



Secure Electronic Environment (S.E.E.)

Paper 14 – International and New Zealand PKI Experiences Across Government

5th May 2003

Version 1.0

1	Introduction	3
1.1	Definitions	3
1.1.1	Public Key Infrastructure, PKI	3
1.1.2	Certificate Authority, CA	3
1.1.3	Digital Certificate	3
1.2	Why are Digital Certificates important?	3
2	Overseas Government experiences	4
2.1	Hong Kong	4
2.2	Finland	4
2.3	Germany	4
2.4	US	5
2.5	Australia	6
3	New Zealand Government Experiences	6
3.1	Current Use of Digital Certificates	6
3.2	Exiting of a Certificate Supplier	7
4	Other Observations	7
4.1	Rationalisation of the PKI market	7
4.2	PKI vulnerability impacts	7
5	Conclusions Drawn	8
5.1	International Experiences	8
5.2	New Zealand Experiences	9
6	Final Conclusion (PKI - Approach with caution)	9

1 Introduction

- 1 Over the last five years, several governments have implemented Public Key Infrastructure (PKI) systems. In addition, the New Zealand government has implemented several projects using PKI. This report documents the information learned from these projects. Note: Much of the international information is obtained from media sources, as such information is not typically available on an official website.

1.1 Definitions

1.1.1 Public Key Infrastructure, PKI

- 2 A Public Key Infrastructure (PKI) is a system of digital certificates and Certificate Authorities that verify and authenticate the validity of each party involved in an Internet transaction.

1.1.2 Certificate Authority, CA

- 3 A Certificate Authority (CA) is a trusted organization or company that issues digital certificates used to create digital signatures and public-private key pairs. The role of the CA in this process is to guarantee that the company or individual granted the unique certificate is, in fact, entitled to it. A CA is a critical component in data security and electronic commerce because they provide greater assurance that the two parties exchanging information are really who they claim to be.

1.1.3 Digital Certificate

- 4 A Digital Certificate is the digital equivalent of an ID card used in conjunction with a public key encryption system. Also called "digital IDs," digital certificates are issued by trusted parties known as certification authorities (CAs) after verifying that a public key belongs to a certain user (company or individual). The certification process varies depending on the CA and level of certification.

- 5 There are many types of digital certificates:

- E-Mail Certificates - used to identify an individual or company, and preserve the confidentiality and integrity of a message
- Browser Certificates - used to identify a browser session, and preserve the confidentiality and integrity of an online transaction
- Server (SSL) Certificates - used to identify a server, and preserve the confidentiality and integrity of an online transaction
- Software Signing Certificates - used to identify a software manufacturer, and confirm the integrity of a software package

1.2 Why are Digital Certificates important?

- 6 Core Internet protocols such as TCP, IP, UDP, DNS and HTTP do not support fundamental security properties of integrity, confidentiality or authenticity. The digital certificates provided by a PKI are a popular method to provide security on the Internet, because they can offer a high standard of non-repudiation and provide strong authentication.

2 Overseas Government experiences

2.1 Hong Kong

- 7 Hong Kong's certification authority, Hongkong Post has only sold 110,000 e-Certs since it was introduced in 2000. It is taking another shot at popularising e-Cert, its digital signature service, by offering every smart ID card holder an option to embed an e-Cert in the card's memory chip for one year at no charge. From July, Hong Kong identity card holders will be issued smart ID cards to replace existing ID cards. The process will take four years.
- 8 [Copyright (c) 2003 South China Morning Post, 25th March 2003, SMART IDS PLAN GIVES A LIFELINE TO E-CERT HONGKONG POST PUSHES ITS ELECTRONIC SIGNATURE PRODUCT BY OFFERING IT FREE TO USERS OF THE NEW HK IDENTITY CARD]

2.2 Finland

- 9 Finland's Population Registration Centre started issuing chip-based ID cards to citizens over two years ago. For only 10 euros more, the government offered to load a digital certificate onto the cards for citizens. Only 10% or fewer have decided the money was worth it.
- 10 [Copyright 2003 Thomson Media Inc, 5th March 2003, DIGITAL SIGNATURE CARDS: FOR PROFESSIONALS ONLY?]

