Higher Education National Certificate Authority

Enabling secure interoperation

Rodney McDuff, The University of QLD

Viviani Paz, AusCERT

THE UNIVERSITY OF QUEENSLAND AUSTRALIA
QUESTnet2005
AusCERT Australian Computer Emergency Response Team

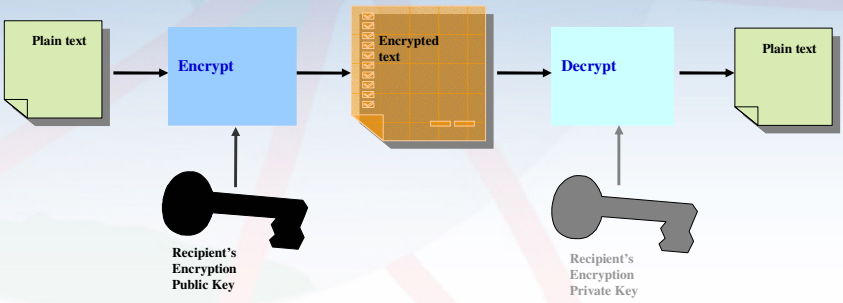
Outline

- Introduction to PKI
- Higher Education Sector PKI
  - CAUDIT PKI Pilot
  - Certificate Levels
  - Trust Model
  - Certificate Path Processing
- Conclusion

Introduction to PKI

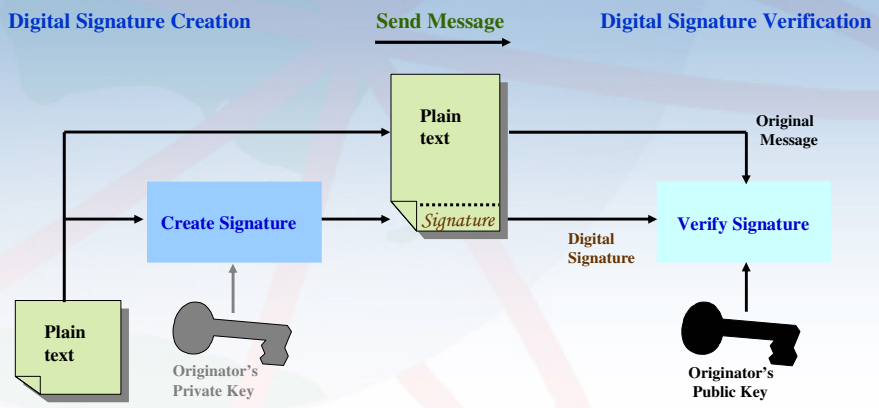
Introduction to PKI

- Reliable infrastructure for information/resource sharing.
- Public-key cryptography
  - 1976 Diffie and Hellman



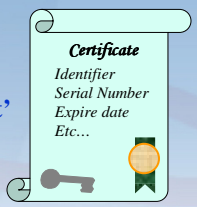
Introduction to PKI Cont.

- Digital Signature = Electronic Signature



Introduction to PKI Cont.

- Digital Certificate
  - Digitally signed data structure
  - 'Electronic "credit card" that establishes one's credentials when doing transactions on the Internet'
- Certification Authority (CA)
  - Issues and manages digital certificates
- Registration Authority (RA)
  - Supports the CA in the end-entity registration requirements
  - Verifies user requests for digital certificates and initiates the certificate process with CA
- Certificate Policy (CP)
  - High-level document that describes requirements/limitations associated with the proposed use of the certificates issued under such a policy.
- Certification Practice Statement (CPS)
  - Detailed document that describes internal operating procedures used by the CA when issuing certificates



X.509

Higher Education Sector PKI

Collaboration
and
Interoperation

THE UNIVERSITY OF QUEENSLAND AUSTRALIA
QUESTnet2005
AusCERT Australian Computer Emergency Response Team

Higher Education Sector PKI

- **CAUDIT PKI Pilot -** ***September 2004***
- **Proposal**
  - **Pro-actively develop policies and standards to avoid retro-fitting implementations and ensure interoperability with overseas PKIs**
  - **Implement a proof of concept system**
- **Benefits**
  - **Enable a collaborative framework for implementation across sector**
  - **Ongoing governance mechanism to support the collaborative framework**
  - **Share lessons learned with the sector**
  - **Reduce the cost of implementation of PKI across the sector**
- **Funded by GrangeNet and DCITA**
  - **$ 171,000.00**

Higher Education Sector PKI Cont.

- Managed by the CAUDIT PKI SC

NZ Vice Chancellors Standing Committee on Information Technology

Higher Education Sector PKI Cont.

- Research
  - Policies, Technologies, Pros, Cons
  - Lack of Standards
  - Federated Approach
  - Certificate use
    - Strongly Identity based + Authentication
    - Authorisation via attribute certificates or Shibboleth
- Identify initial PKI requirements
- Services
  - Authentication
    - Entity identification
    - Data origin identification → Non repudiable evidence
  - Integrity
  - Confidentiality

Higher Education Sector PKI Cont.

