## Contents

1. **FOREWORD** ........................................................................................................5

2. **INTRODUCTION** ..................................................................................................7
   2.1 Overview .............................................................................................................7
   2.2 System Overview ..................................................................................................7
   2.3 CA Roles and Responsibilities ..............................................................................7
   2.4 Operation/Administrative Structure .....................................................................7
   2.5 Assumptions, Standards and Reference Documents ...............................................7

3. **PUBLICATIONS AND REPOSITORY RESPONSIBILITIES** .....................................8
   3.1 Repositories and Publication Information ..............................................................8

4. **IDENTIFICATION AND AUTHENTICATION** ..............................................................8
   4.1 Naming ..................................................................................................................8
   4.2 Initial Identity Validation ........................................................................................9
   4.3 Identification and Authentication for Renewal Requests .........................................9
   4.4 Identification and Authentication for Revocation Request ......................................9

5. **CERTIFICATE LIFE CYCLE OPERATIONAL REQUIREMENTS** ..................................10
   5.1 Hours of Operations and Business Continuity .......................................................10
   5.2 Certificate Management .......................................................................................10
   5.3 Certificate Suspension Request (if applicable) .......................................................10

6. **FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS** ..............................11
   6.1 Physical Security Controls ....................................................................................11
   6.2 Procedural Controls ..............................................................................................11
   6.3 Personnel Security Controls ................................................................................12
   6.4 Audit Logging Procedures ....................................................................................13
   6.5 Records Archival ................................................................................................14
   6.6 Compromise and Disaster Recovery ....................................................................14
   6.7 CA Termination .....................................................................................................15
## 6. TECHNICAL SECURITY CONTROLS

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>Subscriber Key Pair Generation and Installation</td>
<td>15</td>
</tr>
<tr>
<td>6.1.1</td>
<td>Private Key delivery to Subscriber</td>
<td>15</td>
</tr>
<tr>
<td>6.1.2</td>
<td>Public Key delivery to Certificate issuer</td>
<td>15</td>
</tr>
<tr>
<td>6.1.3</td>
<td>Public Key delivery to Relying Parties</td>
<td>16</td>
</tr>
<tr>
<td>6.1.4</td>
<td>Hardware/software Key generation</td>
<td>16</td>
</tr>
<tr>
<td>6.1.5</td>
<td>Key renewal/changeover</td>
<td>16</td>
</tr>
<tr>
<td>6.2</td>
<td>Private Key Protection</td>
<td>16</td>
</tr>
<tr>
<td>6.3</td>
<td>Other Aspects of Key Pair Management</td>
<td>17</td>
</tr>
<tr>
<td>6.3.1</td>
<td>Public Key archival</td>
<td>17</td>
</tr>
<tr>
<td>6.4</td>
<td>Activation Data</td>
<td>17</td>
</tr>
<tr>
<td>6.4.1</td>
<td>Activation data generation and installation</td>
<td>18</td>
</tr>
<tr>
<td>6.4.2</td>
<td>Activation data protection</td>
<td>18</td>
</tr>
<tr>
<td>6.5</td>
<td>Life Cycle Technical Controls</td>
<td>18</td>
</tr>
<tr>
<td>6.5.1</td>
<td>System development controls</td>
<td>18</td>
</tr>
<tr>
<td>6.5.2</td>
<td>Security management controls</td>
<td>18</td>
</tr>
<tr>
<td>6.6</td>
<td>Network Security Controls</td>
<td>19</td>
</tr>
<tr>
<td>7</td>
<td>CERTIFICATE, CRL AND OCSP PROFILES</td>
<td>19</td>
</tr>
<tr>
<td>7.1</td>
<td>CRL Management and Distribution Advice</td>
<td>19</td>
</tr>
<tr>
<td>8</td>
<td>COMPLIANCE AUDITS AND OTHER ASSESSMENTS</td>
<td>19</td>
</tr>
<tr>
<td>9</td>
<td>OTHER BUSINESS AND LEGAL MATTERS</td>
<td>19</td>
</tr>
<tr>
<td>9.1</td>
<td>Confidentiality of Information</td>
<td>19</td>
</tr>
</tbody>
</table>
FOREWORD

This document has been developed using the RFC3647 Certificate Policy and Certification Practices Framework as a guide to assist an applicant for Gatekeeper Accreditation/Recognition to effectively address primary issues identified in Certificate Policies (CPs) and Certification Practice Statements (CPS).