2.3 Germany

- 11 The country's two largest commercial banks, Deutsche Bank and HypoVereinsbank, launched tests last spring, loading certificates and keys onto consumer smart cards. HypoVereinsbank has issued far fewer cards for the test than it had originally planned (approx 150). The bank last spring had planned to issue 10,000 cards for the test, but decided it had an insufficient business case for this.
- 12 In 2001, organizers of a German government-funded Internet security project ordered 10,000 chip-based digital signature cards for the 15,000-plus student body of the University of Bremen, lawyers in the community and the city of Bremen in general. The project received an 8.7 million-euro grant from the federal government. The result: Fewer than 1% of the university students have requested the cards and associated card readers, despite heavily subsidized prices. While the students and other ordinary citizens conducted a combined 300 transactions per month with the digital signature cards in the last six months, the lawyers did 10 times as many during the same period - with only a combined 20 to 30 cards.
- 13 One of the country's four trust centers, organizations that issue digital certificates, has already effectively shut down. That centre, run by Deutsche Post, could not find enough business to meet expenses and stays open now only to maintain its existing certificate, sources say.
- 14 So, while early tests indicate signature cards hold some promise in the hands of professionals, large rollouts are unlikely for years to come. The expense and complexity of PKI, make prospects for anything more than scattered trials of signature cards look remote for the next few years, even in PKI-friendly Germany.
- 15 [Copyright 2003 Thomson Media Inc, 5th March 2003, DIGITAL SIGNATURE CARDS: FOR PROFESSIONALS ONLY?]

2.4 US

- 16 The United States General Accounting Office has just finished a report - "GAO-03-144: Progress in Promoting Adoption of Smart Card Technology". The report found there had been significant steps forward in the creation of a standard smart card ID that all U.S. government employees could use to enter buildings, for travel-related purposes and to make small payments. According to the report, 18 agencies had launched 62 smart card projects as of November 2002.
- 17 It found that the full cost of a smart card system can be greater than originally anticipated because of the costs of related technologies, such as PKI.
- 18 In July 2002, the Department of the Treasury announced plans to launch a pilot project to assess the use of smart cards for multiple purposes, including both physical and logical access. Treasury plans to distribute smart cards equipped with biometrics and PKI capabilities to approximately 7,200 employees during its pilot test. Treasury's project manager estimates the overall cost for the department wide effort at between US\$50 and US\$60 million.
- 19 A Department of Transportation smart card pilot project aims to distribute smart cards to approximately 10,000 FAA employees and contractor personnel for access to the department's facilities; costs for the FAA pilot project, which have not yet been fully determined, are likely to exceed US\$2.5 million.
- 20 At least US\$4.2 million was required to design, develop, and implement the WGA Health Passport Project (HPP) in Nevada, North Dakota, and Wyoming and to service up to 30,000 clients. A report on that project acknowledged that it was complicated and costly to manage card issuance activities. The states encountered problems when trying to integrate legacy systems with the smart cards and had difficulty establishing accountability among different organizations for data stored on and transferred from the cards. The report further indicated that help-desk services were difficult to manage because of the number of organizations and outside retailers, as well as different systems and hardware, involved in the project; costs for this service likely would be about US\$200,000 annually. WGA officials said they expect costs to decrease as more clients are provided with smart cards and the technology becomes more familiar to users; they also believe smart card benefits will exceed costs over the long term.
- 21 The US Department of Defence initially budgeted about \$78 million for the Common Access Card (CAC) program in 2000 and 2001 and expected to provide the device to about 4 million military, civilian, and contract employees by 2003. It now expects to expend over US\$250 million by 2003—more than double the original estimate. Many of the increases in CAC program costs were attributed by DOD officials to underestimating the costs of upgrading and managing legacy systems and processes for card issuance. Card issuance costs likely will exceed US\$75 million out of the over US \$250 million now provided for CAC through 2003, based on information provided by DOD. These costs are for installing workstations, upgrading legacy systems, and distributing cards to personnel.
- 22 According to DOD program officials, the department will likely expend over US\$1 billion for its smart cards and PKI capabilities by 2005. In addition to the costs mentioned above, the military services and defense agencies were required to fund the purchase of over 2.5 million card readers and the middleware to make them work with existing computer applications, at a cost likely to exceed US\$93 million by 2003. The military services and defense agencies are also expected to provide funding to enable applications to interoperate with the PKI certificates loaded on the cards. DOD provided about US\$712 million to issue certificates to cardholders as part of the PKI program but provided no additional funding to enable applications.

- 23 The Veterans Administration, which three years ago projected issuing 4.6 million smart cards so military veterans could access the agency via the Internet, now no longer expects its pilot to lead to a full-scale rollout. "Executive-level priorities had changed and support for a wide-scale smart card project had not been sustained," the report states.

2.5 Australia

- 24 A parliamentary inquiry into the Management and Integrity of Electronic Information by the Joint Committee of Public Accounts and Audit has been told the Gatekeeper standard is too expensive and difficult to implement.
- 25 The ATO paid more than A\$1.75 million for implementation, licences and maintenance of its PKI system in the past 12 months. The only other agency ready to implement Gatekeeper in the near future is Australian Customs, which will use PKI to identify parties communicating through its new Customs Connect Facility gateway and assure the integrity of messages.
- 26 National Office for the Information Economy said there was no indication Gatekeeper should be scrapped, but assumptions made three years ago about the growth of PKI in both government and non-government sectors had proved incorrect.
- 27 [© AUSTRALIAN 22nd April 2003, GATEKEEPER GOES MISSING]

3 New Zealand Government Experiences

3.1 Current Use of Digital Certificates

- 28 Digital certificates are typically used by the New Zealand government for business applications requiring strong authentication, confidentiality and integrity, such as:
- SEEMail - uses digital certificates for sending secure messages across the Internet. This system currently has over 30 agencies using it, with many others expected to join by the end of 2003.
 - The Treasury - uses digital certificates for browser authentication of Crown Financial Information System (CFISnet) users. There are approximately 290 users, of which 25% are internal Treasury users, 50% are from other government agencies, and 25% from SOEs and crown entities. The Treasury also uses digital certificates to authenticate users to its external workspace, to encrypt laptops, and for remote access authentication.
 - LINZ - uses digital certificates to identify individual users of the Landonline system. It currently has 4,000 users with a final intended audience of 8,000 users.
 - Health Sector - uses digital certificates for Health Providers to access to various health systems. The estimated audience is approximately 10,000 users.
 - Education Sector - uses digital certificates to identify particular staff at each tertiary provider. There are over 350 tertiary providers involved with the system.
 - The Ministry of Social Development has used elements of PKI in its business, since 1999, to encrypt login sessions and to authenticate users to applications. For MSD and CYF being their "own" CA has proven a very cost effective way for automated user management, in a number of critical infrastructure components. This has allowed them to manage approximately 9,000 users with an incremental cost of around NZ\$12/user.

3.2 Exiting of a Certificate Supplier

- 29 In 2002, the major supplier of digital certificates to government was BaycorpID. BaycorpID indicated its intention to leave the marketplace in December 2002, as they were unable to make the business economic. During the lead up to its deadline for closure of services, the quality of certificates and the level of service dropped significantly.
- 30 Agencies using digital certificates found they were at increased risk because:
- Supplier issues - They were unable to find an alternative supplier for new certificates, so new users would not be able to access their systems.
 - Application issues - Some applications were so tightly bound to the existing CA, that transition to a new CA was difficult.
- 31 For users such as the Treasury, and the Health sector, PKI was already a critical piece of internal infrastructure, used for purposes such as securing laptops, securing VPN access, and accessing web-based applications.
- 32 The Treasury has chosen to use internal expertise and self-issue certificates. This reduces its reliance on external certificate suppliers, but carries additional operational costs.
- 33 The Health sector has chosen to find another commercial supplier of certificates. Although this solves the pressing issue of certificate supply, it does not address the long-term issue of CA viability.

4 Other Observations

4.1 Rationalisation of the PKI market

- 34 Certificate Authorities appear to be consolidating, as they seek a sustainable business model:
- In New Zealand, BaycorpID has exited the CA market. Telecom is phasing out its SecureKey CA offering.
 - In the US, IBM has transferred its business to VeriSign.
 - In Germany, one of the country's four trust centers, organizations that issue digital certificates, has already effectively shut down. That centre, run by Deutsche Post, could not find enough business to meet expenses and stays open now only to maintain its existing certificates.
 - In the United Kingdom, Chambersign, one of the two Certificate Authorities used by the Government Gateway has exited the business. The Chambersign certificate holders have been given the option to transfer to the Royal Bank Scotland.
- 35 In addition, RSA Keon, one of the major providers of PKI technology, has sold its PKI business to the original developers, TFS Technology in Switzerland. Instead they are concentrating on zero-client based forms of authentication such as one-time tokens.

4.2 PKI vulnerability impacts

- 36 It is of concern that PKI technology has been used / evaluated by many organisations over the last five years, yet technical vulnerabilities are still being discovered. One implication is that

organisations have accepted the technology at face value, without seeking to identify vulnerabilities. In a similar fashion, this also casts doubt on the expertise of companies who sell PKI services, who had not discovered this vulnerability.

