



– AGIMO –

Gatekeeper PKI Framework

AGIMO - Gatekeeper - Privacy
Impact Assessment (PIA)
(v09 20 June 2006)

Contact: Galexia

Suite 95 Jones Bay Wharf, 26-32 Pirrama Road,
Pyrmont (Sydney) NSW 2009, Australia

ACN:097 993 498

Ph: +61 2 9660 1111

Fax: +61 2 9660 7611

WWW: www.galexia.com

Email: gatekeeper-manage@galexia.com

Document Control

Client

This document has been written for AGIMO (Australian Government Information Management Office).

Document Purpose

This document is the Privacy Impact Assessment (PIA) (Output 5.1) for the *Gatekeeper PKI Project* as at June 2006.

Document Identification

Document title: Output 5.1 Privacy Impact Assessment (PIA) (v09 20 June 2006)
Document filename: gc209_output_5_1_pia_v09_20060620_final.doc
Document date: 20/06/2006 3:44 PM
Published to Extranet: https://www.galexia.com/extranet/agimo-gatekeeper/extranet_document_store/output_5_privacy/output_5_1_pia/

Document Production

Client Contacts: AGIMO - Australian Government Information Management Office
Minter Ellison Building
25 National Circuit
Barton ACT

Drew Andison
Team Leader, Gatekeeper
Email: Drew.Andison@finance.gov.au
Direct: +61 (0) 2 6215 1544
Fax: +61 (0) 2 6215 1659

Consultant Contact: Peter van Dijk (Engagement Director)
Galexia
Suite 95 Jones Bay Wharf
26-32 Pirrama Road, Pyrmont NSW 2009
Phone: +612 9660 1111
Fax: +612 9660 7611
Email: agimo-gatekeeper-manage@galexia.com
Mobile: +61 419 351 374 (Peter van Dijk)

Document Authors: Galexia
Galexia Reference: GC209
Project extranet: <https://www.galexia.com/extranet/agimo-gatekeeper/>

Copyright

Copyright © 2006 Australian Government Information Management Office (AGIMO) and Galexia.

Contents

1.	Executive Summary.....	5
2.	Scope and Methodology	8
	2.1. <i>Scope</i>	8
	2.2. <i>PIA guidelines</i>	8
	2.3. <i>Privacy legislation</i>	9
	2.4. <i>Potential privacy law reform</i>	10
	2.5. <i>Gatekeeper Privacy Requirements</i>	11
3.	Gatekeeper PKI Framework	15
	3.1. <i>Overview</i>	15
	3.2. <i>The future of Gatekeeper privacy protection</i>	16
4.	Personal Information to be Collected	18
	4.1. <i>Background</i>	18
	4.2. <i>Gatekeeper compliance</i>	18
	4.3. <i>Current Gatekeeper protections</i>	19
	4.4. <i>Personal Information to be Collected finding</i>	20
5.	Method of Collection	21
	5.1. <i>Background</i>	21
	5.2. <i>Gatekeeper compliance</i>	21
	5.3. <i>Current Gatekeeper privacy protections</i>	22
	5.4. <i>Method of Collection finding</i>	22
6.	Purpose, Use and Disclosure.....	23
	6.1. <i>Background</i>	23
	6.2. <i>Gatekeeper compliance</i>	23
	6.3. <i>Current Gatekeeper privacy protections</i>	25
	6.4. <i>Purpose, Use and Disclosure finding</i>	26
7.	Choice	27
	7.1. <i>Background</i>	27
	7.2. <i>Gatekeeper compliance</i>	27
	7.3. <i>Current Gatekeeper privacy protections</i>	28
	7.4. <i>Choice finding</i>	29
8.	Security.....	30
	8.1. <i>Background</i>	30
	8.2. <i>Gatekeeper compliance</i>	30
	8.3. <i>Current Gatekeeper privacy protections</i>	31
	8.4. <i>Security finding</i>	32
9.	Data Quality	33
	9.1. <i>Background</i>	33
	9.2. <i>Gatekeeper compliance</i>	33
	9.3. <i>Current Gatekeeper privacy protections</i>	34
	9.4. <i>Data Quality finding</i>	34

10.	Access and Correction.....	35
	10.1. Background	35
	10.2. Gatekeeper compliance	35
	10.3. Current Gatekeeper privacy protections	36
	10.4. Access and Correction finding	36
11.	National ID Potential.....	37
	11.1. Background	37
	11.2. Gatekeeper and National ID potential	37
	11.3. Current Gatekeeper privacy protections	38
	11.4. National ID Potential finding	38
12.	Complaints	39
	12.1. Background	39
	12.2. Gatekeeper compliance	39
	12.3. Current Gatekeeper privacy protections	39
	12.4. Complaints finding	39
13.	Function Creep	40
	13.1. Background	40
	13.2. Gatekeeper compliance	40
	13.3. Current Gatekeeper privacy protections	41
	13.4. Function Creep finding	41
14.	Reform of Gatekeeper Privacy Requirements	42
15.	Appendix – Gatekeeper Privacy Criteria	43
16.	Appendix – GPKA Privacy Recommendations to the CEO	44
	16.1. GPKA R1 – Multiple Use of Key-Pairs or Certificates	44
	16.2. GPKA R2 – Key-Pair Generation	44
	16.3. GPKA R3 – Personal Choice as to Issuers of Certificates and Tokens	44
	16.4. GPKA R4 – Personal Possession and Control of Tokens	45
	16.5. GPKA R5 – Pseudonymity	45
	16.6. GPKA R6 – Key Revocation	45
	16.7. GPKA R7 – Non-Intrusive Identification Processes	45
	16.8. GPKA R8 – Centralised Storage of Identification Details	45
	16.9. GPKA R9 – Freedom from Appropriation and Cancellation of Identity	46
17.	Appendix – OPC PKI Guidelines	47
	17.1. OPC PKI Guideline 1 – Agency Client Choice on the Use of PKI Applications	47
	17.2. OPC PKI Guideline 2 – Awareness and Education	47
	17.3. OPC PKI Guideline 3 – Privacy Impact Assessments (PIAs)	47
	17.4. OPC PKI Guideline 4 – Evidence of Identity	47
	17.5. OPC PKI Guideline 5 – Aggregation of Personal Information	47
	17.6. OPC PKI Guideline 6 – Single or Multiple Certificates	48
	17.7. OPC PKI Guideline 7 – Subscriber Generation of Keys	48
	17.8. OPC PKI Guideline 8 – Public Key Directories	48
	17.9. OPC PKI Guideline 9 – Pseudonymity and Anonymity	48

1. Executive Summary

This document is a Privacy Impact Assessment (PIA) for the *Gatekeeper PKI Framework* as at June 2006.

This PIA is being conducted in accordance with draft *PIA Guidelines* issued by the Office of the Privacy Commissioner¹.

The broad purpose of this PIA is to assess the potential privacy legal issues and privacy perception issues that arise from the reform of Gatekeeper as reflected in the Gatekeeper PKI Framework and related documents.

Information contained in this Privacy Impact Assessment (PIA) is based on:

- Meetings with the Australian Government Information Management Office (AGIMO);
- Review of available Gatekeeper documentation;
- General research and literature review on PKI and privacy;
- Review of relevant privacy legislation;
- Review of existing Gatekeeper Privacy Requirements; and
- Review of PKI Privacy Guidelines published by the Office of the Privacy Commissioner.

Galexia's advice in this PIA concentrates on Commonwealth *Privacy Act* compliance and community perceptions.

Galexia's initial conclusions, based on an understanding of the Gatekeeper PKI Framework as currently described are:

- **A. Personal information**
The Gatekeeper PKI Framework requires significant collection of personal information. However, the level of intrusion is mapped to risk, and if an appropriate category of certificate is selected, the collection of information will be set at an appropriate level.
(Refer to *Section 4. Personal Information to be Collected* at page 18.)
- **B. Method of collection**
The method of collection in all Gatekeeper categories will be lawful and fair. Some limited third party collection may occur, and this will require detailed explanation to certificate holders.
(Refer to *Section 5. Method of Collection* at page 21.)

