The Office of the Federal Privacy Commissioner

Privacy and Public Key Infrastructure: Guidelines for Agencies using PKI to communicate or transact with individuals

Table of Contents

Foreword by the Federal Privacy Commissioner

A key issue for the Australian community in the information age is how they can be confident of their privacy while taking advantage of the developments offered in information and communications technology. This is reflected, for example, in recent research into attitudes to privacy conducted by my Office that indicated more than half of all internet users had *more* concerns about the security of personal information when using the internet.

Public key technology (PKT) and its surrounding infrastructure – public key infrastructure (PKI) – is a powerful technology which offers benefits to enhance privacy of individuals. It can, for example, provide confidentiality of online communications, authentication of parties in online transactions, as well as non-repudiation of transactions and message integrity. However, there are privacy risks associated with PKI and these need to be carefully managed.

My interest as Privacy Commissioner is to think about such privacy issues and to work with business and community to put in place structures and standards that will help individuals take up the technology, if they choose, with confidence. I was happy to take up NOIE's suggestion to consider the need for guidelines for the use of PKI in the government sector as there is an increasing trend for all manner of dealings to be online.

After considering the issues, I decided that guidelines could assist agencies to implement privacy best practices in the area of PKI. *Privacy and Public Key Infrastructure: Guidelines for Agencies using PKI to communicate or transact with Individuals* identify privacy risks associated with PKI and set out guidance for Commonwealth and ACT agencies where they provide services to individuals using PKI. The guidelines establish privacy standards based on and in addition to the Information Privacy Principles in the *Privacy Act 1988*, with which agencies must comply.

An important theme reflected in the guidelines is the need for consumers to be informed about the proper use of PKI, as well as the need to build in choice for consumers regarding whether or not to use the technology.

It is also important that the guidelines work effectively for agencies. To this end, I undertook a wide consultation as part of the development process, including with Commonwealth Government agencies, PKI experts, industry representatives and consumer and privacy advocates. I would like to especially thank the National Office of the Information Economy for their advice and collaboration in the development of the guidelines, and to thank the Reference Group for their guidance and assistance.

Due to the fast-developing changes in this area, I have decided to review the guidelines in eighteen months. My review will consider a number of issues, including developments in the use of PKI in the private sector and the need for guidelines to be issued for private sector organisations.

Malcolm Crompton
Federal Privacy Commissioner

21 December 2001

Foreword by the Chief Executive Office of the National Office for the Information Economy

The National Office for the Information Economy welcomes the issuance by the Federal Privacy Commissioner of guidelines for the use by Commonwealth agencies of Public Key Infrastructure (PKI). NOIE, as manager of the Gatekeeper PKI trust framework, is concerned to ensure the secure issue and use of Gatekeeper digital certificates.

For this reason, NOIE invited the Privacy Commissioner in late 2000 to consider developing best practice guidelines for Commonwealth agencies to assist them in designing and implementing PKI applications and processes when using Gatekeeper digital certificates with individual clients.

Developing public confidence in the technology and trust framework is an important part of the Government's objective of encouraging the growth of online services delivered by the Commonwealth Government. This in turn will encourage the development of the information economy, with potential benefits of lower costs and greater convenience for all participants.

An expanding and client-sensitive use of PKI by agencies should continue to play a significant role in these objectives. I note that the new guidelines are couched in relatively general terms and are likely to be reviewed in due course, allowing agencies and their clients to consider a range of privacy-sensitive authentication models as authentication technology and agency business plans develop.

I commend the adoption of these guidelines by agencies.

John Rimmer
Chief Executive Officer
National Office for the Information Economy

Introduction

Privacy, Public Key Infrastructure and Commonwealth agencies

The Internet and other electronic means of communicating provide many opportunities. However, there are challenges to be met, including the need to think carefully about privacy where online interactions replace traditional face-to-face or paper-based interactions. These challenges include:

- protecting the confidentiality of transmissions; and
- in some cases, the need to be sure about the identities of transacting parties.

Public key infrastructure (PKI) is one method of dealing with these issues. PKI can be a privacy-enhancing tool in that it provides secure channels of communication and greater certainty about the identity of parties in online interactions. However, it also carries privacy risks if the security processes breakdown and because of the potential for more information to be collected in more circumstances or for the greater aggregation of data about individuals.

The Commonwealth Government has developed a PKI known as Gatekeeper that aims to facilitate e-commerce and the take up of online delivery of government services in Australia. Gatekeeper establishes a trust framework that includes processes for identifying participants and issuing encryption keys and digital signatures. It applies stringent privacy protections, or rules, to these processes. To date, the Gatekeeper has been used mainly in communications between the business sector and government. However, governments could also use it when offering services or assistance to individuals.

Privacy issues may also arise when PKI is used in communications between governments and individual clients. As noted, the Gatekeeper framework includes privacy rules. However, these apply to bodies in the trust framework that confirm identity (registration authorities) or issue certificates (certification authorities). The Gatekeeper rules do not apply directly to the government agency/client relationship.

The use of PKI by agencies for transactions with individuals is subject to the *Privacy Act 1988* (Cth) (the Privacy Act) that sets general standards for the handling of personal information about individuals. This paper, and the guidelines it includes, complements the standards in the Privacy Act by addressing privacy issues that are specific to PKI.

The development of the Guidelines

In late 2000, the National Office for the Information Economy (NOIE), as the agency responsible for managing Gatekeeper, invited the Federal Privacy Commissioner to consider issuing guidelines on the privacy implications and good practices for Commonwealth agencies using PKI for individuals. At that time a number of Commonwealth agencies were considering the use of PKI applications for transactions

with individuals. During initial discussions with NOIE and agencies it appeared that there was a need for privacy guidance for agencies using PKI for transactions with individuals.

The Privacy Commissioner sought to ensure that his consideration of privacy issues was well informed and based on wide consultation. He invited key stakeholders including consumer representatives, agencies and industry representatives to form a reference group for this project. The Reference Group assisted in defining the scope of the project, identifying priority issues to be addressed, and suggesting possible guidelines. It also made suggestions about who should be consulted.

In addition, the Office of the Federal Privacy Commissioner, (the Office) held a series of meetings with agencies that have indicated an interest in using PKI in online service delivery for individuals. Further, NOIE has also collaborated closely on the development of these Guidelines, both as the manager of Gatekeeper and because of its general brief to facilitate the take up of online government services in Australia.

On 12 June 2001 the Office published a Consultation Paper (including draft Guidelines) in order to seek wide public comment on privacy issues raised by agency use of PKI for individuals.

In the light of the responses to the Consultation Paper the Privacy Commissioner has decided to issue guidelines, *Privacy and Public Key Infrastructure: Guidelines for Agencies using PKI to communicate or transact with individuals* (the guidelines), under section 27.1(e) of the Privacy Act. This provision allows the Privacy Commissioner to:

> ".. prepare, and to publish in such manner as the Commissioner considers appropriate, guidelines for the avoidance of acts or practices of an agency that may or might be interferences with the privacy of individuals or which may otherwise have any adverse effects on the privacy of individuals…".

Scope of the Guidelines

The Privacy Act protects personal information – that is information about individuals whose identity is apparent, or can reasonably be ascertained, from the information[1].

In general, the Privacy Act protects individuals in both private and business capacities. In other words, individuals:

- in their private (non-business) capacity as clients, tax-payers and recipients of Government services and customers of agencies;
- who are designated representatives of corporate entities; or
- who are sole traders or partners involved in business activities.

[1] For definition of 'personal information', see section 6 of the *Privacy Act 1988*

The guidelines focus primarily on the first of these three categories. However, the issues identified may also be relevant for the individuals in the other two categories.

Privacy issues may arise in relation to a number of aspects of PKI and the guidelines address these issues. Broadly these can be grouped as follows:

- client choice to use PKI transactions;
- client education in the proper use and privacy risks of PKI;
- risk assessment and management and Privacy Impact Assessments (PIAs);
- the application and registration processes for digital certificates, particularly in respect to Evidence of Identity (EOI);
- the aggregation of personal information collected during PKI transactions;
- the associated trust framework including public key directories and Certificate Revocation Lists;
- single and multiple certificates;
- subscriber generation of keys; and
- anonymity and pseudonymity.

The guidelines are set out in Chapter 2 of this document. They focus on the use of PKI by agencies for the provision of services to individuals. They are advisory in nature and address particular privacy issues in the use of PKI.

Review of the Guidelines

Due to the dynamic nature of the PKI industry and the information economy, the Privacy Commissioner has decided to review these Guidelines eighteen months after their publication. In conducting this review, the Commissioner will assess the use of the guidelines by agencies and the effectiveness of the Guidelines. He will also consider developments in the technology (for example the use of digital signature certificates that identify a characteristic or attribute of a person – such as their entitlement to a particular benefit – rather then identifying the person as such, and subscriber key generation), developments in private sector use of PKI and any other relevant issues.

The Privacy Commissioner will also be particularly interested in whether there are any unintended or indirect privacy issues that may emerge from PKI implementation in the public sector. For example, if it appears that most agencies decide to rely on certificates issued by one or a few agencies, it may be that stronger guidelines or a legislative response is needed to offset the potential for the certificate of one agency to be used widely as an administrative or matching number across all or many agencies and organisations.

