BALTIMORE

global
e-security

PKI in *e*Government

Rory Brennan
Director, Professional Services

www.baltimore.com

BALTIMORE

global
e-security

Presentation Content

- PKI and Government
- Considerations
- National Initiatives
- Challenges Ahead
- The Model for the Future ?
- Summary

www.baltimore.com

BALTIMORE

global e-security

PKI & Government

- Provides Authentication Framework
  - National ID & Business Credentials
  - Trust `Model
- Internal Government Services
  - Secure Workflow
  - Administrative Efficiencies
- *e*Government Services
  - Faster, Easier Access to Services
    - Tax
    - Social Welfare
    - Health
    - Supply Chain Management
    - Trading and Customs
  - Kiosk Services (ESD)
    - Common Services
    - Personal Credentials

www.baltimore.com

global e-security

Considerations

- Must be Good for:
  - Government
  - People
  - Business
  - International Trade
- Sets Low Water Mark
- Recognises Heterogenous Environments

- Should Encourage Take-up
  - Flexibility
  - Trusted Technology
  - Legal Protection
  - Ease of Use
  - Low Cost of Entry

www.baltimore.com

BALTIMORE

global e-security

Good for Government ?

- Standard Policies and P.O.I.
- Generic Certificate Content and Attributes
  - Single Directory ?
- Efficiency & Ease of Use
- Inherent Value of Signature
- Streamline Identity Services
  - Police and Internal Security
  - Elections
  - Other

www.baltimore.com

BALTIMORE

global e-security

Good for People ?

- Privacy
- Single Certificate for Everything
- Access to Information
- Awareness and Understanding
- Easier than Paper
- Free

www.baltimore.com

BALTIMORE

global e-security

Good for Business & International Trade ?

- Legal Framework
  - Digital Signature = Physical Signature
  - Defined Terms & Conditions
- More Cost Effective than Paper
- Harmonisation of International Standards
- Saves or Makes Money

www.baltimore.com

BALTIMORE

global e-security

Different Strategies [1]

- China, Korea, Utah and Others
  - National and/or Proprietary Policy
- National Root
- Technology Specific
- Highly Controlled Paradigm
  - Liability Cap
  - High Cost to Entry

www.baltimore.com

BALTIMORE

global e-security

Different Strategies [2]

- Singapore, Hong Kong, Germany
  - Technology Neutral
- Technology Control Point
  - Singapore: CCA
  - Hong Kong: CARO
- Many CA's and Trust Models

www.baltimore.com

BALTIMORE

global e-security

Different Strategies [3]

- Australia
  - Law is Technology Neutral
- Electronic Authentication Law
  - Digital = Physical
  - Provided it has been agreed

www.baltimore.com

BALTIMORE

global e-security

The Australian Experience

- Gatekeeper Accreditation
  - Necessary for Government
  - Mandates “Trusted Technology”
  - Articulates Minimum Requirements
    - Key Size and Source
    - Algorithms
    - Secure Facility

www.baltimore.com

BALTIMORE

global e-security

Australia - Interested Parties

- Attorney General
  - Legal Policy
- Office of Government On-line
  - eGovernment Services
- National Office for Information Economy
  - PKI Policy
- National Computer Security Advisory Authority
  - Accreditation
- National Electronic Authentication Council
  - Advisory

BALTIMORE

global e-security

The Ideal Model ?

- Consider Two Certificates
  - Identity
    - Anonymous/Pseudonymous Certificates ?
  - Attributes
- No Reliance Limits in ID Certificates
- Easy and Affordable
  - Technology Agnostic
- Unobtrusive

www.baltimore.com

BALTIMORE

global e-security

Challenges Ahead

- Digital Signature Law
- Privacy Legislation
- Licensing of CA's
- Maturity of Technology
- One Size Fits All

www.baltimore.com

BALTIMORE

global e-security

Summary

- PKI is Only an Enabler
  - The Oil in the Engine
- Learn from Other Countries
- Keep an Open, Flexible Perspective
- Seek Advice !

www.baltimore.com

BALTIMORE

global
e-security

www.baltimore.com