

The eSecurity Framework project has investigated a number of activities to assist in deploying a PKI aligned with Shibboleth and Grid technologies for the sector, while considering options to minimise PKI uptake costs by the sector. Outcomes of this project will assist in deploying the Australian Access Federation.

## Disseminating eSecurity Framework Information

A communications plan was developed to provide project progress updates to the community with information disseminated by posting information in the eSecurity Framework website and wiki, providing reports at CAUDIT general meetings, and running seminars for executive and technical university personnel.

The following communication mechanisms were established to support information dissemination:

- The [esecurity.edu.au](http://www.esecurity.edu.au) domain was registered and a web site developed for the project <http://www.esecurity.edu.au/>. A wiki (<https://wiki.esecurity.edu.au>) was also developed for use by AAF working groups assisting with the project.
- A mailing list was created for the SC and the MSC to discuss project-related issues. The project team presented at a number of seminars and conferences including *2006 Middleware Forum and CAMP, Questnet2006, Educause2007, AusCERT2007*
- The project team is also committed to present workshops at *eResearch Australasia 2007, APAC2007* and other events.
- Various working groups were developed to supplement discussions regarding the AAF PKI implementation for the sector and its alignment with Shibboleth and the Grid community requirements. For more information, see the next section.



### Project Report

## AAF Working Groups

The project uses the following working groups to assist in the AAF implementation:

### ***auEduPerson Working Group***

The Working Group is tasked with drafting and recommending data attribute schemas for use with the Australian Access Federation (AAF), based on the community's requirements and on interoperability with other key federations. The Working Group is chaired by Patty McMillan of UQ/MAPS and contains representation from UQ/AusCERT, Macquarie/MAMS, Monash, DEST/eFramework, VPAC, AARNet, WALAP, and NZ SCIT. International affiliates from TERENA and JISC also participate.

The Working Group has identified the key tasks to be completed, including agreement on a Common Attribute Schema Policy based on attributes from established schemas, profiling eduPerson for the AAF, and determining whether there are additional attribute requirements for creating an auEduPerson extension.

The Working Group has canvassed CAUDIT members regarding the proposed Common Attribute Schema Policy to get their feedback regarding whether they would be able to hold, generate, or map to a proposed set of common attributes within their directories. The Working Group is also compiling a set of use cases for analysing additional attribute requirements.

It is anticipated that the work being carried on by this working group will not be concluded by the end of this project. It is recommended that this work continue into the AAF project.

The auEduPerson Working Group has held fortnightly meetings since 17 April. Meetings are normally conducted via teleconference with some face-to-face and Access Grid meetings.

### ***Grid working group***

The Working Group is tasked with providing expert support and advice to the AAF project team to ensure that the solution proposed by AAF meets the expectation of the Grid community and the wider higher education and research sector, while maintaining compatibility with international Grids that are compliant to IGTF standards.

The Working Group is chaired by Viviani Paz of AusCERT with representatives from UQ/MAPS, Macquarie/MAMS, VPAC, VerSI, The Australian National University, James Cook University and The University of Auckland/BeSTGRID.

The Working Group has identified the potential for the AAF to benefit the Compute Grid, Data Grid and HPC communities in the following ways:

- **Identity:**
  - Leveraging the IdM processes of Federation Members; and
  - Providing a Level of Assurance concerning the strength of the IdM process a particular user has undergone to Grid and HPC services and applications.
- **Authentication:**
  - Providing a Level of Assurance concerning the strength of a users' authenticating act to Grid and HPC services and applications; and
  - Potentially providing a greater range of authentication methods to gain access to Grid and HPC services and applications.
- **Authorization:**
  - Leveraging users' attributes in the directories of Federation Members and Virtual Organizations for authorization to gain access to Grid and HPC services and applications; and
  - Providing a Level of Assurance concerning the veracity of a user's attributes.

The Working Group has also identified project opportunities of potential benefit to the Grid community. Some projects will be recommended to the AAF SC to be considered and



### Project Report

evaluated in the AAF project. It is understood that some of these projects will need to be investigated in light of security aspects. These projects description are listed in Appendix B.

The Grid Working Group has held fortnightly meetings since 19 April, normally via teleconference with some face-to-face meetings

#### **Levels of Assurance working group (LOAWG)**

The LOA Working Group is a combined effort from the eSecurity Framework and MAMS projects teams.

The Working Group is tasked with providing expert support and advice to the AAF project team to ensure that the identification, authentication and authorisation levels of assurance implemented under the AAF are suitable and adhere to international implementation, as to not exclude AAF from participating in the international environment.

