AusCERT
Australian Computer Emergency Response Team

The Australian Higher Education and Research Sector Certification Authority

Viviani Paz (AusCERT)
Rodney McDuff (UQ)
John Zornig (UQ)

Content

- Objectives
- Collaboration and Interoperation
- Australian HE and Research Federation Model
- Trust Fabric
- Identification Process
- Certification Levels
- Future Steps
- Integration with Grid Computing

eSecurity Framework for Research

- **Funded by** Australian Government Department of Education, Science and Training **$649K**
- **Lead Institution** The University Of Queensland AUSTRALIA
- **Supported by**

MAMS META ACCESS MANAGEMENT SYSTEM

CAUDIT Council of Australian University Directors of Information Technology

apac australian partnership for advanced computing

aarnet

- http://www.esecurity.edu.au

eSecurity Framework for Research

Objectives

- **Take PKI into Production**
  - **Australian Higher Education and Research Certification Authority**
- **Reduce the Systems Cost barriers to entry for PKI**
  - **Dissemination of information**

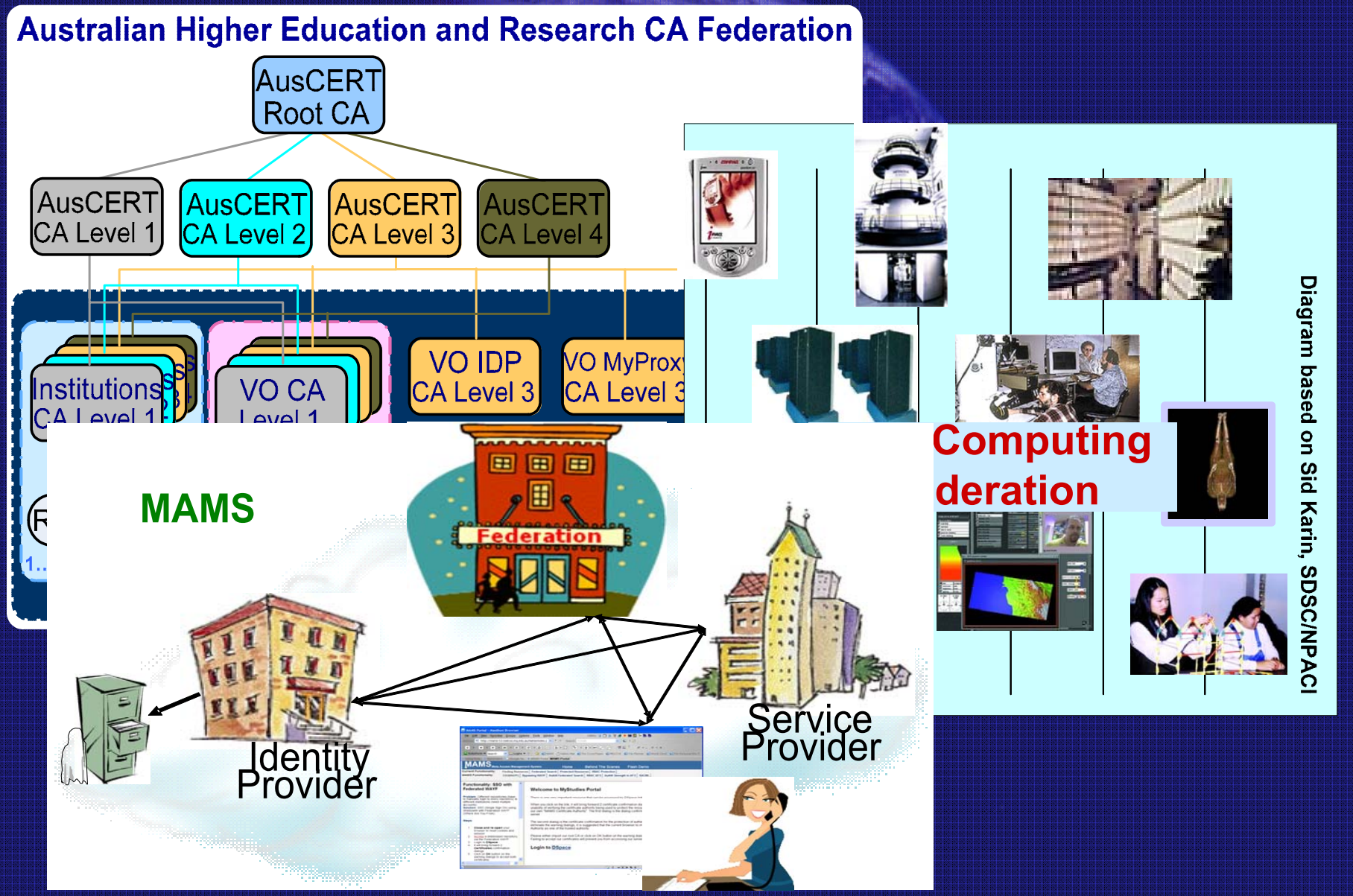
- **Establish PKI/Shibboleth alignment**
  - **Common Trust Federation for Australian HE sector**
- **Aiding the integration of Grid technologies with PKI/Shibboleth in the Australian HE sector**