¹ <<http://www.privacy.gov.au>>

- **C. Purpose use and disclosure**

Controls on purpose, use and disclosure need to be exercised at the application level, and they can be difficult to apply to a broad framework like Gatekeeper. A combination of general Information Privacy Principle (IPP) compliance and a specific Gatekeeper Privacy Requirement in relation to Certificate Revocation Logs (CRLs) will result in an appropriate level of privacy protection.
(Refer to *Section 6. Purpose, Use and Disclosure* at page 23.)
- **D. Choice**

The provision of user choice in relation to Gatekeeper is affected by both Gatekeeper policy and market conditions. Specific Gatekeeper Privacy Requirements ensuring user choice may need to be provided – such as the consideration of alternative authentication channels and the acceptance of multiple certificates. The reforms contained in the revised Gatekeeper PKI Framework should have a positive impact on user choice, especially as they would allow the development of anonymous and pseudonymous certificates in appropriate circumstances in the Bronze category (and perhaps in relation to some Special Purpose Certificates).
(Refer to *Section 7. Choice* at page 27.)
- **E. Security**

Gatekeeper facilitates compliance with the minimal security requirements contained in privacy legislation. Gatekeeper is itself an enhanced security regime, mapped carefully to the levels of risk in any transaction. Some specific Gatekeeper Privacy Requirements in relation to security may be required to ensure an appropriate level of privacy protection. These could focus on key generation and subscriber security of keys.
(Refer to *Section 8. Security* at page 30.)
- **F. Data quality**

Gatekeeper facilitates compliance with the data quality requirements contained in privacy legislation. Gatekeeper is, itself, a system for ensuring that information is created, transferred and maintained with a high degree of accuracy.
(Refer to *Section 9. Data Quality* at page 33.)
- **G. Access and correction**

Gatekeeper does not appear to raise any specific access and correction issues.
(Refer to *Section 10. Access and Correction* at page 35.)
- **H. National ID potential**

The reforms contained in the revised Gatekeeper PKI Framework do have an impact on the National ID potential of Gatekeeper, in that the Silver category anticipates the possibility of a single certificate for use with multiple Commonwealth agencies. However, this issue can be alleviated since the Gatekeeper Framework does allow for multiple providers of Silver certificates operating in the market place. In combination with other privacy protections contained in Gatekeeper (eg in relation to Choice), the National ID potential of Gatekeeper should remain limited.
(Refer to *Section 11. National ID Potential* at page 37.)
- **I. Complaints**

Gatekeeper does not appear to raise any specific issues in relation to complaints.
(Refer to *Section 12. Complaints* at page 38.)

—

J. Function creep

Gatekeeper does have the potential to raise issues of function creep. A specific Gatekeeper Privacy Requirement in relation to function creep may be necessary. It could focus on the ongoing conduct of Privacy Impact Assessments or Privacy Compliance Checklists as appropriate.

(Refer to *Section 13. Function Creep* at page 40.)

Galexia's overall conclusion is that although some new issues are raised by the Gatekeeper reforms, existing Gatekeeper Privacy Requirements effectively cover most issues.

However, a problem arises because the existing Gatekeeper Privacy Requirements are fragmented. There are multiple documents that contain overlapping privacy requirements relating to Gatekeeper.

This issue is considered throughout this Privacy Impact Assessment (PIA) and will be the subject of further discussion in the subsequent Privacy Management Strategy (PMS).

Some initial advice on consolidating Gatekeeper Privacy Requirements is provided. The result (if these recommendations are accepted) would be a general agreement to comply with the Information Privacy Principles (IPPs) (contained, for example in the Head Agreement) plus four short additional Gatekeeper Privacy Requirements (contained, in accredited service provider evaluation criteria).

This consolidation should significantly reduce the paperwork and compliance burden in Gatekeeper, with no reduction in overall privacy protection.

2. Scope and Methodology

Galexia² is conducting a Privacy Impact Assessment (PIA) for the *Gatekeeper PKI Framework*. Currently, parts of the Framework are under development – this PIA represents an analysis of the privacy impact of a “snap shot” of Gatekeeper, as it is currently described (June 2006).

2.1. Scope

The scope of this PIA is limited to the following items:

In Scope	Out of Scope
<ul style="list-style-type: none"> • Broad overview of relevant privacy laws. • <i>Gatekeeper PKI Framework</i> and the published documents and guidelines. • Broad implications of all proposed Gatekeeper reforms. • Insight from sample stakeholders. • Survey of existing (relevant) data on community attitudes. 	<ul style="list-style-type: none"> • Detailed consideration of individual agency implementations. • Detailed consideration of audit and enforcement regime for Gatekeeper (subject to further review later in 2006). • Detailed stakeholder consultation. • Original research or data collection on community attitudes.

2.2. PIA guidelines

This PIA is being conducted in accordance with *PIA Guidelines* issued by the Office of the Privacy Commissioner (OPC). Currently, the *PIA Guidelines* are in draft form, and the OPC is accepting submissions on the draft.

Galexia considered two other forms of PIA guidance, although not in the same amount of detail as the OPC Guidelines. These were:

- **Attorney General’s Department (Commonwealth) Privacy Checklist**
A Privacy Impact Checklist (PIC) has been developed by the Attorney-General’s Department to assist agencies to take proper account of privacy in the early developmental stages of a proposed project or policy. It is a tool designed to help agencies consider the requirements of the Commonwealth’s privacy regime (the *Privacy Act* including the IPPs and agency-specific privacy requirements) early in program or policy development.
- **Victorian Privacy Commissioner’s PIA Guidelines**
Similarly, the Victorian Privacy Commissioner’s Privacy Impact Assessments – a guide (released in August 2004) is intended to help organisations (both public and private) to assess how effectively they are managing their legal obligations and privacy risks, while encouraging identification of improved ways to enhance privacy in their operations.

² <<http://www.galexia.com.au>>

Please note that the headings used in this PIA reflect the OPC *PIA Guidelines* with some customisation by Galexia.

2.3. Privacy legislation

Relevant privacy laws in Australia include:

- Commonwealth, State and Territory privacy legislation;
- Information Standards (for example, Queensland);
- Health specific privacy legislation (where health information is being collected);
- Privacy and confidentiality provisions within other laws;
- Codes of conduct; and
- The common law.³

Australia has the following general privacy legislation (or guidelines) in place:

Jurisdiction	Legislation	Regulator
Cth	<i>Privacy Act 1988 (Cth)</i>	Federal Privacy Commissioner
ACT	<i>Privacy Act 1988 (Cth)</i>	Federal Privacy Commissioner
NSW	<i>Privacy and Personal Information Protection Act 1998 (NSW)</i>	NSW Privacy Commissioner
NT	<i>Information Act 2002 (NT)</i>	NT Information Commissioner
Qld	<i>Information Standard 42</i>	Queensland Ombudsman
SA	Cabinet Administrative Instruction 1/89	Privacy Committee of South Australia
Tas	<i>Personal Information and Protection Act 2004 (Tas)</i>	Tasmanian Ombudsman
Vic	<i>Information Privacy Act 2000 (Vic)</i>	Victorian Privacy Commissioner
WA	No law. Note discussion paper (May 2003). ⁴	–

The State and Territory legislation in this list generally applies to the activities of State and Territory public sector agencies.

This PIA has been written with a focus on current Commonwealth privacy legislation – the *Privacy Act 1988*. The Act sets out the Information Privacy Principles (IPPs), which regulate the collection, use and disclosure of personal information by Commonwealth agencies. The Act also includes a complaints, audit and enforcement regime.

³ There is continuing academic discussion and occasional judicial consideration of whether or not a tort of privacy exists in Australian common law. However, for the purposes of this PIA it is safe to assume that the dominant privacy protection in Australian law comes from legislation, rather than the common law. This is likely to be the case for many years to come.

⁴ Office of the Attorney General for Western Australia, *Privacy Legislation for Western Australia Discussion Paper*, May 2003, <http://www.ministers.wa.gov.au/mcginty/docs/features/McGinty_privacy_legislation.pdf>.

The Commonwealth legislation applies to both the Commonwealth public sector, and significant parts of the private sector. However two different standards of privacy protection exist in the Commonwealth legislation:

- **Information Privacy Principles (IPPs)**
Eleven IPPs that apply to Commonwealth and ACT government agencies.
- **National Privacy Principles (NPPs)**
The *Privacy Act* was amended in 2001⁵ to include ten NPPs that apply to parts of the private sector (those that earn more than \$3 million annually and all health service providers).

2.4. Potential privacy law reform

Commonwealth privacy legislation is currently the subject of a review by the Australian Law Reform Commission. The ALRC review builds on earlier work by a Senate Committee and by the Office of the Privacy Commissioner. It is possible that changes to the IPPs and NPPs may result from this review. This PIA is based on existing law, and should be reviewed if the *Privacy Act* is amended in the future.

- **Office of the Privacy Commissioner (OPC) Review (2005)**
The OPC Review focused on the private sector provisions of the *Privacy Act*. A final report was published in May 2005 and included several important recommendations for achieving greater consistency in Australian privacy legislation. The Government has not responded to these recommendations, and it is likely that any response will be delayed until the conclusion of the ALRC review (below).
- **Australian Law Reform Commission (ALRC) Review (2006)**
The ALRC has been given broad terms of reference to review all aspects of Australian privacy law, including the matters raised in the earlier OPC review. This review will also cover the public sector provisions of the *Privacy Act*.

One potential impact of the ALRC review is that Commonwealth, State and Territory governments may be reluctant to seek substantial amendments of privacy law prior to the completion of the ALRC review. The ALRC is not due to report until 2008, and the Government's response to the report may take several months after this to prepare. The implementation of any recommendations will take longer.

⁵ *Privacy Amendment (Private Sector) Act 2000* (Cth).

2.5. Gatekeeper Privacy Requirements

The determination of what particular privacy protections that apply to Gatekeeper is complex. The current Gatekeeper FAQ on privacy states:

What privacy protections are in place within Gatekeeper?

Gatekeeper has an extensive range of privacy protections in place. There are 12 criteria for accreditation as a service provider that relate specifically to privacy. These criteria are further explained in detailed privacy recommendations from the former Gatekeeper Policy Advisory Council (GPAC). The Head Agreement that Gatekeeper service providers must sign with AGIMO binds the service provider to the Information Privacy Principles as contained in the Privacy Act 1988. Head Agreements also contain a number of other requirements to protect personal information. Privacy Audits may be conducted within the terms of these agreements. Users must have the option to possess multiple key pairs under the Gatekeeper framework. Gatekeeper supports pseudonymous certificates. Key escrow is not required under Gatekeeper. The Gatekeeper Policy Committee (GPC) includes the Office of the Privacy Commissioner as an Observer to reflect wider community interest⁶.

In practice a mixture of legislated privacy protections and privacy guidance is contained in the following documents:

- *Information Protection Principles (IPPs)*
- *Gatekeeper Privacy Criteria*
- *GPKA Privacy Recommendations*
- *OPC PKI Privacy Guidelines*
- *Other privacy requirements*

⁶ AGIMO, *Gatekeeper Frequently Asked Questions - Legal* (Revised: 6 May 2005), <http://www.agimo.gov.au/infrastructure/gatekeeper/faq#legal>.

2.5.1. *Information Protection Principles (IPPs)*

Commercial service providers that have received Gatekeeper accreditation are contractually bound (through the Head Agreement) to comply with the Information Privacy Principles (IPPs) as contained in the *Privacy Act 1988* as if they were a government agency.

There are two sub-categories of binding to the IPPs:

- **Statutory binding**
Where an organisation is providing services as a Contracted Service Provider (CSP) they are bound by the IPPs through the provisions of Section 95 B of the *Privacy Act*. The majority of service provision in Gatekeeper will be subject to this requirement, as accredited service providers are effectively providing an outsourced authentication function for Government Agencies.
- **Contractual binding**
Where an organisation is providing services to third parties, who may or may not be Commonwealth Agencies (eg State Agencies or the private sector), they may not meet the definition of a Contract Service Provider (CSP) in the *Privacy Act*. However, it will still be a condition of their use of the Gatekeeper brand that they comply with the IPPs. This “contractual binding” will be located in the Head Agreement.

The main difference between the two sub-categories is that complaints to the Office of the Privacy Commissioner (OPC) and some OPC audit functions only apply in the first category. The Gatekeeper Competent Authority would have responsibility for investigating privacy breaches in the second category.

2.5.2. *Gatekeeper Privacy Criteria*

The Gatekeeper framework includes additional privacy rules that apply to accredited service providers (RAs and CAs). The full criteria are included in *Appendix – Gatekeeper Privacy Criteria* at page 43. Briefly, they cover:

- **PC01** – Manner and extent of collection of personal information;
- **PC02** – Security safeguards in relation to personal information;
- **PC03** – Openness about the types of information held and handling policies;
- **PC04** – Procedures for correction of personal information by subjects;
- **PC05** – Accuracy of personal information;
- **PC06** – Personal information is used only for relevant purposes;
- **PC07** – Limits placed on the use of personal information;
- **PC08** – Limits placed on disclosure of personal information;
- **PC09** – Privacy protection for publicly accessible information;
- **PC10** – Multiple certificates;
- **PC11** – Notification Procedure; and
- **PC12** – Support of Anonymous or Pseudonymous Certificates.

These Gatekeeper rules do not apply directly to individual Agency/client relationships (such issues are covered by the OPC PKI Guidelines discussed below).

2.5.3. GPKA Privacy Recommendations

In May 2000 the Government Public Key Authority (now the Gatekeeper Policy Committee) made certain recommendations to the Chief Executive Officer of the then Office for Government Online (OGO) (now AGIMO). The recommendations were accepted and incorporated into Gatekeeper policy⁷.

Their current status is uncertain – the AGIMO website states that “although they are not themselves evaluated they do form part of the Head Agreement for subsequent Gatekeeper Service Provider accreditations”.

The full recommendations are included in *Appendix – GPKA Privacy Recommendations to the CEO* at page 44. Briefly, they cover:

- GPKA R1 – Multiple Use of Key-Pairs or Certificates;
- GPKA R2 – Key-Pair Generation;
- GPKA R3 – Personal Choice as to Issuers of Certificates and Tokens
- GPKA R4 – Personal Possession and Control of Tokens;
- GPKA R5 – Pseudonymity;
- GPKA R6 – Key Revocation;
- GPKA R7 – Non-Intrusive Identification Processes
- GPKA R8 – Centralised Storage of Identification Details; and
- GPKA R9 – Freedom from Appropriation and Cancellation of Identity.

2.5.4. OPC PKI Privacy Guidelines

Privacy issues may also arise when PKI is used in communications between governments and individual clients. In 2001, the Office of the Privacy Commissioner published the *Privacy and Public Key Infrastructure – Guidelines for Agencies using PKI to communicate or transact with individuals*.⁸

The Guidelines are formal Guidelines in that they were issued 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.

⁷ They are available at:
<<http://www.agimo.gov.au/infrastructure/gatekeeper/advisory/recommendations>>

⁸ The Office of the Federal Privacy Commissioner, *Privacy and Public Key Infrastructure - Guidelines for Agencies using PKI to communicate or transact with individuals*, (2001) <<http://www.privacy.gov.au/publications/pki.rtf>>.

The full Guidelines are included in *Appendix – OPC PKI Guidelines* at page 47. Briefly, they cover:

- OPC PKI Guideline 1 – Agency Client Choice on the Use of PKI Applications
- OPC PKI Guideline 2 – Awareness and Education
- OPC PKI Guideline 3 – Privacy Impact Assessments (PIAs)
- OPC PKI Guideline 4 – Evidence of Identity
- OPC PKI Guideline 5 – Aggregation of Personal Information
- OPC PKI Guideline 6 – Single or Multiple Certificates
- OPC PKI Guideline 7 – Subscriber Generation of Keys
- OPC PKI Guideline 8 – Public Key Directories
- OPC PKI Guideline 9 – Pseudonymity and Anonymity

2.5.5. *Other privacy requirements*

In practice, the Certificate Policies of Gatekeeper accredited service providers have included text similar to the following:

1. The CA and the Relevant RA must comply with their obligations under the *Privacy Act 1988* (Cth), including (where applicable) the National Privacy Principles (NPPs) or any approved privacy code.
2. When providing services to or in relation to a Commonwealth Agency, the CA and the relevant RA must also comply with the Information Privacy Principles (IPPs), as if they were Agencies of the Commonwealth of Australia.
3. When providing services to or in relation to a State or Territory Agency, the CA and the relevant RA must also comply with:
 - (a) any privacy law applicable to service providers to that agency; and
 - (b) any other privacy obligations imposed by or in relation to that agency.