The Working Group is chaired by Viviani Paz of AusCERT and contains representation from UQ and Macquarie/MAMS.

The LOA Working Group has held electronic discussions since February and meetings since 8 June, normally via teleconference with some face-to-face meetings.

For more information on the Working Groups please refer to <https://wiki.esecurity.edu.au/display/esecurity/AAF+Technical+Working+Groups>.

#### **PKI-enabled Application Survey**

To better understand the current and anticipated use of PKI-enabled applications this project surveyed Australian and New Zealand universities with CAUDIT and AusCERT member universities invited to provide input. Target institutions included those institutions involved in (or with a stake in) end-user applications.

The survey was well received by the sector with 28 respondents representing a number of universities in Australia and New Zealand. The responses influenced the makeup of the certificate interoperability study developed by the project. This survey was available at the CAUDIT web site.

Participant institutions included Australian National University, Charles Stuart University, Curtin University of Technology, Deakin University, Flinders University, Griffith University, James Cook University, LaTrobe University, Murdoch University, Queensland University of Technology, RMIT University, The University of Queensland, The University of Sydney, The University of Waikato, The University of Wollongong, University of Melbourne, University of Otago, University of Southern Queensland, University of Western Australia and University of Western Sydney. For more information on survey results, please see the survey summary at [http://www.esecurity.edu.au/docs/application\\_survey\\_summary.pdf](http://www.esecurity.edu.au/docs/application_survey_summary.pdf)



### Development of Trust Federation

Discussions have progressed between the Australian Grid, PKI and Shibboleth communities in forming a common alignment in policies and practices that provide the initial work required to develop the Australian Access Federation (AAF). More information is available at <https://wiki.esecurity.edu.au/display/esecurity/Trust+Federation>.

A PKI Test-Bed federation was developed and is currently operational. This test-bed can include multiple universities and participants can issue user and server certificates. Further information regarding the PKI Test-Bed is available at <https://wiki.esecurity.edu.au/display/esecurity/AAFCA++PKI>

This PKI can also issue GRID certificates and issue SAML certificates for use in the MAMS test-bed federation level 2 to strengthen the trust fabric.

Progress has been made in devising a common alignment for the Australian Grid, PKI and Shibboleth communities' policies and practices, which will be used to support the AAF.

A testing Grid environment was created to prove the suitability of certificates issued under this PKI hierarchy and its compatibility with the APAC Grid environment. The approach used in creating the Certification Authority for Grid community is available at <https://wiki.esecurity.edu.au/display/esecurity/AAFG++Grid>. Additionally information interoperability tests developed can be found at <https://wiki.esecurity.edu.au/display/esecurity/Interoperability+tests>

Certificate profiles developed during the CAUDIT PKI project were refined in line with the AAF PKI requirements and alignment with the APAC Grid environment. Profiles are available at: <https://wiki.esecurity.edu.au/display/esecurity/AAF+PKI+Prototype+Certificate+Profiles>

A Shibbolised wiki was developed and used to help disseminate information regarding PKI deployment. The wiki also allows the Australian Higher Education and Research community to collaborate and participate in the processes necessary to help define policy and practice for the federation. Information on lessons learned during Shibboleth implementation studies and Shibbolising Confluence can be found at <https://wiki.esecurity.edu.au/display/esecurity/AAFS++Shibboleth>

A Virtual IdP was temporarily setup by MAMS for Institutions that are not part of the MAMS level 2 testbed Federation (<http://openidp2.federation.org.au/>) but want to contribute to the eSecurity Framework and AAF projects. Instructions on how to access this wiki and how to request an account are available at <http://www.esecurity.edu.au/wiki>.

Significant progress has been made with regards to Certificate Management Systems (CMS) being evaluated during this project, which may be adopted by the Higher Education sector. Test results highlight product strengths and weaknesses.

Certificate Management Systems evaluated include OpenCA, ejbCA, RedHat Certificate System and Microsoft Certificate Services. Evaluation also included the nCipher network Hardware Security Module. Preliminary results are available at <https://wiki.esecurity.edu.au/display/esecurity/Evaluations+of+technologies%2C+products+and+implementations>. It is recommended that the RSA Certificate System and other Hardware Security Modules be evaluated under the AAF project to assist in architecture deployment decisions.

Certificate profiles were revised for the AusCERT Root CA Certificate, Sub CAs Certificate and University CA Certificate including end entity and server certificates. Certificate profile templates are available at <https://wiki.esecurity.edu.au/display/esecurity/AAF+PKI+Prototype+Certificate+Profiles>.