Collaboration and Interoperation

- **Develop the Trust Fabric between Australian Higher Education and Research Institutions**
  - **Trust Fabric between Institutions and AusCERT will help**

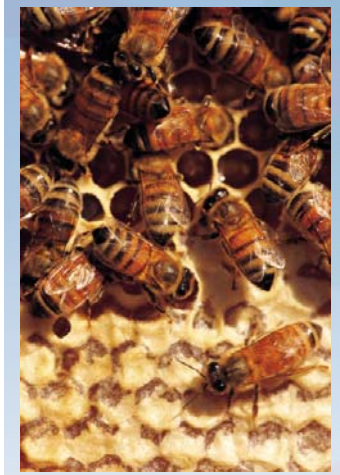
- **Develop common policies, practices and standards**
- **Evolve a PK Infrastructure as a vehicle to enable this trust fabric**
- **Avoid retro-fitting other implementations**
- **Ensure interoperability with other national and international PKIs and Federations**

Australian Higher Education and Research Federation

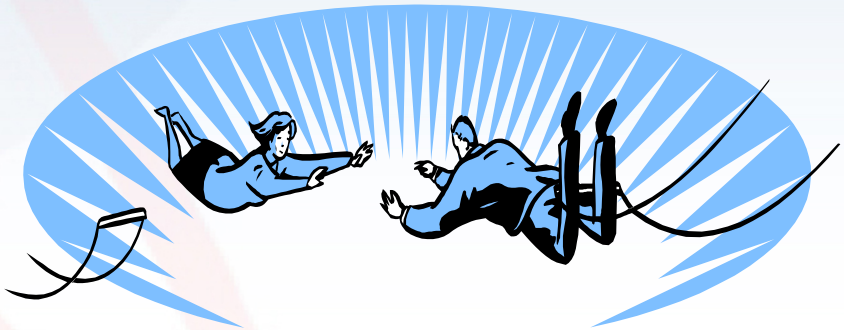


Earth image from http://nssdc.gsfc.nasa.gov/image/planetary/earth/gal_australia.jpg

What does Trust mean to us?



- **Predictable behaviour**
  - Expectations are understood and agreed upon
  - Institutions follow agreed set of rules
- **Beneficial to all Australian HE community**
  - Institutions work together towards a common goal
- **Confident reliance**
  - Identification Process



Trust Fabric Commonality

Based on the Strength of the Identification Process

- **Simple**
  - **Based on Australian Law and Breeder Documents**
    - **Identification Record for a Signatory to an Account**
      - **100 Point Check**
      - **http://www.austrac.gov.au/guidelines/forms/201.pdf**
      - **Primary Documents**
        - **Proof of identity**
      - **Accrued Points**
  - **IdM an integral part of any institution**
- **Minimal Impact**
  - **Only measures the strength of an institution's identification process. Doesn't change it!**
  - **An Institution can pick and choose what it wants to implement**

Trust Fabric Commonality

- Authentication Process Agnostic
- Authorization Process Agnostic
- Independent of Technology
- Auxiliary Processes and Practices need to complete the whole picture
  - For PKI needs CP/CPS
    - http://www.esecurity.edu.au/esecurity-framework-project-overview.data/CAUDIT-PKI-Draft_CP-CPS-v0.2.pdf
  - For Shibboleth needs Federation Participation Agreement
    - InCommon (http://www.incommonfederation.org/)
    - MAMS Federation (http://federation.org.au)

