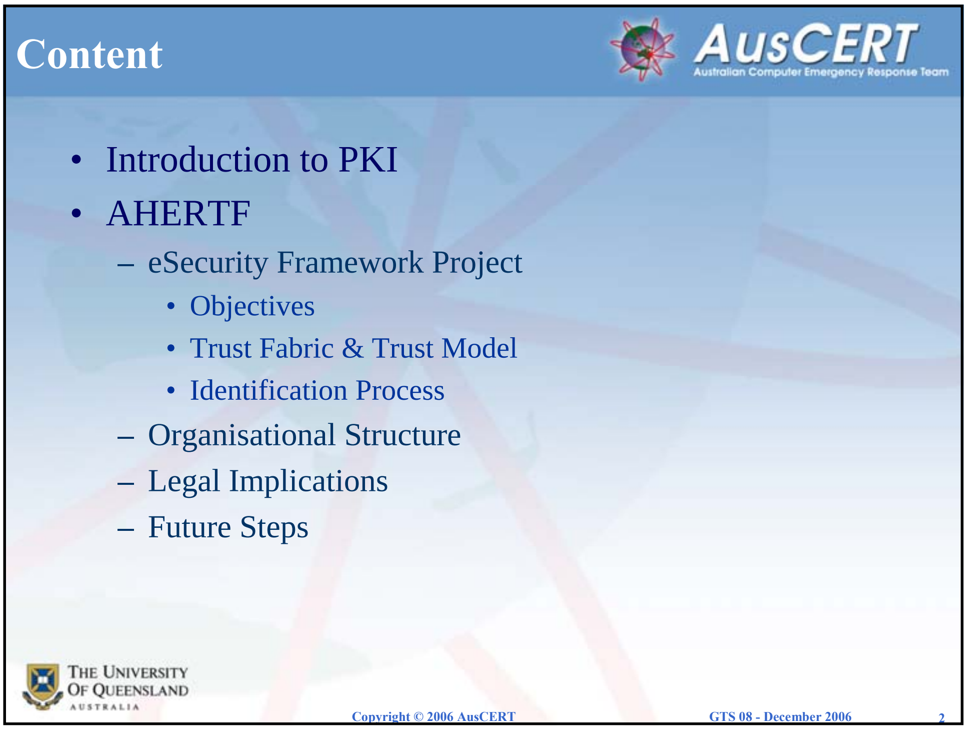
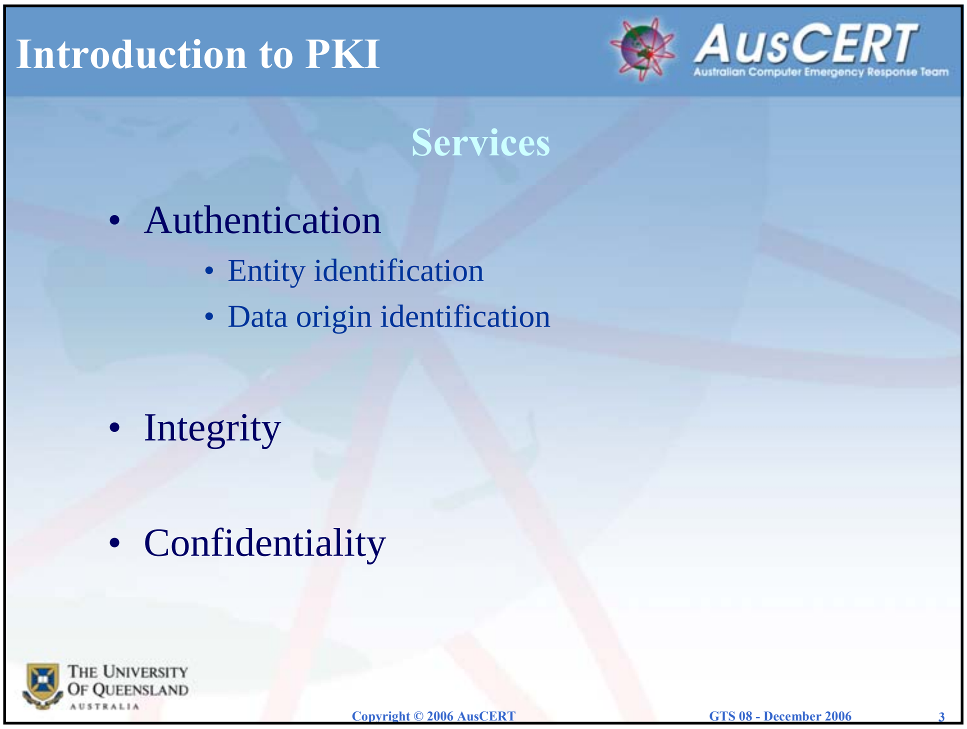
# The Australian Higher Education and Research Sector Trust Federation (AHERTF)

Viviani Paz (AusCERT)



## Content

- Introduction to PKI
- AHERTF
  - eSecurity Framework Project
    - Objectives
    - Trust Fabric & Trust Model
    - Identification Process
  - Organisational Structure
  - Legal Implications
  - Future Steps



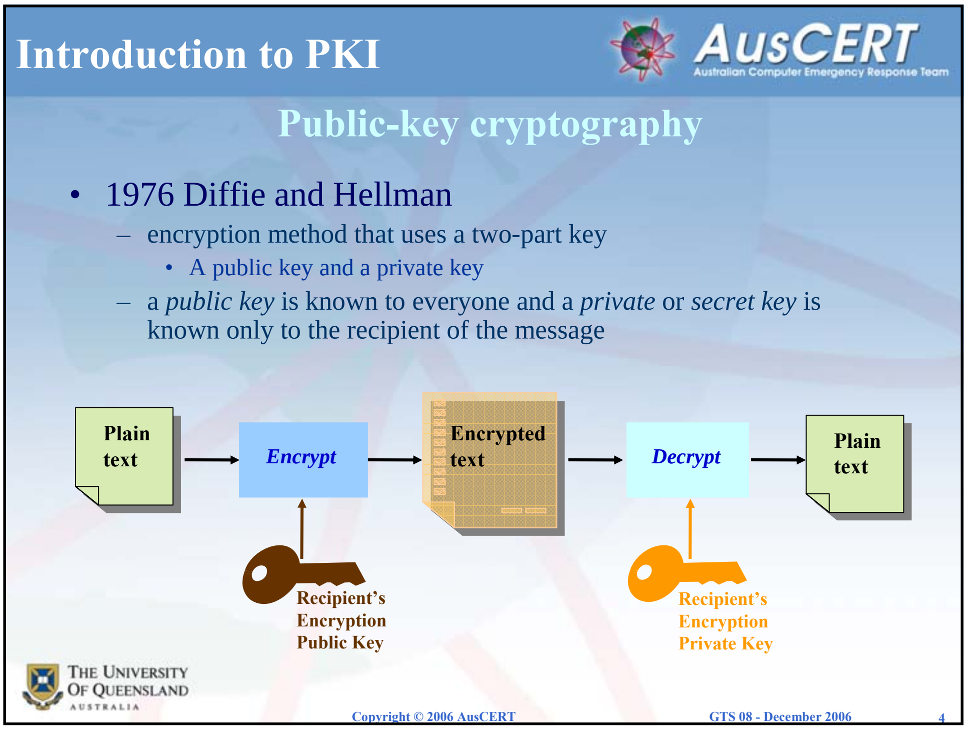
## Introduction to PKI

AusCERT Australian Computer Emergency Response Team

### Services

- Authentication
  - Entity identification
  - Data origin identification
- Integrity
- Confidentiality

The University Of Queensland Australia



## Introduction to PKI

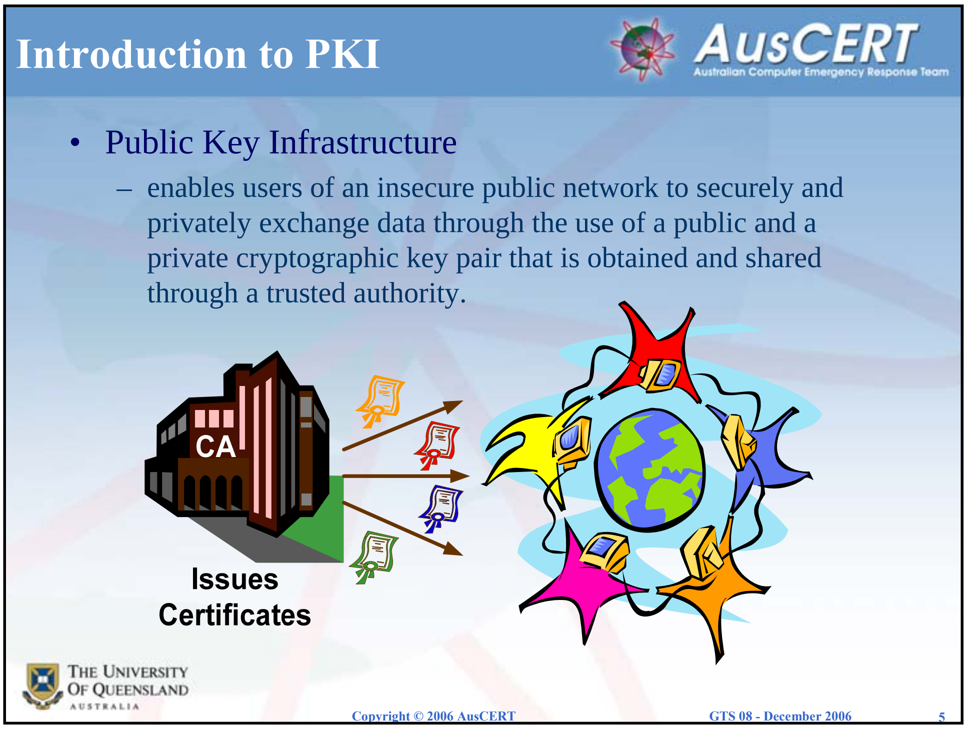
AusCERT Australian Computer Emergency Response Team

### Public-key cryptography

- 1976 Diffie and Hellman
  - encryption method that uses a two-part key
    - A public key and a private key
  - a *public key* is known to everyone and a *private* or *secret key* is known only to the recipient of the message

Plain text
*Encrypt*
Encrypted text
*Decrypt*
Plain text
Recipient's Encryption Public Key
Recipient's Encryption Private Key

