Release of Guidelines by the Privacy Commissioner for Agencies using PKI: implications for Agencies, government contractors and private sector organisations

*By Vincent Liu, Freehills**

Vincent Liu is a solicitor in the Canberra office of Freehills. He specialises in privacy, commercial litigation, corporate insolvency and administrative law.

1. Introduction

The Guidelines issued by the Federal Privacy Commissioner on 21 December 2001 entitled "*Privacy and Public Key Infrastructure: Guidelines for Agencies using PKI to Communicate or Transact with Individuals*" ("the Guidelines") apply to Commonwealth government agencies ("Agencies") in their use of Public and private key infrastructure technology in dealing with individuals.

In 1997, the Commonwealth Government initiated the Gatekeeper Program as a strategy for the implementation of Public Key Infrastructure ("PKI") for Agencies as a means of enhancing service delivery and streamlining government transactions internally. The use of PKI in Agencies has significant privacy implications for those individuals who wish to conduct their transactions with the relevant Agency electronically.

This paper will briefly describe what public key technology is, followed by a close examination of the Guidelines issued by the Privacy Commissioner and the liability of Agencies and government contracted service providers ("contractors") for interference with the privacy of an individual.

1.1 Personal information and Government Agencies

Agencies have been regulated by the Information Privacy Principles set out in the *Privacy Act* 1988 (Cth) ("the *Privacy Act*") since 1988. The Information Privacy Principles regulate the collection, use and disclosure of personal information by Agencies.

Personal information is defined in the *Privacy Act* to include information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent or can be reasonably ascertained from the information or opinion.[1]

The *Privacy Act* protects individuals in both private and business capacities from interference with their privacy by Agencies:

(a) in their private (non-business) capacity as clients, tax-payers and otherwise as recipients of government services and customers of Agencies;

(b) who are designated representatives of corporate entities; or

(c) who are sole traders or partners involved in business activities.

Although the Guidelines are not binding on an Agency in its use of PKI in electronic communications and transactions with individuals, breach of the Guidelines may lead to a finding by the Commissioner that the Agency has interfered with the privacy of an individual.

The privacy regime provides penalties for an interference with privacy. The Privacy Commissioner is able to order an Agency which breaches one or more of the Information Privacy Principles to redress loss or damage or pay compensation suffered by an individual.[2]

Perhaps more importantly, an Agency or contractor which is found to have interfered, or allegedly interfered with an individual's privacy may end up in a public relations predicament: on the front pages of the papers or listed on the internet by informal consumer and privacy interest groups. Recent experience in the United States has seen the emergence of a large number of self-appointed privacy watchdogs, identifying and listing privacy breaches for all to see, and rating web pages with privacy standards. This may have political implications for the relevant Agency and the portfolio Minister.

1.2 Relevance to Private Sector Organisations

PKI technology is in wide spread use in the United States, United Kingdom and Canada especially in the finance and health care sectors.[3] The adoption of PKI technology by Australian private sector organisations has been slow, with only approximately 21 per cent of Australian private sector organisations using some sort of encryption technology.[4] This suggests that the Commonwealth Government is spearheading the use of PKI in Australia.

The Guidelines issued by the Privacy Commissioner only relate to Agencies, they do not relate to private sector organisations. For those organisations, which are utilising PKI, the National Privacy Principles rather than the Information Privacy Principles will apply to regulate the collection, use and disclosure of personal information in the PKI process.[5] Such organisations, in ensuring that they comply with the National Privacy Principles, may have some regard to the Guidelines as they will provide some guidance as to how the Commissioner will decide whether there has been an interference with the privacy of an individual by an organisation in its use of PKI.

The Privacy Commissioner has stated in the Guidelines that:

> *"The guidelines were developed to address the particular risks associated with government use of PKI with its individual clients. Where private sector organisations*

use PKI applications in on-line dealings with their customers, there will also be privacy issues to be considered. However, the context and solutions for the private sector are likely to be different, at least in some respects, than those for the public sector. Wide consultation specifically with the private sector stakeholders would be critical before PKI privacy guidelines could be developed for this sector.'[6]

The Privacy Commissioner has also stated in the Guidelines that the most appropriate time to consider private sector issues will be in the context of the proposed review of the guidelines in eighteen months.[7]

In the meantime, private sector organisations may review the Guidelines for assistance as to the Commissioner's view on certain issues relating to the use of PKI and how the Commissioner may determine a complaint involving an interference with the privacy of an individual by private sector organisations using PKI technology.