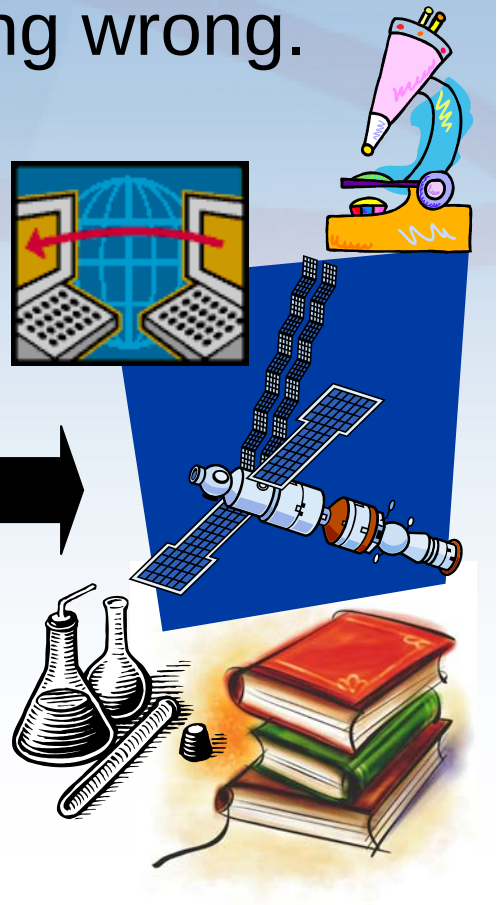
Why concentrate on Identity?

Because that is where it all starts going wrong.

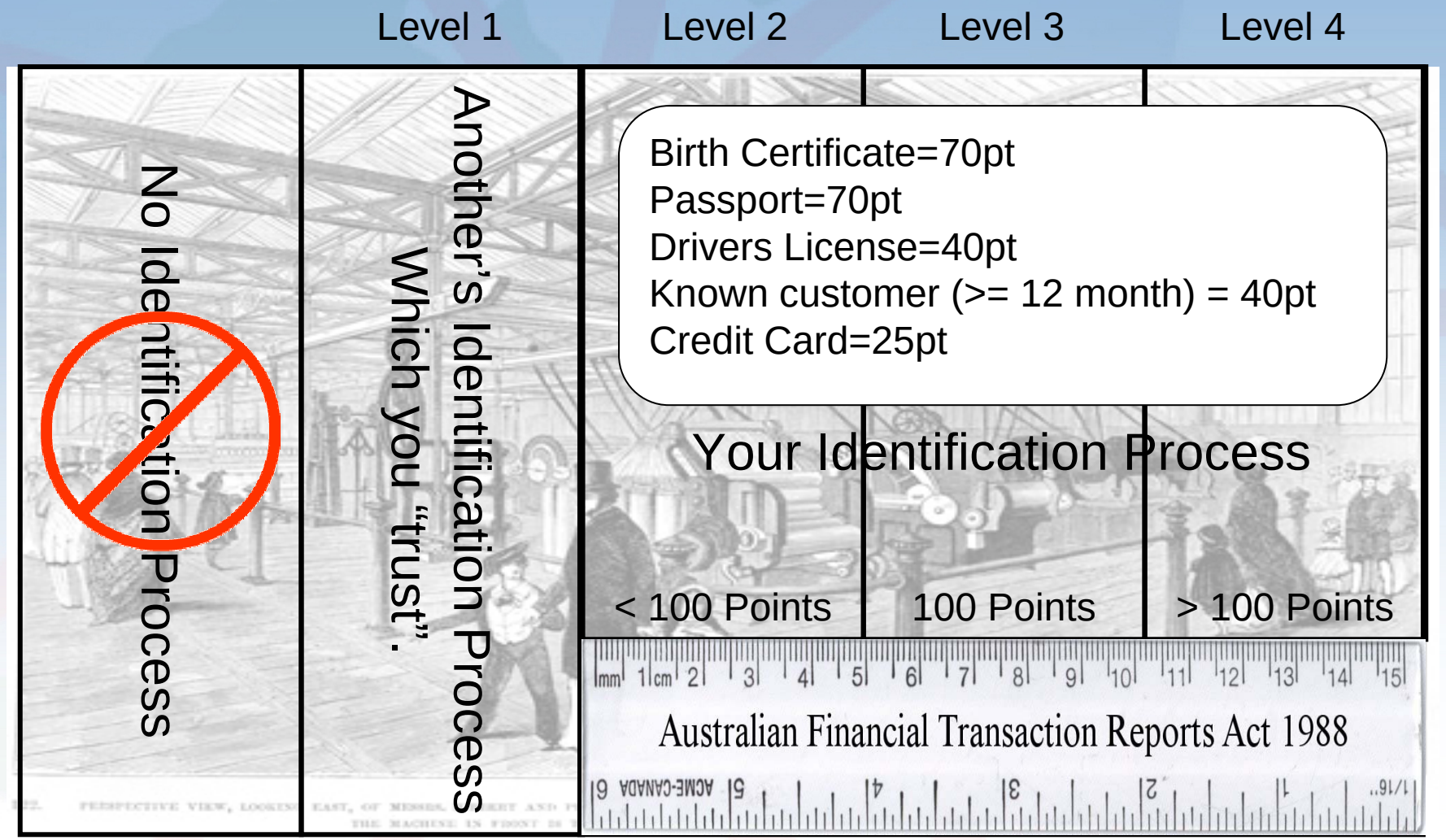
Identification Process. Issuance of Credentials.