Guidelines for the Private Sector

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 online dealings with their customers there will also be privacy issues to consider. 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 private sector stakeholders would be critical before PKI privacy guidelines could be developed for this sector.

The Privacy Act applies to many private sector organisations from 21 December 2001 and the Privacy Commissioner will monitor developments in the use of PKI by private sector organisations. In particular, he will watch for individual complaints in this area that may indicate systemic problems or practices.

The Privacy Commissioner expects 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. At that time the Commissioner would consider with other stakeholders whether he or another organisation or body should have carriage of the issue.

Implications for NOIE

PKI service providers accredited to work with Commonwealth agencies are bound by specific Gatekeeper privacy related requirements. The Privacy Commissioner understands that NOIE will review those requirements in the light of the consultation process and guidelines.

Chapter 1 – Privacy and Public Key Infrastructure – An Overview

The Scope of this Chapter

This chapter is intended to provide an overview of privacy, PKI and the privacy implications of PKI. It briefly describes the nature of privacy, the Privacy Commissioner's jurisdiction, public key technology (PKT), PKI, Gatekeeper and discusses a number of privacy issues and the risks associated with PKI.

Chapter 2 then sets out the privacy guidelines that aim to address the residual risk.

The nature of Privacy

Privacy is about protecting our sense of self – that is, who we are, what we know, what we think, what we have done and what we want to do. One important aspect of this is the extent of control we have over personal information about us. Exercising choice about our own information can also be an important aspect of retaining personal dignity and humanity in a relationship with another party.

Privacy is not about protecting wrongdoing or encouraging secrecy. There is no absolute right to privacy. Society accepts that there are public interest reasons for particular limitations on individuals' right to privacy. These include law enforcement, fraud control and public safety.

David Banisar[2] of EPIC suggests privacy can be divided into four separate but related concepts:

- information privacy – involving rules for the handling of personal data;
- bodily privacy – protection of our physical selves against invasive procedures;
- privacy of communications – security and privacy of mail, telephones etc.; and
- territorial privacy – setting limits on intrusions into domestic and other environments.

The Privacy Act applies in the main to information privacy. A certain amount of information sharing occurs in most relationships that individuals have with other people or organisations. As a consequence, there may be a reduction in control over that information because someone else holds it. The individual's right to privacy sometimes must be balanced against a particular benefit that the individual receives from such relationships. It is also the case that the extent to which individuals will be prepared to divulge their personal information in online transactions will vary from person to person.

[2] Banisar D, 2000, Privacy and Human rights: an international survey of privacy laws and developments, Electronic Privacy Information Centre, Washington. www.privacyinternational.org/survey/

However, it is clear that privacy is an important issue for Australians. In the last few years privacy has become a vital issue in policy and regulatory debates. Privacy issues have emerged particularly in the context of increasing use of information technology, the Internet and developments in e-commerce. Recent research into attitudes to privacy conducted by this Office indicated that 90% of people regard monitoring of Internet usage without the individual's knowledge as an invasion of privacy.

The Privacy Act and the Privacy Commissioner's Jurisdiction

In Australia the Privacy Act protects personal information held by most Commonwealth and ACT agencies. Personal information is defined in section 6 of the Privacy Act as:

> …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.

The Act sets standards called the Information Privacy Principles (IPPs) for the collection, use and disclosure of personal information and for individuals to access and correct information about them. It also regulates the use of Tax File Numbers (TFNs) whether held in the public or private sector and, since 1992, consumer credit information and reporting.

In December 2000 the Commonwealth Parliament passed the *Privacy Amendment (Private Sector) Act 2000* that amended the Privacy Act to extend privacy protection in the private sector. This legislation came into effect on 21 December 2001 and sets out information handling standards called the National Privacy Principles (NPPs) for private sector organisations.

The Act does not apply to small businesses, those with an annual turnover of $3 million or less, provided that they do not handle personal information for a benefit, service or advantage (without the consent of the individual) or constitute a 'health service' holding 'health information'.

The Act also provides for organisations to administer their own privacy code. Privacy codes can replace the NPPs if they provide at least equivalent levels of privacy protection and are approved by the Privacy Commissioner.

The Act also gives the Privacy Commissioner a range of functions, including the investigation of complaints from individuals about possible breaches of privacy, the provision of advice to government and organisations about privacy matters and the issue of guidelines for good privacy practices.

More information about the Privacy Act and the Privacy Commissioner's jurisdiction can be found at www.privacy.gov.au.

Public Key Technology and Public Key Infrastructure

See Appendix 2 for a glossary of PKT/PKI terminology.

Public key technology (PKT) is a form of cryptography and relies on two keys - a public key and a private key. The subscriber must keep the private key secret. The public key can be made known to others and made publicly available.

A 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 certificates.

A PKI provides four functions:

- **Authentication**. The identity of a subscriber can be assured in online transactions by the subscriber 'signing' an electronic communication with their private key. This authentication is performed by the application of the public key to the digital signature;
- **Integrity**. Where a subscriber signs an electronic document a message digest or hash of the message is produced, this is essentially a number (hash value) derived from the text of the message, any other message will produce a different number. If the hash value remains the same after the message has been received then the message integrity is assured. That is, the message hasn't been altered in transit;
- **Non-repudiation**. Where an electronic message is signed with a digital signature, the fact that it was signed with a particular key cannot be repudiated or denied. In practice, this means that there will be irrefutable evidence of this, unless it can be shown that the private key was applied by other than its unique and rightful holder;
- **Confidentiality**. This is achieved by encrypting a message with a subscriber's public key. The message can only be decrypted with the subscriber's private key.

Depending on the design and application of the system, PKT can deliver some or all of these. For example, it may be used just to provide confidentiality of communications.

Public Key Infrastructure - Components

The main components of a PKI are:

- Certification Authorities (CAs) – issue and revoke digital certificates;
- Registration Authorities (RAs) – conduct the initial verification of a potential subscriber's identity and/or attributes;
- subscribers – digital certificate holders;
- relying parties –entities when relying on the contents of a digital certificate in communicating with subscribers; and

- directories – may store public keys, digital certificates or Certificate Revocation Lists (CRLs).

The main operations and processes of PKI are:

- registration – the process whereby a potential subscriber makes themselves and/or their relevant attributes known to the CA directly (or through an RA);
- key generation – the generation of one or more key pairs by the CA or by the subscriber;
- certification – the issue by a CA of a digital certificate to a subscriber;
- certificate expiry – the allocation of a period for which a digital certificate will remain valid;
- certificate revocation – the revocation of a digital certificate prior to its expiry (eg where the private key has been compromised); and
- Certificate Revocation Lists (CRLs) – lists of revoked digital certificates.

Digital Certificates

A digital certificate is an electronic document signed by a CA that associates a subscriber with a key pair. The certificate contains the subscriber's public key and other information including the cryptographic algorithm supported a serial number, and the distinguished name of the subscriber. The certificate is issued to the subscriber.

Signing and encryption key pairs

Two key pairs are used, a signing key pair and an encryption (or confidentiality) key pair. The signing key pair is used to authenticate, verify the integrity of and prevent repudiation of a message. The encryption key pair is used to provide the confidentiality function of PKI .

The keys operate as inverses:

- Only the holder of a private key can decrypt a message someone else has encrypted with the corresponding public key. The sender of a message who wants the contents to be kept confidential during transit uses the public key (which is freely available) of the recipient's encryption key pair to encrypt the message – only the recipient holds the private key so only they can decrypt and read the message;
- Conversely, a message, which can only be decrypted using a public key, must have been encrypted using the corresponding private key. The sender of a message who wants to prove to the recipient that they are the sender and verify the integrity of the message uses the private key of their signing key pair to encode the message (or a hash of the message) – the recipient uses the sender's public key to decrypt the message and knows that it could only have been sent by the sender.

Subscribers of public-key based systems must be confident that when they use a public key (whether to decrypt a 'signed' message they receive or to encrypt a confidential message they are sending) the person they are communicating with owns and controls the associated private key.

Gatekeeper

As noted above, Gatekeeper is the Commonwealth Government's strategy for the policy and implementation of PKI in government. It is managed by NOIE. Australian states and Territories have agreed in-principle to the adoption of the Gatekeeper strategy. NOIE manages the accreditation of CAs and RAs and sets the accreditation criteria. The Gatekeeper Policy Advisory Committee (GPAC) includes representatives of the Commonwealth government, State and Territory governments, industry representatives and a privacy consultant. The GPAC has advised NOIE on the policy framework for Gatekeeper.

There are a number of privacy protections contained in:

- Gatekeeper Head Agreements (which contractually binds Gatekeeper accredited CAs and RAs to the Gatekeeper accreditation criteria on an ongoing basis), see appendix 5;
- within the Gatekeeper accreditation criteria; and
- a set of guidelines for privacy protection entitled, *Privacy Recommendations to the Chief Executive Officer, OGO, in relation to the use of Gatekeeper Certificates by Individuals* which contain privacy requirements on top of the IPPs. See Appendix 6.