2. Public Key Technology and Public Key Infrastructure

2.1 Public Key Technology

Public Key Technology ("PKT") is the term used generally to refer to a method of encryption of electronic data sent from one person to another which relies upon the use of two keys – a public key and a private key.[8] These keys are created at the same time and consist of randomly generated numbers and related algorithms that have a special relationship to each other. It is not possible to deduce the value of one key from the other. Data that is encrypted with one key can only be decrypted with the related key and not in any other manner.[9]

The private key's primary role is to decrypt information that has been encrypted by somebody else using that particular individual's public key. The private key can also be used to encrypt information in order to help a sender authenticate information sent to a receiver. This means that a person can encrypt information with a private key, and the person to whom the information is sent can decrypt the information using the public key.[10]

The subscriber (defined below) or the holder of the private key must keep the private key secret. The public key may be made known to others and may be made publicly available. Two key pairs are usually used in the signing and encryption of electronic communication, a signing key pair (to authenticate, verify the integrity of, and prevent repudiation of a communication) and an encryption pair (to provide the confidentiality function of PKI).[11]

2.2 Public Key Infrastructure

PKI is a system of cryptographic technologies and standards, management entities, management processes, policies and controls, to enable the widespread and open use of public key technologies.[12] A PKI generally has the following four functions:

(a) Authentication that an electronic communication was in fact sent from one person to another through the use of the signature key pair;

(b) Assuring a receiver of an electronic communication of its integrity (ie that the document has not been amended by another party in transit) through use of the signature key pair and review of the hash value of the communication. A "message digest" or "hash", is a number produced upon signing of the communication. Any amendments to the communication will produce a different hash value. If the communication is altered in transit then the hash value received will be different from the original hash value produced on signing;

(c) If an electronic message is signed with a digital signature, then it will be very difficult for a particular holder of a signature private key to deny that he or she has applied the signature key to the communication or transaction unless it can be shown that the private key was applied by someone other than its unique and rightful holder; and

(d) Protecting the confidentiality of an electronic communication through use of the encryption key pair.[13]

The parties who may be involved in the PKI process may include the following:

(a) **Certification Authorities (CAs)** – These are certified bodies that issue and revoke digital certificates. A digital certificate is an electronic document signed by a CA that associates a subscriber with a key pair;

(b) **Registration Authorities (RAs)** – These are entities which register applicants for keys and certificates. They conduct the initial verification of a potential subscriber's identity and/or attributes;

(c) **Subscribers** – digital certificate holders; and

(d) **Relying parties** – entities who rely on the contents of a digital certificate in communicating with subscribers.

The main operations and processes of PKI include the following:

(a) **Registration** – the process whereby a potential subscriber makes themselves and/or their relevant attributes known to the CA directly (or through an RA);

(b) **Key generation** – the generation of one or more key pairs by the CA or by the subscriber;

(c) **Certification** – the issue by a CA of a digital certificate to a subscriber;

(d) **Creation of directories** – which may store public keys, digital certificates or certificate revocation lists;

(e) **Certificate expiry** – the allocation of a period for which a digital certificate will remain valid; and

(f) **Certificate revocation** – the revocation of a digital certificate prior to its expiry (eg where the private key has been compromised).[14]

3. Commonwealth Government's Gatekeeper strategy

3.1 History of Gatekeeper Project

Gatekeeper is the Commonwealth Government's strategy for the policy and implementation of PKI for Agencies as a means of enhancing service delivery and streamlining government transactions internally.[15] All Australian states and territories have agreed in-principle to the adoption of the Gatekeeper strategy.[16]

The Commonwealth decided to take the lead in the development of a national framework for the authentication of users of electronic on-line services by establishing Project Gatekeeper ("Gatekeeper") in October 1997. Gatekeeper had three identifiable aims:

(a) to establish a rational voluntary mechanism for the implementation of PKT by Agencies;

(b) to facilitate interoperability and allow users to choose from a panel of service providers whose products and methods have been evaluated and accredited to meet prescribed government standards for integrity and trust; and

(c) to provide an operational mechanism to manage the Commonwealth's activities and interests in the area of PKT.[17]

The key requirements for Gatekeeper included interoperability, addressing privacy issues, confidentiality, non-repudiation, integrity, ease of use, marketability and archiving.[18] The Commonwealth Government's publication named *Gatekeeper: A strategy for public key technology use in Government* 1998 ("the Gatekeeper Report") was released in 1998 after extensive consultation with a number of government departments and review of the relevant issues relating to the implementation of PKT.

