Why GovernmentOnline?

- Consumer and business demand
  - Over 6 million users (Nov 99)
  - 1.8 million households connected to the Internet
  - 800,000 users purchased or ordered goods over the Internet
  - Business connections
    - 87% of large sized firms
    - 82% of medium sized firms
    - 48% of small sized firms
Strategic priorities

- Agencies to take full advantage of the opportunities the Internet provides
- Ensure the enablers are in place
  - Authentication, privacy and security are recognised enablers
- Enhance GovernmentOnline services in regional Australia
- Enhance IT&T industry development impact of GovernmentOnline initiatives
Strategic priorities (cont.)

- Government business operations to go online
- Monitor best practice and progress
- Facilitate cross-agency services
  - Customer focused channels
- Communicate with stakeholders
What’s the role of the Office for Government Online

- To consult and work with Commonwealth agencies
- To support and assist agencies deliver Government Online
- To facilitate responses to inhibitors and impediments
- To facilitate partnerships for solutions
Where does Gatekeeper fit in GovernmentOnline?

- Authentication, privacy and security are among the set of enablers that need to be in place to support GovernmentOnline.
- Public Key Infrastructure (PKI) technology is a robust solution for authentication, privacy and security for online communications and transactions.
- Gatekeeper is the Commonwealth government’s PKI strategy.
What is PKI

- Public Key Infrastructure (PKI) is a set of applicable laws, policies, standards, systems and security services that enable the use of public key cryptography and digital certificates across a distributed network (such as the Internet or intranets).
- The use of a PKI enables organisations and individuals to authenticate and protect their electronic communications and business transactions.
Public Key Cryptography

- Public key cryptography uses two electronic keys: a public key and a private key.
- The public key can be known by anyone while the private key is kept secret by its owner.
- As long as there is strong binding between the owner and the owner’s public key, the identity of the origin of a message or transaction can be traced to the owner of the private key.
Digital certificates

- Digital certificates are electronic tokens that are used to bind the user’s identification with the user’s public key in a trusted bond.
- These certificates contain information such as the user’s name and the associated public key and the identity of the certification authority (CA) that issued the certificate.
- The certification authority certifies the user’s identity and association with the user’s public key.
Digital signatures

What is a digital signature?
A process which can be used to attach to an electronic message a digital code that is unique to the "signer" of the message. A digital signature results from the use of a "Private Key" to "sign" a message. The recipient of the electronic message can use the signer's "Public Key" to verify whether or not the digital signature is valid, and whether the message has been altered since it was signed.

-------BEGIN SIGNATURE-------
IQB1AwUBMVSiA5QYCuMfgNYjAQFAKgL/ZkBfbeNEsbthba4BlrcnjaqbcKgNv+a5kr4537y8RCd+RHm75yYh5xelws4S87UX80cLBtBcN6AACf11qymC2h+Rb2j5SU+rmXWru+=QFMx
-------END SIGNATURE-------
PKI - the business case

- The Internet is an inherently open system. Its strengths are built around this openness, cheapness and ease of access.
- This openness is also a source of major threat to users of the Internet. The open nature of the system makes it relatively easy for web sites and Internet communications to be compromised.
- This leads to reduced user confidence and minimise the benefits that could be obtained from the use of the Internet.
- PKI can play an important role in providing needed security services including authentication, non-repudiation, confidentiality and integrity.
Background

- 1989 – Commonwealth *Privacy Act, 1998*
- 1992 – Australia adopts OECD Guidelines for the security of information systems
- 1996 – Standards Australia SAA MP75 Report
  - Strategies for the Implementation of a Public Key Authentication Framework (PKAF) in Australia
- 1997 – *Investing for Growth*, the Government’s online agenda
- 1997 – OGIT initiates Project Gatekeeper
Aims of the strategy

- To establish a rational voluntary mechanism for the implementation of PKT by government agencies
- To facilitate interoperability and allow users to choose from a panel of service providers whose products and methods of delivery have been evaluated and accredited to meet prescribed government standards for integrity and trust
- To provide an operational mechanism to manage the Commonwealth’s activities and interests in the area of PKT
Gatekeeper policy development

- GPKI Branch
  - Manage the Gatekeeper Strategy and accreditation process
  - Advise Government agencies on the use of PKT
  - Research into legal, operational and technical issues and consult with stakeholders

- GPKA
  - The authority established to advise on policy and standards and to oversee the accreditation of service providers
GPKA composition

Members
- Office for Government Online (Chair)
- Attorney-General’s
- ATO
- Australian Procurement and Construction Council
- Business Entry Point
- Centrelink
- DSD
- HIC
- NOIE

Observers
- Australian Information Industries Association
- Australian Electrical and Electronics Manufacturers Association
- Privacy advocate

Government Online
GPKA functions

- Develops policy for GPKI
- Issues and revokes accreditation
- Monitors and adjusts standards as required
- Monitors standards compliance
- Point of contact for GPKI
Gatekeeper policy framework