The result is that additional privacy requirements from the National Privacy Principles (NPPs), relevant industry codes of conduct and/or State and Territory privacy legislation are incorporated into the Gatekeeper documentation.

3. Gatekeeper PKI Framework

3.1. Overview

The Australian Government's vision is to make greater use of Information and Communications Technology (ICT) to enable a transformation of the business of government. A critical element of enabling electronic service delivery is having the means to authenticate and secure on-line transactions. Choice of service models will be available but increasingly individuals and business are choosing to utilise electronic authentication to participate in electronic transactions.

Simplified sign-on procedures to access connected government services in an environment of privacy and security may reduce the cost and complexity of interacting with government.

One of the initiatives achieve this vision has been the development of a new Gatekeeper Framework for the use of Public Key Infrastructure (PKI) by citizens and business in their interactions with government. The Gatekeeper PKI Framework (the Framework) will:

- Facilitate the deployment of a broader range of digital certificates designed to meet specific business requirements of agencies and their clients.
- Facilitate adoption of a risk management approach aligned to the Australian Government e-Authentication Framework (AGAF) and Government Security Standards.
- Facilitate increased use of PKI by both business and the broader community through reducing the cost and complexity of producing, acquiring and using digital certificates.
- Foster a competitive market for digital certificates.

A copy of the Framework can be found at: <<http://www.gatekeeper.gov.au>>

The Framework includes a commitment to reducing the paperwork and compliance burden associated with Gatekeeper accreditation. In particular the Framework states that:

- Gatekeeper documentation will be rationalised to reduce the paper burden on service providers and streamline the accreditation process.
- Accreditation will focus on security requirements rather than business and legal aspects.
- Commercial and legal aspects will largely be managed through relationships between service providers and agencies.
- Existing Gatekeeper criteria and policies where applicable, shall be incorporated into the Framework

The Framework states that:

Protection of the privacy of personal and corporate data will be a major consideration. Compliance with the *Privacy Act 1988* shall be a requirement⁹.

3.2. The future of Gatekeeper privacy protection

One clear issue that emerges from a consideration of Gatekeeper and privacy is that privacy protection within Gatekeeper is confused and fragmented. As described in 2.5. *Gatekeeper Privacy Requirements* above, there are multiple documents that contain privacy requirements relating to Gatekeeper.

This issue is considered throughout this Privacy Impact Assessment (PIA) and will be the subject of further discussion in the Privacy Management Strategy (PMS). However, some initial considerations can be set out at this stage:

3.2.1. *The Information Protection Principles (IPPs)*

Generally, the IPPs are too broad and generic to effectively protect all aspects of privacy in Gatekeeper. Nevertheless, they are mandatory for Government Agencies and their contractors, and should be embedded in Gatekeeper. References to the IPPs should be consolidated to one Gatekeeper document – the Head Agreement – thus incorporating them at the highest possible level¹⁰.

3.2.2. *Gatekeeper Privacy Accreditation Requirements*

The current twelve (12) Gatekeeper Privacy Accreditation Requirements could potentially be reduced to a single evaluation criteria, with a smaller set of sub-criteria. The current requirements may also need to be altered to reflect the Gatekeeper reforms. Consideration should be given to only including requirements that go beyond the IPPs, as the IPPs will be incorporated elsewhere.

3.2.3. *GPKA Privacy Recommendations*

The status of these Recommendations is unclear. They would appear to deliver no additional value as a stand-alone document in the current Gatekeeper PKI Framework. The elimination of this set of requirements would help to simplify the compliance burden for Gatekeeper, and the content can be incorporated in other requirements.

3.2.4. *OPC PKI Privacy Guidelines*

The OPC guidelines were intended to fill a gap in privacy coverage, as the relationship between Agencies and end users was not technically covered by Gatekeeper Privacy Requirements. However, the Guidelines are now dated and may not reflect the Gatekeeper reforms. Abandoning the Guidelines may be difficult as they were published as formal Guidelines under Section 27 of the *Privacy Act 1988*.

⁹ At page 5.

¹⁰ Note: The IPPs are well understood by Agencies and a simple reference to the IPPs should be sufficient. There should be no need to incorporate the entire text of the IPPS in any document, schedule or appendix.



3.2.5. *Other privacy requirements*

Gatekeeper documentation may need to continue to incorporate other privacy requirements (eg the NPPs and State/territory privacy legislation) as required. However, this may not require prescription in Gatekeeper.

4. Personal Information to be Collected

4.1. Background

The *PIA Guidelines* issued by the Office of the Privacy Commissioner contain a set of hints and risks under the category of personal information to be collected.

The privacy risks they have identified include:

- Collecting unnecessary or irrelevant personal information, or intrusive collection; and
- Bulk collection of personal information, some of which is unnecessary or irrelevant.

In addition to these risks, the collection of personal information should generally be kept to a minimum and personal information should normally be collected from the data subject.

4.2. Gatekeeper compliance

Under the Gatekeeper reforms, both Relationship and Known Customer models have the potential for organisations to collect significantly more information than the minimum necessary for the issuance of a digital certificate. The Known Customer model requires not only evidence of prior Evidence of Identity (EOI) but also evidence of a transaction history- implying the organisation has maintained records of its interactions with its clients and is thus holding potentially a significant amount of information.

The OPC PKI Guidelines suggested some categories of information that should be considered in a PKI Privacy Impact Assessment (PIA). Some of the categories are only relevant to specific applications, but the following general categories are relevant to the Framework:

Personal information to be collected in Gatekeeper	
List and describe the personal information (information about an identifiable individual) to be collected.	
A. Identifying information such as the individual's name or any identifying number assigned to the individual	Significant identifying information will be collected in all Gatekeeper categories; including name and address details, email address, and in some categories relevant identification numbers may be collected (eg membership numbers in Bronze).
B. Attribute or eligibility information such as the educational, medical, criminal, employment or financial history of the individual	Some limited attribute information may be collected in particular PKI applications, however its collection is not mandatory. Most attribute information will only be collected in the Bronze category.
C. Evidence of Identity (EOI) information	Significant EOI information will be collected, particularly in Gold and Platinum categories. In Bronze and Silver there are opportunities to limit additional EOI information by relying on EOI information previously supplied or collected as part of the existing relationship.
D. Sensitive information	The Framework does not require or mandate the collection of any sensitive information.
E. Biometric information	The Framework does not require or mandate the collection of any biometric information.

The issue of how much EOI information should be provided before a digital certificate is issued to a client is important. Under the Bronze Relationship and Silver Known Customer models, organisations will collect and hold a substantial amount of information not all of which is necessary for the issuance of a certificate, i.e. in terms of constructing a basic certificate request. However having the information in the first place is required in order for the organisation to “qualify” as a Relationship Organisation or Known Customer Organisation.

CAs must be able to give their clients (including agencies) confidence that digital certificates have in fact been issued to the correctly identified party, and 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 the proposed Gatekeeper PKI Framework, EOI levels are mapped to risk, so the registration process may be quite intensive for some categories of certificates (eg Gold and Platinum).

However, intrusiveness can be minimised if agencies carefully consider which category of certificate to promote, and which level of EOI is appropriate to their application.

4.3. Current Gatekeeper protections

The collection of EOI information in Gatekeeper is also subject to existing privacy constraints:

- **Information Protection Principles (IPPs)**
 - IPPs 1 and 7 require information collected to be necessary and relevant.
- **Gatekeeper Privacy Criteria**
 - **PC01**
Evaluation Criteria PC01 covers the “manner and extent of collection of personal information” and requires compliance with IPP 1.
- **GPKA Privacy Recommendations**
 - **GPKA R7 – Non-Intrusive Identification Processes**
The Recommendations 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”.
- **OPC PKI Guidelines**
 - **OPC PKI Guideline 4 – Evidence of Identity**
Guideline 4 requires agencies to ensure that “only minimum EOI that is necessary for, or directly related, to the process is collected”.