3.2 Gatekeeper: Current arrangements

Gatekeeper is currently managed by the National Office for the Information Economy ("NOIE") which is concerned to ensure the secure issue and use of Gatekeeper digital certificates.[19] NOIE also manages the accreditation of CAs and RAs and sets the accreditation criteria in relation to CAs and RAs.[20]

The Gatekeeper Policy Advisory Committee ("GPAC") includes representatives of the Commonwealth Government, State and Territory Governments, industry representatives and a privacy consultant, and advises NOIE on the policy framework for Gatekeeper.[21]

3.3 Privacy protection

Some of the disadvantages and privacy risks regarding the use of PKI are listed below in paragraph 4.1.
In addition to the Guidelines issued by the Commissioner, there are a number of means by which the privacy of an individual is protected under the Gatekeeper strategy:

(a) **Gatekeeper Head Agreements** – which contractually bind Gatekeeper accredited CAs and RAs to the Gatekeeper accreditation criteria on an ongoing basis.

(b) **The Gatekeeper accreditation criteria** – regulate CAs and RAs collection, storage, use and disclosure of personal information.

(c) **Privacy Recommendations** to the Chief Executive Officer, Office of Government On-line in relation to the use of Gatekeeper Certificates by Individuals - a set of Guidelines for privacy protection which contain privacy requirements in addition to the Information Privacy Principles.

The Gatekeeper Report emphasises the need for the use of PKT to comply with the relevant Information Privacy Principles and the privacy protection set out in the *OECD Guidelines for Cryptography Policy 1997*.[22] The Gatekeeper Report also emphasised the importance that the framework include a clear commitment to avoid the system being viewed as a national identification scheme. The three important aspects to this framework are:

- the freedom for individuals to possess multiple key pairs;
- the ability to hold key pairs with a variety of different labels or pseudonyms; and
- the dispersal of certificate revocation lists.[23]

The primary purpose of the Guidelines issued by the Privacy Commissioner is to assist Commonwealth Agencies in implementing Gatekeeper. In the interpretation of the Guidelines, it is important that one examines their provisions in this context.

4. Guidelines for Agencies using PKI to communicate or transact with individuals

In late 2000, NOIE invited the Privacy Commissioner to consider developing best practice guidelines for Agencies to assist them in designing and implementing PKI applications and processes when using Gatekeeper digital certificates with individual clients.[24] These Guidelines were issued by the Privacy Commissioner on 21 December 2001.

4.1 Privacy advantages and disadvantages of PKI technology

PKI has enormous privacy advantages for an individual dealing with an Agency or organisation. By being able to encrypt and decrypt electronic communications, an individual can ensure that his or her electronic communication will remain confidential and that it may not be read by any third party. The use of the signature key pairs also ensures that the receiver of the electronic communication can feel confident that the electronic communication came from the sender and not another person.[25]

Through use of the authentication key, individuals can be sure that a received electronic communication was in fact sent by the person claiming to have sent it and not another person. It will also be possible for an individual to check whether the communication sent to him or her has been altered in any way between encryption by the author and his or her decryption (see above).[26]

Some of the potential privacy risks outlined by the Privacy Commissioner in the Guidelines include the following:

(a) If Agencies or their contractors collect more personal information

than is necessary for their functions or activities in ascertaining the identity of the individual, then the collection and registration phase of PKI may interfere with the privacy of an individual.[27]

(b) A potential privacy risk arises from the browsing of public key directories or the content of public key certificates which are publicly available to third parties. These documents may contain personal information and a review of these documents by third parties may reveal that an individual has an association with a particular Agency. Third parties may also be able to track a pattern of transactions through associating the name on the digital certificate with the certificate's serial number.[28]

(c) If servers hosting public key directories, certificate revocation lists and other PKI transactions, and maintained by CAs and Agencies, keep logs of accesses and on-line transactions, this may allow CAs and Agencies to use logs to track an individual's transactions and then compile profiles of individuals using these services.[29]

(d) If keys are not generated under the control of the individual concerned or the private key leaves the possession of the subscriber without strong security precautions being taken, then it may be possible for the subscriber to be convincingly impersonated by another person when communicating with a third party.[30]

(e) If individuals use one digital certificate in their dealings with all Agencies, then a particular Agency may be able to use the information gathered from the individual's digital certificate to compile a profile of the individual in his or her dealings with other government Agencies.[31]

Many of the issues raised above have the potential to become interferences with the privacy of an individual subscriber by either the Agency or the CAs or RAs under the *Privacy Act*. For example, if an Agency uses its logs of accesses and on-line transactions to track an individual's transactions and then to compile profiles of individuals using these services, this may amount to a use of personal information by the Agency for the secondary purpose of monitoring these individuals without their consent. If reasonable security measures are not put in place to protect private keys or digital certificates held by an Agency under escrow, then an Agency may be found to have breached the privacy of an individual where an impostor obtains and uses the private keys or digital certificate.