## Including the AusCERT Root in Browsers

Discussions with various vendors have progressed for including the AusCERT Root Certificate for this environment in browsers. This work cannot be concluded during this project and must wait until a production environment is established.

To add the AusCERT Root certificate to the browser and other applications, the AAF PKI production must pass a WebTrust audit. The WebTrust audit, software and hardware infrastructure are outside the scope of the eSecurity Framework project and is being funded under the AAF project.

Additionally for the AAF PKI to cross-certify with other Bridge Certification Authorities, it must follow world-wide acceptable best-practice security and standards that include an independent, world-wide recognised, third-party audit.

Once certified, additional annual audits are required to maintain bridge membership. The Federal Bridge Certification Authority (FBCA) in USA is an example of these requirements.

The Higher Education Bridge Certificate Authority (HEBCA) and the Federal Bridge Certificate Authority (FBCA) - both in America – have expressed an interest to cross-certify with the Australian Access Federation Certificate Authority once its production PKI environment is commissioned. The cross-certification between the AAF PKI Prototype and Test HEBCA is progressing.

## Documentation

During this project extensive testing occurred with associated processes results documented.

Extensive information describing these processes and guidelines can be found at eSecurity Framework wiki at

<https://wiki.esecurity.edu.au/display/esecurity/eSecurity+Framework+Project+Wiki>.

Additional information on the eSecurity Framework Project, including presentations is available at <http://www.esecurity.edu.au>.

## Federated directory service (People Picker)

The Federated directory service tool, previously known as the People Picker, was designed and developed by the MAMS team with financial support from the eSecurity Framework Project. The first version of this tool performs query-based searches against Identity Provider directories under the MAMS level 1 testbed federation.

Additional information on this tool is available in Appendix C.



## Recommendations' Summary

This section summarises the recommendations made in this report.

### ***Develop PKI Production***

Extensive investigation was done regarding interoperability and capability of Certificate Management Systems for use in a PKI production environment. This project was originally only tasked to test open source Certificate Management Systems, however early trials clearly indicated the need to include commercial products in the trial and investigate the products for feature options for deploying the AusCERT Root CA and Sub CAs.

Although the ability to modify code and draw on community expertise is an extremely useful attribute of open source software, in the case of Open CA and other open source tools there are also drawbacks including:

- lack of support for installation, maintenance, code development, bug fixes and emergencies;
- no assurance of on-going support or release cycles;
- lack of rigorous change control and testing of new releases or patches;
- lack of package installation methods;
- difficulty in sourcing skilled resources;
- lack of controls for check-in/code updates/source repositories that can potentially lead to compromised code.

Generally speaking, there are limited “standards” enforced in development from a code quality perspective, also most products are not designed for high scalability.

As investigations progressed regarding the inclusion of the AusCERT Root Certificate into vendors trust lists; it was clear that evaluating vendor products including Hardware Security Modules was fundamental to determine the products most suited to the AAF PKI that also met the WebTrust requirements.

The project team believes the RSA Certificate System and additional Hardware Security Modules should be tested under the AAF project to help determine the software and hardware most capable of supporting the AAF PKI deployment.

While negotiations with vendors to include the AusCERT Root Certificate in their trust lists progressed significantly during this project, they cannot be concluded until the PKI infrastructure is deployed and is in production. We therefore recommend continuing negotiations with vendors to include the AusCERT Root Certificate in their trust lists continue during the AAF project and the engagement of a consulting organization to assist in devising a pre-audit plan.



### Project Report

#### **Establishing PKI/Shibboleth Alignment**

The eSecurity Framework project has successfully aligned the PKI trust model with Shibboleth by developing common policies to address federated identity, credential and attribute management.

The LOA Working Group made significant progress towards defining the levels of assurance required to support AAF and its participation internationally. However further work is required to refine these policies in light of the production environment.

We anticipate the work being undertaken by the LOA working group will not be concluded by the end of this project and we recommend this work continue into the AAF project.

The first version of the Federated directory service tool has been developed and is operational. However further work is required in reviewing the graphical user interface requirements and extensions to improve privacy protection and to minimize the risk of denial of service attacks. It is recommended that this work continue into the AAF project.

#### ***Reducing the Systems Cost barriers to Entry for PKI***

The eSecurity Framework project has successfully developed and documented the evaluations undertaken during this project. The documentation outlines the benefits and problems encountered during tests to help facilitate the work to be undertaken by institutions wanting to deploy a PKI.