- Participant Universities

- Technical Activities Group
  - Test and evaluate available technologies for certificate management systems
  - Input into CP and CPS

Higher Education Sector PKI Cont.

- Training
  - Induct CAs, RAs and other users
- Investigate additional requirements
  - PKI + Shibboleth
- Proposal for Production PKI and PKI/Shibboleth alignment project
  - Funding through Systemic Infrastructure Initiative (SII)
  - Supported by

Certification Levels

THE UNIVERSITY OF QUEENSLAND AUSTRALIA
QUESTnet2005
AusCERT Australian Computer Emergency Response Team

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.

 Identification Record for a Signatory to an Account: http://www.austrac.gov.au/guidelines/forms/201.pdf

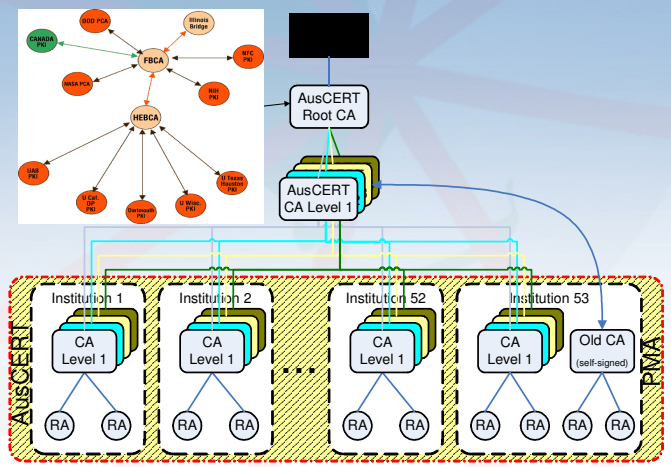
Trust Model

What is Trust?

Certificate Path Processing

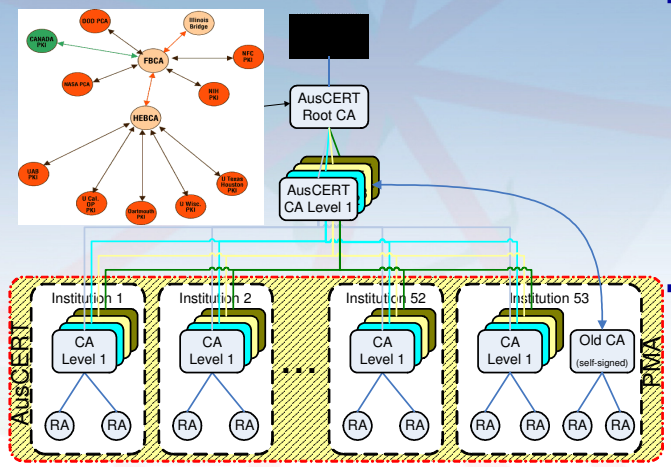
- Psychologically need to
  - Construct a "sense of trust" between a relying party and an end entity.
- Technologically need to
  - Construct a valid unbroken chain of CAs between a relying party's trust anchor and an end entity's certificate.
- Certificate Path Construction
- Certificate Path Validation
- Most common PKI enabled application disappoint here

Trust Model



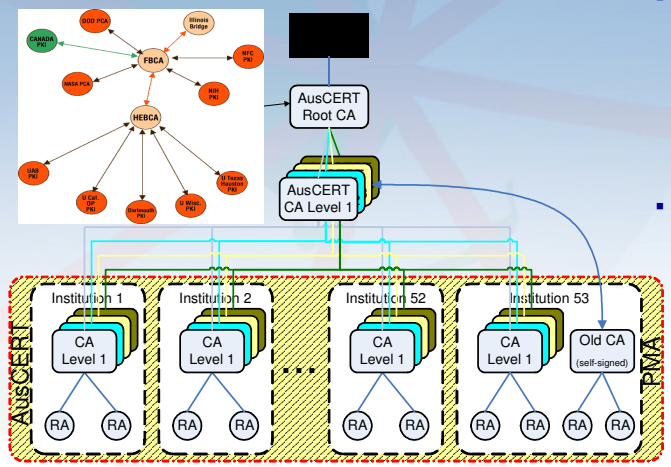
- AusCERT Root CA is trust anchor for CAUDIT PKI.
- Root CA signed subordinate AusCERT CA for each Certification Level.
  - Good for PKI networking.
- Each institution has CA for each Certification Level signed by appropriate AusCERT subordinate CA.

Trust Model Cont.



- Institutions with old PKI can deploy new CA but old CA cross-certify with appropriate sub CA.
  - Old certs will continue working and get access to CAUDIT PKI.
- AusCERT cross-certify with national, international and global PKIs.
  - Like HEBCA.

Trust Model Cont.