The Certification Authority (CA) Operations Manual is an internal staff manual detailing the policies and procedures to be followed by staff for performing their day-to-day operations. It is linked to unclassified public documents such as the CPS as well as to sensitive internal security related documents (the Security Profile (SEC1)) and the Disaster Recovery and Business Continuity Plan (DRBCP). Finance will review the applicant’s Operations Manual for consistency with the content of the CPS, SEC1 and the DRBCP.

To facilitate this review, the Operations Manual should ideally follow the same structure as the CPS and make explicit references to the DRBCP and SEC1. The CA Operations Manual should contain sufficient information to enable CA staff to understand what is required without the need to cross reference a range of other documents in order to obtain that knowledge.

Where an Applicant is seeking Gatekeeper Accreditation as both a Certification Authority and a Registration Authority (RA), separate Operations Manuals should be prepared - one for the CA and one for the RA. This document outlines procedures for preparation of a CA Operations Manual.

All Gatekeeper documents referenced in this document are available at www.gatekeeper.gov.au.

Duplication of SEC1 information in the Operations Manual should be kept to a minimum to reduce the extent to which multiple documents are required to be edited when the CA’s policies and procedures are revised; and to ensure that the security classification of the Operations Manual remains at an appropriate level to enable access by staff across the Organisation.

Content and Structure

A CA Operations Manual should contain, at a minimum, the following information or provide appropriate cross references to the CPS, SEC1 and DRBCP:

- operational procedures describing the manner in which all nominated personnel employed within the CA perform any task undertaken within the CA;
- reference to the DRBCP and any other emergency procedures;
• details of all emergency procedures in place;
• detailed descriptions of the procedures followed for the following events:
  – Key Generation;
  – loading of Keys and Certificates onto physical tokens or other removable media;
  – Certificate revocation;
  – Certificate Revocation List publication;
  – publication of Certificate information;
  – method of distribution of end-entity Keys and Certificates;
  – routine Certificate renewal;
  – Certificate renewal after revocation;
  – access control measures and procedures for CA facilities; and
  – backup and archive procedures;
• details of all functions of the CA consistent with those described in the CPS and CP;
• descriptions of the roles of specific CA staff responsible for critical CA functions;
• details of all interaction between the CA and the RA;
• details of interactions between the CA and Known Customer Organisations, Threat/Risk Organisations and Relationship Organisations as appropriate; and
• a complete Glossary of Terms used in the document.

Contact:

The Australian Government Information Management Office
Department of Finance and Deregulation
Phone: (02) 6215 1544
Email: gatekeeper@finance.gov.au
1 INTRODUCTION

1.1 Overview

Provide a general introduction to the document describing its purpose:

- what it is meant to achieve and
- who it is for.

1.2 System Overview

Provide a descriptive paragraph and a system diagram of the total PKI system, including interactions, as applicable, between the CA and RA; CA and Known Customer Organisations (KCOs); CA and Threat/Risk Organisations (TROs); and CA and Relationship Organisations (ROs). This should also include Certificate application, Evidence of Identity (EOI) processes, Key Generation, Certificate flow, delivery, acceptance, and proof of possession.

1.3 CA Roles and Responsibilities

Describe the roles and responsibilities of the CA from senior organisation management through to operational staff.

1.4 Operation/Administrative Structure

Provide an organisational diagram indicating the operation/administrative structure.

1.5 Assumptions, Standards and Reference Documents

- List any underlying assumptions made in relation to this document and provide the justification or rationale for each.
- Provide details of standards applied and reference documents used within the Operations Manual.
2 PUBLICATIONS AND REPOSITORY RESPONSIBILITIES

This section should provide information on a range of legal and general practice topics.

2.1 Repositories and Publication Information

Briefly describe how the publications and repositories are managed, including details on:

- how and where the CA publishes its current CP, CPS and other relevant information, including Certificate Directories and Certificate Revocation Lists (CRLs);
- frequency of publication of this information;
- access control on published information; and
- requirements pertaining to the use of repositories by Subscribers and Relying Parties.