4.2 The content of the Guidelines

The Guidelines issued by the Privacy Commissioner are intended to address the privacy risks raised above in relation to an Agency's use of PKI technology in its dealings with individuals. Whilst the Guidelines are not legally binding upon Agencies, the Guidelines do provide assistance as to the factors that the Commissioner will take into account when handling a complaint about the use of PKI by the Agency.[32] The Guidelines issued by the Privacy Commissioner cover the following topics:

(a) Guideline 1 – Agency client choice on use of PKI applications

Guideline 1 provides that an Agency must provide its clients with a choice as to whether to use PKI for a particular transaction and to offer them an alternative means of service delivery such as transactions over the telephone or through the post. The alternative means does not have to be an on-line alternative.[33]

An Agency must also provide its clients with sufficient information on the advantages, disadvantages and risks associated with PKI and the alternatives offered so as to allow its clients to make an informed decision as to whether to use PKI for a particular transaction. This Guideline is consistent with Guideline 2 of the *OECD Guidelines for Cryptographic Policy 1997*, agreed to by Australia, which states that users should have a right to choose any cryptographic method subject to applicable law.[34]

(b) Guideline 2 – Awareness and education

Guideline 2 provides that an Agency and its contracted PKI service providers should co-operate closely to ensure that clients are fully informed of the proper use of PKI and of the risks and responsibilities associated with the use of PKI including the secure management of private keys. Some of the means suggested by the Commissioner by which an Agency or a contracted PKI service provider could promote awareness and education on the use of PKI technology include provision of information to clients about security risks and CAs ensuring that subscriber agreements impose obligations relating to security upon clients in relation to their use of PKI.[35]

(c) Guideline 3 – Privacy Impact Assessments

Guideline 3 provides that Agencies should undertake a Privacy Impact Assessment before implementing a new PKI system or significantly revising or extending an existing PKI System.[36] Appendix 1 of the Guidelines includes a model privacy impact assessment which could be used by Agencies in order to comply with Guideline 3.[37] Use of a privacy impact assessment by an Agency may allow the Agency to identify the business need for the use of PKI and explore other alternatives available to PKI. Privacy Impact Assessments provide a means by which Agencies could identify the privacy risks associated with a proposed PKI system so that these risks may be addressed when PKI systems are being designed, implemented, revised or extended. The process is a tool to assist Agencies to minimise intrusiveness, maximise fairness and satisfy expectations of an individual dealing with the Agency.

(d) Guideline 4 – Evidence of identity

Guideline 4 seeks to ensure that an Agency or contractor will only collect the personal information from an individual in the registration stage of the PKI process that is necessary for the relevant PKI business transaction, and that the collection of personal information relating to evidence of

identity of the subscriber is not unnecessarily intrusive.[38]

(e) Guideline 5 – Aggregation of personal information

Guideline 5 prohibits the creation or use of a detailed history of client transactions by Agencies or contractors except to the extent that this is required for system maintenance or evidentiary purposes. Further, Agencies and contractors may not collect personal information that is not necessary, or directly related to the PKI business transaction. Guideline 5 ensures that CAs and Agencies do not use logs of accesses and on-line transactions of subscribers to track an individual's transactions and then compile profiles of individuals using these services.[39]

(f) Guideline 6 – Single or multiple certificates

Guideline 6 provides that Agencies should allow clients to use more than one digital certificate, if these are fit for the purpose of the relevant application. This Guideline will prevent Agencies from being able to use the information gathered from an individual's single digital certificate to compile a profile of the individual in his or her dealings with other government Agencies.[40]

(g) Guideline 7 – Subscriber generation of keys

Guideline 7 provides that if an Agency issues certificates or contracts for their issue, the Agency should allow its clients the option of generating their own keys, provided that the Agency is satisfied that the subscriber key generation can be implemented securely.[41] This Guideline addresses the issue that from a security viewpoint, a private key will be better protected if it is generated by the subscriber.