The project team has also presented at a number of events to disseminate information on the project's findings and AAF. The project team is also committed to present workshops at *eResearch Australasia 2007*, *APAC2007* and other upcoming events.

We recommend that training continue to be developed under the AAF project.

#### ***Integrating Grid Technologies with PKI/Shibboleth***

The eSecurity Framework project has efficiently refined and integrated the PKI trust model with Shibboleth and the Grid community requirements and has identified potential projects of benefit to the sector.

The Working Group has summarised project opportunities of potential benefit to the Grid community and we recommend these projects be brought to the attention of the AAF project Steering Committee to be considered in light of the AAF and that funding be sought to develop such projects.

For more information on these projects, please refer to Appendix B.



## Project Report

### Project Extension Proposal

In the case of many of the recommendations in this report, work is already underway by the working groups and the AAF project team. This report endorses these actions and emphasises their need.

The outcomes outline below have been identified as eSecurity Framework Project additional work that should be done to complement the work being undertaken by the AAF project. Sufficient funding is available within the eSecurity Framework Project to undertake this work.

#### Outcomes

- Further negotiate and liaise with the vendors in order to include the AusCERT Root Certificate into their browsers.
- Evaluate vendor products including RSA Certificate management System and Hardware Security Modules to determine if products are suited to the AAF PKI production roll out and met the WebTrust requirements.
- Develop a pre-audit plan in order to assist the AAF PKI to undergo the WebTrust audit.

#### Budget

Item	Budget amount
Staff – Evaluation of products	\$58,033
Evaluation of RSA CMS and SafeNet HSMS	\$43,700
Meetings with vendors	\$30,000
Pre-audit plan development	\$100,000
Meetings with HEBCA	\$25,000
Steering committee meetings	\$8,000
Project team travel	\$10,000
<b>Total:</b>	<b>\$274,733</b>



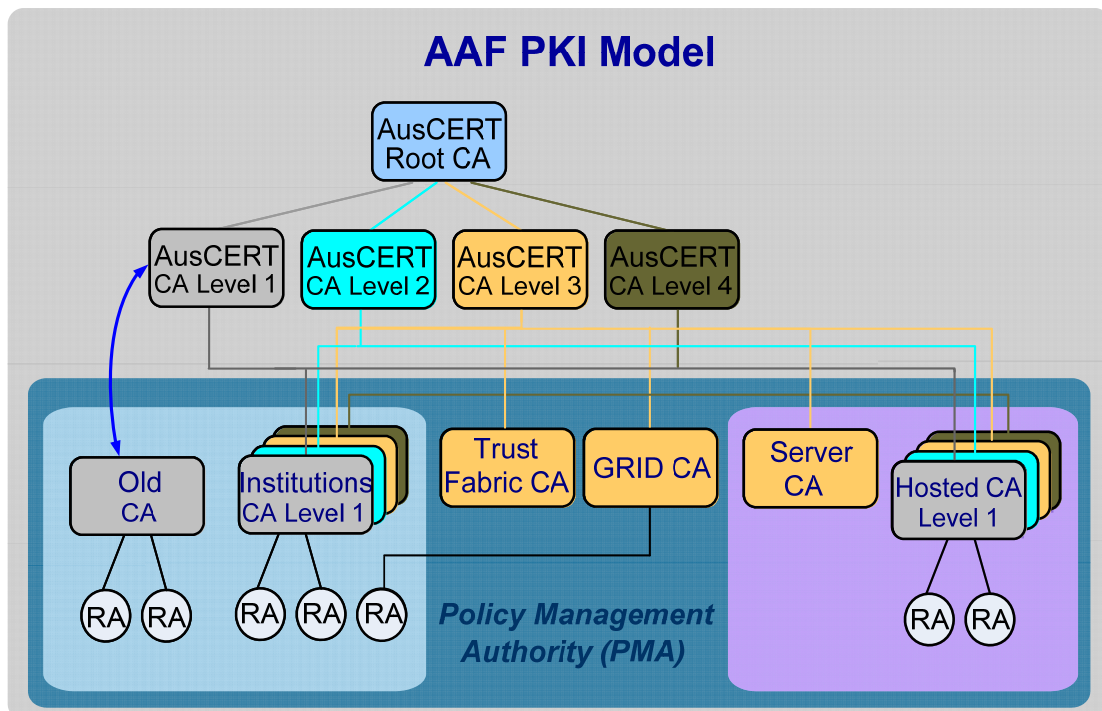
## Appendix A: AAF PKI Model

The AAF PKI to be deployed uses a hierarchical model comprised of a root Certification Authority that signs four sub-level Certification Authorities.