4.4. Personal Information to be Collected finding

The Gatekeeper PKI Framework requires significant collection of personal information. However, the level of intrusion is mapped to risk, and if an appropriate category of certificate is selected, the collection of information will be set at an appropriate level.

In addition, the Information Protection Principles (IPPs) requirements appear to place a sufficient limit on the amount of information collected, as the tests of *necessity* and *relevance* in the IPPs provide a good level of privacy protection.

It may be possible to consolidate the various Gatekeeper Privacy Requirements regarding the collection of personal information, and rely solely on the IPPs for protection on this issue.

5. Method of Collection

5.1. Background

The *PIA Guidelines* issued by the Office of the Privacy Commissioner contain a set of hints and risks under the category of method of collection. The Commissioner asks:

How will the information be collected? Might individuals feel the method of collection is unreasonably intrusive? For example, requiring individuals to divulge intimate or sensitive information in a public area where others can overhear or collecting video footage of individuals' activities without their knowledge.

The privacy risks they have identified include:

- Individuals unaware of the collection or its purpose; and
- Covert collection is generally highly privacy invasive, and should only occur under prescribed circumstances.

5.2. Gatekeeper compliance

The following PIA tool can be used to assess compliance with privacy law requirements for the method of collection of data. Note that this tool is designed for use with specific applications, and is only partly relevant to the assessment of a framework such as Gatekeeper.

Method of collection	Yes	No	Notes
A. Will personal information be collected only from the individual to whom the information relates?	√		<p>The majority of information will be collected from the individual.</p> <p>However, under Relationship/KC the information will derived from a relationship or transaction history and the individual may not realise the information is being retained or being used for the purpose of issuing or requesting issuance of a certificate.</p> <p>Some exceptions may occur. For example, the collection of status details from membership organisations in the Bronze category of for Digital Credentials.</p> <p>Note: There may be a perception issue regarding third party collection in the Bronze and Silver categories.</p>
B. Is the personal information being collected by lawful and fair means?	√		All anticipated information collection methods in Gatekeeper will be based on lawful and fair means.

Method of collection	Yes	No	Notes
C. Is the personal information to be collected on one occasion only (i.e. not ongoing)?	√		<p>Some ongoing collection may occur in the Bronze category, in relation to the status of certificate holders.</p> <p>In silver there will be some ongoing collection to ensure continued compliance with standard/ Gatekeeper requirements.</p> <p>In other categories, ongoing collection will be very limited (eg change of details or circumstances)</p>

5.3. Current Gatekeeper privacy protections

The method of collection of information in Gatekeeper is also subject to some existing privacy constraints:

- **Information Protection Principles (IPPs)**
 - IPPs 1, 2 and 3 require information to be collected by lawful means and contain some restrictions on third party collection.
- **Gatekeeper Privacy Criteria**
 - **PC01**
Evaluation Criteria PC01 covers the “manner and extent of collection of personal information” and requires compliance with IPPs 1, 2 and 3

The PC01 requirement appears to duplicate the IPPs. Overall, these requirements are easily met in the Gatekeeper PKI Framework.

However, there may be a perception issue that information is being collected from third parties in the Bronze and Silver categories, where use of the *known customer* approach may result in the issuing of a Certificate with pre-populated information. If that information was provided some time in the past to a third party, this could result in confusion about the source of data. In practice, the individual would have originally supplied the information.

5.4. Method of Collection finding

The method of collection in all Gatekeeper categories will be lawful and fair. Some limited third party collection may occur, and this will require detailed explanation to certificate holders.

The existing Gatekeeper Privacy Requirements for the method of collection could be collapsed into compliance with the IPPs without reducing overall privacy protection on this issue.

6. Purpose, Use and Disclosure

6.1. Background

The *PIA Guidelines* issued by the Office of the Privacy Commissioner contain a set of hints and risks under the category of purpose, use and disclosure.

The privacy hints they have identified include:

- No surprises! Use personal information in ways that are expected by the individual; and
- No surprises! Tell the individual about disclosures.

The privacy risks they have identified include:

- Using personal information for unexpected secondary purposes;
- Unnecessary or unexpected data linkage; and
- Unexpected disclosures can lead to privacy complaints.

6.2. Gatekeeper compliance

The Gatekeeper PKI Framework includes an ongoing commitment to the maintenance of significant information in public registers, including public key directories and Certificate Revocation Lists (CRLs).

However, in some Gatekeeper categories 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.

CAs maintains servers hosting public key directories and CRLs. CAs will normally keep logs of access to these directories that identify the relevant Relying Party. 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. 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.

The following tables provide an overview of the key privacy compliance issues at this stage:

Purpose	Yes	No	Notes
A. Is personal information obtained in relation to the Gatekeeper applications used exclusively for the purposes made known to the individual (use requires either consent or lawful authority)?	√		<p>Overall, Gatekeeper is compliant with this criterion, as the information collected has a clear link to certificate applications that are disclosed to the consumer.</p> <p>With respect to Bronze Relationship and Silver Known Customer certificates, some personal information has in the past been collected for one purpose and is now being used for issuing a certificate. This will require consent.</p> <p>In addition, the potential use of public register information, particularly CRLs, confuses this issue. Use is difficult to anticipate, describe and restrict. CRLs in Silver will be open. CRLs in Bronze would be accessible only to the relevant Community of Interest.</p> <p>Current Gatekeeper privacy protections also attempt to cover this issue by restricting access to CRLs and allowing multiple certificates to be used.</p>

Secondary use	Yes	No	Notes
A. If a secondary use can be made of data already collected, is the use consistent with uses notified to or consented to by the individual?	√		<p>Overall, Gatekeeper is compliant with this criterion, as secondary use is likely to be consistent with the primary purpose of the certificate.</p> <p>However, some secondary use may occur in relation to public register information, particularly CRLs. This secondary use may be difficult to anticipate, describe and restrict. This secondary use results from the CRL being public and readily accessed. Therefore, this form of secondary use may not occur in Bronze, where the information on the CRLs is itself limited and may not contain detailed personal information.</p> <p>Current Gatekeeper privacy protections do attempt to cover this issue by restricting access to CRLs and allowing multiple certificates to be used.</p>
B. Can an individual opt not to consent to the secondary use and still be entitled to receive the services offered utilising the original application?	√		<p>Current Gatekeeper privacy protections do discuss user choice. In practice, options are limited by the small PKI market in Australia and limited alternative options for authentication.</p>

Consent	Yes	No	Notes
A. Will notice of the purpose for which the personal information is being collected be provided to the user?	√		<p>Yes. This is a straightforward IPP compliance issue and compliance with the IPPs is entrenched in Gatekeeper documentation.</p>
B. Will the user be informed if the collection of the personal information is authorised or required by or under law?	√		<p>Yes. This is a straightforward IPP compliance issue and compliance with the IPPs is entrenched in Gatekeeper documentation.</p>
C. Will the individual be informed of the people, bodies or agencies to which the collecting agency usually discloses personal information of the kind being collected?	√		<p>Yes. This is a straightforward IPP compliance issue and compliance with the IPPs is entrenched in Gatekeeper documentation.</p>
D. Is the individual asked at or prior to collection to consent to the collection and use of the personal information?	√		<p>For most categories of certificates, this is a straightforward IPP compliance issue and compliance with the IPPs is entrenched in Gatekeeper documentation. The requirement forms part of the typical application form.</p> <p>However, for Bronze Relationship and Silver Known Customer Certificates a specific consent process may</p>

Consent	Yes	No	Notes
			need to be included.

Disclosure	Yes	No	Notes
A. Will disclosure of personal information be made for processing purposes?	√		Some personal information will be disclosed for processing (eg by accredited Registration Authorities), subject to compliance with Gatekeeper security requirements
B. Will disclosure be made for any other purposes (not covered by secondary use discussion above)		X	None known.