NOIE has advised that it intends to review the existing Gatekeeper privacy requirements to ensure consistency with these guidelines and continuing best practice for accredited PKI service providers.

Contractual Arrangements between Agencies and PKI Service Providers

It is important to note that RAs/CAs that are contracted by a Commonwealth agency to provide services, may be subject to the IPPs, as well as Gatekeeper.

Section 95B (1) of the Privacy Act requires an agency entering into a Commonwealth contract to take contractual measures to ensure that a contracted service provider for the contract does not do an act, or engage in a practice that would breach an IPP if done or engaged in by the agency.

Section 95B (2) requires that a Commonwealth contract does not authorize a contracted service provider to engage in an act or practice that would breach an IPP.

So when an agency enters a contract with a PKI service provider, the contract should include a provision requiring the contractor not to breach the IPPs. Also, the contract should not authorise any such breach.

Privacy Implications of PKI

PKI can be privacy enhancing

While this chapter concentrates on identifying some of the privacy risks that emerge from PKI applications, it is important to recognise these applications can also be privacy enhancing.

PKI applications can allow individuals to utilise a wider range of communication channels when dealing with agencies. Individuals who have privacy concerns about speaking to an agency via telephone (for example, in a shared household or at the workplace) can use e-mail or web-based communication instead. The use of digital certificates also reduces the need to constantly provide primary EOI (such as a driver's license) or answer questions about one's date of birth, home address and so on in order to authenticate oneself.

PKI supports confidentiality of communications (encryption of messages). Individuals who are concerned about sending text messages to agencies would have the facility to encrypt their messages with the agency's public key so that it can only be decrypted by the agency. Conversely, an individual could require the agency to encrypt any messages they send to the individual with their public key so that only they can decrypt it. This security of communications provided by PKI is certainly privacy enhancing.

These privacy benefits are additional to other consumer benefits offered by PKI, in particular, confidence that their message cannot be altered in transit and that they are in fact dealing with the party they intended.

PKI and Privacy Risks

The next sections discuss a number of privacy issues and the risks associated with PKI.

The approach taken in relation to each of the risks is to:

- briefly describe the context or activity in which the risk arises;
- describe the risk;
- identify the measures in place to deal with the risk (Gatekeeper, Information Privacy Principles).

In the discussion that follows it is important to note that some PKI privacy issues by their nature relate only to the activities of CAs and RAs – these are generally dealt with in the Gatekeeper framework and are therefore the particular concern of NOIE as manager of the Gatekeeper policy and accreditation framework.

The relative roles of CAs/RAs and agencies in privacy sensitive PKI functions are outlined in the following sections that summarise the major areas of privacy sensitivity.

Implications may arise directly from the way agencies use PKI and the personal information they collect and handle in this context. The Privacy Act, complemented by these guidelines, addresses these issues.

The Registration Process

The issue of how much EOI should be provided before a digital certificate is issued to a client, and how that is obtained, relates to both agencies and CAs/RAs. CAs must be able to give their clients (including agencies) confidence that digital certificates have in fact been issued to the correctly identified party.

An RA must collect EOI information from an individual in order for them to be issued with keys and a digital certificate by a CA. Under Gatekeeper, CAs set identification levels, sometimes at the request of any agency that has commissioned them to issue digital certificates to their clients. Gatekeeper EOI levels are set at 50, 100 or 150 points by reference to the requirements, set out under the *Financial Transaction Reports Act 1988* (Cth).

The registration process may be intrusive as individuals would generally be required to attend an RA with their EOI documentation. Another issue is that a particular identification level selected might be unduly high and not warranted by the nature of the application. This is seen as more likely if a single digital certificate were used across multiple agencies or applications since it would require an identification level that represented the highest common factor.

In response to this, Gatekeeper Privacy Criterion 1 (PC 1) requires RAs to comply with IPPs 1-3, which include the requirement to collect only information for a lawful purpose 'directly related to a function or activity of the collector'. Gatekeeper Privacy Policy (*Privacy Recommendations to the Chief Executive Officer, OGO, in relation to the use of Gatekeeper Certificates by Individuals)* "requires a PKI design that ensures that individuals are only subjected to appropriate identification procedures to meet agency authentication requirements or to satisfy applicable law and that intrusive procedures are minimised to the greatest extent possible".

Intrusiveness will be minimised if agencies carefully consider which level of EOI is appropriate to their application in order to assure that the personal information collected is necessary for or directly related to the application. Guideline 4 expects agencies to require a level of identification that is sufficient, but not excessive for their business needs.

There will also be benefits for agencies and their clients in accepting, as adequate for their own purposes, a Gatekeeper compliant identification process already obtained by their subscriber with another agency or RA. This would avoid the inconvenience and possible expense for clients of multiple identifications, but would require the client's

consent to allow the existing RA or CA to demonstrate that identity to the subsequent agency or its CA.

Note that Gatekeeper rules are designed to prevent the sharing of RA collected and stored identity information (for example, copies of identification documents or qualification / membership / eligibility documentation) with CAs or agencies, as this would lead to the centralised storage of personal data.

Public Key Certificates

Concerns have been raised in respect to the possible extent of personal information contained in certificates. Certificates are also normally publicly available. The risk here is that this may facilitate possible tracking of an individual's transactions.

This is a matter for CAs as certificate issuers and for NOIE as Gatekeeper manager. Gatekeeper Privacy Criterion 1 requires CAs to comply with IPPs 1-3, in order to minimise the amount of personal information collected and made public. This is reflected in NOIE's approved profile for digital certificates which only allows personal information in the 'Distinguished Name' field and which limits that field to a subscriber's name or pseudonym.

Public Key Directories and Certificate Revocation Lists

A further potential privacy risk arises from the possible browsing of public key directories, downloading bulk data from them or using them in other ways that may interfere with the privacy of individuals. For example, the downloading of digital certificates from a public key directory may reveal an association of an individual to a particular agency, and associating the name with the digital certificate's serial number may allow tracking of a pattern of transactions.

In some implementations of PKI it may not be necessary for a public key directory to be published. If the relevant agency is itself a CA, or uses a CA to manage a closed PKI community exclusively for its purposes, the agency will have its own access to its clients' public keys. In that event, there would be no reason for publishing the clients' public keys.

The issue to consider, from a privacy perspective, is whether PKI applications require the publication of a public key directory. If publication is considered necessary then a privacy protective option is to allow individual clients to opt out of having their public keys listed in the directory. This is similar to the way telephone subscribers may opt out of having their phone number published in the phone directory.

Gatekeeper Privacy Privacy Policy, Criterion 9 sets out specific requirements for CAs for CRLs and 'other directory services' including Public Key Directories. This Criterion limits personal information published in CRLs and other directory services, and places limits on personal information collected, logged and disclosed.

Gatekeeper privacy policy 'require a PKI design that incorporates effective privacy controls over the information contained in CRLs and how CRLs are accessed and searched'. This means for example that, while revocation of a certificate must be published in a CRL, the reasons for revocation or suspension must not be disclosed. Also, access to a Certificate Directory or CRL will generally be limited to single searches. In practice, NOIE requires CRLs and other public directories to be configured such that only one search can be made at a time and then only against a certificate serial number (not the Distinguished Name).

The Gatekeeper requirements for CAs can be reinforced by a guideline requiring those agencies, which commission CAs to issue certificates to their clients, to ensure that their digital certificates or revocations are not posted to a publicly available directory if a subscriber opts out (see Guideline 8).

Logs and ephemeral data

Servers hosting public key directories, CRLs and other PKI transactions and maintained by CAs and agencies, will normally keep logs of accesses and online transactions. Agencies would legitimately expect to maintain records of checks as non-repudiable evidence of their transactions.

However, it is possible that CAs and agencies could use logs to track their transactions and then compile profiles of individuals using these services.

Gatekeeper Privacy Criterion 9 provides in part that :

- RA/CAs shall collect and hold minimal personal information when logging accesses to CRLs or other directory services; and
- RA/CAs should not disclose personal information collected by logging access to CRLs or other directory services (except for designated law enforcement purposes).

Agency servers hosting PKI transactions with individuals will also log transactional data. Gatekeeper Privacy Criterion 9 will only apply to agencies if they are also an RA or a CA. Guideline 5 proposes similar guidance for agencies.

Access to Logs by Law Enforcement Agencies and under Legal Authority

Law enforcement agencies, government agencies exercising their statutory powers or other parties may become interested in personal data logged or collected in a PKI application, just as they might be interested in other information held or collected in other networks and systems.

There are three types of data that may be of interest:

- raw, encrypted data - this is simply the data as it is communicated. It may establish simply that a communication between two parties took place at a certain time or location (which may be of interest) without divulging any further details;
- identification data - this data may identify one or more individuals involved in a communication. As identification is part of many PKI applications, this type of data will be common; and
- decrypted data - this data may reveal the actual content of a communication. This may occur in a PKI application because some information has been sent in a decrypted form, or because the recipient has subsequently decrypted the information (or has the capacity to decrypt the information). This type of data is common to most PKI applications.

In respect to such data held by agencies, IPPs 11.1 (d) provides for disclosures, which are required by or under law, and IPP 11.1 (e) for where disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty or for the protection of the public revenue.