(h) Guideline 8 – Public key directories

Guideline 8 provides that an Agency's clients should be allowed to opt out of including their public keys in a public key directory where the directory is published.[42] Because of the potential privacy risks involved in publishing one's public key in a published key directory, individual clients may, under this Guideline, be given the opportunity of opting out of having their public key listed on the directory and for the public key to be sent on a case by case basis to third parties with whom they propose to transact for the purposes of:

(1) authentication of the identity of the subscriber through use of the authentication public key; and

(2) access of a subscriber's encrypted message through use of the subscriber's confidentiality public key.

(i) Guideline 9 – Pseudonymity and anonymity

Agencies should provide their clients with anonymous and pseudonymous options for transacting with them, to the extent that this is not inconsistent with the objectives and operation of the relevant on-line application.[43] Even though, there is no equivalent of National Privacy Principle 8 in the Information Privacy Principles, the Commissioner is of the view that it will be good practice for an Agency to allow individuals to transact anonymously or pseudonymously.

4.3 Contrast with New Zealand Guidelines

The New Zealand Government also issued *Draft Interim Guidelines for the use of Public Key Technology in Government* in November 2000 ("NZ Guidelines") pursuant to the Secure Electronic Environment Project ("SEEP").[44] These Guidelines serve as a useful contrast by which to examine the adequacy of the Commissioner's Guidelines in Australia for the use by Agencies of PKI.

It is proposed under SEEP that the adoption of the NZ Government PKI be made mandatory for all public service departments, Crown entities, State Owned Enterprises, Crown Owned Companies, and other governmental organisations that fall within the commonly accepted definition of the NZ State Sector.[45] SEEP is a project for the development of a public key infrastructure for use among New Zealand Government agencies with the expectation that the policies and practices of New Zealand Government agencies will be able to be adopted by private sector organisations wishing to use PKT for their own purposes.[46]

It is interesting to note that the New Zealand Government has chosen to prescribe lengthy guidelines dealing with each aspect of the PKI process with some sections dealing with privacy rather than to provide general privacy guidelines in relation to the overall processes involved in PKI. For example, in relation to CAs, the NZ Guidelines provide that:

> *"The level of identification required for an individual to be issued with a digital certificate is very much dependent on the intended usage, other processes around granting access to a system and other uses to which the certificate could be put."*[47]

Another Guideline provides that:

> *"All private key handling including key generation, escrow, retrieval from escrow and token loading must be handled in a highly secure manner designed to avoid any potential for private key compromise."*[48]

There are also further detailed Guidelines dealing with the security of the private keys. However, from the author's review of the NZ Guidelines, they seem to cover certain topics such as private key protection in a more detailed manner than the Guidelines and neglect to mention other areas which have been set out by the Commissioner in the Guidelines such as subscriber generation of keys and aggregation of personal information. In this regard, the Australian Guidelines appear to have a broader application than the New Zealand Guidelines.

5. Potential application to private sector organisations and government contracted service providers

5.1 Government contracted service providers (RAs and CAs)

(a) Increasing numbers of RAs and CAs

According to the NOIE website, six organisations have achieved full Gatekeeper accreditation:

- Australia Post - 20 December 2001 as a Registration Authority;

- Telstra Corporation Limited - 9 October 2001 as a Certification Authority and Registration Authority;
- eSign Australia Limited - 5 April 2001 as a Certification Authority and Registration Authority;
- Health eSignature Authority Pty Ltd - 19 January 2001 as a Registration Authority - Extended Services;
- Baltimore Certificates Australia Pty Ltd (CAPL) - 20 November 2000 as a Certification Authority; and
- Australian Taxation Office - 16 June 2000 as a Certification Authority and Registration Authority.[49]

Other private sector organisations which have applied for Gatekeeper accreditation include SecureNet, KPMG Information Solutions, KNX Asia Pacific (Key Trust), ANZ Bank and 90 East.[50]

(b) Application of the *Privacy Act* and Guidelines to Commonwealth Government Contracted Service Providers

From 21 December 2001, the majority of businesses which provide services to Commonwealth Government or Agencies under a contract (referred to as "contractors") will be subject to the National Privacy Principles.[51] That regime will overhaul the way contractors collect, use and disclose personal information, that is, information which identifies an individual, or enables an individual to be identified. Previously, contractors were obliged to observe an "obligation of confidence" in respect of any personal information gathered in fulfilling that contract.[52] An "obligation of confidence" operates to prevent the use or disclosure of personal information without the consent of the government or government Agency. Contractors may also have been contractually bound under their contract for services with the Commonwealth to comply with the Information Privacy Principles.[53]

