

## **PKI lessons from Australia**

---

Global eBusiness Forum  
Geneva 9 December 2003

Chris Joscelyne & Stephen Wilson  
Australian IT Security Forum

## **Best practice PKI applications**

---

**Health eSignature Authority**    [www.hesa.com.au](http://www.hesa.com.au)



- 7,000+ certificates issued to healthcare professionals
- USB dongles & smartcards
- Applications focus on doctors' reports & forms to govt.
- New applications in medical records and doctor-to-doctor

## Best practice PKI applications (continued)

---

### Australian Tax Office

#### THE NEW TAX SYSTEM



- One of the biggest PKIs in the world
  - 100,000 certificates for business tax reporting (GST)
  - Several 100,000 certificates for personal tax returns
- Led to “Australian Business Certificate” ABN-DSC
- ANZ Bank (Identrus) cross recognised by Gatekeeper

## Best practice PKI applications (continued)

---

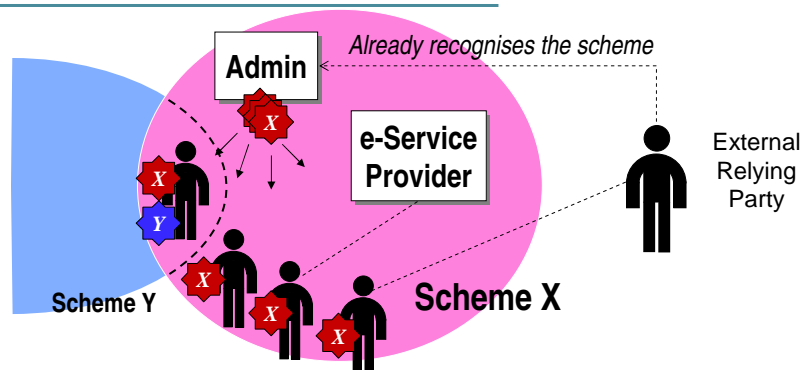
### Similar schemes:

- Land Information New Zealand  
*10,000 certificates*
- Tradelink Hong Kong  
*100,000+*
- US Patent & Trademark Office  
*Several hundred*
- Electronic Conveyancing Victoria (planned)  
*Several thousand*

## “Scheme-based” PKI

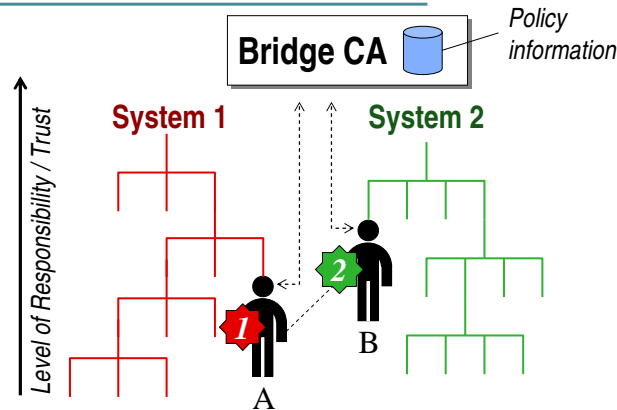
- Fundamental aim is to *automate paperless transactions*
- One party recognises the affiliation of the other party
- Parties already have a business relationship
  - Doctors, lawyers, accountants, other professionals
  - Licence holders (stock brokers, taxi drivers ...)
  - Credit card holders
- Existing context, terms & conditions, liability arrangements
- PKI is specific to an application or class of applications

## Comparing Scheme-based PKI ...



Membership credentials confer rights to carry out certain types of transactions governed by the scheme. The scheme is not necessarily closed, but all Relying Parties must recognise the authority of the scheme. For example, investors recognise Accounting bodies which govern the auditors of listed companies. The Relying Party's questions are: (1) *Was the credential issued by a body authoritative in the context of the transaction?* And (2) *Was the credential issued from well run infrastructure?*

### ... with Bridge CA model



In a typical **government PKI**, trust levels are akin to security clearances. Officials in different systems need to be able to tell one another's trust level, to judge whether classified information can be disclosed/trusted. The Relying Party's question is: *Is your trust level equivalent to mine, or is it higher or lower?*

### Cross recognition of PKI

- Relying Parties have two questions:
  1. *Was the certificate issued by a body authoritative in the context of the transaction?*
  2. *Was the certificate issued from a trusted infrastructure?*
- Certificate Authority audit standards in place
  - General purpose: tScheme, WebTrust for CAs
  - Sector specific: Identrus, Gatekeeper
- Core elements of cross recognition already exist
  - Independent accreditation schemes
  - National accreditation authorities
  - Harmonisation through Mutual Recognition Arrangements

### **The role of government**

---

- Promote e-business & PKI applications
  - ATO, HeSA, Australian Customs ...
- Lead by example
  - The Gatekeeper Framework
  - Intention to outsource Gatekeeper administration and management
- Facilitate security certification/accreditation
  - Common Criteria, AISEP
- Australian Government to lead regional cross recognition negotiations

### **Historical sticking points: Technology neutrality**

---

- Does not mean that technology doesn't matter
- Does not mean that PKI might be superseded soon
- Technology neutrality is a correct *mindset*
- Ensures e-signature laws are robust over long term ...
- ... and applicable to broadest possible set of scenarios

## Historical sticking points: Root CAs

---

- Vague fears about Root CAs:
  - Are they “Big Brother”? No
  - Do they hold copies of everyone’s keys? No
  - Is the Root CA’s liability infinite? No
- The business requirement is quality control, to ensure fitness for purpose, independent of each CAs’ purpose

## Root CAs (continued)

---

- National accreditation bodies would be good Root CAs
  - *National Association of Testing Authorities (Australia)*
  - *Swiss Accreditation Service*
  - *UK Accreditation Service*
  - *NIST/NVLAP (USA)*
  - *Over 40 others*
- Cross border recognition via international arrangements:
  - *Asia Pacific Laboratory Accreditation Cooperation (APLAC)*
  - *European Cooperation for Accreditation (EA)*
  - *International Laboratory Accreditation Cooperation (ILAC)*
  - *etc.*