Each sub-level certification authority corresponds to the strength of the users' identification process undertaken by the universities. Each university can select the level of identification strength they want to adopt. Universities' Certification Authorities will be signed by the appropriate sub-level certification authority.

A Hosted Certification Authority service will be deployed for universities unable or unwilling to implement their own Certification Authority including issuing of end-user certificates and server certificates.

A Grid Certification Authority will also be deployed for the grid community, and the Trust Fabric Certification Authority that issues certificates used by Shibboleth. The following illustrates the AAF PKI hierarchical model:





## Appendix B: Grid WG Proposed Projects

### ***Shibboleth-enabled command line access to compute resources ShibPAC***

This section contains additional information for the ShibPAC project that aims to provide Shibboleth-enabled command line access to computer resources.

The ShibPAC project aims to provide Shibboleth-enabled command line access to computer resources and addresses how to meet PAC requirements using development based on the AAF Shibboleth service. This would allow PAC to have accounts for any Shibboleth user in the federation; and users could use their Shibboleth authentication for ssh or portal access to the PAC's systems.

ShibPAC would be a service operated by the PAC for managing PACusers and providing login access to PAC systems for the PACusers.

The PAC has full administrative control; however authenticating and supplying basic attributes would be delegated to the user's institutional IdP.

The PAC can specify additional supplementary attributes and user agreements and would automatically disable the account if the user leaves their institute. Passwords for accessing the PAC systems would have short-term validity (e.g. minutes to hours).

Note: This is not Grid access and does not involve user certificates; however users can use a certificate as their Shibboleth credential.

There is overlap between the ShibPAC signup and approval component and the FAPPS project.

The process for a new user wanting to become a PACuser would be to:

1. Access the ShibPAC Sign-up web page
2. Read the terms and conditions and click the Sign-up button to redirect the user is redirected to their IdP.
3. The user authenticates using their normal Shibboleth credentials and is presented with a form showing their attributes.
4. If the user is missing any required , a message is displayed requesting the user consult their local IdP admin to ensure proper attribute release. The PAC username is either auto generated or created interactively by the user (based on PAC policy).
5. If the user has all required attributes, the user is informed they will receive an email when their PACuser account is activated.

After requesting signup, the page automatically sends an email to the PACadmin user detailing the new PACusername, eduPersonPrincipalName, email, phone and other required attributes.

The PACadmin user goes to the ShibPAC Admin page, signs in and selects Approvals. The PACadmin user searches for the PACusername and then either approves or deletes the PACuser.

The Approvals process emails the user indicating account approval/rejection. Creating the actual accounts on the PAC systems should be done by the PACadmin user at the time of approval.

PACusers wanting to login to a PAC system via ssh must acquire a short-term password by directing their web browser to the ShibPAC Login Assistant web page.



### Project Report

This initially redirects the user to their institute's IdP where the user must authenticate using their usual Shibboleth credentials. Users are then presented with the Login Assistant page detailing their PACusername, a short-term password, and the validity period for the password. Users can then run ssh in a terminal and the PAC system will prompt for username (i.e. their PACusername). The system prompts the user for a password (i.e., they can copy/paste the short-term password). Login is successful if the validity time period has not expired.

Note: Users can use the same password on any PAC system until the password validity period expires. In this situation, users can use the Login Assistant to obtain a new short-term password.

PACusers wanting to access a PAC system via a web portal can select the Shibboleth Login button on the portal page. It redirects the user to their institute's IdP where the user must authenticate using their usual Shibboleth credentials. Users are then returned to the portal and automatically logged in as their PACusername and the portal can access PAC systems as the user's proxy.

In some situations, a PAC system may require users to agree to specific terms and conditions or supply additional attributes not supplied by their IdP.

In this situation, if the user has not supplied this information, the system will direct the user to a URL. The user can use their browser to open the URL and be redirected to their IdP for authentication using their usual Shibboleth credentials.

The user will then see the relevant information (e.g. terms and conditions, etc.) and complete a form or accept the terms and conditions and submit the information. After completing this process, the user can access the PAC resource.

The ShibPAC Admin page also allows PAC administrators to delete PACusers, email PACusers and add supplementary attributes to the PACuser's record.

When an existing PACuser leaves their institute, the institute's IdP will no longer accept the user's Shibboleth credential. This results in the ShibPAC account becoming automatically inoperative.