Gatekeeper Privacy Criteria 9 requires RA/CAs not to disclose personal information collected by logging access to CRLs or other directory services (except for designated law enforcement purposes).

Security of the Private Key

A significant privacy concern in relation to use of PKI is the security of the private key. The integrity of a PKI depends on the subscriber keeping the private key inaccessible to any other party.

Digital certificates and their corresponding key pairs can be stored in a number of ways – on dedicated tokens such as smart cards or directly on computer disk drives. Each storage method has a set of benefits and deficiencies. The choice of particular storage solutions is a matter for each agency in planning its PKI implementation and for clients in reaching a conclusion about using a particular digital certificate. Gatekeeper does not specify particular storage devices, nor does it make any judgment on the merits of any particular storage method.

Gatekeeper requirements on CAs to advise of security breaches and to post revocations on CRLs also play an important support role for securing the integrity of private keys.

Educating clients as to the best way to protect their private key is clearly a critical strategy in dealing with this issue. The approach that CAs take in relation to their requirements for how private keys are generated and held will also be critical.

Guideline 2 encourages agencies to ensure that that their clients are aware of the relevant privacy and security risks. Guideline 7, Subscriber Generation of Keys, is also relevant.

National Identifiers

One of the aims of these guidelines is to mitigate the risk of PKI of, through its use, becoming a de-facto national identification system. This might happen if individuals used the one digital certificate in their dealings with all agencies (and possibly in the future with state or local governments and private sector organisations) and the agencies or organisations then permanently recorded some feature of the certificate, possibly the distinguished name and/or the certificate registration number, with other records of personal information about the person. The risk then would be that the information from the certificate was sufficient to allow easy and accurate matching of personal information about the individual across a range of situations.

At present, there is a significant body of Commonwealth legislation that sets rules to ensure the confidentiality of tax, health and social security information about individuals. Consistent with a key overall objective of this legislation which is to avoid the creation of a national identifier, Gatekeeper Privacy Criterion 10 requires clients to be allowed more than one certificate from the same CA where this is not inconsistent with the purpose of the digital certificates and when dealing with multiple agencies.

Guidelines 1 and 6 also seek to address this issue. However, even where agencies are willing to offer choice and to accept certificates issued by another agency there may still be a risk that one certificate will predominate. This is more likely to occur if only one or a few agencies decide to implement PKI and other agencies 'piggy back' on their arrangements.

The Privacy Commissioner will closely monitor PKI to identify if this or other privacy risks relative to the potential for a de-facto national identification number to emerge.

Function Creep

Function creep is a progressive accumulation of uses for an application or identifier. An example of function creep relates to the TFN which initially was to be used only for taxation purposes but which additionally came to be used for other purposes including the administration of the welfare system.

An example of this in the PKI setting may be the use of personal information collected for the EOI process for another purpose. It is difficult to predict what other forms of function creep may arise in a PKI.

Agencies need to be wary of any accumulation of additional uses for certificates or associated personal information.

User Choice

Building in a high degree of consumer choice into PKI applications will help address a number of the issues identified above. This has been recognised in Guideline 2 of the

OECD Guidelines for Cryptographic Policy which relates to Choice of Cryptographic Methods, which provides that:

> *Users should have a right to choose any cryptographic method, subject to applicable law.*

As a member of the OECD, Australia has agreed to these OECD Guidelines. Gatekeeper, in respect of CAs and RAs, supports this right.

In practice, many agencies and CAs will be limited to certain technology platforms, certificate types and key management systems. While all will be Gatekeeper compliant and meet prescribed security and privacy standards, not all may have features that some privacy-sensitive clients might prefer.

While, as a result of the factors set out above, the range of choices that an agency may offer will be limited, it should be possible to provide clients with a choice about whether or not to transact using PKI, subject to legislative requirements. Guideline 1 provides choice to individuals as to whether to use PKI applications and requires agencies to provide alternative means of service delivery.

Anonymity and Pseudonymity

Gatekeeper can support anonymous transactions. Although there has not been a demand for digital certificates of this type, Gatekeeper Criterion PC12 states that:

"The CA shall have the ability to provide anonymous or pseudonymous certificates where appropriate."

Gatekeeper Privacy Policy requires that "Gatekeeper requires a PKI design that enables individuals to:

- choose to use any distinguished name in a certificate, except where it would be impractical to do so; and
- conduct pseudonymous transactions except where the agency demonstrates that it is impractical to do so."

It is therefore possible for agencies, where appropriate, to issue digital certificates in any reasonable name the subscriber might choose and for the same person to have additional digital certificates issued with another pseudonym for use with another agency.

It is also likely there will be transactions facilitated by a PKI in which identification of the individual is not necessary. Where a PKI has been implemented to enable a range of online transactions some of which may require identification and some of which may not, then clients should be able to make the latter transactions without revealing their identity.

There may be scope for CAs to issue special purpose attribute certificates which simply represent the individual's eligibility for a service without identifying them, however, at this point in time, an attribute certificate framework has not been developed by the

relevant standards bodies and is not yet part of Gatekeeper. Guideline 9 expects agencies to provide clients with pseudonymous or anonymous alternatives, where appropriate. Agencies might also consider a secure online application, other than PKI, to allow individual clients to deal securely and anonymously with them.

Chapter 2 - Guidelines for Agencies

This Chapter sets out guidelines for agencies considering the use of PKI to help them minimize any privacy risks for individuals.

Overview of the guidelines

While there may be economic and technical limits to the extent that Agencies can offer their clients choice in respect to PKI, clients will be in a better position to make privacy choices that suit them if they are able to choose whether or not to participate in online transactions (whether they involve PKI or not).

The guidelines emphasise the importance for agency clients, as potential PKI users, of being able to make informed choices about using PKI. An important part of this is having sufficient information, including about how to protect privacy, on which to base a decision.

Agencies should also carefully consider whether PKI is appropriate for their online applications. Generally speaking, PKI may not be necessary for applications that do not require authentication and non-repudiation. Other technology may be more appropriate.

Although PKI can be privacy enhancing it also carries privacy risks. The guidelines aim to assist agencies and potential clients to make decisions to use PKI only after proper consideration of the issues and risks.

While the Guidelines focus on agencies, there are several instances where privacy sensitivities stem from the activities of other participants in the PKI, especially accredited PKI service providers (CAs and RAs). Where relevant, this is pointed out in the guidelines. CAs and RAs are bound by specific Gatekeeper accreditation requirements for privacy and security which apply together with the Gatekeeper Privacy Policy. These guidelines would apply, where relevant, to agencies that choose to contract a CA or RA to issue certificates on behalf of their clients as well as to agencies that choose to use or accept digital certificates.

Status of the guidelines

Agencies must comply with the IPPs in the Privacy Act (and with other relevant legislation such as that applicable in the health, social security and taxation sectors). These guidelines complement these legal requirements by offering agencies assistance in developing and applying PKI applications.

The guidelines indicate some factors the Commissioner may take into account when handling a complaint about use of PKI. They are not legally binding.

An agency would not fail to comply with the guidelines by virtue of taking any action that is required or specifically authorised by law.

While the Privacy Commissioner may take these guidelines into consideration in assessing compliance with the IPPs these guidelines aim to encourage in some respects a higher standard of regard for people's privacy rights in relation to PKI than is required by bare compliance with the IPPs and an agency would not necessarily breach the IPPs if it did not adhere to these guidelines.

The Privacy Act provides the Privacy Commissioner with the power to audit agencies, to investigate complaints and to undertake investigations on his or her own account. In respect to audits, while the Commissioner can conduct audits of agency compliance with the IPPs, he can also take into account compliance with advisory guidelines (such as these PKI Guidelines) where this represents the Commissioner's advice on good privacy practice.

The use of these guidelines by agencies reflects both good management practices and agencies' commitment to the protection of individuals' privacy rights.

Agencies are responsible for applying the guidelines to their PKI activities and for determining whether it is appropriate to apply particular requirements to a particular PKI application.

The OFPC undertakes to consult agencies in the event of any proposal for compliance with the Guidelines to be mandated for agencies.

The date of effect of these guidelines is 21 December 2001.

Guideline 1 – Agency Client Choice on the Use of PKI Applications

Agencies should allow their clients to choose whether to use PKI for a particular transaction and to offer them alternative means of service delivery. The alternative need not always be an online alternative. In providing this choice agencies should advise their clients of the privacy risks and advantages associated with their use of PKI and alternative methods for that transaction.

Commentary

Clients should have choice as to whether to participate in PKI for a particular transaction, subject to any legislative requirements. They should also be given sufficient information on the advantages, disadvantages and risks associated with PKI and alternatives to make a fully informed choice.

This Guideline seeks to ensure that agency clients have a choice over whether to use PKI for their online transactions. In many cases not using PKI may mean that the client cannot use the online application, as the risks of less rigorous online authentication and security arrangements may inhibit the use of alternate online authentication.

Client choice should be supported in respect to particular PKI transactions. It should not be assumed that because a client chooses not to use PKI for a particular transaction that they will not choose to use PKI for all or other transactions.

Guideline 2 – Awareness and Education

Agencies and their contracted PKI service providers should co-operate closely to ensure that their 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.