The University Of Queensland Australia



## Introduction to PKI

AusCERT
Australian Computer Emergency Response Team

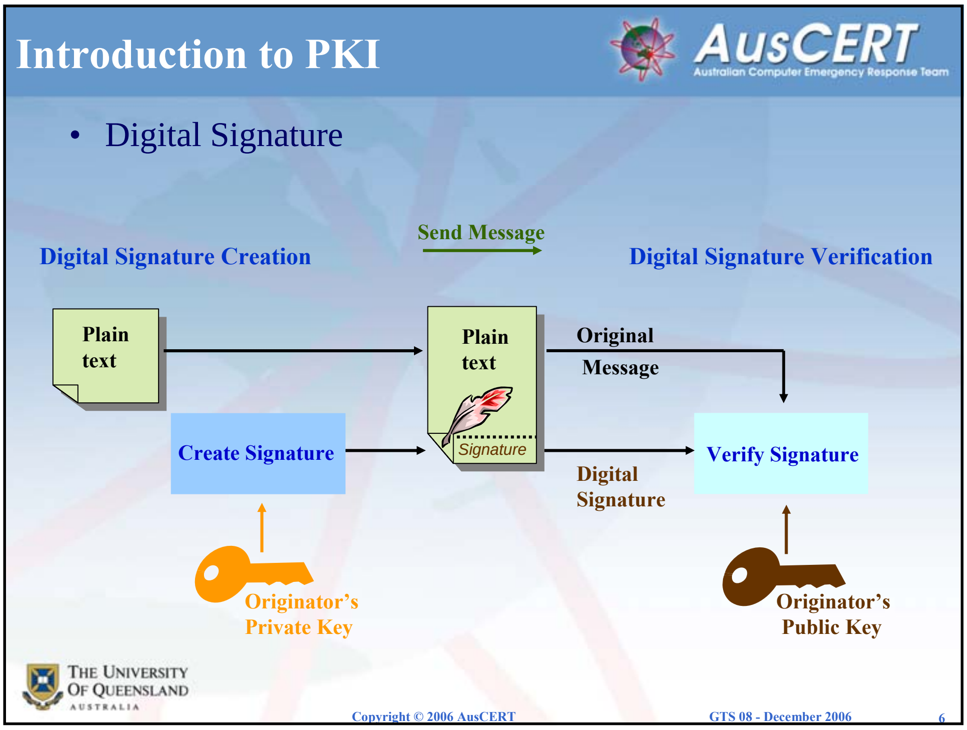
- Public Key Infrastructure
  - – enables users of an insecure public network to securely and privately exchange data through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority.

THE UNIVERSITY OF QUEENSLAND AUSTRALIA

Copyright © 2006 AusCERT

GTS 08 - December 2006

5



## Introduction to PKI

AusCERT
Australian Computer Emergency Response Team

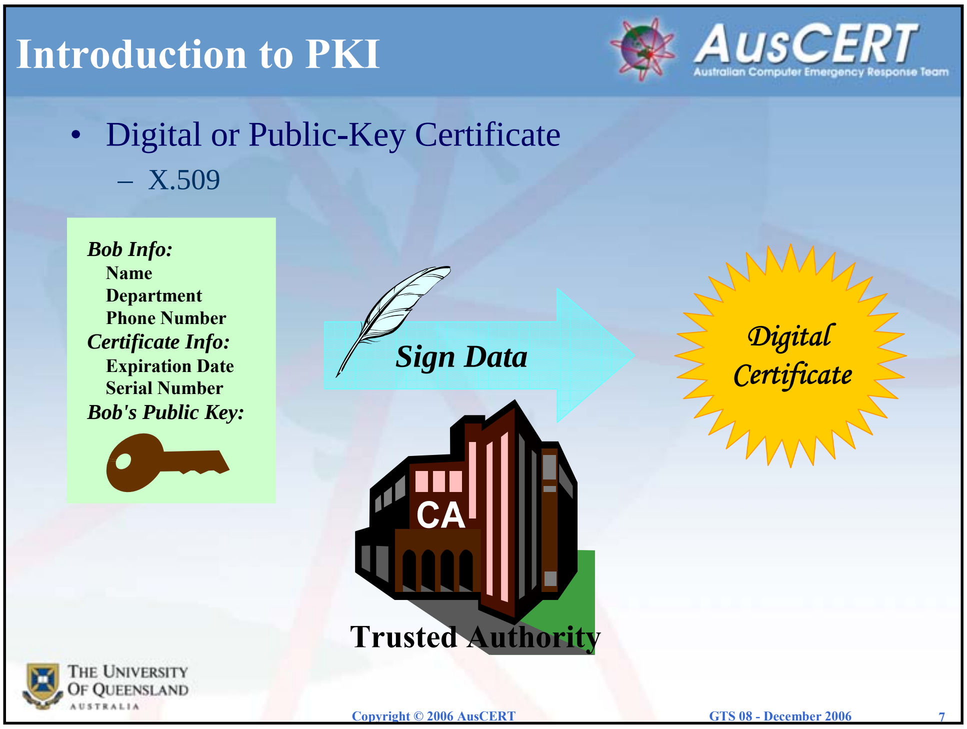
- Digital Signature

THE UNIVERSITY OF QUEENSLAND AUSTRALIA

Copyright © 2006 AusCERT

GTS 08 - December 2006

6



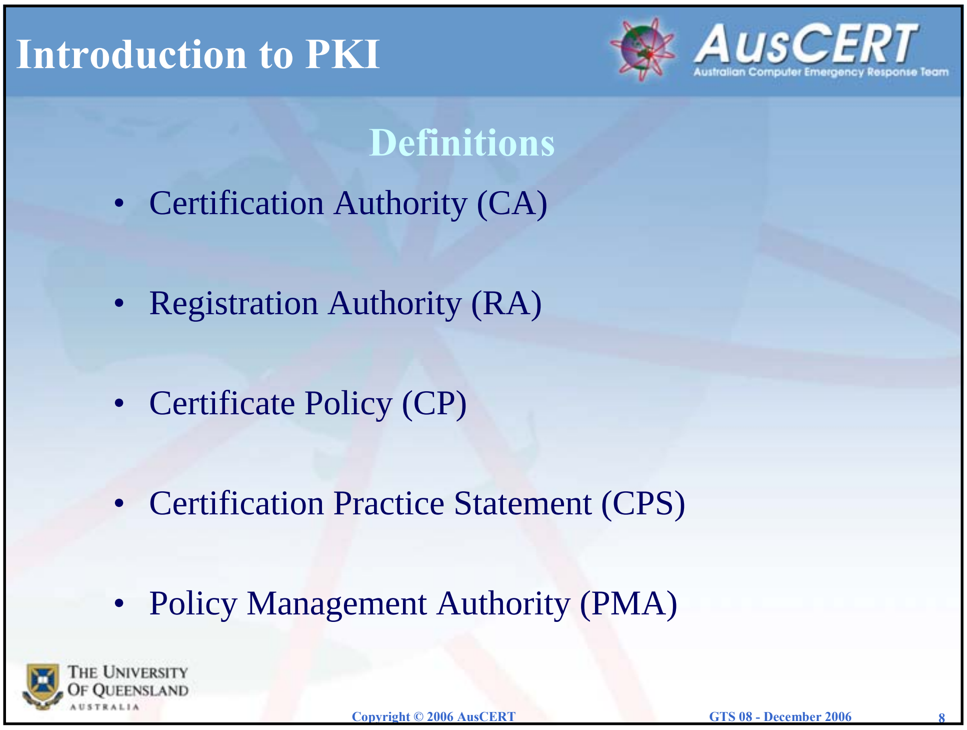
## Introduction to PKI

AusCERT Australian Computer Emergency Response Team

- Digital or Public-Key Certificate
  - X.509

*Bob Info:*
**Name**
**Department**
**Phone Number**
*Certificate Info:*
**Expiration Date**
**Serial Number**
*Bob's Public Key:*

The University Of Queensland AUSTRALIA



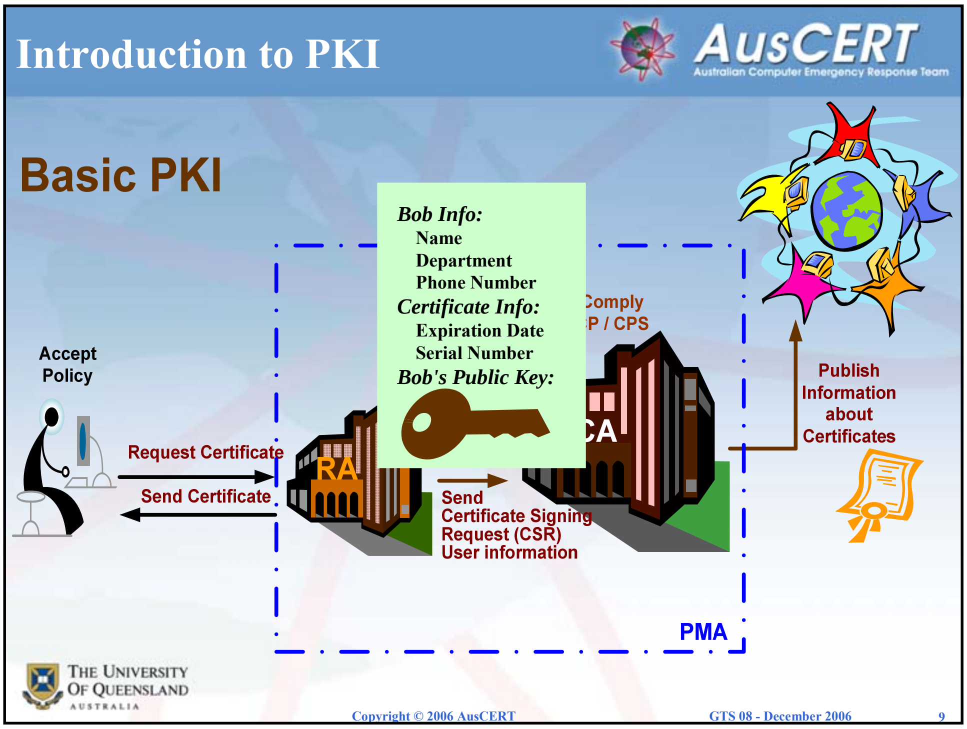
## Introduction to PKI

AusCERT Australian Computer Emergency Response Team

### Definitions

- Certification Authority (CA)
- Registration Authority (RA)
- Certificate Policy (CP)
- Certification Practice Statement (CPS)
- Policy Management Authority (PMA)