6.3. Current Gatekeeper privacy protections

The purpose, use and disclosure of information in Gatekeeper is subject to some existing privacy constraints:

- **Information Protection Principles (IPPs)**
 - IPP 2 requires the purpose of collection to be identified to the data subject.
 - IPPs 9,10 and 11 place restrictions on the use and disclosure of information.
- **Gatekeeper Privacy Criteria**
 - **PC06**
Personal information is used only for relevant purposes. This duplicates IPP 9.
 - **PC07**
Limits placed on the use of personal information. This duplicates IPP 10.
 - **PC08**
Limits placed on disclosure of personal information. This duplicates IPP 11.
 - **PC09**
Privacy protection is provided for personal information published in publicly accessible lists / registers via controls over how personal information is accessed, searched and used. No personal information shall be made publicly available in CRLs and other directory services. CAs/RAs shall collect and hold minimal personal information when logging accesses to CRLs or other directory services. CAs/RAs should not disclose personal information collected by logging access to CRLs or other directory services¹¹.

¹¹ PC09 includes an exception to this last requirement: "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".

- **OPC PKI Guidelines**
 - **OPC PKI 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.
 - **OPC PKI 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.
- **GPKA Privacy Recommendations**
 - **GPKA R6 – 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.

6.4. Purpose, Use and Disclosure finding

Controls on purpose, use and disclosure need to be exercised at the application or deployment level, and they can be difficult to apply to a broad framework like Gatekeeper. However, it appears that a combination of general Information Privacy Principle (IPP) compliance and a specific Gatekeeper Privacy Requirement in relation to Certificate Revocation Lists (CRLs) will result in an appropriate level of privacy protection.

There is significant overlap in the plethora of current Gatekeeper Privacy Requirements on this issue. It may be possible to replace these eight separate requirements with a general requirement to comply with the IPPs plus one additional Gatekeeper Privacy Requirement restricting search access to Certificate Revocation Logs (CRLs).

The reforms contained in the revised Gatekeeper PKI Framework do not have a specific impact on this issue.

7. Choice

7.1. Background

Best practice privacy protection generally allows an organisation's clients (data subjects) alternative ways of doing business without undue acquisition of personal information and without its acquisition in unduly intrusive ways. For example, a toll road operator might allow road users to purchase windscreen e-stickers by reference only to the number plate of his or her car rather than requiring name and address details.

7.2. Gatekeeper compliance

The level of choice in Gatekeeper has been the subject of detailed consideration over many years. This has been categorised as:

- Choice between PKI and other authentication techniques;
- Choice between a single certificate or multiple certificates; and
- Choice between anonymous and identified transactions.

The broad framework for choice is also influenced by Australia's international obligations. Australia, as a member of the OECD, has agreed to comply with Guideline 2 of the OECD Guidelines for Cryptographic Policy¹², which relates to Choice of Cryptographic Methods. It states:

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

In practice, both the PKI market and the broader authentication market in Australia are still limited. Many agencies will be limited to certain technology platforms, certificate types and key management systems.

Although the range of choices that an agency may offer will be limited, it should still be possible to provide clients with some degree of choice. Depending on their business requirements that lead to adoption of PKI, several options are available:

- Agencies might also consider a secure online application, other than PKI, to allow individual clients to deal securely (and in some cases anonymously) with them. The Australian Government Authentication Framework (AGAF) provides guidance for Agencies on the appropriate choice of Authentication method;
- Users can be provided with the opportunity to acquire and use multiple certificates (in the same Gatekeeper Category) if they wish to do so. This limits the potential for a comprehensive trail of use to develop through a single CRL;
- 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 identity¹³; or

¹²<http://www.oecd.org/document/11/0,2340,en_2649_34255_1814731_1_1_1_1,00.html>

- Under the revised Framework, there may be scope for CAs to issue special purpose attribute certificates that simply represent the individual's eligibility for a service without identifying them.

7.3. Current Gatekeeper privacy protections

Choice issues in Gatekeeper are subject to numerous existing privacy constraints:

- **Gatekeeper Privacy Criteria**
 - **PC10 – 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, i.e. Users should not be limited to one certificate when dealing with more than one agency.
 - **PC12 – Support of Anonymous or Pseudonymous Certificates**

The RA should have the ability to provide anonymous or pseudonymous certificates where appropriate.
- **OPC PKI Guidelines**
 - **OPC PKI 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.
 - **OPC PKI 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.
 - **OPC PKI 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.
- **GPKA Privacy Recommendations**

¹³ Many agencies will not want to see PKI used for anonymous transactions and under the AGAF where there is no requirement for authentication PKI seems irrelevant.

- **GPKA R1 – 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.
- **GPKA R3 – 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.
- **GPKA R5 – 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.

7.4. Choice finding

The provision of user choice in relation to Gatekeeper is affected by both Gatekeeper policy and market conditions. Some specific Gatekeeper Privacy Requirements in relation to choice may be required to ensure an appropriate level of privacy protection.

However, there is significant overlap in the numerous current Gatekeeper Privacy Requirements on user choice. It may be possible to replace these eight separate requirements with one additional Gatekeeper Privacy Requirement ensuring that user choice is provided through the consideration of alternative authentication channels and the acceptance of multiple certificates.

The reforms contained in the revised Gatekeeper PKI Framework would appear to have a positive impact on user choice, especially as they would allow the development of anonymous and pseudonymous certificates in appropriate circumstances in the Bronze category (and perhaps in relation to some Special Purpose Certificates).

8. Security

8.1. Background

The *PIA Guidelines* issued by the Office of the Privacy Commissioner contain a set of hints and risks under the category of security.

The privacy risk they have identified is:

- **Unauthorised internal and external access and use.**

8.2. Gatekeeper compliance

Broadly, Gatekeeper facilitates compliance with the minimal security requirements contained in privacy legislation. Gatekeeper is itself an enhanced security regime, mapped carefully to the levels of risk in any transaction.

This is described briefly in the following table:

Security	Yes	No	Notes
A. Does the level of security in the application match the potential harm caused by breaches of privacy?	√		The Gatekeeper Framework specifically maps the categories of certificates against risk. However, some security issues do arise in relation to: <ul style="list-style-type: none"> • Key generation • Subscriber security of keys.
B. Will detailed access trails be retained and scrutinised for security breaches?	√		Detailed logging protocols are in place at all levels of Gatekeeper. Gatekeeper accredited service providers are subject to an ongoing audit compliance framework.
C. Does the level of security provided by third parties providing processing or support services for the product match the potential harm caused by breaches of privacy?	√		Although third parties do play a significant role in Gatekeeper, they are subject to security accreditation and ongoing security audits.

The two outstanding security issues in Gatekeeper are related to key generation and subscriber security of keys:

- **Key generation**
Depending on the procedures and security in place, key generation can be considered insecure if it is done by the issuer, rather than the certificate holder.
- **Subscriber security of keys**
Subscribers are often consider the weak link in the PKI security chain, as they can lose or misplace keys, and choose inappropriate methods to secure their keys (eg weak passwords).

8.3. Current Gatekeeper privacy protections

Security issues in Gatekeeper are subject to several existing privacy protections:

- **Information Protection Principles (IPPs)**
 - IPP 4 includes general security requirements.
- **Gatekeeper Privacy Criteria**
 - **PC02**
Security safeguards in relation to personal information. Duplicates IPP 4 plus reference to the Commonwealth Protective Security Manual.
- **OPC PKI Guidelines**
 - **OPC PKI 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.
- **GPKA Privacy Recommendations**
 - **GPKA R2 – 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.
 - **GPKA R4 – 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 keys.
 - **GPKA R9 – 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 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.

8.4. Security finding

Gatekeeper facilitates compliance with the minimal security requirements contained in privacy legislation. Gatekeeper is itself an enhanced security regime, mapped carefully to the levels of risk in any transaction.

Some specific Gatekeeper Privacy Requirements in relation to security may be required to ensure an appropriate level of privacy protection. These could focus on key generation and subscriber security of keys.

However, there is significant overlap in the current Gatekeeper Privacy Requirements on security. It may be possible to replace these six separate requirements with a general requirement to comply with the IPPs plus one additional Gatekeeper Privacy Requirement on security.

The reforms contained in the revised Gatekeeper PKI Framework would appear to have a positive impact on security, as they strengthen the mapping of certificate categories against risk levels.

9. Data Quality

9.1. Background

The *PIA Guidelines* issued by the Office of the Privacy Commissioner contain a set of hints and risks under the category of personal information to be collected.

The privacy risks they have identified include:

- Retaining personal information unnecessarily; and
- Making decisions based on poor quality data.