In limited circumstances, contractors may be exempt from a breach of the National Privacy Principles or requirements of an approved code where the contract between the contractor and the Commonwealth Government specifically authorises the action which constitutes a breach of the National Privacy Principles or an approved code.[54] However, if the contractor's act amounts to a breach of the contract, the contractor will not be shielded from the consequences of its interference with the privacy of an individual.[55]

Some contractors may fall into the categories of businesses and organisations exempted from the operation of the new privacy regime. For example, some may qualify as a "small business operator", which is defined as a business with an annual turnover of $3,000,000 or less.[56] However, the National Privacy Principles will apply to these contractors from 21 December 2002.[57]

Section 95B of the *Privacy Act* also requires an Agency entering into a Commonwealth contract to take contractual measures to ensure that the contracted service provider for the contract does not do an act, or engage in a practice that would breach an Information Privacy Principle if done or engaged in by the Agency. The Agency must also ensure that the Commonwealth contract does not authorise a contracted service provider for the contract to do or engage in an act or practice which would breach an Information Privacy Principle.

CAs or RAs who are contracted by the Commonwealth Government will have to comply with both the National Privacy Principles and their relevant contract with the Commonwealth. This is in addition to a contractual obligation under Clause 32.1 of the Head Contract[58] to comply with the Information Privacy Principles.

Contractors who may be accredited as a CA or a RA must ensure, in the registration stages of PKI, that they provide a privacy statement to individual subscribers outlining what type of information is collected by the contractor, why the information is collected, and the processes by which a user may gain access or complain to the contractor about its use of the information. Contractors may also need to seek the consent of an individual subscriber at this stage as to whether he or she wishes his or her public key to be included in any public key directories or certificate revocation lists. Contractors will also be required to provide access to the information collected by the contractor to the subscriber and allow him or her to correct any errors. Finally, one of the most important National Privacy Principles which may become a problem area for CAs would be NPP 4 relating to security of any private keys held by the CAs.

Contractors who have not as yet put in place steps to ensure compliance with the privacy regime may be found liable for breaches of privacy and may be ordered to pay compensation to individuals whose privacy may have been breached. Further, breaches of privacy may result in damage to the relationship between the contractor and the Commonwealth and may also damage the contractor's business reputation and its further dealings with other customers and clients.

(c) Recent case

Recently in the United States of America, a CA allegedly admitted that it issued two digital certificates to an impostor posing as a Microsoft employee. The CA discovered this approximately 2 weeks after allegedly issuing the certificates whilst conducting a background check based on information provided by the impostor.[59] This meant that unless a user took the initiative to manually check the CA's certificate revocation list before installing any software signed with these certificates, the users' computer would trust any program signed with the fraudulent certificates. The matter has been referred to the Federal Bureau of Investigation.

If this occurred in Australia in relation to a CA who is a government contracted service provider under the Gatekeeper project in relation to an individual, the contractor may be found to have disclosed personal information to a third party without the consent of the subscriber and the contractor may be found to be liable to compensate the subscriber for any loss suffered in relation to use of the digital certificates by the impostor.

6. Concluding Comments

The Privacy Commissioner's Guidelines on Privacy and Public Key

Infrastructure will have major implications for Agencies. A particularly significant issue involves the liability of contractors who are accredited by the Commonwealth as CAs or RAs for interference with the privacy of an individual. These organisations will have to ensure that they comply with both the Information Privacy Principles and the National Privacy Principles or an approved code. The Guidelines issued by the Commissioner will also apply to these organisations.

Further, these organisations may also be subject to further privacy regulation through their respective contracts with the Commonwealth. These organisations may have to conduct an audit of their personal information handling practices in relation to the use of PKI technology to minimise the risk of an interference with privacy. They will also be subject to potential liability for an interference with the privacy of an individual and may be ordered to pay compensation in certain cases.

---

* The author would like to thank Penny Karvouniaris for her assistance in conducting research for this journal article. The author would also like to thank Michael Will and Zoe McKenzie for their assistance in reviewing drafts and providing advice to the author in relation to the drafting of this article.

1 Section 6, *Privacy Act* 1988 (Cth).

2 Division 2, Part V of the *Privacy Act* 1988 (Cth).

3 "Canada presses on with PKI projects, but smart cards on back burner" (2001) Issue 6 *Card Technology Today* 4-5. See also "UK government trials PKI technology" (2001) Issue 4 *Card Technology Today* 4; Jan Lovorn, "The power of PKI"(2001) 22(12) *Health Management Technology* 20-22; Young Etheridge, "PKI – how and why it works" (2001) 22(1) *Health Management Technology* 20-22.