ShibPAC would be a Shibboleth Service Provider operated by the PAC. ShibPAC would use a local database that contains entries for all PACusers. Each database entry would list information including the PACusername, eduPersonPrincipalName, email, phone, additional attributes from the user's IdP, as well as supplementary PAC attributes and agreed terms and conditions. ShibPAC would also perform as a local non-federated IdP for PAC portals.

The ShibPAC home page would have a menu of links to the other pages.

The home page would contain a sign up button that redirects the user to a Shibboleth-protected dynamic page that requests the user attributes from the IdP, creates a PACuser entry in the database, copies the attributes into the database and sends an email containing the PACuser name and attributes to the PAC admin for approval.

The PAC Admin page is a Shibboleth-protected dynamic page allowing administrators to search for a PACuser and perform various functions including approving or deleting PACusers, adding supplementary attribute values or sending an email.

User agreements and supplementary attributes pages are Shibboleth-protected form pages that update user database record fields.

The PAC Login Assistant page is a Shibboleth-protected page that shows the user their PACusername, short-term password, and password validity period. The short-term password is generated at random and stored in the database together with the password expiry time.

A Pluggable Authentication Module PAM/shibPAC module (PAM) module must be compiled and installed on each PAC system supporting ssh login for PAC users. The PAM plug-in takes the username/password entered by the user and performs a SOAP (or similar) request to the shibPACauthn service at the ShibPAC server and returns a success/failure message.



### Project Report

The ShibPACauthn service looks up the login id to find the user record and checks for a valid password match. If the password matches, the service responds to the PAM plug-in indicating the user is authenticated.

Portal login is implemented by making the portal a Shibboleth-protected resource with the IdP being the PACIdP on the ShibPAC server. The portal requests the PACusername and PACuserpassword attributes, and uses these to access a PAC system on the user's behalf.

The ShibPAC server could be implemented in Perl, Ruby on Rails or JSP. The PAM/shibPAC module would be written in C or C++ for Linux and other Unix style OSes.



### ***Federated Account Approval and Provision System (FAPPS)***

The FAPPS system will allow end users to use their federated identity to request an account on a multi-user computing resource (e.g. High Performance Computers).

Users can request accounts via a shibbolised portal by providing information including:

- Name of computer system;
- Contact details including phone number(s); and
- SSH public key.

Information from the shibboleth attribute exchange will inject a request to an approval workflow that may utilise one or more approvers. After approving the request, the account will be created for the user on HPC resource and account details transmitted securely to the end user.

This tool could also implement portal, command line or graphical user interfaces for HPC users.



### Project Report

#### ***Shibboleth Integrated Credential Service (SICS)***

SICS is an implementation of a CA and supporting software that meets the constraints of the IGTFs Member Integrated Credential Service (MICS) profile.

The SICS CA will issue both short-lived and long-lived certificates to users (and potentially servers) for use in the Grid. Rather than requiring an in-person identification when issuing certificates, the SICS CA will rely on an AAF Shibboleth authentication producing an authentication assertion that expresses levels of assurance for both the end entities previous identification process and the current authentication method. If these levels of assurance meet the requirements of the MICS profile, a certificate is automatically issued to the end entity.

This project will examine and provide proof of concept for:

- Expression of identity level of assurance in SAML assertions and the subsequent reliance on this LoA.
- Expression of authentication level of assurance in SAML assertions and the subsequent reliance on this LoA.
- Automated generation of Grid certificates.
- Trust configuration for Grid certificates.

The project requires the following to be implemented:

- A Shibboleth IdP and associated Identity Management System supporting identity LoA attribute and multiple authentication methods mapped to authentication strength LoA.
- A SICS CA with certificate enrolment workflow protected by Shibboleth authentication.
- A Grid trust root configuration for the SICS CA.



## Appendix C: Federated directory service

### PeoplePicker Project Report - June 07

Author: Neil Witheridge [nwitheridge@melcoe.mq.edu.au](mailto:nwitheridge@melcoe.mq.edu.au)

Version: 1.0

Date: 20th June 2007

## Functionality Overview

### Background

PeoplePicker's (PP) core functionality is performing a query-based search against Federation Identity Provider directories.

(Shibboleth Identity Providers are configured with "Attribute Resolver" and "Attribute Release Policy" information which specify 1. which attributes are supported and where they are sourced from, and 2. which attributes are release to SPs on a users behalf, respectively.)