The University Of Queensland AUSTRALIA

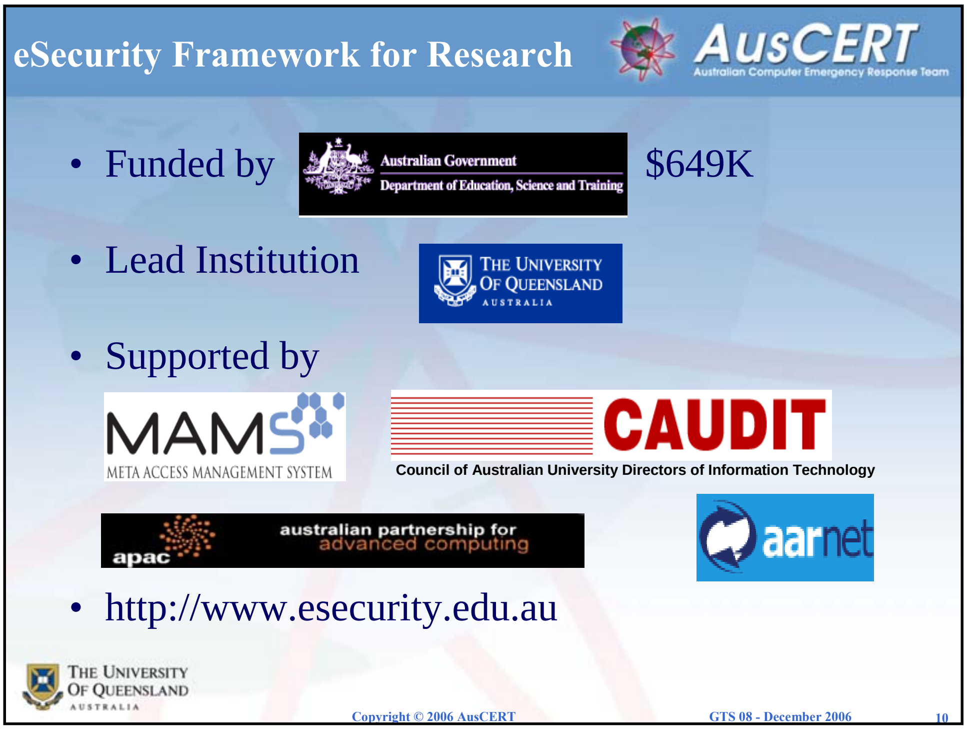


## Introduction to PKI

AusCERT
Australian Computer Emergency Response Team

### Basic PKI

The University Of Queensland
Australia



## eSecurity Framework for Research

AusCERT
Australian Computer Emergency Response Team

- 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

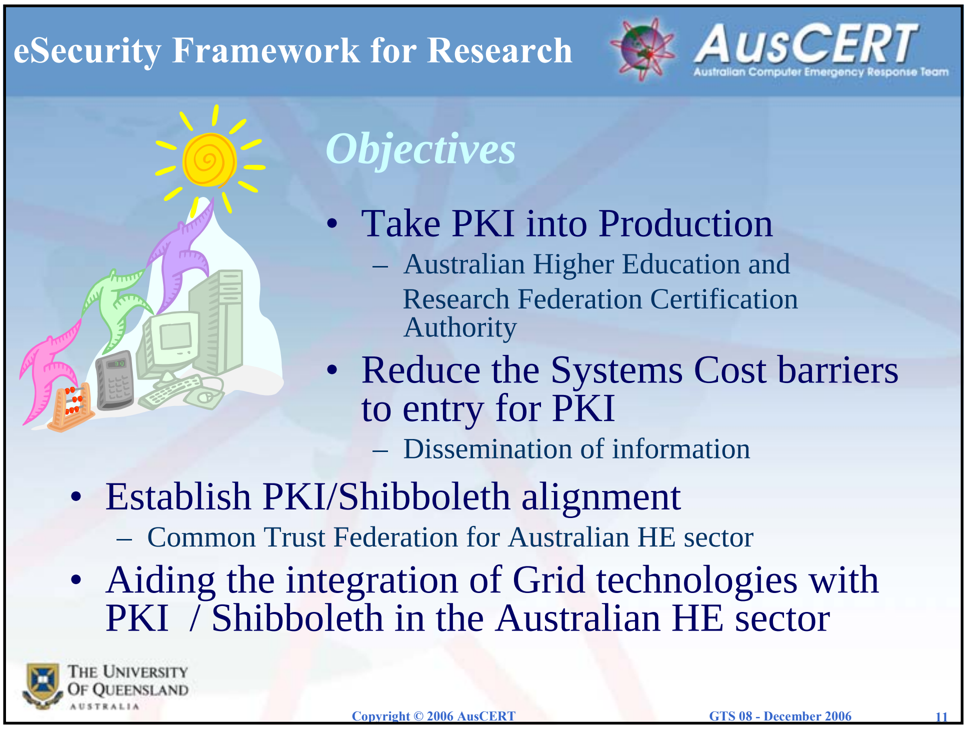
CAUDIT Council of Australian University Directors of Information Technology

apac australian partnership for advanced computing

aarnet

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

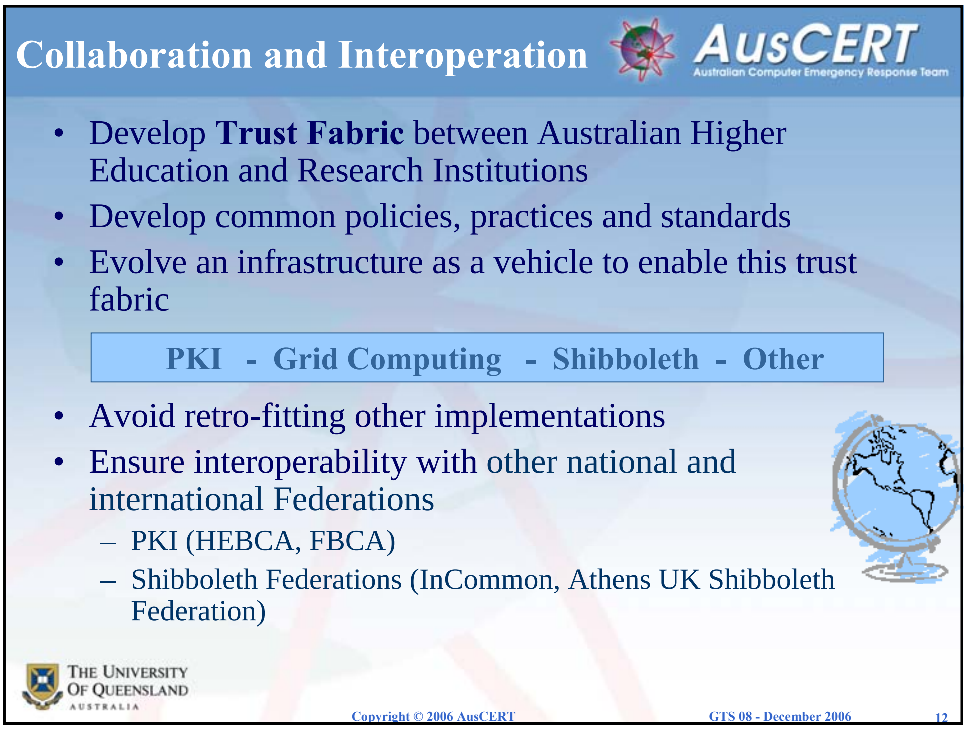
The University Of Queensland
Australia



## eSecurity Framework for Research

### *Objectives*

- Take PKI into Production
  - Australian Higher Education and Research Federation 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

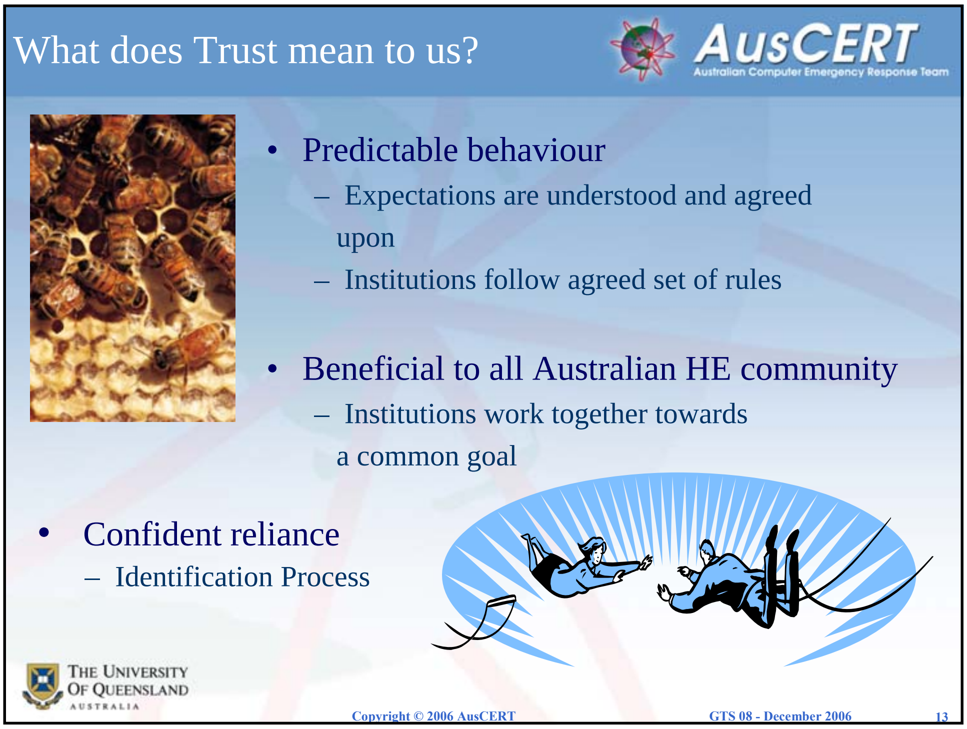


## Collaboration and Interoperation

- Develop **Trust Fabric** between Australian Higher Education and Research Institutions
- Develop common policies, practices and standards
- Evolve an infrastructure as a vehicle to enable this trust fabric

**PKI - Grid Computing - Shibboleth - Other**

- Avoid retro-fitting other implementations
- Ensure interoperability with other national and international Federations
  - PKI (HEBCA, FBCA)
  - Shibboleth Federations (InCommon, Athens UK Shibboleth Federation)