4 "PKI in Australia: Govt leads the way" (2001) http://www.zdnet.com.au/newstech/ebusiness/story/0,2000024981,20223332,00.htm.

5 The *Privacy Amendment (Private Sector) Act* 2000 (Cth) was passed by the Commonwealth Parliament on 6 December 2000 and will commence operation on 21 December 2001. This piece of legislation applies the National Privacy Principles to private sector organisations.

6 The Office of the Federal Privacy Commissioner, Privacy and Public Key Infrastructure: Guidelines for Agencies using PKI to communicate or transact with individuals (21 December 2001) at page 11.

7 Ibid at page 11.

8 "PKI in Australia: Govt leads the way" (2001) http://www.zdnet.com.au/newstech/ebusiness/story/0,2000024981,20223332,00.htm.

9 Roger Clarke, "Privacy requirements of public key infrastructure" (2000) 3(1) *Internet Law Bulletin* 2-6 at page 2. See also Privacy and Public Key Infrastructure: Guidelines for Agencies using PKI to communicate or transact with individuals (21 December 2001) at page 14 – 15.

10 "Cryptography and pretty good privacy" (1996) http://www.privacy.gov.au/publications/p7_3.doc. See also Privacy and Public Key Infrastructure: Guidelines for Agencies using PKI to communicate or transact with individuals (21 December 2001) at page 14 – 15.

11 Ibid at page 1.

12 The Office of the Federal Privacy Commissioner, Privacy and Public Key Infrastructure: Guidelines for Agencies using PKI to communicate or transact with individuals (21 December 2001) at pages 14 – 15.

13 "Cryptography and pretty good privacy" (1996) http://www.privacy.gov.au/publications/p7_3.doc. See also Privacy and Public Key Infrastructure: Guidelines for Agencies using PKI to communicate or transact with individuals (21 December 2001) at pages 14 – 15.

14 The Office of the Federal Privacy Commissioner, Privacy and Public Key Infrastructure: Guidelines for Agencies using PKI to communicate or transact with individuals (21 December 2001) at pages 14 – 15.

15 Office of Government Information Technology, "Gatekeeper: A strategy for public key technology use in the Government" (2002) http://www.govonline.gov.au/publications/GatekeeperStrategy.pdf at page 4.

16 The Office of the Federal Privacy Commissioner, Privacy and Public Key Infrastructure: Guidelines for Agencies using PKI to communicate or transact with individuals (21 December 2001) at page 16.

17 Office of Government Information Technology, "Gatekeeper: A strategy for public key technology use in the Government" (2002) http://www.govonline.gov.au/publications/GatekeeperStrategy.pdf at page vi.

18 Ibid.

19 The Office of the Federal Privacy Commissioner, Privacy and Public Key Infrastructure: Guidelines for Agencies using PKI to communicate or transact with individuals (21 December 2001) at page 16.

20 Ibid. See also Office of Government Information Technology (now NOIE), "Gatekeeper: Criteria for Accreditation of Certification Authorities" (2001) http://www.govonline.gov.au/publications/CA_AccreditationCriteria_v9.pdf.

21 Office of Government Information Technology, "Gatekeeper: A strategy for public key technology use in the Government" (2002) http://www.govonline.gov.au/publications/GatekeeperStrategy.pdf at page vii.

22 Ibid. See also Organization for Economic Cooperation and Development, "Guidelines for Cryptography Policy" (1997) http://www.cybercrime.gov/oeguide.htm. See also Patrick Fair, "GateKeeper: Setting Australia's standard for online security" (1998) 1(6) *Internet Law Bulletin* 85-88 at page 87.

23 Office of Government Information Technology, "Gatekeeper: A strategy for public key technology use in the Government" (2002) http://www.govonline.gov.au/publications/GatekeeperStrategy.pdf at page 10.

24 The Office of the Federal Privacy Commissioner, Privacy and Public Key Infrastructure: Guidelines for Agencies using PKI to communicate or transact with individuals (21 December 2001) at page 7.

25 Ibid at page 17.

26 Ibid at page 17.

27 Ibid at page 18.

28 Ibid at page 19. See also Roger Clarke, "Privacy requirements of public key infrastructure" (2000) 3(1) *Internet Law Bulletin* 2-6 at 3.