3 IDENTIFICATION AND AUTHENTICATION

This section should describe:

- the procedures used to authenticate a digital certificate applicant to a CA prior to Certificate issuance (including references as appropriate to arrangements with RAs KCOs, TROs and ROs);
- how parties requesting renewal or revocation are authenticated; and
- details of naming practices, including name ownership recognition and name dispute resolution processes.

3.1 Naming

Briefly describe the following elements of the naming process for entity registration or Certificate issuance:

- types of names assigned;
- whether or not names have to be meaningful;
- how name claim disputes are resolved; and
- recognition, authentication, and role of trademarks.
3.2 Initial Identity Validation

Briefly describe the following elements of the identification and authentication process for individual or entity registration for Certificate issuance:

- authentication requirements for organisational identity of subject (CA, RA, KCO, TRO, RO or end entity); and

- authentication requirements for a person acting on behalf of a subject (CA, RA, KCO, TRO, RO or end entity), including as appropriate:
  - number of pieces of identification required;
  - whether or not the individual must present personally to the authenticating RA;
  - how an individual as an organisational representative is authenticated; and
  - describe the EOI process undertaken and the CA interface procedures.

3.3 Identification and Authentication for Renewal Requests

Describe the identification and authentication procedures for:

- routine key renewal and

- key renewal after the subject Certificate has been revoked.

3.4 Identification and Authentication for Revocation Request

Describe the identification and authentication process for Certificate revocation.
4 CERTIFICATE LIFE CYCLE OPERATIONAL REQUIREMENTS

This section should provide employees with working details of how the CA operates.

4.1 Hours of Operations and Business Continuity

- Detail the hours of operation and the availability of services.
- Detail any external technical support, including contact details of external providers, if applicable.

4.2 Certificate Management

This section should identify:

- staff responsible for Certificate issuance and Certificate revocation;
- the procedures and processes used for Certificate issuance and Certificate revocation;
- any PIN/Password management procedures required;
- Certificate acceptance procedures for the Subscriber and subsequent publication of Certificates;
- Certificate Revocation List (or other) mechanisms, frequency, back up;
- staff responsible for processing backup, storage and transport; and
- timelines.

4.3 Certificate Suspension Request (if applicable)

Describe the identification and authentication process for Certificate suspension:

- circumstances for suspension;
- who can request Certificate suspension;
- procedures in place for Certificate suspension request; and
- timelines.
5 FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

5.1 Physical Security Controls

Describe in general terms the physical security measures that are in place in the facility housing the CA systems and identify day-to-day responsibilities of staff, including position of staff responsible for monitoring ongoing compliance.

The section should address and identify staff responsible for:

- the maintenance of the facility to ensure that operations meet their availability requirements, including power and air conditioning; water exposures and fire prevention and protection facilities;
- monitoring and recording of visitor access to non public areas;
- the protection of electronic and paper records and media against unauthorised access;
- secure destruction of electronic and paper waste, including media; and
- off-site backup of records.

Describe staff access controls including password management (where utilised) to the main site and other areas. This may be completed by reference to the organisation’s Security Profile (SEC1).

5.1.1 Breaches of physical security

Describe how breaches of security and/or trust are reported, to whom these are reported and how and where they are recorded.

5.2 Procedural Controls

Describe in general terms the various procedures employed for trusted roles and provide appropriate cross references to SEC1 and the DRBCP:

- describe the trusted roles (i.e. Positions of Trust) in the operation of the CA;
- state the number of people required per task;
- describe how identity and authentication is verified before access is granted;
- state the security level cleared for personnel in trusted roles;
- define any “no lone zones” and describe how access is controlled; and
- describe how physical access to secure areas is recorded.
5.2.1 **Logical access control**

Describe how logical access is managed and controlled:

- name the position within the organisation that authorises;
- name the positions that are permitted access.

5.2.2 **Configuration management**

Provide details on and identify who is responsible for:

- organisational configuration management plan;
- software version control;
- hardware configuration; and
- database management.

5.2.3 **Loss or compromise of CA Keys**

Describe the procedures to be followed in the event of loss or compromise.

5.2.4 **Control of removable media**

Provide information on who is responsible for inventory control measures for removable magnetic media and legacy hardware.

5.2.5 **Storage/handling procedures**

- