

PUBLIC KEY INFRASTRUCTURE (PKI): AN AUSTRALIAN SOLUTION

JENNIFER SEBERRY

Centre for Computer Security Research
University of Wollongong, NSW, Australia
Jennifer_seberry@uow.edu.au

ABSTRACT:

- The Australian Government solution for a PKI infrastructure to allow businesses to conduct secure interactions with the Government

Components of a PKI

- Certification Authorities
- Registration Authorities
- Certificate or key holders
- Relying parties
- Repositories

Employing Digital Certificates

- One of the primary reasons why digital certificates have been implemented using fit-for-purpose designed applications is that most applications employed by Internet users vary greatly in the manner in which they handle digital certificates.

Employing Digital Certificates

2.

- There is growing pressure on application developers to create open standards where digital certificates can be employed and used in the same manner across all Internet applications.
- In the meantime, ‘central validation’ or ‘trust centre’ type facilities, where digital certificates from multiple providers are validated, are warranted.



Business Continuity and Implementation Considerations

- In developing a case for PKI, agencies will need to consider some important continuity issues, particularly where information is encrypted. An agency's ability to continue business might be severely hampered if the information cannot be accessed for some reason

Record Keeping Implications

- Agencies should consider how records subject to authentication and encryption processes will be managed and stored, taking into account privacy and security requirements.
- The National Archives of Australia is developing record keeping guidelines for agencies that use authentication and encryption processes.

Public Key Technology

- Public Key Technology (PKT) is used within PKI to provide users of the technology with the ability to communicate with confidence in an electronic environment.

.....cont.

Public Key Technology 2

- In order to do this, they need to know:
 - authentication
 - integrity
 - non-repudiation
 - confidentiality

How PKI Works

- For two people to communicate electronically with each other, they need to digitally sign and protect their messages. To do this they use 'public and private keys' to digitally sign and verify messages, prove who they are and encrypt (or protect) the content of their message.

A Typical PKI Process Flow

The general process flow in a PKI environment is as follows:

- An applicant applies to a CA or RA for a digital certificate.**
- The CA engages a Registration Authority (RA) to undertake verification of the applicant's identity.**
- The RA advises the CA that identity has been established and that keys and certificates can be issued.**

»

.....cont

A Typical PKI Process Flow 2

- The CA issues keys and certificates to the applicant.
- The Subscriber can then digitally sign an electronic message with their private key to ensure sender authentication, message integrity and non-repudiation and send the message to a relying party.

»

.....cont

A Typical PKI Process Flow 3

- The Relying Party receives the message and verifies the digital signature.
- The Relying Party then accepts or rejects the certificate depending on the result returned from the CRL and/or their own business judgement.

A Digital Signature Is Not the Same As a Digitized Signature

- A digitized signature is a computerized image of the written signature of an entity.
- A digital signature is a cryptographic technique that encrypts a document by applying a mathematical algorithm with a Certificate Holder's private key

How to Use Digital Signatures

- Digital signatures can function on electronic documents in the same way as physical signatures do on paper
- they can be used to automate transactions that are currently carried out on paper.
- Digital signatures can be applied to email, Internet transactions, World Wide Web pages and more.

Gatekeeper – the Australian Commonwealth Government Policy

- Gatekeeper is the application of policies and practices, particularly in the areas of privacy, security and liability. It is also the application of applicable law such as *The Privacy Act (Cth)* 1988 and *The Electronic Transaction Act (Cth)* 1999 and the application of technologies such as PKI and digital certificates.

Australian Government Requirements

- Australian Commonwealth agencies wishing to use digital certificates to identify their clients and trading partners are required to use Gatekeeper-accredited services and service providers.
- Gatekeeper certificates issued by an Australian State/Territory agency will be accepted by Australian Commonwealth agencies and vice versa.



The Australian Business Number Digital Signature Certificate ABN-DSC

- The Australian Business Number – Digital Signature Certificate (ABN-DSC) concept was developed to meet the Australian Government's policy requirement for a broad use digital certificate based around the Australian Business Number (ABN) to simplify business-to-government and business-to-business transactions online

Australian Government Requirements

- Australian Commonwealth Government decisions in 1999 have required Australian Commonwealth agencies to use the ABN, the Gatekeeper PKI framework and the ABN-DSC.

The ABN-DSC and Project Angus

- Project Angus is a working group involving the major Australian banks. It aims to establish a framework for e-commerce trust and authentication using the international Identrus' scheme

Business Authentication Framework (BAF)

- The BAF will provide a centralized facility that will verify the online identity of business users by securely passing ABN-DSC validation requests between business subscribers, government agencies and ABN-DSC providers.

The End of Trust As We Know It?

- In early 2001 Microsoft acknowledged that an errant code-signing certificate was in the wild. Verisign, a provider of fully integrated PKI managed service, erroneously issued two digital certificates in Microsoft's name to people posing as valid employees.

Conclusion

- The PKI infrastructure adopted in Australia is only one of many authentication technologies that can be used.
- PKI together with biometric authentication is thought to provide a high level of confidence for on-line business with the Australian Government

Other Concerns

- Countries with much larger populations than Australia need to consider the most appropriate structures for PKI. How hierarchical should it be?
- What of other community needs when individuals do not have an Australian Business Number, is a Government mandated solution which is right for them?

THE END