- **September 1998** – Dept Prime Minister and Cabinet mandated:
  - Commonwealth agencies acquiring new encryption capability can purchase only from the DSD Evaluated Products List (EPL)

- **July 1999** – Cabinet decided:
  - Any future authentication certificates issued by Commonwealth agencies to business and individuals must be Gatekeeper compliant
Gatekeeper privacy and security

- Commonwealth Privacy Act 1988
  - Eleven Information Privacy Principles
- Protective Security Manual
  - Government policy on information and physical security and risk assessment
- ACSI-33
  - Security guidelines for Government IT systems
- ACSI-37
  - Security requirements for Government IT systems at the Highly protected classification
Gatekeeper accreditation

- A rigorous accreditation process ensures that transactions using digital certificate and public key technology from Gatekeeper accredited Certification and Registration Authorities provides a high level of trust to both agencies and users.
- Accreditation by the GPKA confers a recognised trusted status to companies supplying CA services to the Commonwealth.
Gatekeeper accreditation

- Privacy considerations
- Legal and liability position of the Commonwealth
- Security policy and planning
- Physical security
- Technology evaluation
- Certification Authority administration
- Certification Authority policy
- Personnel vetting
- Contracts
  - Preferred supplier
  - GPKA Head agreement
Gatekeeper accreditation

- **Australian Taxation Office**
  - Granted full Gatekeeper accreditation on 16 June 2000

- **Certificates Australia Pty Ltd (CAPL)**
  - A division of Baltimore
  - Granted entry-level accreditation on 24 May 1999

- **eSign**
  - Australian partner of VeriSign
  - Granted entry-level accreditation on 31 March 2000

Note: **Entry level accreditation** allows organisations to issue Gatekeeper Type 1 Grade 1 certificates that are for use in circumstances involving non-sensitive information and no financial risk
Gatekeeper accreditations in progress or planned

<table>
<thead>
<tr>
<th>SecureGate</th>
<th>Secure Network Solutions</th>
<th>KPMG</th>
</tr>
</thead>
<tbody>
<tr>
<td>KeyPost</td>
<td>Globesmart</td>
<td>Adacel</td>
</tr>
<tr>
<td>Telstra</td>
<td>Australian Health network</td>
<td>Health Insurance Commission</td>
</tr>
<tr>
<td>eTax CPA</td>
<td>KNX (Asia Pacific) Pty Ltd</td>
<td>Maddock, Lonie and Chisholm</td>
</tr>
</tbody>
</table>
Agencies implementing PKI

- **Australian Taxation Office**
  - *A New Tax System (GST)*
  - 200,000 plus certificates to businesses

- **Health Insurance Commission**
  - Location certificate
  - Health Care Provider certificate

- **Australian Customs**
  - Secure e-mail
  - Customs clearance online

- **Austrade**
  - Export Market Development Grants Scheme
  - Electronic Lodgment of Grant Claims (e-Lodge)
Gatekeeper futures

- **Gatekeeper 2**
  - A review of the original *Gatekeeper* report to encompass developments in standards, policies and practices since its release
  - Based on wide consultation

- **Gatekeeper Accreditation Certificate**
  - To be issued to Gatekeeper accredited CA’s
  - Will facilitate interoperability and cross recognition
  - CA’s will maintain unique certificate policies
  - To be recognised internationally
Gatekeeper futures

- Cross-recognition
  - Singapore
  - Hong Kong
  - USA
  - Canada
  - APEC initiative

- Gatekeeper - a Commonwealth, State and Territories PKI strategy
  - A working party is being established to look at potential for a national approach to PKI
ABN-DSC

- An ABN based digital signature certificate
- A mechanism to foster B2G and B2B e-Commerce
- A common digital certificate profile and core certificate policy
- To be issued by any Gatekeeper accredited CA
- To be used by Commonwealth agencies to identify businesses online
Gatekeeper and the ABN-DSC

GATEKEEPER compliant certificates issued by Government agencies

ABN-DSC Certificates

ATO Certificates

GATEKEEPER compliant certificates Issued by private sector CA’s
Online resources

http://www.govonline.gov.au

http://www.gatekeeper.gov.au

- **Gatekeeper**: a strategy for public key technology use in the Government
- Accreditation criteria
- Background and FAQs
Gatekeeper contacts

**Accreditation**
Doug Conn  
Phone: (02) 6271-1531  
E-mail: doug.conn@ogo.gov.au

**Strategy and Planning**
Glen Nicolson  
Phone: (02) 6271-1530  
E-mail: glenton.nicolson@ogo.gov.au

**Legal and Regulatory**
Ian Booth  
Phone: (02) 6271-1230  
E-mail: ian.booth@ogo.gov.au

**Implementation**
Udo Rockmann  
Phone: (02) 6271-1519  
E-mail: udo.rockmann@ogo.gov.au
Questions