The initial release of the PP prototype included 'social networking' functionality: 'Contacts' and personal 'Profile & Privacy'. Contacts enabled the user to store other users' Federation identity information denoted as a personal contact and identified according to a certain classification e.g. 'buddy', 'business contact'. The Profile & Privacy functionality enabled the user to view their own identity as stored by their IdP and maintain and control access to a set of self-asserted attributes.

As the primary value of the PP to the federation is in performing federated search, the focus on functionality for the first release of PP will be the Federation directory search. Contacts and Profile functionality will not be provided.



Project Report

Prototype Deployment

The development host on which the latest PP service is running is:

<http://y11.mams.org.au/myppws> (note this is a development machine, hence access not guaranteed)

Choose: Testfed OpenIdP, login as staff:test

Odepicts the initial PP web page.

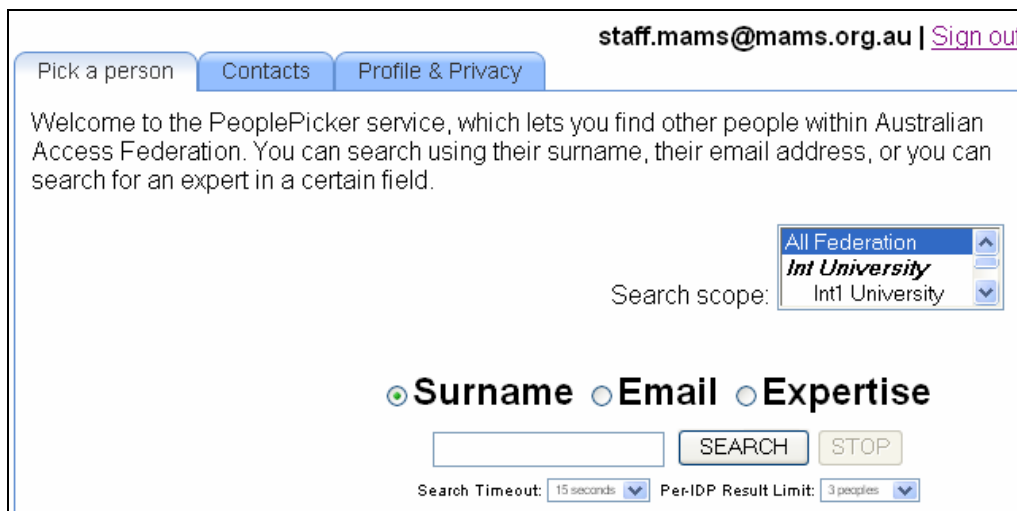


Figure 1. Prototype PP Interface

Odepicts the result of performing a search by surname.

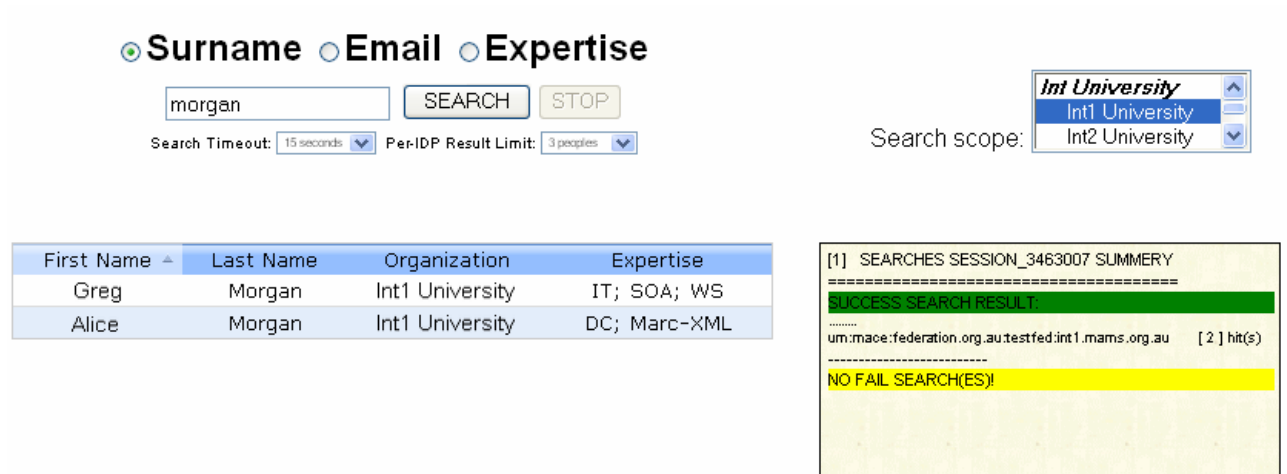


Figure 2. Search by Surname

Note the search configuration options:

- Search scope (IdPs to be searched)
• Search Time-out (time waiting for a response from an IdP before search is aborted)
• Per-IdP result limit (number of rows displayed for each IdP searched)

Note also the result statistics displayed (Search statistics summary).