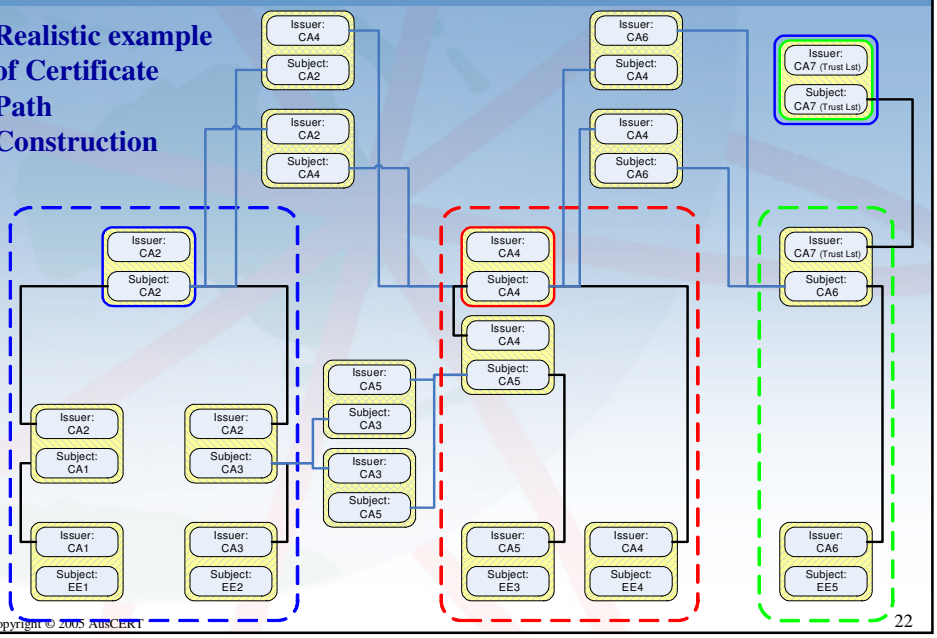
- **AusCERT to provide:**
  - **PMA**
  - **Directory of Directories**
  - **Single point Certificate Dissemination.**
  - **Single point CRL and OCSP.**
  - **Virtual CA for institutions that can't deploy own PKI.**
- **Pilot project needed to do extensive interoperability survey**
  - **Range of CMSs.**
    - **Microsoft**
    - **Sun One**
    - **Open CA**
  - **Common applications.**
    - **Browsers, mail clients.**
  - **Specialized applications**
    - **Access and Computation Grids.**
    - **Shibboleth.**

Certificate Path Construction and Validation

Certificate Path Construction

- Two CAs must have a trust relationship to form a link. Either:
  - One must be subordinate to other, or
  - Must be Cross-Certified. (Unilateral or Bilateral?)
  - Relationships should be forged due to common policies or procedures or interests. Otherwise there is a dilution of trust.
- Must be able to locate and retrieve candidate CAs for chain
  - Don't need end entity's certificate. Already have it.
  - Some protocols can provide them. SSLv3/TLSv1, S/MIME.
  - Some certificate attributes can hint at where to find them.
    - Authority Information Access Extension.
  - Some X.500 or LDAP directories can contain them.
- Can't construct path, can't construct "sense of trust".

Realistic example of Certificate Path Construction



Certificate Path Validation

- Once a path is constructed each link of chain must be checked
  - Is integrity of certificate sound?
    - Issuer signature must be verified.
  - Is the certificate being used within its validity period?
  - Has certificate been revoked?
    - Not trivial pursuit. Need external information. CRL. OCSP.
    - Where do I find these? Some X.509 extensions hint at locations.
  - Has it been used for its intended purpose?
  - Is the candidate path too long?
  - Does one of the CA certificates prohibit the candidate path?
  - Does one of the CA certificates prohibit the policy of another?
- Can't validate path, can't construct "sense of trust"
- If path doesn't validate sirens go off
- If path does validate (suddenly) nothing happens
  - But who does my application think is the trust anchor and how did it get there? Check the Padlock!!!

The Good, The Bad and The Ugly

- X.509 and RFC3280 imprecise about Certificate Path Processing.
  - Has lead to vendor inoperability problems
  - Common applications can't do dynamic path construction
    - Netscape/Mozilla/Firefox. (Hope on the horizon with SUN.)
  - Others do it but with varying degrees of success
    - Microsoft Windows CryptoAPI (IE, Outlook)
  - Can get third party CPP engines.
    - Entrust Entelligence.
  - CPP can be very intensive and untimely for relying party
- Delegated Path Construction and Validation. (DPP and DPV)
  - Certificate Authority Module (CAM)
    - Freely available
    - Used by HEBCA and FBCA
  - Simple Certificate Validation Protocol (SVCP)
    - Coming soon to a RFC near you
  - W3C XML Key Management Specification (XKMS)
    - Total refactoring of PKI way from ASN.1

Conclusion

- CAUDIT PKI Project
  - Infancy
  - Technology is not all it could be
  - Potential
  - Production
  - Participants Universities
    - Support
    - Feedback
  - Interoperability with other PKIs

Thank You!

Any Questions?