- 37 As an example - in August 2002¹, it was discovered that Microsoft's CryptoAPI had a vulnerability that could enable an attacker who had a valid end-entity certificate to issue a subordinate certificate that, although bogus, would nevertheless pass validation. CryptoAPI has been used by a wide range of applications since Windows 98, so this could enable a variety of identity spoofing attacks including:
- Setting up a web site that poses as a different web site, and "proving" its identity by establishing an SSL session as the legitimate web site.
 - Sending emails signed using a digital certificate that purportedly belongs to a different user.
 - Spoofing certificate-based authentication systems to gain entry as a highly privileged user.
 - Digitally signing malicious software using a fake Authenticode certificate supposedly from a software company that users might trust.
- 38 Microsoft released a patch for the problem on 05 September 2002. On 09 September 2002, they advised that some customers who installed the patch could see unexpected error messages when installing new hardware, or in some cases might be unable to install new hardware altogether. On 20 November 2002, an updated version of the patch was released to not only eliminate the problems with the 09 September patch, but also to eliminate a newly discovered variant of the original vulnerability that could enable an attacker to gain control over a user's system.
- 39 Depending upon how a PKI application was implemented, this vulnerability could have caused serious problems. For example, some agencies when receiving S/MIME signed messages, verify the signature, but then strip it, so as not to cause problems at the client desktop. If an agency had not kept a copy of the signed message, then doubt could be cast on the integrity of the message.

5 Conclusions Drawn

5.1 International Experiences

- 40 The following conclusions are drawn from the International experiences:
- The technology is very complicated, technical and expensive (Germany, US)
 - Business cases are uncertain - where there are no enabled applications, there are no motivated users
 - Citizen uptake will be significantly less than forecast (Hong Kong, Finland, Germany)
 - Subsidisation (of cards or readers) doesn't motivate users (Hong Kong, Finland, Germany)

¹ More information at <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms02-050.asp>

- PKI uptake is greatest when governments have regulated users to adopt it (Hong Kong, Australia) or used it internally (US)
- The full cost of a PKI system is greater than originally anticipated because associated costs are not taken into account (US)
- The commercial supply of certificates is not stable (Germany, UK, NZ)
- The full cost of a PKI system is never retrospectively calculated (all)
- Vendors do not implement PKI technology correctly and Governments do not test the technology sufficiently (Microsoft et al)

5.2 New Zealand Experiences

41 The following conclusions are drawn from the New Zealand experiences:

- The technology is very complicated, technical and expensive
- The full cost of a PKI system is never retrospectively calculated
- Auto-update service or security packs can break your PKI application (Microsoft)
- The technical skills of some of your users will be much less than you expect
- The helpdesk support cost during implementation will be higher than you expect
- End-user security will hamper implementation
- The withdrawal of a commercial CA service can threaten the entire project
- The availability, quality and performance of a CA's services (registration, CRL, renewal) may not always be as good as originally planned

6 Final Conclusion (PKI - Approach with caution)

- 42 Based upon overseas and New Zealand experiences, it is obvious that a PKI implementation project must be approached with caution. Implementers should ensure their risk analysis truly shows PKI is the most appropriate security mechanism and wherever possible consider alternative methods.
- 43 The following table draws upon the PKI experiences previously noted, and provides a list of warning signs. This warning is applicable at both an all-of-government and individual agency level. Obviously the more warning signs, the more closely the project should be scrutinised.

Warning Signs	Positive Signs
The vendor who proposed you implement PKI, sells PKI	Your security vendors are separate from your PKI vendors. (Ideally your security vendors sell a competing PKI product)
Your vendor assures you that they can implement PKI, because they have all the relevant experience	You have spoken in depth to government agencies that have implemented PKI
PKI is the latest technology, and has been recommended by your vendor	You have considered several alternatives including PKI and it is the best
You have not considered business compliance costs, including time to get system going, downtime, minimum hardware/bandwidth requirements, etc	The business compliance costs stack up

Warning Signs	Positive Signs
You accept at face value that major vendors have implemented PKI correctly	You have extensively tested to satisfy yourself that your vendor has implemented PKI correctly
You accept the vendor's word that PKI transactions will always be usable in the future	You have considered the risks and have developed processes to manage them, so you can cope with expired certificates, obsolescence in PKI technology, etc.
Your PKI solution is tightly coupled to a single CA provider	Your PKI solution can work with multiple CA providers
You have no experienced staff and are involving vendors	You have staff with a sound technical knowledge of PKI to a level that allows for solid planning (both risk mitigation and implementation planning)
Your user audience is large (more than 1,000)	Your user audience is small
You have little control over your users PCs and technical environment	You can control your users PCs and technical environment
Your application is thin-client or requires downloads or modifications to the user's PC	Your application is zero-client
Your application is simple and manages PKI without the user being aware it exists	Your application requires multiple complex steps to be undertaken by the user, or requires them to make judgements about the validity of a security statement e.g. "The name of this server does not match the name in the digital certificate – do you wish to proceed?"
Your commercial CA has a small number of users, with little ability to achieve economies of scale.	Your commercial CA is well established with a large number of users.
The supporting PKI processes for CA and RA are complex, slow and partially automated or worse, manual.	The supporting PKI processes for CA and RA are simple, fast and fully automated.
The infrastructure costs are high.	The infrastructure costs are low.