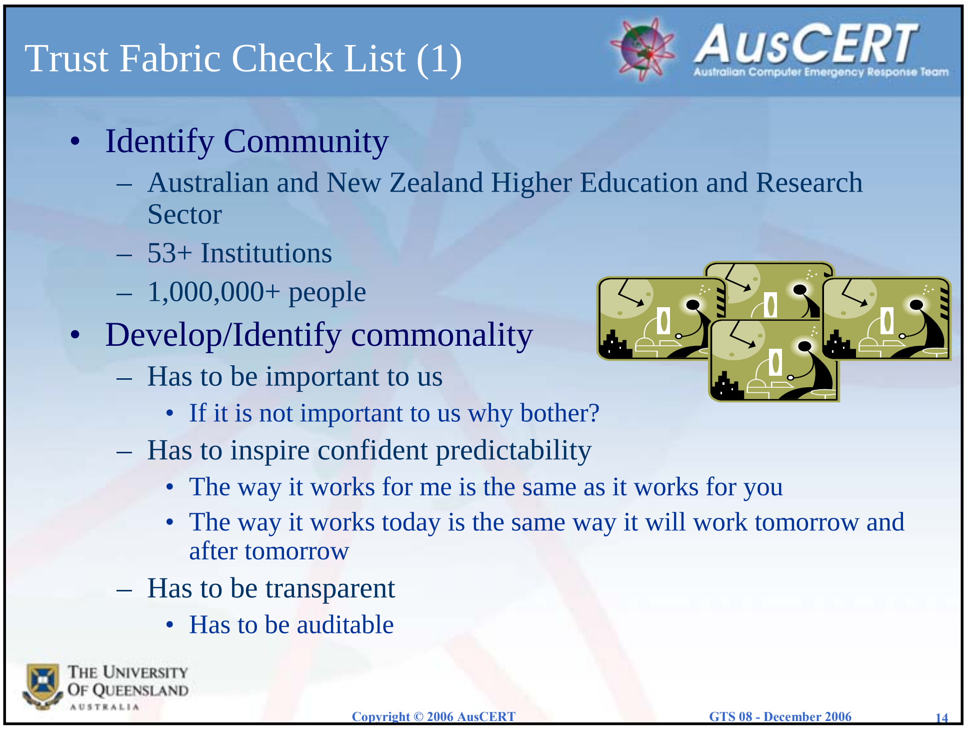


## What does Trust mean to us?

AusCERT
Australian Computer Emergency Response Team

- 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

The University Of Queensland
Australia

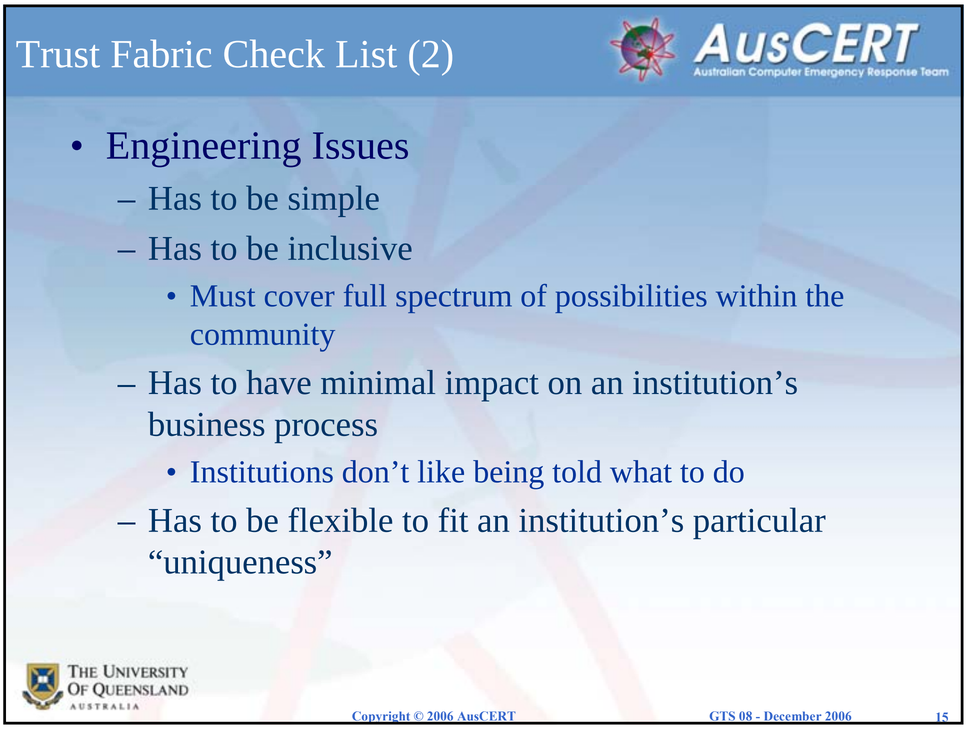


## Trust Fabric Check List (1)

AusCERT
Australian Computer Emergency Response Team

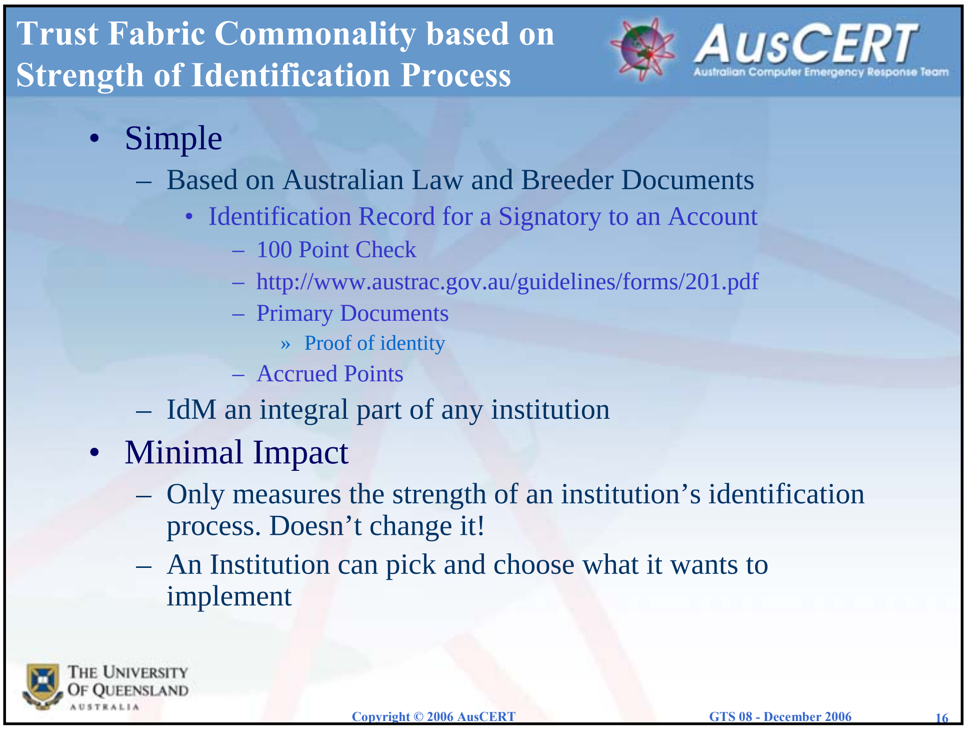
- Identify Community
  - Australian and New Zealand Higher Education and Research Sector
  - 53+ Institutions
  - 1,000,000+ people
- Develop/Identify commonality
  - Has to be important to us
    - If it is not important to us why bother?
  - Has to inspire confident predictability
    - The way it works for me is the same as it works for you
    - The way it works today is the same way it will work tomorrow and after tomorrow
  - Has to be transparent
    - Has to be auditable

The University Of Queensland
Australia



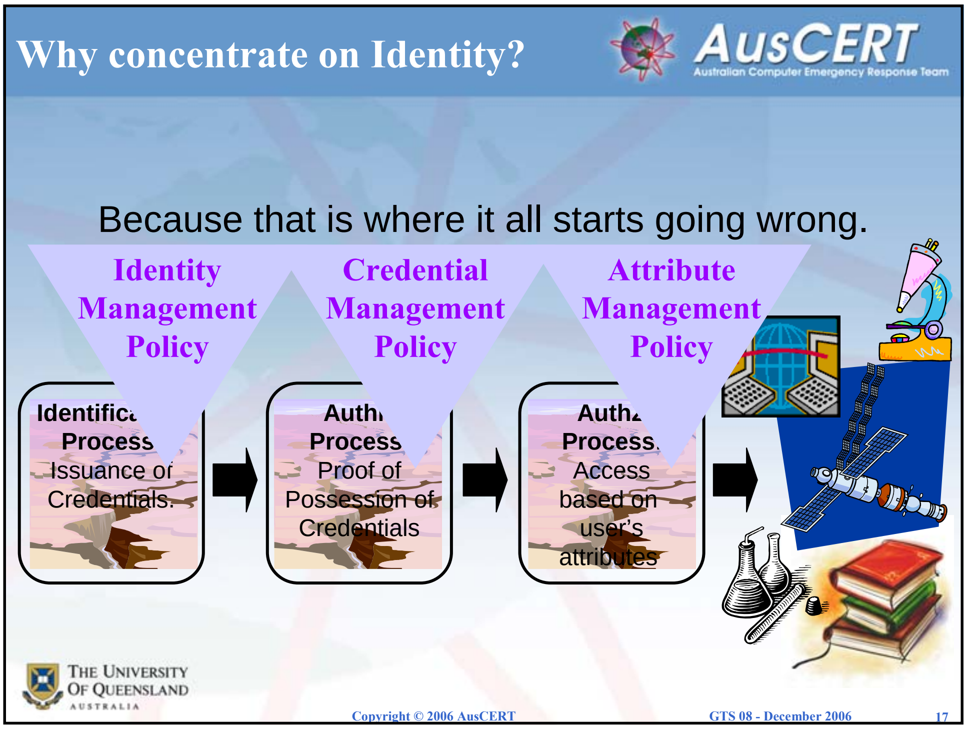
## Trust Fabric Check List (2)

- Engineering Issues
  - Has to be simple
  - Has to be inclusive
    - Must cover full spectrum of possibilities within the community
  - Has to have minimal impact on an institution’s business process
    - Institutions don’t like being told what to do
  - Has to be flexible to fit an institution’s particular “uniqueness”



## Trust Fabric Commonality based on Strength of 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



## Why concentrate on Identity?

AusCERT
Australian Computer Emergency Response Team

Because that is where it all starts going wrong.

Identity Management Policy

Credential Management Policy

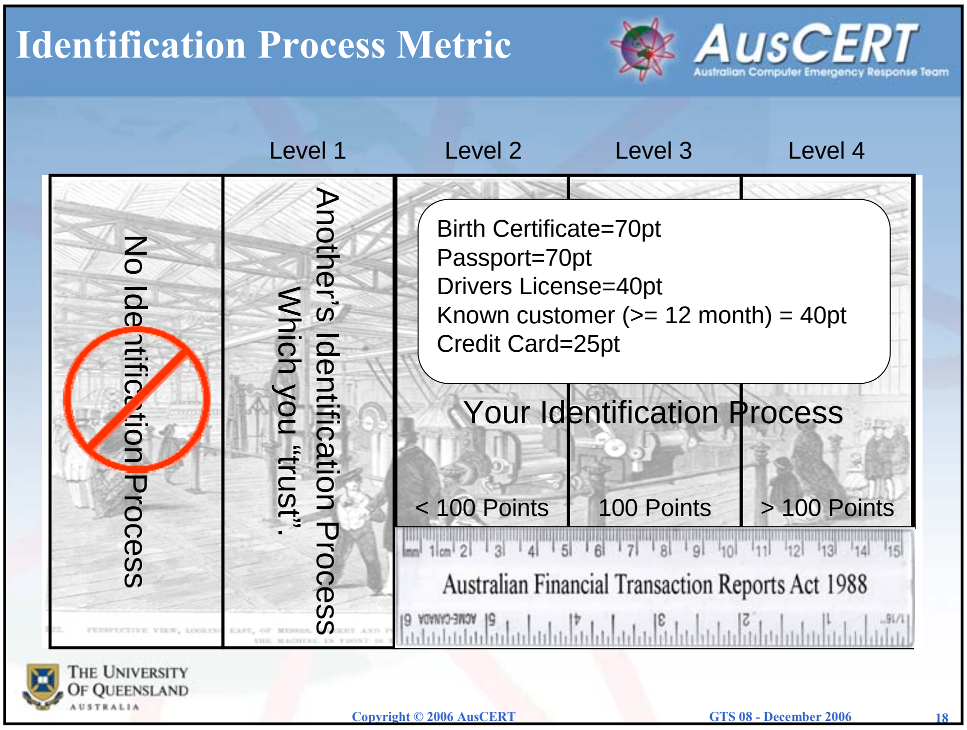
Attribute Management Policy

Identifica Process Issuance of Credentials.