AuthN Process. Proof of Possession of Credentials

AuthZ Process. Access based on user's attributes



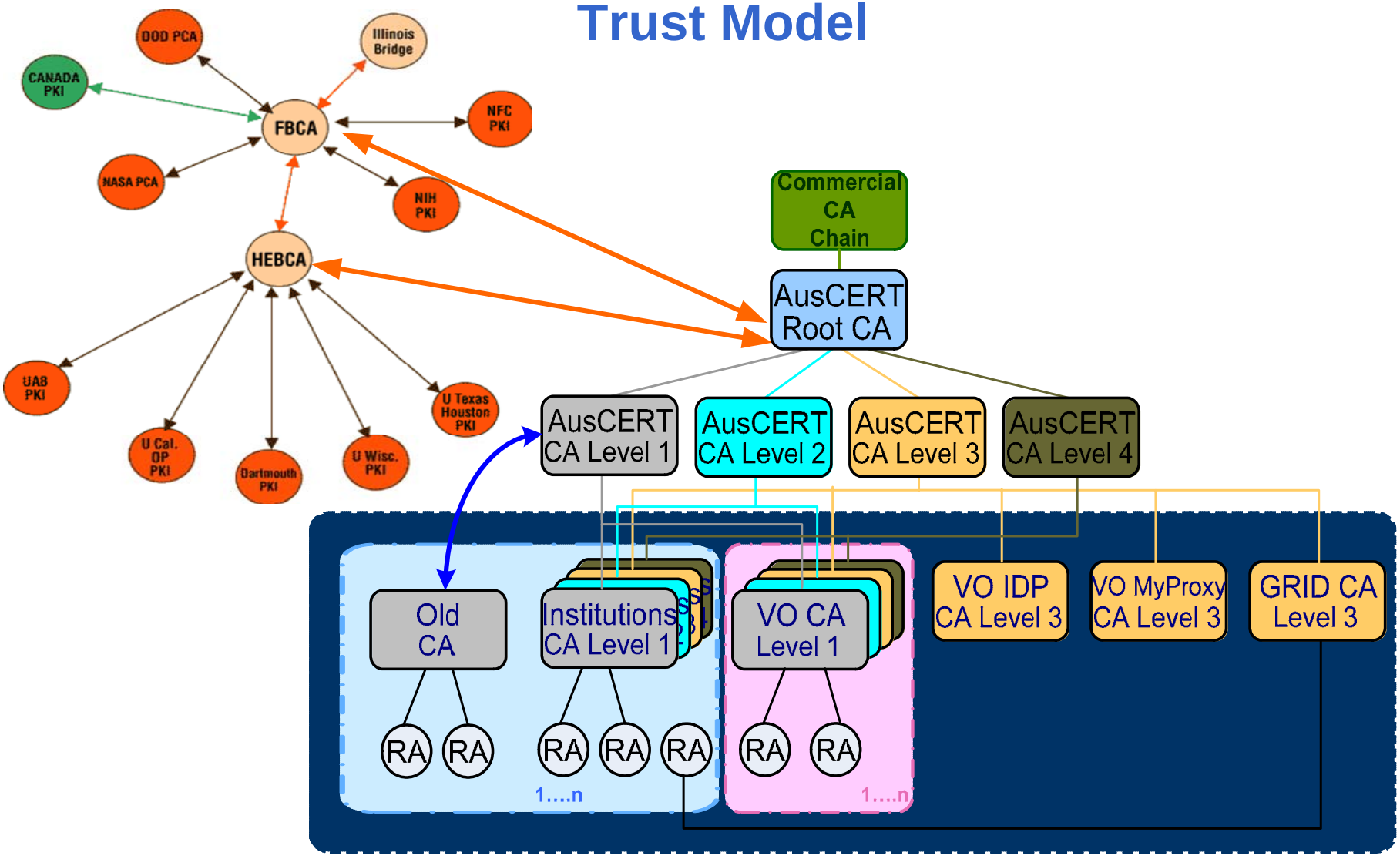
Identification Process Metric



Certification Levels

Certificate Level	Description
Level 1	No proactive identity check has been provided to the RA. However identity information has been provided by a body that the RA has a trust relationship. Example: A student being enrolled in at least one subject is sufficient for the certificate issuing however identity information has only been supplied by QTAC (or similar state body).
Level 2	Subject is required to provide proof of identity by an in-person appearance to the RA. However the individual for what ever reason can not provide the required 100 points of identification. Example: A contractor, who is at an institution for a short time but needs access to a system protected by PKI, may not have enough credentials on her person to meet the 100 points check but can provide some credentials like a drivers licence and/or credit card.
Level 3	Subject is required to provide proof of identity by an in-person appearance to the RA. That proof should accrue to at least 100 points of identity. Example: A foreign staff member that has a valid passport and has a written reference from an acceptable referee.
Level 4	Subject is required to provide the same information for Level 3 certification in addition to a positive check to be conducted by an appropriate external agency.

Australian Higher Education and Research CA Federation Trust Model



Future Steps

- Further develop the Australian HE Trust Fabric
- Implement the Trust Model that supports the Trust Fabric
- Aid further integration with Shibboleth and Grid Technologies
- Seek Australian HE input
  - Application survey results (http://www.esecurity.edu.au/esecurity-framework-project-overview.data/application_survey_summary.pdf)
  - Technical Working Group Mailing list (pkitag@auscert.org.au)
  - Wiki
  - Test and evaluate available technologies for certificate management systems
  - Further develop Interoperability test
  - Input into draft CP/CPS
  - Revision of Certificate Profile
  - Questions/Comments: pki@auscert.org.au
- Keep PKI uptake costs low
  - Share lessons learnt
    - Training, disseminate information, guidelines, policies, procedures

PKI for Grid Computing

PKI for Grid Computing

- **A process for deriving one trust relationship from another i.e. a transfer of trust**
- **Computing resources do** Authentication **(AuthN) and** Authorization **(AuthZ) with** User ID**'s (UID) defined, and trusted locally**
- **A grid user needs to use many, possibly remote, resources. Without account creation and AuthN at every resource.**

The Grid Challenge

- Grid infrastructure distributes the user's task to the remote resources
- The resources would see these tasks as anonymous and not run them
- Grid infrastructure must allow the resource to trust a task is from a particular user and map that user to a local UID for AuthZ and accounting

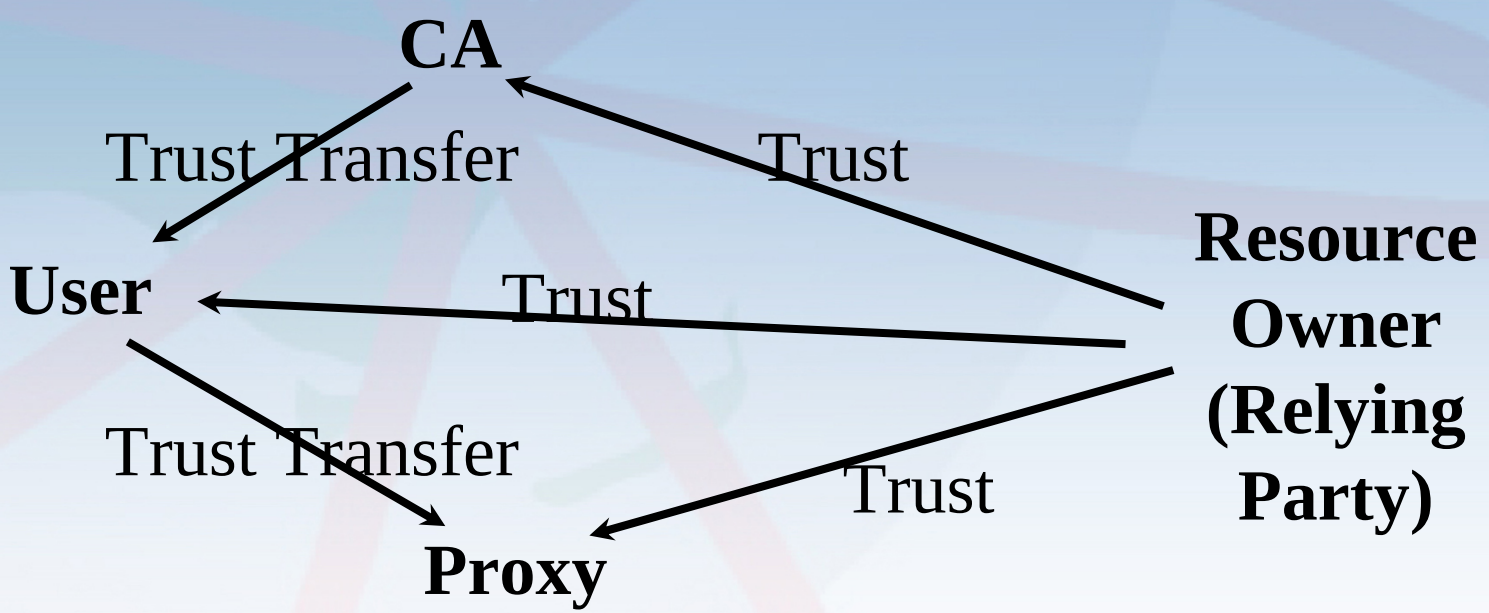
Root of Trust

- **PKI depends upon the relying party (resource owner) trusting the** Certification Authority **(CA) to operate the PKI Infrastructure and identify the user as detailed in the** Certification Practice Statement **(CPS)**
- **The embodiment of this trust is the resource owner installing the CA Certificate locally as a** trusted root

Transfer of trust

- This allows a resource owner to trust the identity of a user based on a Certificate issued by the root CA, or issued by a sub-CA of the root CA (if CPS allows)
- In the Grid, PKI enables a proxy to transfer that trust so the resource owner trusts the proxy is acting for the user

Trust



Introduction

- A "Pilot Certification Level 3 CA v0.2" Certification Authority has been created for the "Grid Computing Federation" Virtual Organisation within the CAUDIT PKI Pilot infrastructure.
- The purpose of this VOCA is:
  - Show the suitability of the CAUDIT eSecurity Framework for this purpose
  - To develop procedures for operating VOCAs for Grid Computing
  - Test compatibility of Grid Infrastructure with the eSecurity Framework PKI.

Suitability

- AusCERT provides simple creation and operation of CA infrastructure within AHERCA
- Documented, tested, audited CA policies
  - Aim to be a default trusted root in browsers
- Operational Infrastructure
  - Secure Facility, Servers, Network
  - CA Software, Hardware Security Module
  - Operations Staff, Incident Response Capability

Compatibility

- Globus Toolkit 4 configuration files and installation procedures (demo)
- Pilot Installation of Grid Infrastructure (documented)
- Ongoing Interoperability testing
- eSecurity Framework Wiki provides a community resource for reference, development and collaboration

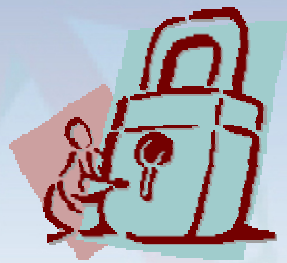
Operations

- RA Operations, CA Operations, CRLS, OCSP Server, LDAP
- Certificate Profiles (User, Host, Service)

Future Work on Grid Computing

- Acquiring user attributes for AuthZ via Shibboleth
- Using the trust fabric so users can use an existing Certificate as credentials for obtaining a Grid certificate
- Using the trust fabric so users can use one certificate anywhere in the federation
- Transitioning to production mode

Thank You!



Any Questions?

pki@auscert.org.au