Commentary

As PKI applications develop, it will be important to promote client awareness regarding the use of PKI. The responsibility of individual clients for key management is an important part of the security of PKI.

Below are four approaches agencies may wish to consider adopting to promote awareness and education around PKI:

- agencies could take general steps to ensure that clients are aware of security risks (this information should be provided to clients before the certificate is issued, or if it is not practicable, as soon as possible thereafter);
- CAs could ensure that subscriber agreements detail all the necessary security guidance. This is already recommended under Gatekeeper and adopting this position in these Guidelines will strengthen this position;
- agencies could identify risks and manage these risks appropriately – including clearly informing clients regarding their privacy and security responsibilities. Agencies could consider they are not simply transferring risk to clients by providing them with security information;
- agencies may take specific steps to ensure that clients are aware of security risks, such as education campaigns, publishing reader-friendly brochures or information sheets and providing information on their website. A whole of government approach to raising awareness of PKI and related privacy issues may also be appropriate.

Guideline 3 - Privacy Impact Assessments (PIAs)

Agencies should undertake a Privacy Impact Assessment before implementing a new PKI system or significantly revising or extending an existing PKI system.

Commentary

Privacy Impact Assessments (PIAs) provide a method of identifying privacy risks so that these can be highlighted and addressed when PKI systems or PKI-supported business applications are being designed, implemented, revised or extended. A PIA may be part of a larger risk assessment and management procedure. Properly done, this assessment will include an understanding of which parties will bear what risks.

Agencies that are Gatekeeper accredited may have substantially met this requirement by conducting a risk assessment process regarding privacy as part of the Gatekeeper accreditation process.

A PIA may also play an important role in the formulation of the Agency's security awareness campaign, as it can identify issues that can directly affect clients and highlight areas of particular privacy sensitivity.

PIAs are discussed in more detail in Appendix 1 and a sample PKI PIA is also provided The sample PIA is provided to assist agencies in meeting this Guideline. Agencies may wish to adopt the whole or part of this sample PIA in undertaking their own PIA.

Guideline 4 – Evidence of Identity

When developing PKI applications or contracting with PKI services providers, agencies should ensure that only minimum EOI that is necessary for, or directly related, to the process is collected.

In addition, where a client wishes to obtain more than one certificate then the client should be given a range of options including:

- **consenting to use a Gatekeeper certificate of equal or higher value to apply for a new certificate;**
- **consenting to the re-use of EOI documentation previously provided by the client;**
- **or providing documentation on registration for an additional certificate.**

Commentary

Gatekeeper individual certificates are designed to allow a CA or an agency to specify either 50, 100 or 150-point checks (using the framework in the *Financial Transaction Reports Act 1988 (*Cth). Agencies should carefully consider which level of EOI is fit for the purpose of the transactions it wishes to undertake with its clients and should only collect personal information that is necessary for or directly related to that level of EOI.

Individuals will have to provide proof of identity documentation and may be required to attend a face-to-face interview in order to obtain their first certificate. To avoid requiring clients to undergo multiple EOI processes, agencies should consider the generation of additional certificates on the basis of possession of a certificate. The agency client should be able to obtain additional certificates of equal or lower grade to the certificate already possessed.

Another option would be to allow one EOI process to be used for multiple certificates. This may require interaction between accredited gatekeeper providers such as the passing of EOI information between them. Where this occurs it should be with the client's consent.

Guideline 5 – Aggregation of Personal Information

In the course of PKI transactions with clients, agencies and their contracted PKI service providers should ensure that no detailed history of client transactions is created or used by the agency or contracted PKI service provider, except to the extent that this is required for system maintenance or evidentiary purposes.

Agencies and contracted PKI service providers, should not use PKI transactions to collect personal information that is not necessary, or directly related to, the PKI business transaction.

Commentary

PKI applications may collect ephemeral data about the client, including transaction and eligibility data, and their relationship with agencies. This information may be automatically recorded in application logs. It may be possible to build detailed profiles about the client by using this information.

There will be some circumstances where it is legitimate and lawful for logs of an individual to be aggregated. These include system maintenance where a user has reported problems over a period of time and an aggregated log for the user may be used to diagnose technical problems. It is likely that this would be permitted by IPP 10 (1) (e) as the aggregation would be generally constitute a use directly related to the purpose for which the information was obtained.

Other such circumstances may include where a law enforcement agency seeks to obtain an aggregated log relating to an individual where this is reasonably necessary for law enforcement or where an agency wishes to use aggregated information about its staff or a client for similar purposes. Where the use of personal information from logs for a purpose other than for which it was collected is considered, then such use must only be as permitted by IPP 10. Similarly where disclosure of such personal information is considered, this must only be as permitted by IPP 11.

Agencies and contracted PKI service providers should also avoid the collection or logging of information that is not necessary or directly related to the relevant PKI transaction.

Guideline 6 – Single or Multiple Certificates

Agencies should allow clients to use more than one certificate, where these are fit for the purpose of the relevant application. Agencies should also recognise certificates they have not issued where these certificates are fit for the purpose of the relevant application.

Commentary

In practice, a client of an agency might prefer a single certificate option for applications with that agency for reasons of simplicity and cost. However, where a client has several unrelated transactions with that agency, he or she may prefer to use different certificates.

Similarly, an agency client may wish to use a different certificate for his or her dealings with different agencies – where the client does not wish to use one certificate for dealing with any two or more agencies.

This Guideline would allow agencies to offer a single certificate for a group of PKI applications with similar privacy sensitivities, subject to client's choice.

This Guideline should help prevent any development of a single certificate as a de-facto national identifier. In addition, the more certificates a subscriber can use, the less the risk that their transactions, habits and movements can be tracked by reference to a single certificate's properties.

Guideline 7 – Subscriber Generation of Keys

Where 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 subscriber key generation can be implemented securely.

Commentary

To maximise security in a PKI, the client's private key should be in the sole possession of the client. Gatekeeper requires that this be the case once a key pair has been generated and that any copies of the private key generated by a CA be destroyed when the key is issued to the subscriber. Appropriate software would have to be issued by service providers to clients in order to generate their own keys.

To minimise the exposure of a private key, orthodox PKI policies the world over encourage key generation to be performed by, or under the sole control of, the subscriber. This desire has to be balanced against the equally important requirement that key generation be conducted securely and in compliance with accepted standards.

Gatekeeper policy already supports this option. Gatekeeper policy "requires a PKI design that ensures that the key pair which constitutes the signature will be generated and distributed in such a way that:

- the private key is only available to its owner;
- it precludes any person other than the owner from ever being in possession of a private authentication key without the owner's consent; and
- the certifying authority can be satisfied that the public key corresponds to the owner's private key."

An agency may decline to accept a digital signature if the generation process is not compliant with established quality or standards and end-user product key generation accreditation if applicable.

Gatekeeper policy requires that any key generation system either be under evaluation, or approved, on the Commonwealth Endorsed Products List (EPL). It is acknowledged that there is currently no product on the EPL which allows subscriber generation of keys. However, it is important to note the need for such products is widely recognised.

Guideline 8 – Public Key Directories

Agency clients should be allowed to opt out of including their public keys in a public key directory (PKD) where the PKD is published.

Commentary

In a PKI the role of the public key directory is to allow general access to public keys for two purposes. The first would be in respect to authentication so that the authentication public key can be accessed in order to authenticate the identity of the subscriber. The second purpose would be to access a subscriber's confidentiality public key to send them an encrypted message.

Privacy concerns arise from the risk of possible browsing of public key directories, downloading bulk data from them or using them in other ways that may be privacy-invasive. It is understood that PKDs, as designed by some CAs, may contain e-mail addresses. This being the case, the publication of PKDs entails the following privacy risks:

- E-mail address harvesting for spamming purposes; and
- Information published in PKDs may be combined with other publicly available information to create profiles of individuals and their activities for marketing or other purposes.

It is an established privacy protection procedure that individuals be permitted to opt out of published registers and directories. For example, an opt out regime exists in respect to telephone directories.

Gatekeeper does not require the publication of a PKD. In closed PKIs for example, PKDs are not normally published. If the relevant agency holds or has access via a commissioned CA to copies of the public keys then it will be able to authenticate messages from a client and also send encrypted messages to them. Even where a published directory is considered to be significantly beneficial, individual clients should be given the opportunity to opt out of having their public keys listed on the directory and, instead, to send them on a case-by-case basis to particular parties they propose to transact with.

This Guideline applies to PKDs and not to CRLs.

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 online application.

Commentary

The National Privacy Principles (NPPs) set out in the *Privacy Act 1988* acknowledge that anonymous methods of conducting transactions should be made available where appropriate (NPP 8) and, while there is no similar requirement in the IPPs, the provision of anonymous alternatives has emerged as best practice in privacy protection.

Gatekeeper itself does not at this stage support anonymous certificates in part because this is precluded by the current X.509 standard for PKI certificates. However, it is not the intention of Gatekeeper to restrict agencies to use only identity certificates. Gatekeeper privacy requirement 12 – *Support of anonymous or pseudonymous certificates* reads:

> "The CA shall have the ability to provide anonymous or pseudonymous certificates where appropriate. Gatekeeper policy requires a PKI design that enables individuals to: choose to use any Distinguished Name in a certificate, except where it would be impractical to do so; and conduct pseudonymous transactions except where the agency demonstrates that it is impractical to do so."