9.2. Gatekeeper compliance

Broadly, Gatekeeper facilitates compliance with the data quality contained in privacy legislation. Gatekeeper is itself a system for ensuring that information is created, transferred and maintained with a high degree of accuracy.

This is described briefly in the following table:

Data quality	Yes	No	Notes
A. For the purpose for which it is used, will the personal information collected be up-to-date at all stages and on all occasions that it is used, relevant, accurate and complete.	√		Gatekeeper includes processes for checking and maintaining the accuracy of information, including comprehensive registration processes and an ongoing regime of certificate revocation.
B. Will records be maintained of the date of the last update of the personal information held and used by the agency and the source of updates to personal information?	√		Gatekeeper includes detailed logging protocols at almost all levels of the Framework. RAs and CAs also record specific notifications from the individual updating their information where this is performed physically, and logs where this is performed electronically.

Retention and destruction	Yes	No	Notes
A. Will a retention policy / destruction schedule be developed which requires retention of personal information only for the period required for use?	√		This requirement is difficult to apply to a broad Framework such as Gatekeeper – it is better suited to specific applications. The Certification Practices Statement (CPS) contains a detailed description of a CA's records archival plan, and this plan is based on strict Gatekeeper security criteria.
B. Is personal information de-identified as soon as possible?	√		Gatekeeper mandates quite lengthy archival periods for documents (compliant with Archive Act requirements), as one objective of the framework is to assist in establishing non-repudiation of historical documents.

9.3. Current Gatekeeper privacy protections

Data Quality issues in Gatekeeper are subject to several existing privacy constraints:

- **Information Protection Principles (IPPs)**
 - IPPs 7, 8 and 9 cover data accuracy and relevance.
- **Gatekeeper Privacy Criteria**
 - **PC05**
Accuracy of personal information. Duplicates IPP 8 and reference to the Commonwealth Protective Security Manual
 - **PC06**
Personal information is used only for relevant purposes. Duplicates IPP 9 and reference to the Commonwealth Protective Security Manual.

9.4. Data Quality finding

Gatekeeper facilitates compliance with the data quality requirements contained in privacy legislation. Gatekeeper is itself a system for ensuring that information is created, transferred and maintained with a high degree of accuracy.

Specific Gatekeeper Privacy Requirements in relation to data quality are unnecessary. It may be possible to replace the existing separate requirements with a general requirement to comply with the IPPs.

The reforms contained in the revised Gatekeeper PKI Framework would appear to have no significant impact on data quality.

10. Access and Correction

10.1. Background

The *PIA Guidelines* issued by the Office of the Privacy Commissioner contain a set of hints and risks under the category of personal information to be collected.

The privacy hint they have identified is:

- Getting access to personal information should be clear and straightforward.

The privacy risk they have identified is:

- Inaccurate information can cause problems for agencies and individuals.

10.2. Gatekeeper compliance

The following PIA tool can be used to assess compliance with privacy law requirements for access and correction. Note that this tool is designed for use with specific applications, and is only partly relevant to the assessment of a framework such as Gatekeeper.

Access and correction	Yes	No	Notes
A. 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?	√		This is a straightforward IPP compliance issue and compliance with the IPPs is entrenched in Gatekeeper documentation.
B. Will the costs incurred in accessing personal information be reasonable?	√		This is a straightforward IPP compliance issue and compliance with the IPPs is entrenched in Gatekeeper documentation.
C. Can the data or records about an individual be updated as a result of an individual seeking correction of personal information?	√		This is a straightforward IPP compliance issue and compliance with the IPPs is entrenched in Gatekeeper documentation.
D. Will corrections and annotations be disseminated to third parties to whom personal information has previously been disclosed?		X	This may be very difficult to achieve in a PKI without having an unnecessary impact on other aspects of privacy protection. As noted elsewhere, there are restrictions on the maintenance and searching of Certificate Revocation Logs (CRLs), so it may not be possible to track all parties who have relied on a previously presented Certificate (although the user may have their own record).

10.3. Current Gatekeeper privacy protections

Access and correction issues in Gatekeeper are subject to several existing privacy constraints:

- **Information Protection Principles (IPPs)**
 - IPPs 6 and 7 provide access and correction rights.
- **Gatekeeper Privacy Criteria**
 - **PC04**
Availability of procedures to allow subjects of personal information to access and correct the information. Duplicates IPPs 6 and 7 and reference to the Commonwealth Protective Security Manual.

10.4. Access and Correction finding

Gatekeeper does not appear to raise any specific access and correction issues.

Specific Gatekeeper Privacy Requirements in relation to access and correction are unnecessary. It may be possible to replace the existing separate requirements with a general requirement to comply with the IPPs.

The reforms contained in the revised Gatekeeper PKI Framework would appear to have no significant impact on access and correction.

11. National ID Potential

11.1. Background

The Australian community is likely to measure any proposals for large-scale identification systems against their potential to be used as a national ID (or contribute to the development of a national ID).

All Privacy Impact Assessments (PIAs) involving identity management in Australia need to assess the proposed implementation in the context of the broader debate about national identifiers and ID cards.

Australians continue to show only limited levels of support for national identifiers and national ID cards:

- On 23 July 2005, the Canberra Times reported that a Morgan poll [an Australian-wide cross-section of 651 men and women aged 14 and over] conducted by phone found that 62% of Australians agreed with the introduction of a national ID card with a photograph, while 32% opposed it, and 6% were undecided.
- On 1 February 2006, the Australian reported the results of a Newspoll survey on “The ID card [then] under consideration by the federal Government”. 53% of respondents were in support of the proposition and 31% were against.

11.2. Gatekeeper and National ID potential

Significant work has already been done in the history of Gatekeeper to mitigate the risk of PKI, through its use, becoming a de-facto national identification system. This could have happened if individuals used the one digital certificate in their dealings with all agencies (and possibly 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 would have been 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.

However, Gatekeeper was developed with this risk in mind, and privacy protections were included that helped to avoid this risk. Indeed one of the basic objectives of the original Gatekeeper Strategy was to develop a commercial CA industry – thus for most classes of certificates there would be multiple providers – this objective has been retained in the Framework.

In addition, the working model of PKI has matured in recent years, and there is a general recognition that a single digital certificate is ill suited to whole of Government or whole of sector use. Closed or more restricted PKIs have developed as a result, and this change is reflected in the revised Gatekeeper PKI Framework.

However, the reforms contained in the revised Gatekeeper PKI Framework do have an impact on the National ID potential of Gatekeeper, in that the Silver category anticipates the use of a single certificate with multiple Commonwealth agencies. This could be of particular concern if there is only one provider of Silver Certificates.

11.3. Current Gatekeeper privacy protections

National ID issues in Gatekeeper are subject to one existing privacy constraint:

- **GPKA Privacy Recommendations**
 - **GPKA R8 – 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.

11.4. National ID Potential finding

Specific Gatekeeper Privacy Requirements in relation to National ID are unnecessary. It may be possible to cover this issue with a general requirement to comply with the IPPs.

The reforms contained in the revised Gatekeeper PKI Framework do have an impact on the National ID potential of Gatekeeper, in that the Silver category anticipates the use of a single certificate with multiple Commonwealth agencies.

However, this issue can be alleviated if the Framework is designed in a manner that:

- Results in multiple providers of Silver certificates operating in the market place;
- Places limitations on the scope of application for a Silver certificate;
- Allows for alternative certificates being accepted by a relying party to another agency's Silver certificate; and/or
- It is not possible for a single agency to use a certificate to access and track information in databases it does not hold.

In combination with other privacy protections contained in Gatekeeper (eg in relation to Choice), the National ID potential of Gatekeeper should remain limited.

12. Complaints

12.1. Background

The *PIA Guidelines* issued by the Office of the Privacy Commissioner contain a set of hints and risks under the category of method of collection. The Privacy Commissioner asks:

- Is there provision for complaint-handling, audit and oversight, including emergency procedures?

12.2. Gatekeeper compliance

Gatekeeper includes provisions embedding compliance with the IPPs. The complaints structure is fairly simple, with all matters referable to the Office of the Privacy Commissioner. There is no history of Gatekeeper related privacy complaints.

12.3. Current Gatekeeper privacy protections

Complaints issues in Gatekeeper are subject to one existing privacy constraint:

- **Gatekeeper Privacy Criteria**
 - **PC11 – Notification Procedure**

CAs and 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 CA/RA for the purpose of issuing and managing certificates, and the applicable mechanism for making and investigating privacy complaints.

12.4. Complaints finding

Gatekeeper does not appear to raise any specific issues in relation to complaints.

Specific Gatekeeper Privacy Requirements in relation to complaints are unnecessary. It may be possible to cover this issue with a general requirement to comply with the IPPs.

The reforms contained in the revised Gatekeeper PKI Framework would appear to have no significant impact on complaints.

13. Function Creep

13.1. Background

The Privacy Commissioner has defined function creep as:

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 system¹⁴.

Function creep is considered a significant privacy risk in Australia. However, the management of function creep is difficult, and there are no “magic bullets” available to help avoid function creep.

The core mechanisms for avoiding function creep at the time of a new technology implementation are:

- Having a clearly defined primary purpose;
- Prohibitions on use for other purposes (eg use in another sector);
- Limiting “discretionary” secondary use and disclosure;
- Monitoring complaints; and
- Reviewing purpose and use (eg every three years).

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.

13.2. Gatekeeper compliance

Function creep is difficult to assess without reference to specific proposals for new applications, and it is difficult to assess function creep in relation to a broad framework such as Gatekeeper.

Obviously, agencies need to be wary of any accumulation of additional uses for certificates or associated personal information. This may require the use of Privacy Impact Assessments or Privacy Compliance Checklists.

¹⁴ The Office of the Federal Privacy Commissioner, *Privacy and Public Key Infrastructure - Guidelines for Agencies using PKI to communicate or transact with individuals*, (2001) <<http://www.privacy.gov.au/publications/pki.rtf>>.

13.3. Current Gatekeeper privacy protections

Function creep in Gatekeeper is subject to one existing privacy constraint:

- **OPC PKI Guidelines**

- **OPC PKI 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.

13.4. Function Creep finding

Gatekeeper does have the potential to raise issues of function creep.

A specific Gatekeeper Privacy Requirements in relation to function creep may therefore be necessary. It could focus on the ongoing conduct of Privacy Impact Assessments or Privacy Compliance Checklists as appropriate.

This issue will be the subject of further consideration in the Gatekeeper Privacy Management Strategy (PMS)

14. Reform of Gatekeeper Privacy Requirements

A number of individual privacy compliance risks and privacy perception risks have been identified in this Privacy Impact Assessment (PIA). Although some new issues are raised by the Gatekeeper reforms, most issues are effectively covered by existing Gatekeeper Privacy Requirements.

A problem is that the existing Gatekeeper Privacy Requirements are confused and fragmented. There are multiple documents that contain overlapping privacy requirements relating to Gatekeeper.

This issue is considered throughout this PIA and will be the subject of further discussion in the Privacy Management Strategy (PMS). However, the following table provides some initial advice on consolidating Gatekeeper Privacy requirements.

The result (if these recommendations are accepted) would be a general agreement to comply with the Information Privacy Principles (IPPs) (contained, for example in the Head Agreement) plus four short additional Gatekeeper Privacy Requirements (contained, for example, in accredited service provider evaluation criteria)

Section	Risk	Proposed Gatekeeper Privacy Requirement
4. Personal Information to be Collected	<ul style="list-style-type: none"> No unique issues 	<ul style="list-style-type: none"> IPPs
5. Method of Collection	<ul style="list-style-type: none"> No unique issues 	<ul style="list-style-type: none"> IPPs
6. Purpose, Use and Disclosure	<ul style="list-style-type: none"> Public directories particularly CRLs pose a unique privacy risk 	<ul style="list-style-type: none"> IPPs Specific Gatekeeper Privacy Requirement restricting search access to Certificate Revocation Logs (CRLs) and directories in Bronze COIs
7. Choice	<ul style="list-style-type: none"> Alternative authentication channels should be available (subject to market considerations) Use of multiple certificates should be available 	<ul style="list-style-type: none"> IPPs Specific Gatekeeper Privacy Requirement ensuring that user choice is provided through the consideration of alternative authentication channels and the acceptance of multiple certificates
8. Security	<ul style="list-style-type: none"> Some unique security issues in relation to key generation. Also some concern regarding subscriber security of keys. 	<ul style="list-style-type: none"> IPPs Specific Gatekeeper Privacy Requirement with a focus on key generation and subscriber security of keys.]
9. Data Quality	<ul style="list-style-type: none"> No unique issues 	<ul style="list-style-type: none"> IPPs
10. Access and Correction	<ul style="list-style-type: none"> No unique issues 	<ul style="list-style-type: none"> IPPs
11. National ID Potential	<ul style="list-style-type: none"> Some potential concerns regarding Silver certificates 	<ul style="list-style-type: none"> Requires additional work elsewhere in the framework, rather than a specific Gatekeeper Privacy Requirement. IPPs otherwise sufficient
12. Complaints	<ul style="list-style-type: none"> No unique issues 	<ul style="list-style-type: none"> IPPs
13. Function Creep	<ul style="list-style-type: none"> Some benefit in maintaining requirement to conduct Privacy impact Assessments (PIAs) 	<ul style="list-style-type: none"> IPPs Specific Gatekeeper Privacy Requirement with a focus on the ongoing conduct of Privacy Impact Assessments or Privacy Compliance Checklists as appropriate

15. Appendix – Gatekeeper Privacy Criteria

PC	Criteria
01	Manner and extent of collection of personal information Deemed to Comply Standards/ Documents <ul style="list-style-type: none"> • IPP 1, 2 and 3 & Commonwealth Protective Security Manual
02	Security safeguards in relation to personal information Deemed to Comply Standards/ Documents <ul style="list-style-type: none"> • IPP 4 & Commonwealth Protective Security Manual
03	Openness about the types of personal information held and information handling policies Deemed to Comply Standards/ Documents <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • IPPs 6 and 7 & Commonwealth Protective Security Manual
05	Accuracy of personal information Deemed to Comply Standards/ Documents <ul style="list-style-type: none"> • IPP 8 & Commonwealth Protective Security Manual
06	Personal information is used only for relevant purposes Deemed to Comply Standards/ Documents <ul style="list-style-type: none"> • IPP 9 & Commonwealth Protective Security Manual
07	Limits placed on the use of personal information Deemed to Comply Standards/ Documents <ul style="list-style-type: none"> • IPP 10 & Commonwealth Protective Security Manual
08	Limits placed on disclosure of personal information Deemed to Comply Standards/ Documents <ul style="list-style-type: none"> • 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. CA/RAs shall collect and hold minimal personal information when logging accesses to CRLs or other directory services. CA/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 <i>Telecommunications Act 1997</i> .
10	Multiple certificates Persons to whom certificates are issued (Users) will be allowed to have more than one certificate from the same CA/RA, wherever the use of multiple certificates is not inconsistent with the purpose of those certificates, i.e. Users should not be limited to one certificate when dealing with more than one agency.
11	Notification Procedure CA/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 CA/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 CA/RA should have the ability to provide anonymous or pseudonymous certificates where appropriate.

16. Appendix – GPKA Privacy Recommendations to the CEO

The following recommendations to the Chief Executive Officer, Office for Government Online (OGO) were made in May 2000 by the Government Public Key Authority. The recommendations were accepted and have been incorporated into Gatekeeper policy. Although they are not themselves evaluated they do form part of the Head Agreement for subsequent Gatekeeper Service Provider accreditations.

16.1. GPKA R1 – 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.

16.2. GPKA R2 – 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.

16.3. GPKA R3 – 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.

16.4. GPKA R4 – 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.

16.5. GPKA R5 – 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.

16.6. GPKA R6 – 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.

16.7. GPKA R7 – 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.

16.8. GPKA R8 – 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.

16.9. GPKA R9 – 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.

17. Appendix – OPC PKI Guidelines

17.1. OPC PKI 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.

17.2. OPC PKI 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.

17.3. OPC PKI 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.

17.4. OPC PKI 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.

17.5. OPC PKI 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.

17.6. OPC PKI 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.

17.7. OPC PKI 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.

17.8. OPC PKI 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.

17.9. OPC PKI 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.