29 Ibid at page 19. See also Roger Clarke, "Privacy requirements of public key infrastructure" (2000) 3(1) *Internet Law Bulletin* 2-6 at 3.
See also Roger Clarke, 'The Fundamental Inadequacies of Conventional Public Key Infrastructure" (2001) http://www.anu.edu.au/people/Roger.Clarke/II/ECIS2001.html at para 3.2 where he stated that:
"Digital signature schemes depend on the public key of the message-sender being available to the recipient. The most practicable methods of achieving this are:
- *Senders can include their public keys in each message;*
- *Senders can store them on a site of their own that is readily accessible (Eg using FTP or HTTP);*
- *public keys may be stored in one or more centrally managed directories, enabling each party to an exchange to look up the public key of the other party.*

All of these approaches are subject to "spoofing", ie an imposter can send a message that includes a public key, or store a public key in a readily accessible directory and thereby fool the other party into thinking the message came from a particular person or organisation."

30 Ibid at page 21. See also Roger Clarke, "Privacy requirements of public key infrastructure" (2000) 3(1) *Internet Law Bulletin* 2-6 at page 3.
See also Roger Clarke, 'The Fundamental Inadequacies of Conventional Public Key Infrastructure" (2001) http://www.anu.edu.au/people/Roger.Clarke/II/ECIS2001.html at para 4.3.

31 Ibid at page 22.

32 The Office of the Federal Privacy Commissioner, Privacy and Public Key Infrastructure: Guidelines for Agencies using PKI to communicate or transact with individuals (21 December 2001) at page 25.

33 The Office of the Federal Privacy Commissioner, Privacy and Public Key Infrastructure: Guidelines for Agencies using PKI to communicate or transact with individuals (21 December 2001) at page 27.

34 Office of Government Information Technology, "Gatekeeper: A strategy for

public key technology use in the Government" (2002) http://www.govonline.gov.au/publications/GatekeeperStrategy.pdf at page vii. See also Organization for Economic Cooperation and Development, "Guidelines for Cryptography Policy" (1997) http://www.cybercrime.gov/oeguide.htm. See also Patrick Fair, "GateKeeper: Setting Australia's standard for online security" (1998) 1(6) *Internet Law Bulletin* 85-88 at page 87.

35 The Office of the Federal Privacy Commissioner, Privacy and Public Key Infrastructure: Guidelines for Agencies using PKI to communicate or transact with individuals (21 December 2001) at page 28.
36 Ibid at page 29.
37 Please see The Office of the Federal Privacy Commissioner, Privacy and Public Key Infrastructure: Guidelines for Agencies using PKI to communicate or transact with individuals (21 December 2001) at pages 36-43.
38 The Office of the Federal Privacy Commissioner, Privacy and Public Key Infrastructure: Guidelines for Agencies using PKI to communicate or transact with individuals (21 December 2001) at page 30.
39 Ibid at page 31.
40 Ibid at page 32.
41 Ibid at page 33.
42 Ibid at page 34.
43 Ibid at page 35.
44 Secure Electronic Environment Project (S.E.E.), "Draft Interim Guidelines for the use of Public Key Technology in Government" (2000). www.e-government.govt.nz/guidelines
45 Ibid at page 3.
46 Ibid at page 3.
47 Paragraph 5.52 at page 10.
48 Paragraph 6.52 at page 13.
49 Gatekeeper Accreditation Information about the criteria and procedures involved in getting accredited under the Gatekeeper strategy set out in http://www.govonline.gov.au/projects/publickey/GatekeeperAccreditation.htm
50 Ibid.
51 The *Privacy Amendment (Private Sector) Act* 2000 (Cth) was passed by the Commonwealth Parliament on 6 December 2000 and will commence operation on 21 December 2001. This piece of legislation applies the National Privacy Principles to private sector organisations.
52 Part VIII of the *Privacy Act* (Cth) 1988.
53 Section 95B of the *Privacy Act* (Cth) 1988.
54 Section 7B(2) of the *Privacy Act* (Cth) 1988.
55 Section 13A of the *Privacy Act* (Cth) 1988.
56 Section 6D of the *Privacy Act* (Cth) 1988.
57 Section 16D, *Privacy Act* 1988 (Cth).
58 This is the proforma contract which is used by NOIE in contracting with CAs and RAs set out in http://www.govonline.gov.au/projects/publickey/GatekeeperAccreditation.htm
59 "VeriSign Fraudulent Certificates" (2001) http://www.pkiforum.com/resources/alert_verisigncerts.html