At the same time, it is expected that Commonwealth agencies employing PKI-enabled applications will usually do so in order to ensure non-repudiation of statutory or contractual transactions. In these cases, the identity of individuals is an important component of the transaction. While pseudonymity should be supported when requested by an agency client, supporting anonymity in these cases will not be possible because an anonymous transaction is one which is not enforceable by or against the transaction party.

However, in other cases where it is appropriate for clients to be able to transact anonymously, agencies should seek to support such an option, provided that would not be inconsistent with any legal requirements on agencies or their clients.

Appendix 3 - Privacy Impact Assessments (PIA)

Guideline 3 recommends that agencies undertake a PIA before implementing a PKI application. This chapter discusses the nature and scope of a PIA.

Purpose and description of a PIA

A PIA is a tool for use in consciously and systematically identifying and addressing privacy issues.[3] PIAs may be viewed as feasibility studies from a privacy perspective.

A PIA is a tool to assist in determining whether a system and related business practices meet the requirements of the privacy laws, codes and accepted or desirable practices (including those which are not covered by the existing IPPs), and attempts to gauge consumer acceptance.[4] It allows for consideration of privacy issues in advance of privacy erosion rather than retrospectively.

The PIA process is not an objective in itself – it should be integrated into decision-making processes surrounding the PKI application under proposal.[5]

The PIA recommended in Guideline 3 requires agencies, in conjunction with their information technology personnel, to identify and address privacy issues as part of the PKI application's design and development. The process is a tool to assist agencies to minimize intrusiveness, maximize fairness and satisfy expectations of the individuals dealing with the agency as to confidentiality of their personal information.[6]

Questions that the PIA report must answer include: What is the business need for the use of digital certificates and the PKI application? What alternatives to the PKI application exist, or are there other ways in which the PKI application can be implemented? For the particular PKI application that is proposed, what negative privacy impacts may arise and how are those negative privacy impacts justified? How can those negative privacy impacts be ameliorated? How will the specific requirements of applicable privacy laws be satisfied by the proposed PKI application? [7]

---

[3] PIAs, Blair Stewart, Office of the Privacy Commissioner New Zealand, 3 Privacy Law and Policy Reporter (1996) 61, www.austlii.edu.au/au/other/plpr/vol3/vol3No04/v03n04a.html. "...even if the future requires a trade off in privacy in favour of some other material benefit a PIA allows us to make such choices rationally and with our eyes open as to their privacy 'downside'": PIAs – an early warning system, Blair Stewart, (1996) 3 PLRP 134, www.austlii.edu.au/au/other/plpr/vol3/vol3No07/v03n07f.html.

[4] John Boufford, I.S.P., President of e-Privacy Management Systems, www3.sympatico.ca/john.boufford/about.htm. See also A2.7 below.

[5] PIAs, Stewart (1996), op cit.

[6] IRS PIA Endorsed as Government-Wide Best Practice, US IRS News Releases, http://taxboard.com/Tax-News/2000/nr00-29.html

[7] PIAs, Roger Clarke, 1999, www.anu.edu.au/people/Roger.Clarke/DV/PIA.html

Importantly, the PIA is a process, rather than the generation of a report, although the findings and analysis should be documented to allow sharing of the process experience and for the process to form a useful decision-making tool.

Who should conduct the PIA?

It is proposed that the agency (rather than the Privacy Commissioner) be responsible for conducting the PIA. Having the agency undertake the PIA means that they can bring to bear past experience and expertise to find solutions or better alternatives that address privacy concerns highlighted by the PIA.

It should be recognised that those agencies, which have achieved Gatekeeper accreditation as an RA or CA, will have developed an approved privacy plan and are subject to auditing in order to have their accreditation renewed. It is expected that these plans would substantially satisfy the features of a PIA.

Sample PIA checklist

While the PIA checklist is framed as a series of questions, most of which are capable of being answered either "yes" or "no", in practice the explanation and analysis that underpin those answers should be documented in order for the report to be a useful decision-making tool.

The checklist covers privacy issues raised by both:

- the establishment and use of digital certificates within the Gatekeeper PKI; and
- the application with which the individual will use their digital certificate.

The purpose of this broader scope for the PIA is that:

- the nature of the privacy concerns raised by the application will be an element in determining whether a digital certificate is the appropriate technology to be used; and
- it will determine, in light of the privacy concerns that digital certificates raise, whether the use of digital certificates is still justified.

The checklist is a sample only. It is by no means exhaustive and is intended as a starting point to stimulate discussion of the process and analysis that agencies may undertake to assess privacy risks. In the following sample checklist, the questions are phrased to clearly identify areas of privacy concern. If the answer to a question is "no", the PIA report should document;

- the reasons, and any legal exceptions or logical exceptions that justify the PKI application not meeting the privacy concern expressed in the question;
- what could be done to make the answer "yes"; and
- if the answer is to remain "no", what procedures are in place to mitigate the possible effects of the identified risk;

- where there are no legal exceptions permitting deviation from the privacy requirements imposed by law or by binding policy (eg Gatekeeper privacy requirements), steps must be taken to amend the PKI application or surrounding process so that the answer becomes “yes”.

PKI Privacy Impact Assessment

PIA 1 - Use of digital certificates	**Yes**	**No**
Are all four features offered by PKI (authentication, integrity, non-repudiation, and confidentiality) necessary for the application? If not, what alternative technology options could be utilized to provide the necessary features without requiring individuals to procure and use digital certificates?		
PIA 2 - Description of application and digital certificates		
Describe the important features of the application, including: • List the project name for the proposed application, the name of the agency responsible and any agencies involved in the project; • Describe the use of digital certificates in plain, non-technical language; and Describe the drivers for the development of the application and the use of digital certificates, including any new needs the application will address and any public benefits the application will provide.		
PIA 3 - Personal information to be collected		
List and describe the personal information (information about an identifiable individual) to be collected in the course of using the application including: • Identifying information such as the individual's name or any identifying number assigned to the individual; • Attribute or eligibility information such as the educational, medical, criminal, employment or financial history of the individual; • Evidence of Identity (EOI) information; • Sensitive information;[8] • Biometric information; • Categories of individuals or groups the personal information will concern – and the classes of personal information collected for each category; and • Any third party personal information that may be collected.		

[8] If a definition is required one is included in the *Privacy Amendment (Private Sector) Act* 2000

PIA 4 - Method of collection	Yes	No
Will personal information be collected in the use of the digital certificate or in the application only from the individual to whom the information relates? If no: • Why can the personal information not be collected from the individual concerned? Why must it be collected from alternate sources? • Is the personal information being collected by lawful and fair means? • Is the personal information to be collected on one occasion only (ie not ongoing)?		

PIA 5 - Purpose, use and disclosure

Limits on collection

	Yes	No
Is the personal information relevant and necessary for the use of the application?		
Is there a statutory power, authority or requirement for the agency to collect and use the personal information?		
Will the information collected not intrude to an unreasonable extent on the personal affairs of the individual (especially EOI information)?		
Can information be collected in a de-identified (anonymous) or pseudonymous manner?		
Are individuals given the option of acquiring the services without having to provide some or all of the personal information sought?		

Purpose

	Yes	No
Is personal information obtained in the use of the digital certificate or in the application used exclusively for the purposes made known to and consented to by the individual?		

Secondary use

	Yes	No
If the agency finds a secondary use that can be made of data already collected, is the use consistent with uses notified to or consented by the individual? If no: • Can an individual opt not to consent to the secondary use and still be entitled to receive the services offered utilising the original application?		

Consent

	Yes	No
Will notice of the following information be given to the individual at or prior to collection: • The purpose for which the personal information is being collected? • Whether the collection of the personal information is authorised or required by or under law? • The people, bodies or agencies to which the collecting agency usually discloses personal information of the kind being collected? • Is the individual asked at or prior to collection to consent to the collection and use of the personal information? • Are uses that the agency considers 'consistent' with the primary purpose (eg audit trails of transactions) also made known to the individual?		

Disclosure

	Yes	No
Is personal information involved in the use of the digital certificate or in the application disclosed to any third party other than those of whom the individual has been notified as potential recipients of the personal information? If no, does some exception under law apply? Is the recipient's use of the personal information limited to the purpose for which it was collected? Will the recipient disclose the personal information to third parties? Will personal information disclosed to third parties be protected from privacy risks to the standard proposed to protect it?		

PIA 6 – Choice

Using PKI, use in personal information, multiple certificates

	Yes	No
Do agency customers have a choice about whether to use PKI? Can clients choose what use is made of their personal information? Do clients have a choice regarding whether they can hold multiple certificates? Are suitable protections in place if a client only wishes to use one certificate?		

Anonymous/pseudonymous

	Yes	No
Are anonymous and pseudonymous options made available to clients involved in the application, where appropriate?		

Can clients use substitute services via other means (ie without using the application) and thereby reduce (or eliminate) the personal information they are required to supply?		