Project Report

Odepicts the display of user information:

First Name	Last Name	Organization	Expertise
Greg	Morgan	Int1 University	IT; SOA; WS
Alice	Morgan	Int1 University	DC; Marc-XML

Greg Morgan ([Add to contacts](#))  
 Email: [gmorgan@int1.edu.au](mailto:gmorgan@int1.edu.au)

**staff**

Telephone:

Expertise: IT; SOA; WS  
[Download vcard](#)

Figure 3. Display of User Information

Deployment Scenarios

The PP is intended to be used as a standalone web application, as a portlet (for example integrated with MAMS' IAMSuite), or as a service accessible from other applications via a Web Services interface.

Hence a three-tier architecture has been adopted (see 0).

The tiers are:

**PP Extension:** Web Service Agent running on each IdP that is to be searched. The PP Extension interacts with Shibboleth to read attributes and perform ARP processing.

**PP Service:** Web Service that accepts WS requests from the PP Clients and makes requests of the PP Extension at each IdP selected to search against.

**PP Client:** An example web application interface that providing the query-based search GUI (and other GUI features, for example those required to provide a Federated White Pages service).

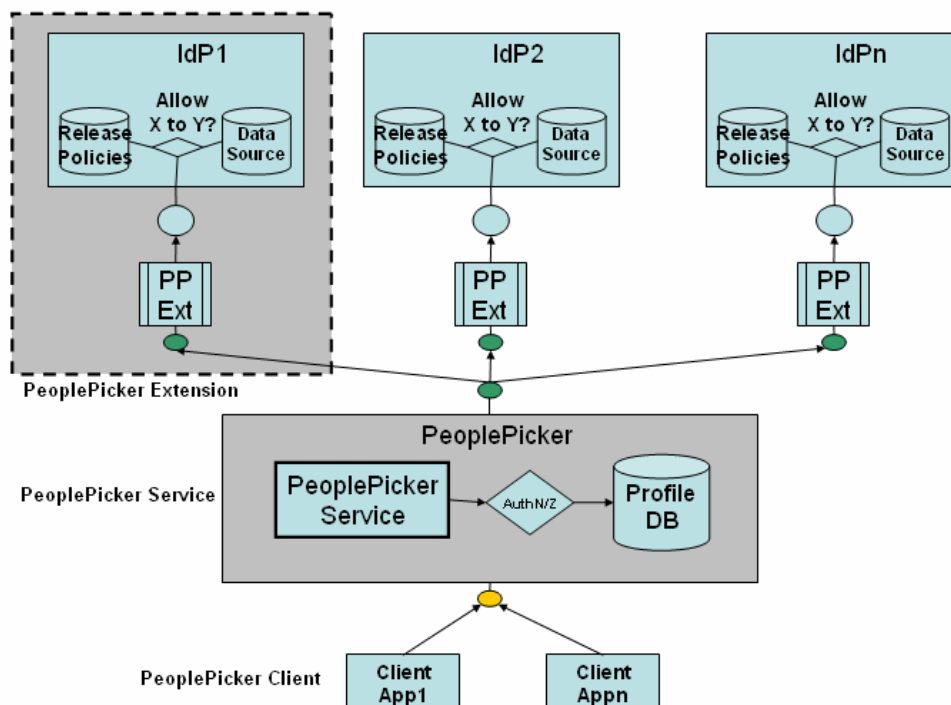


Figure 4. PP Architecture for Production Version



## Project Report

### Operational Version Focus

#### Federation Directory Query-based Search

The focus of the operational release will be on the Query-based search. Contacts and Profile & Privacy functionality will not be delivered in the first operational release.

Refer to the "People Picker User Interface" document for a proposed GUI.

#### IAMSuite Integration

The deployment of a portlet within the secure eResearch VO infrastructure MAMS is currently developing ("IAMSuite") will also be undertaken.

### Target Schedule

Target Completion	Description	Comment/Status
End June	3-Tier Architecture with Web Services Interfaces	On track for completion
End Aug	GUI Improvements (Search results, paging, etc.)	Requirements will be reviewed with eSecurity.
End Aug	IdP Denial of Service prevention	IdP "PP Extension" component functionality will be scrutinised.
End Sept	QA Finalised, Version 1.0 Release	Version 1.0 is targeted to be available for pre-Production release of AAF.