Auth Process Proof of Possession of Credentials

Authz Process Access based on user's attributes

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA



## Identification Process Metric

AusCERT
Australian Computer Emergency Response Team

Level 1 Level 2 Level 3 Level 4

No Identification Process

Another's Identification Process Which you "trust".

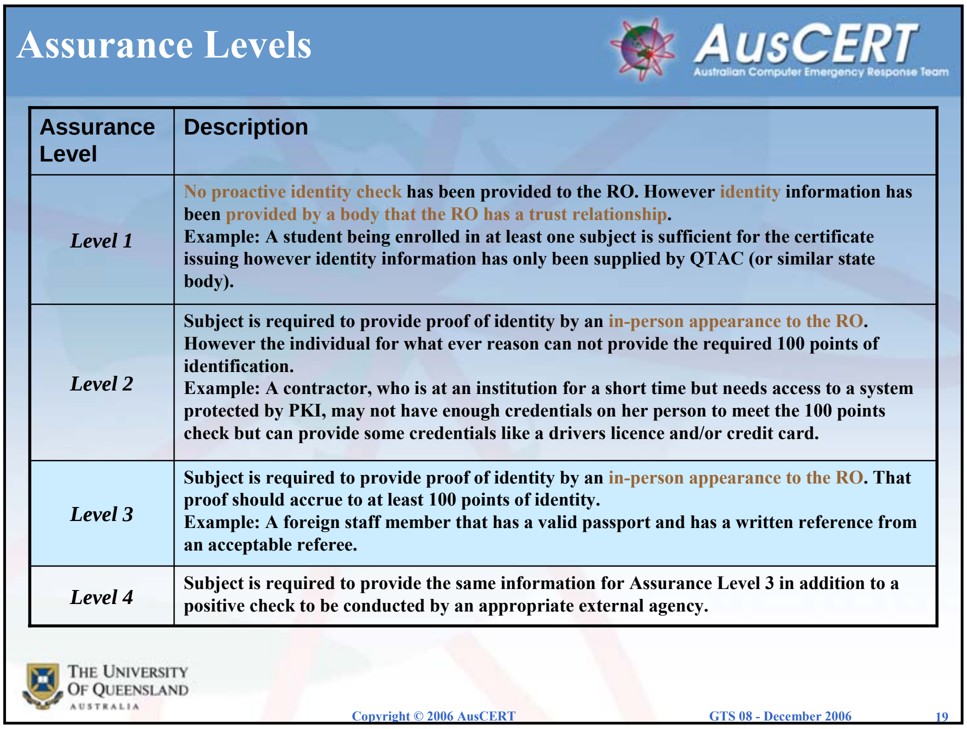
Birth Certificate=70pt
Passport=70pt
Drivers License=40pt
Known customer (>= 12 month) = 40pt
Credit Card=25pt

Your Identification Process

< 100 Points 100 Points > 100 Points

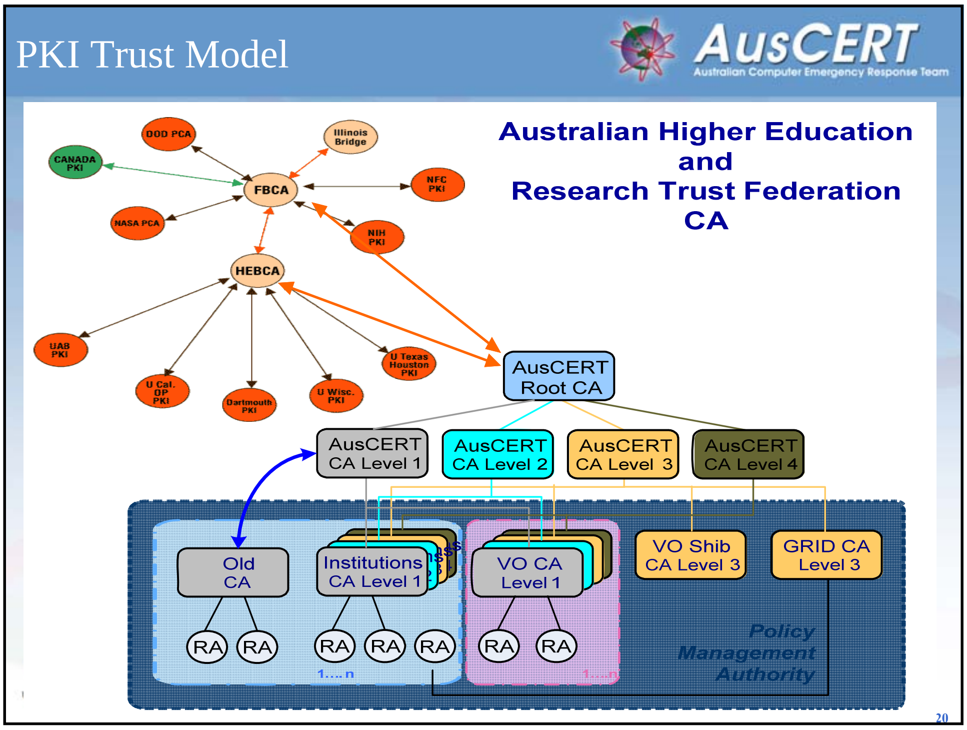
Australian Financial Transaction Reports Act 1988

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA



## Assurance Levels

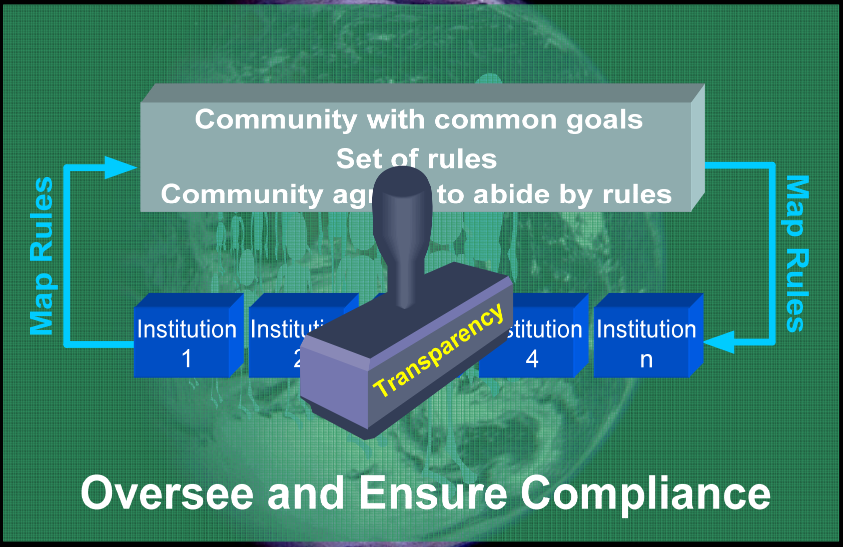
| Assurance Level | Description |
|---|---|
| *Level 1* | No proactive identity check has been provided to the RO. However identity information has been provided by a body that the RO has a trust relationship.<br>Example: A student being enrolled in at least one subject is sufficient for the certificate 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 RO. However the individual for what ever reason can not provide the required 100 points of identification.<br>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 RO. That proof should accrue to at least 100 points of identity.<br>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 Assurance Level 3 in addition to a positive check to be conducted by an appropriate external agency. |



## PKI Trust Model

**Australian Higher Education and Research Trust Federation CA**

## Federation



Community with common goals
Set of rules
Community agr to abide by rules

Map Rules

Map Rules

Institution 1

Instituti 2

stitution 4

Institution n

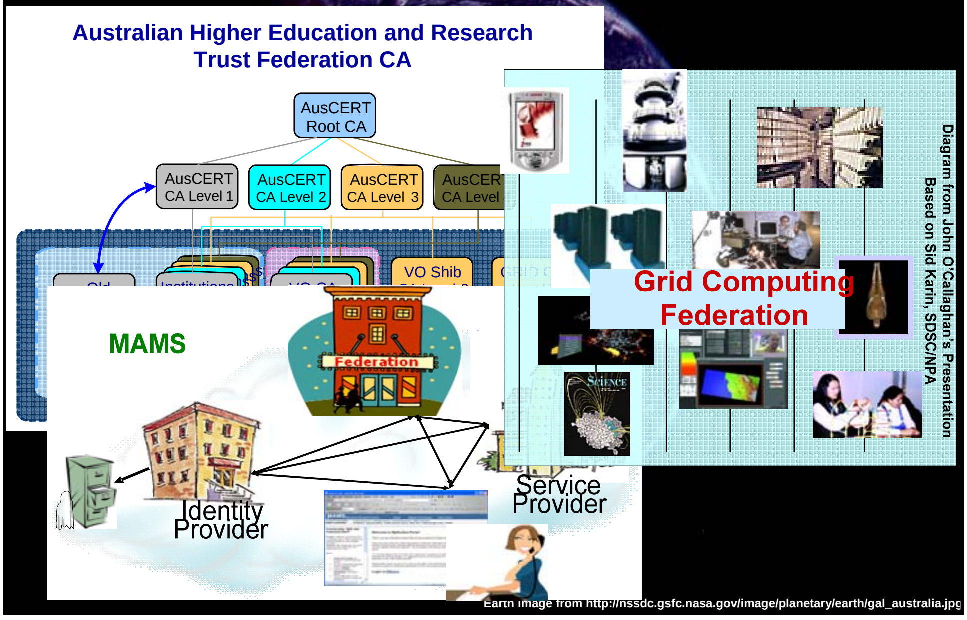
Transparency

Oversee and Ensure Compliance

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

## Australian Higher Education and Research Trust Federation

*Council Authority - Light weight - Transparency*



Australian Higher Education and Research Trust Federation CA

AusCERT Root CA

AusCERT CA Level 1

AusCERT CA Level 2

AusCERT CA Level 3

AusCER CA Level

Old

Institutions

VO CA

VO Shib

GRID C

MAMS

Federation

Identity Provider

Service Provider

Grid Computing Federation

SCIENCE

Diagram from John O'Callaghan's Presentation
Based on Sid Karin, SDSC/NPA

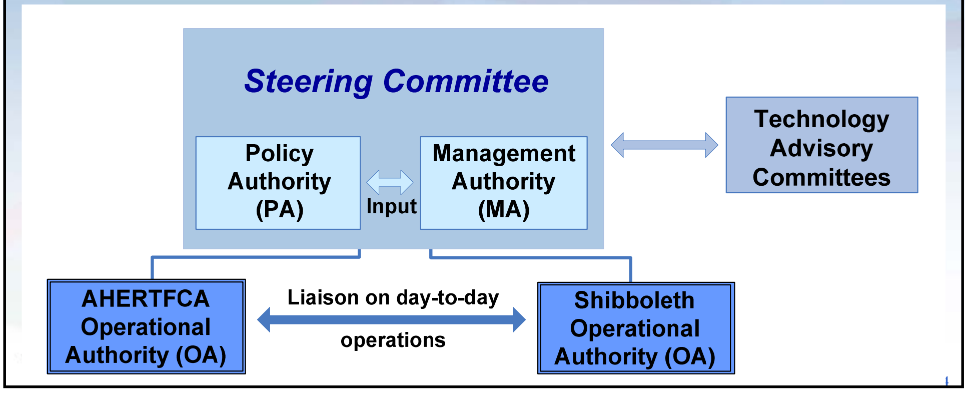
Earth image from http://nssdc.gsfc.nasa.gov/image/planetary/earth/gal_australia.jpg