PIA 7 – Storage		
Security	**Yes**	**No**
Does the level of security provided in the use of the digital certificate or in the application match the potential harm caused by breaches of privacy?		
Is the individual able to generate their own key pair? (Note: there is currently no approved user key generation on the Evaluated Products List (EPL).		
Are individuals given information about the importance and available means of maintaining key security?		
Will security measures to be reviewed over time to address new potential security hazards (eg changes to technology)?		
Retention and destruction	**Yes**	**No**
Will a retention policy / destruction schedule be developed which requires retention of personal information only for the period required for use?		
Is personal information de-identified as soon as possible?		

PIA 8 - Data quality	**Yes**	**No**
For the purpose for which it is used, will the personal information collected in the use of the digital certificate or in the application be up-to-date at all stages and on all occasions that it is used, relevant, accurate and complete.		
Will records be maintained of the date of the last update of the personal information held be maintained and used by the Agency and the source of updates to personal information?		
Will updates and modifications to personal information be disseminated to all third parties to whom personal information has been disclosed?		

PIA 9 - Access and correction	**Yes**	**No**
Can the individual ascertain whether the Agency has records that contain personal information, the nature of that information and the steps that the individual should take to access their record?		
Will the costs incurred in accessing personal information be reasonable?		
Can the data or records about an individual be updated as a result of an individual seeking correction of personal information?		

Will corrections and annotations be disseminated to third parties to whom personal information has previously been disclosed?		

PIA 10 – Potential for aggregation of personal data	**Yes**	**No**
Does the manner in which digital certificates are issued, managed and used for the application prevent the use of an individual's public key as an identifier to link, match or cross-reference personal information about that individual held in different databases?		

PIA 11 - Public register information

Certificate Revocation Lists (CRLs)

	Yes	**No**
Can a subscriber revoke their own certificate?		
Will steps be taken to ensure that no comprehensive log of CRL accesses is kept?		

Public key directories

	Yes	**No**
Is it really necessary by design for users' certificates to be publicly accessible in a directory?		
Does the Agency ensure that detailed histories of directory checks are not created by the application or by the directory manager?		
Will steps be taken to restrict directory searches to single specific searches only?		

Appendix 3 - Glossary

TERM	DEFINITION
Certificate	An electronic document signed by the CA which: (1) identifies a Key-holder; (2) binds the Key-holder to a Key Pair by specifying the Public Key of that Key Pair; and (3) should contain the other information required by the Certificate Profile
Certification Authority (CA)	A body that signs and issues digital certificates which bind clients to their keys.
Public Key Directory or Certificate Directory	The published directory listing Public Key Certificates.
Certificate Profile	The specification of the fields to be included in a Certificate.
Certificate Revocation List (CRL)	The published list of revoked and/or suspended Certificates. The CRL may form part of the Certificate Directory or may be published separately.
Commonwealth	The Commonwealth of Australia.
Compromise (of the private key)	A situation in which the secrecy of a Private Key cannot be relied on, e.g. if there has been unauthorised access to the cryptographic module in which the Private Key is stored or used, or unauthorised access to or loss or theft of media on which the Private Key is stored.
Digital signature	An electronic signature created using a Private Signature Key.
Distinguished Name	A unique identifier assigned to each Key-holder, having the structure required by the Certificate Profile.
Electronic signature	A data element associated with a message that identifies a person and indicates their approval of the contents of the message.
EOI	Evidence of Identity
EPL	Endorsed Products List. (Software evaluated for Government use by the

	Defence Signal Directorate (DSD).
Gatekeeper Accreditation	Accreditation by NOIE, granted on the basis that the CA meet the criteria set out in the Gatekeeper Report.
GPAC	Gatekeeper Policy Advisory Committee.
Gatekeeper Report	*Gatekeeper: A strategy for public key technology use in Government* published by the National Office for the Information Economy. Also available at www.govonline.gov.au.
IPP	Information Privacy Principles
Key	A data element used to encrypt or decrypt a message - includes both Public Keys and Private Keys.
Key Pair	A pair of asymmetric cryptographic Keys (i.e. one decrypts messages which have been encrypted using the other) consisting of a Public Key and a Private Key. Under Gatekeeper 2 key pairs are issued one for authentication (signing) and one for confidentiality (encryption).
NOIE	National Office for the Information Economy
NPP	National Privacy Principles
OFPC	Office of the Federal Privacy Commissioner
PKI Service Provider	Any entity, which has roles, functions, obligations or rights under the CP, other than an End Entity. PKI Service Providers include the RCA, Specification Administration Organizations, the CA and Subordinate Entities.
Private Key	The half of a Key Pair that must be kept secret to ensure confidentiality, integrity, authenticity and non-repudiation of messages.
Public Key	The half of a Key Pair, which may be made public.
Public Key Infrastructure (PKI)	The particular implementation of Public Key Technology described in the CP and other Accredited Documents, under which Keys and Certificates are issued and used.
Registration Authority (RA)	An Entity which registers applicants for Keys and Certificates. RAs may have other functions or obligations specified in the CP.
TFN	Tax File Number

Appendix 3 - List of Reference Group Members

The following public and private agencies were members of the Reference Group.

- Health Insurance Commission
- Health eSignature Authority
- Australian Taxation Office
- Centrelink
- Certification Forum of Australia
- Australian Retailers Association
- Australian Privacy Foundation
- Australian Consumer's Association
- Internet Society of Australia

Appendix 3 - List of Consulted agencies

The following agencies, including ACT Government, were consulted during the development of these Guidelines (these consultations were additional to submissions made by agencies to the Consultation Paper.)

- Health Insurance Commission
- Australian Taxation Office
- Centrelink
- Department of Employment Workplace Relations and Small Business
- Department of Education and Youth Affairs
- Australian Customs Service
- ACT Local Government

Appendix 3 - Selected Documents on Gatekeeper Privacy Protection

The following is an excerpt from the Model Head Agreement between NOIE and Accredited Certification Authorities.

32.1 The Contractor:

(a) acknowledges that it has agreed, in the Accredited Documents, to abide by the Information Privacy Principles as if it were a Commonwealth agency; and

(a) will, in the course of providing the Certification Services to Customers, comply with the obligations set out in this clause 32 in the light of its obligation described in clause 32.1(a).

32.2 The Contractor shall take all reasonable measures to ensure that Personal Information held in connection with this Head Agreement or a Contract is protected against loss, and against unauthorised access, use, modification, disclosure or other misuse in accordance with the procedures set out in the Accredited Documents and that only authorised personnel have access to the Personal Information.

32.3 The Contactor may only vary the security procedures set out in the Accredited Documents insofar as they impact on the protection of Personal Information if it does so in accordance with clause 13 of the Gatekeeper Head Agreement.

32.4 The Contractor shall use any Personal Information held in connection with this Head Agreement or a Contract only for the purposes of fulfilling its obligations under this Head Agreement or the Contract, as the case requires.

32.5 The Contractor shall not disclose any Personal Information obtained in connection with this Head Agreement or a Contract without the prior written approval of NOIE. The Contractor shall immediately notify NOIE where it becomes aware that a disclosure of Personal Information may be required by law.

32.6 The Contractor shall not transfer Personal Information held in connection with this Head Agreement or a Contract outside Australia, or allow parties outside Australia to have access to it, without the prior written approval of NOIE or the Customer, as the case requires.

The Contractor shall ensure that any of its employees or any sub-contractor, requiring access to any Personal Information held in connection with this Head Agreement or a Contract, before accessing that Personal Information, must:

(a) give a written undertaking not to access, use, disclose or retain Personal Information except in performing their duties of employment or as a sub-contractor; and

(a) be informed that failure to comply with the written undertaking may be a criminal offence and may also lead the Contractor to take disciplinary action against the employee and legal action against the sub-contractor.

32.7A Clause 32.7 shall not be read so as to prevent an employee or sub-contractor from using, for their own purposes, any information that it acquires independently of its employment or work for the Contractor.

The Contractor shall, in respect of any Personal Information held in connection with this Head Agreement or a Contract, immediately notify NOIE where the Contractor becomes aware of a breach of clauses 32.2, 32.3, 32.4, 32.5, 32.6 or 32.7.

The Contractor acknowledges that:

(c) any unauthorised and intentional access, destruction, alteration, addition or impediment to access or usefulness of Personal Information stored in any computer in the course of performing its obligations under this Head Agreement or a Contract is an offence under Part VIA of the *Crimes Act 1914* (Cth) for which there are a range of penalties, including a maximum of ten years imprisonment; and

(c) the publication or communication of any fact or document by a person which has come to their knowledge or into their possession or custody by virtue of the performance of any of their obligations under this Head Agreement or a Contract (other than to a person to whom the Contractor is authorised to publish or disclose the fact or document) may be an offence under section 70 of the *Crimes Act 1914* (Cth), the maximum penalty for which is two years imprisonment.

32.10 The Contractor shall in respect of any Personal Information held in connection with this Head Agreement or a Contract co-operate with any reasonable requests or directions of NOIE arising directly from, or in connection with the exercise of the functions of the Privacy Commissioner under the *Privacy Act 1988* (Cth) or otherwise, including, but not limited to, the issuing of any guideline concerning the handling of Personal Information.

32.11 The Contractor shall indemnify the Commonwealth in respect of any liability, loss or expense which is incurred and which arises out of or in connection with a breach of the obligations of the Contractor or any sub-contractor of this clause 32 or for a breach of an obligation of confidence arising under the *Privacy Act 1988* (Cth) except to the extent that the liability, loss or expense was caused by an act or omission of NOIE.

32.12 In clause 32.11 ‘liability, loss or expense’ includes any amount paid by NOIE on behalf of the Commonwealth for an interference with the privacy of an individual being a reasonable amount as compensation for loss or damage for which the Commonwealth would have been liable under the *Privacy Act 1988* (Cth) if such breach had been that of a Commonwealth Agency.

32.13 A complaint alleging an interference with the privacy of an individual in respect of any services performed under this Head Agreement or a Contract shall be handled by NOIE and in accordance with the following procedures:

(a) where NOIE receives a complaint alleging an interference with the privacy of an individual by the Contractor or any sub-contractor, it shall immediately notify the Contractor of only those details of the complaint necessary to minimise any breach or prevent further breaches of the above clauses;

(a) where the Contractor receives a complaint alleging an interference with the privacy of an individual by the Contractor or any sub-contractor, it shall immediately notify NOIE of the nature of the complaint but shall only release to NOIE Personal Information concerning the complainant with that person's consent;

(a) after NOIE has given or been given notice in accordance with clause 32.13(a) or clause 32.13(b), it shall keep the Contractor informed of all progress with the complaint as relates to the actions of the Contractor in connection with the allegation of an interference with the privacy of an individual; and

(a) NOIE shall give the Contractor 10 Business Days written notice of an intention to assume a liability, loss or expense in accordance with this clause 32 including in that notice an explanation of how that liability loss or expense was assessed and the Contractor's proposed share of that liability.

32.14 This clause 32 shall continue to have effect after the termination or completion of this Head Agreement or a Contract.

32.15 The operation of this clause 32, in relation to a particular Customer, is to be read in conjunction with the terms of the Contract with that Customer.

Gatekeeper Accreditation Privacy Criteria

PC	CRITERIA
01	**Manner and extent of collection of personal information** **Deemed to Comply Standards/ Documents** IPP 1, 2 and 3 & *Commonwealth Protective Security Manual*
02	**Security safeguards in relation to personal information** **Deemed to Comply Standards/ Documents** IPP 4 & *Commonwealth Protective Security Manual*

03	**Openness about the types of personal information held and information handling policies** **Deemed to Comply Standards/ Documents** IPP 5 & *Commonwealth Protective Security Manual*
04	**Availability of procedures to allow subjects of personal information to access and correct the information**

	Deemed to Comply Standards/ Documents IPPs 6 and 7 & *Commonwealth Protective Security Manual*
05	**Accuracy of personal information** **Deemed to Comply Standards/ Documents** IPP 8 & *Commonwealth Protective Security Manual*
06	**Personal information is used only for relevant purposes** **Deemed to Comply Standards/ Documents** IPP 9 & *Commonwealth Protective Security Manual*
07	**Limits placed on the use of personal information** **Deemed to Comply Standards/ Documents** IPP 10 & *Commonwealth Protective Security Manual*
08	**Limits placed on disclosure of personal information** **Deemed to Comply Standards/ Documents** IPP 11 & *Commonwealth Protective Security Manual*
09	**Privacy protection is provided for personal information published in publicly accessible lists / registers** (Controls over how personal information is accessed, searched and used) ❑ No personal information shall be made publicly available in CRLs and other directory services. ❑ RAs shall collect and hold minimal personal information when logging accesses to CRLs or other directory services. ❑ RAs should not disclose personal information collected by logging access to CRLs or other directory services, except in circumstances where, if that information were protected telecommunications information, they would be authorised or required to disclose the information under Part 13, Division 3, Subdivision A of the *Telecommunications Act 1997*.
10	**Multiple certificates** Persons to whom certificates are issued (Users) will be allowed to have more than one certificate from the same RA, wherever the use of multiple certificates is not inconsistent with the purpose of those certificates, ie. users should not be limited to one certificate when dealing with more than one agency.
11	**Notification Procedure** RAs will establish and follow procedures to notify users whether the IPPs or National Privacy Principles (NPPs) apply to protect personal information collected and held by the RA for the purpose of issuing and managing certificates, and the applicable mechanism for making and investigating privacy complaints.
12	**Support of Anonymous or Pseudonymous Certificates** The RA should have the ability to provide anonymous or pseudonymous certificates where appropriate.

Appendix 3 - Privacy Recommendations to the CEO, NOIE, regarding the use of Gatekeeper Certificates by Individuals

The Government Public Key Authority (GPKA) made the following recommendations to the Chief Executive Officer of the then Office for Government Online (OGO) (now NOIE) in May 2000. The recommendations were accepted and have been incorporated into Gatekeeper policy and form part of the accreditation requirements for subsequent Gatekeeper service and service provider accreditations.

The GPKA (now GPAC) provides advice on Gatekeeper policy including privacy, and includes a specialist privacy member who is able to reflect community and consumer interests. NOIE has accepted the advice of GPAC in relation to situations where an individual subscriber (the 'user' or 'end user') of a Commonwealth agency is using a Gatekeeper accredited digital signature certificate to support online transactions with the Commonwealth agency.

Multiple Use of Key-Pairs or Certificates

Gatekeeper requires a PKI design that embodies subscriber choice to enable use of the same certificate pairs for multiple purposes or multiple certificate pairs for separate purposes, provided separate key-pairs are used for digital signature (authenticity) and confidentiality; so that in cases where subscribers have multiple certificates and where relying parties may accept one or more of these, a subscriber may choose which certificate he or she will provide to the relying party.

Key-Pair Generation

Gatekeeper requires a PKI design that ensures that the key-pair which constitutes the signature will be generated and distributed in such a way that:

- the private key is only available to its owner;
- precludes (in the case of a subscriber operating as a private person) any person other than the owner from ever being in possession of a private authentication key without the owner's consent; and
- the certifying authority can be satisfied that the public key corresponds to the owner's private key.

This would normally allow a subscriber the option of generating his or her own private key. An agency may decline to accept a digital signature if the generation process is not compliant with established quality or standards and end-user product key generation accreditation if applicable.

Personal Choice as to Issuers of Certificates and Tokens

Gatekeeper requires a PKI design that embodies subscriber choice in relation to both the accredited issuer of certificates and the private key and certificate storage, or contains other forms of safeguard that provides equivalent subscriber protections.

Note: The Gatekeeper strategy expects, over time, to accredit a mature market of PKI service providers from which end subscribers and relying parties may select a service provider based upon individual privacy and business concerns. The strategy will provide subscriber choice also in terms of private key and certificate storage between physical tokens, storage on their hard disk or other means made available by evolving technology.

Personal Possession and Control of Tokens

Gatekeeper requires a PKI design that incorporates subscriber possession and control of tokens, such that the issuer may cancel the validity of a token it has issued but may not compulsorily repossess the private key.

Pseudonymity

Gatekeeper requires a PKI design that enables individuals to:

- choose to use any distinguished name in a certificate, except where it would be impractical to do so.
- conduct pseudonymous transactions except where the agency demonstrates that it is impractical to do so.

Note: Gatekeeper does not generally support anonymous transactions, because it is an authentication framework, and authentication is not possible in the conduct of anonymous transactions. EOI is required to obtain a Gatekeeper certificate. There may, however, be technologies and processes other than PKI that agencies may consider using to allow individual subscribers to deal securely and anonymously with them.

Key Revocation

Gatekeeper requires a PKI design that incorporates effective privacy controls over the information contained in CRLs and how CRLs are accessed and searched.
Note: This means for example that, while revocation of a certificate must be published in a CRL, the reasons for revocation or suspension must not be disclosed. Also, access to a Certificate Directory or CRL will generally be limited to single searches.

Non-Intrusive Identification Processes

Gatekeeper requires a PKI design that ensures that individuals are only subjected to appropriate identification procedures to meet agency authentication requirements or to satisfy applicable law and that intrusive procedures are minimised to the greatest extent possible.

Centralised Storage of Identification Details

Gatekeeper requires a PKI design that ensures that there is no single centralised storage of PKI distinguished name or identification details.
Note: The Gatekeeper strategy has created a framework whereby the storage of personal information needed for identification is diffused between the RA and the CA, in order to prevent centralised storage. Both of the bodies are bound to observe the Information Privacy Principles, and there are limitations on information that an RA can pass to a CA.

Freedom from Appropriation and Cancellation of Identity

Gatekeeper requires a PKI design that ensures a person's identity cannot be appropriated, cancelled or compromised within the PKI structure.

Note: The Gatekeeper accreditation process requires that service providers bind end subscribers to a subscriber agreement obligating them to adequately protect their private key. Also, Gatekeeper expects CAs to prescribe minimum authentication requirements for the lodgement of certificate revocation requests.

Status

These recommendations have been accepted by the CEO, NOIE and now have the force of Gatekeeper policy. They have been incorporated into the appropriate Gatekeeper accreditation requirements.