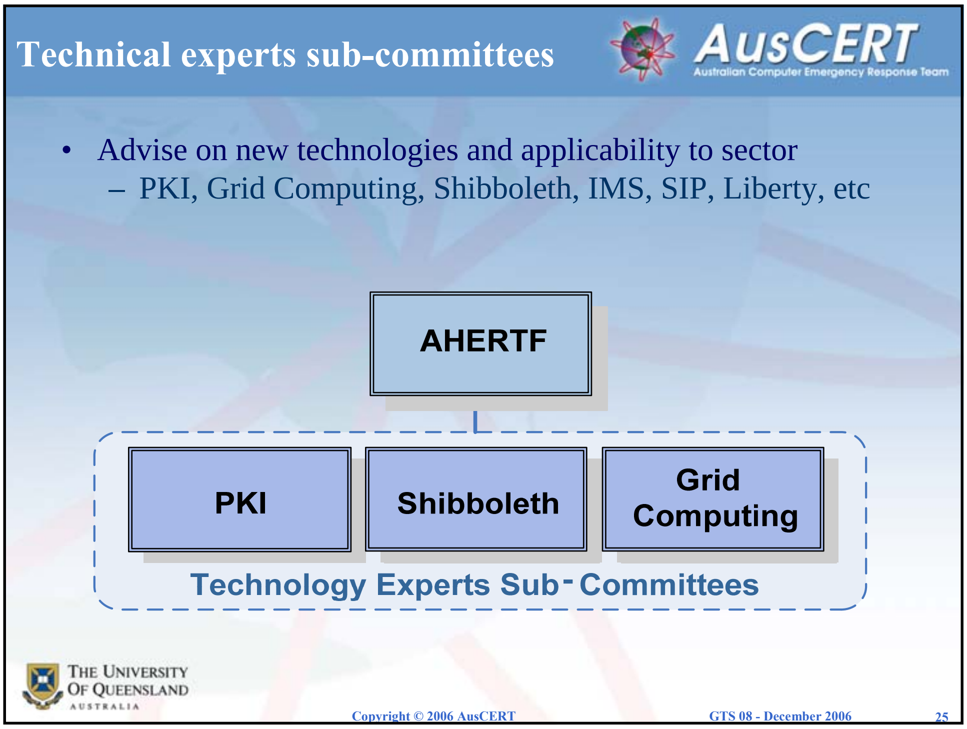
# AHERTF's Council Authority

- Formed by HE and Research representatives
  - CAUDIT to convene
    - Small group formed by IT Directors, Librarians, IT Security, etc
  - Wide HE Sector Membership
- Ensure services provided meet business needs
- Ensure appropriate security and compliance with AHERTF requirements by the sector
- Manage trust agreements and policies
- Provide direction to sector

# AHERTF Council's Role

- Federation Management
  - Management Authority Responsibility
- Establish policies across Federation
  - Policy Authority responsibility
- Monitor/Determine benefit of new technologies
- Oversee Sub-committees
- Operational Authority (OA)
  - AHERTFCA OA
  - Shibboleth OA


Steering Committee
Policy Authority (PA)
Input
Management Authority (MA)
Technology Advisory Committees
AHERTFCA Operational Authority (OA)
Liaison on day-to-day operations
Shibboleth Operational Authority (OA)



## Technical experts sub-committees

AusCERT
Australian Computer Emergency Response Team

- Advise on new technologies and applicability to sector
  - PKI, Grid Computing, Shibboleth, IMS, SIP, Liberty, etc

AHERTF

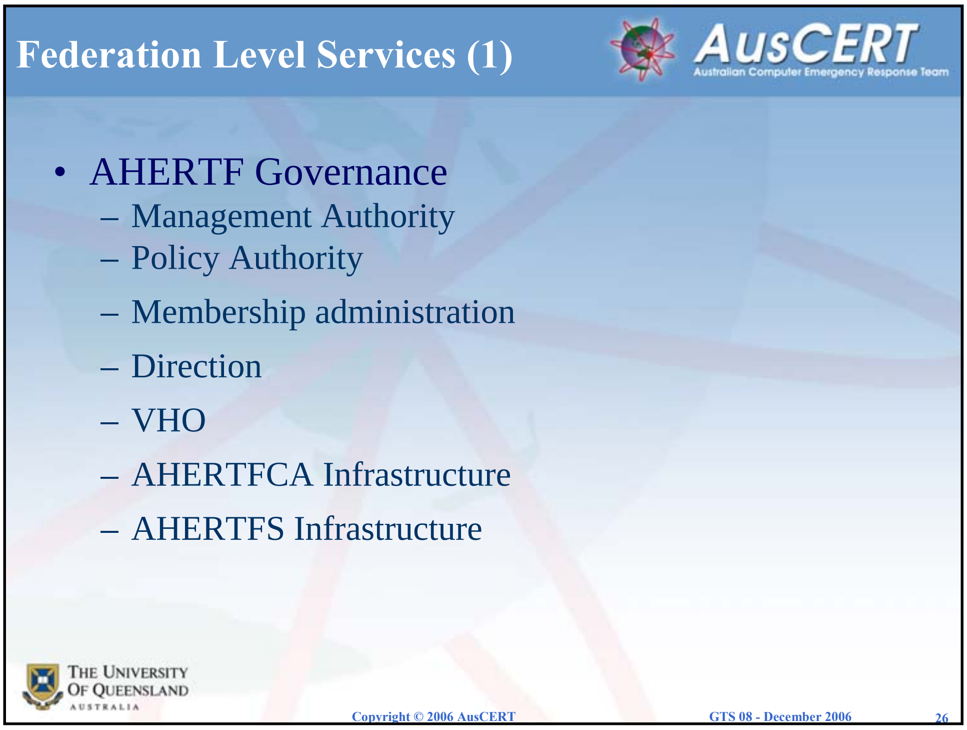
PKI

Shibboleth

Grid Computing

Technology Experts Sub-Committees

The University Of Queensland
AUSTRALIA

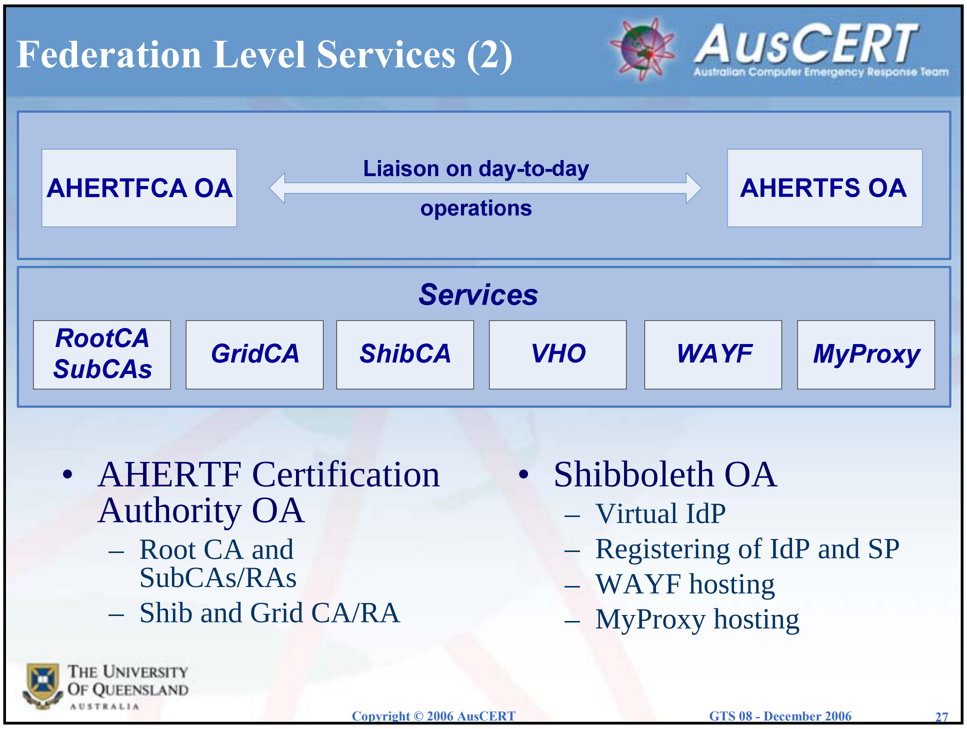


## Federation Level Services (1)

AusCERT
Australian Computer Emergency Response Team

- AHERTF Governance
  - Management Authority
  - Policy Authority
  - Membership administration
  - Direction
  - VHO
  - AHERTFCA Infrastructure
  - AHERTFS Infrastructure

The University Of Queensland
AUSTRALIA



## Federation Level Services (2)

AusCERT
Australian Computer Emergency Response Team

AHERTFCA OA

Liaison on day-to-day operations

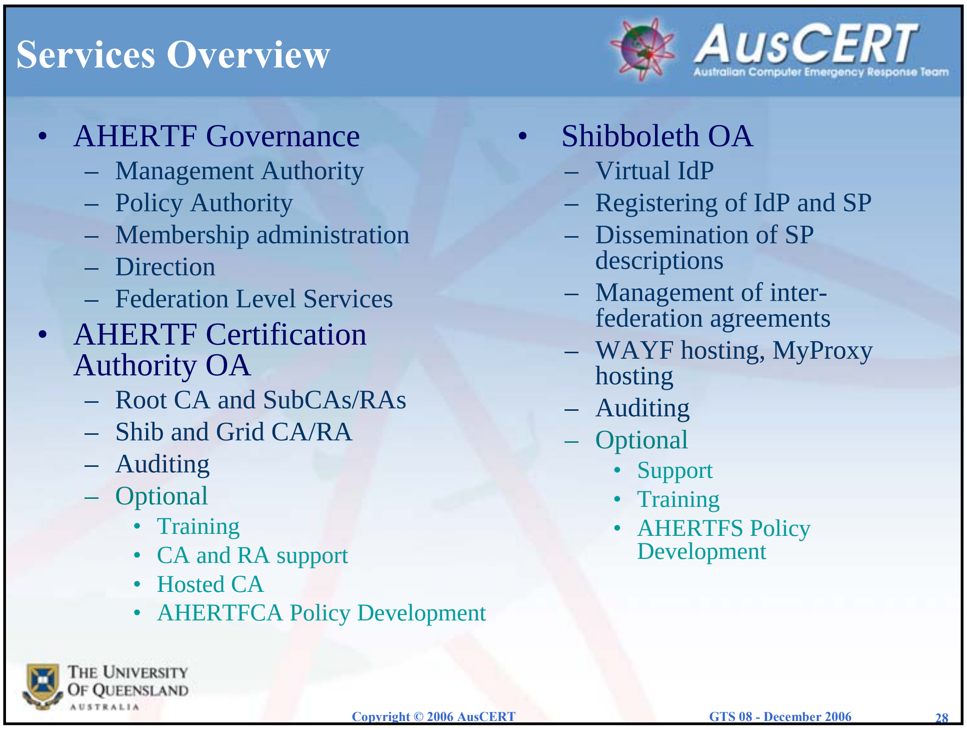
AHERTFS OA

**Services**

RootCA SubCAs | GridCA | ShibCA | VHO | WAYF | MyProxy

- AHERTF Certification Authority OA
  - Root CA and SubCAs/RAs
  - Shib and Grid CA/RA
- Shibboleth OA
  - Virtual IdP
  - Registering of IdP and SP
  - WAYF hosting
  - MyProxy hosting

The University Of Queensland
AUSTRALIA



## Services Overview

AusCERT
Australian Computer Emergency Response Team

- AHERTF Governance
  - Management Authority
  - Policy Authority
  - Membership administration
  - Direction
  - Federation Level Services
- AHERTF Certification Authority OA
  - Root CA and SubCAs/RAs
  - Shib and Grid CA/RA
  - Auditing
  - Optional
    - Training
    - CA and RA support
    - Hosted CA
    - AHERTFCA Policy Development
- Shibboleth OA
  - Virtual IdP
  - Registering of IdP and SP
  - Dissemination of SP descriptions
  - Management of inter-federation agreements
  - WAYF hosting, MyProxy hosting
  - Auditing
  - Optional
    - Support
    - Training
    - AHERTFS Policy Development

The University Of Queensland
AUSTRALIA

## AHERTFCA Services Example

AusCERT Australian Computer Emergency Response Team

### PKI Services provided to all members of AHERTF

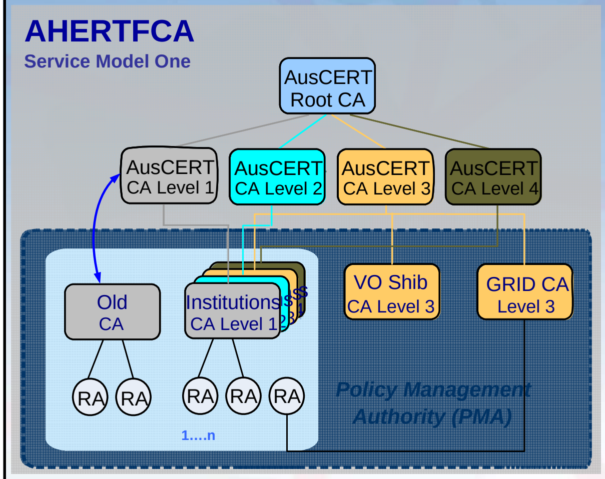
### Subscription Basis

- Organization Authority (OA)
  - ⚡ Signing of University CA certificate.
  - ⚡ University CA certificate revocation.
  - ☇ Certificate dissemination servers.
  - ⚡ Operation of AHERTFCA infrastructure.
  - ☇ Policy development for subsequent approval by council.
  - ⚡ Issuance of certificates used to sign the internal SAML federation requests and assertions.
  - ⚡ Issuance of certificates for the GRID community.
  - – Advise AHERTF Council.

⚡ PKI Testbed

## AHERTFCA Service Models (1)

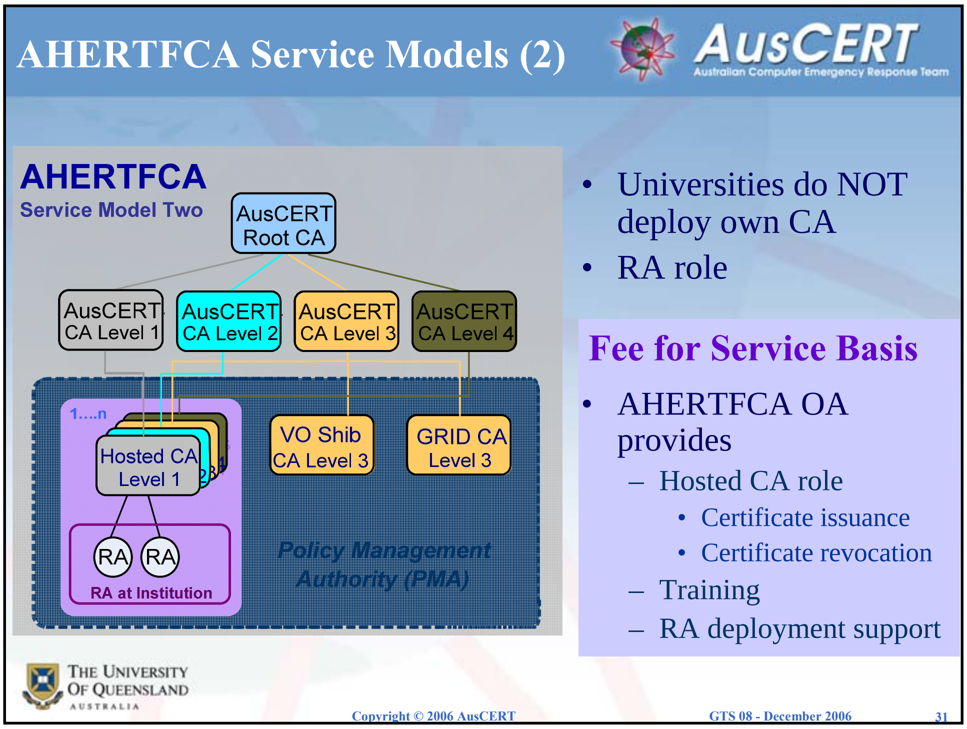
AusCERT Australian Computer Emergency Response Team



- Universities deploy own CA
- Certificate issuance and revocation dissemination

### Fee for Service Basis

- AHERTFCA OA provides
  - Training
  - CA deployment support
  - Annual audit



## AHERTFCA Service Models (2)

AHERTFCA

Service Model Two

AusCERT Root CA

AusCERT CA Level 1

AusCERT CA Level 2

AusCERT CA Level 3

AusCERT CA Level 4

1....n

Hosted CA Level 1

RA

RA

RA at Institution

VO Shib CA Level 3

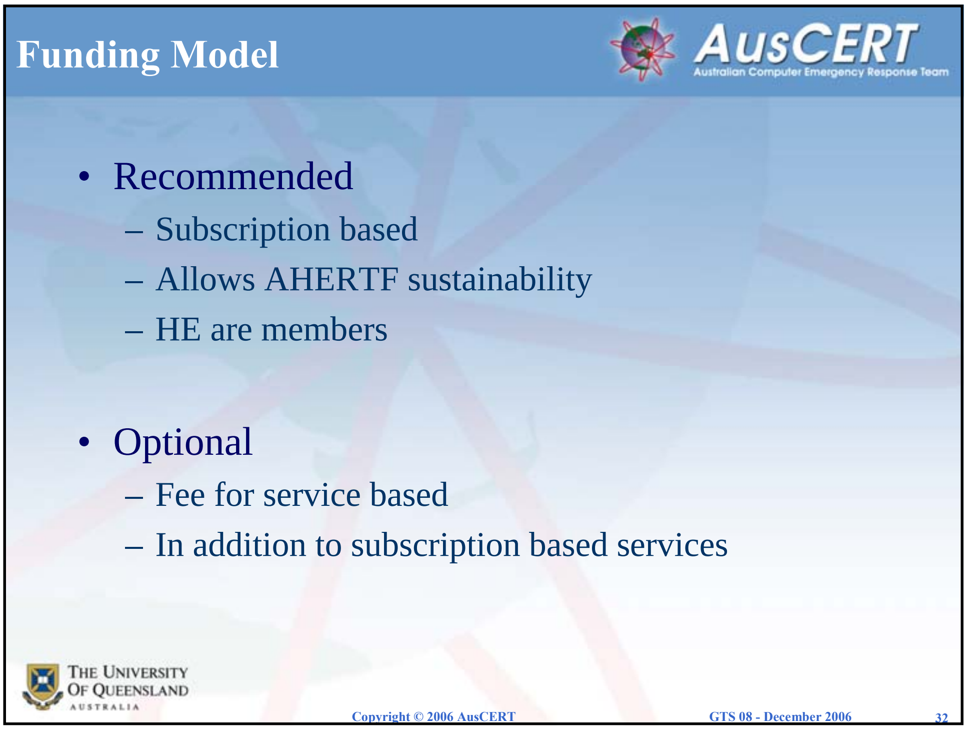
GRID CA Level 3

Policy Management Authority (PMA)

- Universities do NOT deploy own CA
- RA role

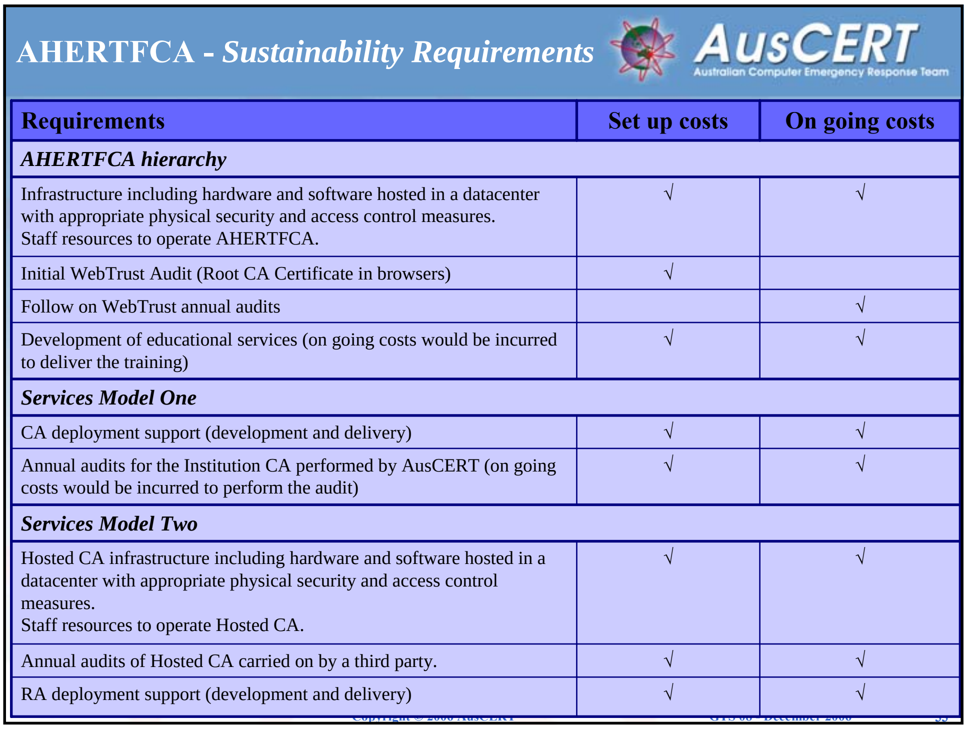
**Fee for Service Basis**

- AHERTFCA OA provides
  - Hosted CA role
    - Certificate issuance
    - Certificate revocation
  - Training
  - RA deployment support



## Funding Model

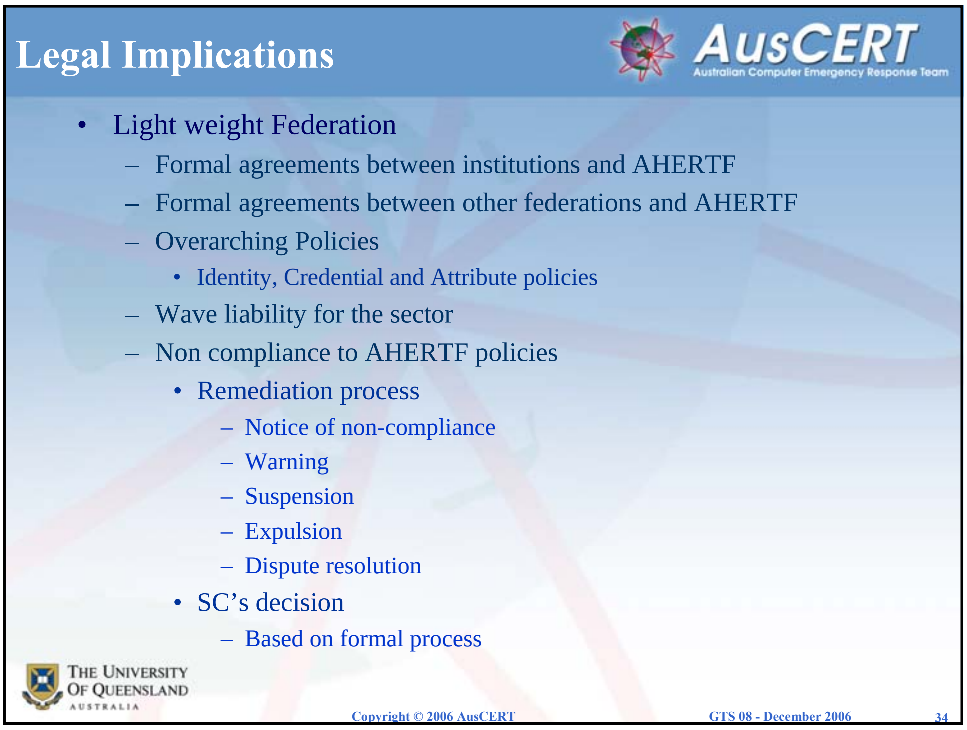
- Recommended
  - Subscription based
  - Allows AHERTF sustainability
  - HE are members
- Optional
  - Fee for service based
  - In addition to subscription based services



## AHERTFCA - *Sustainability Requirements*

AusCERT
Australian Computer Emergency Response Team

| Requirements | Set up costs | On going costs |
|---|---|---|
| ***AHERTFCA hierarchy*** | | |
| Infrastructure including hardware and software hosted in a datacenter with appropriate physical security and access control measures.<br>Staff resources to operate AHERTFCA. | √ | √ |
| Initial WebTrust Audit (Root CA Certificate in browsers) | √ | |
| Follow on WebTrust annual audits | | √ |
| Development of educational services (on going costs would be incurred to deliver the training) | √ | √ |
| ***Services Model One*** | | |
| CA deployment support (development and delivery) | √ | √ |
| Annual audits for the Institution CA performed by AusCERT (on going costs would be incurred to perform the audit) | √ | √ |
| ***Services Model Two*** | | |
| Hosted CA infrastructure including hardware and software hosted in a datacenter with appropriate physical security and access control measures.<br>Staff resources to operate Hosted CA. | √ | √ |
| Annual audits of Hosted CA carried on by a third party. | √ | √ |
| RA deployment support (development and delivery) | √ | √ |

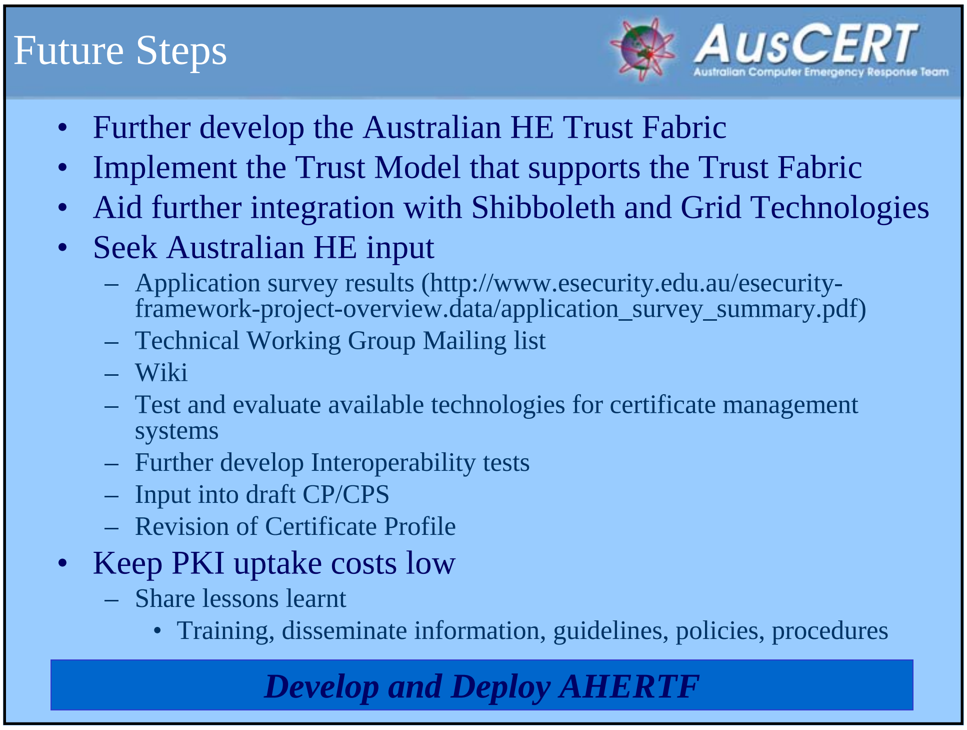


## Legal Implications

AusCERT
Australian Computer Emergency Response Team

- Light weight Federation
  - Formal agreements between institutions and AHERTF
  - Formal agreements between other federations and AHERTF
  - Overarching Policies
    - Identity, Credential and Attribute policies
  - Wave liability for the sector
  - Non compliance to AHERTF policies
    - Remediation process
      - Notice of non-compliance
      - Warning
      - Suspension
      - Expulsion
      - Dispute resolution
    - SC’s decision
      - Based on formal process

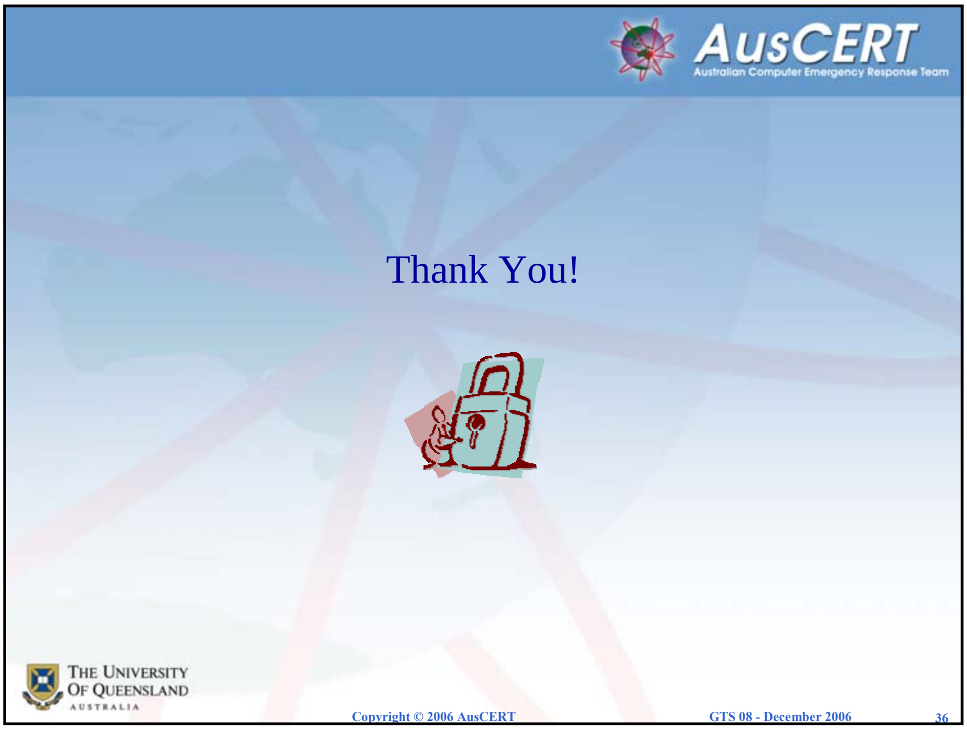
The University Of Queensland
AUSTRALIA



## 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
  - Wiki
  - Test and evaluate available technologies for certificate management systems
  - Further develop Interoperability tests
  - Input into draft CP/CPS
  - Revision of Certificate Profile
- Keep PKI uptake costs low
  - Share lessons learnt
    - Training, disseminate information, guidelines, policies, procedures

***Develop and Deploy AHERTF***



Thank You!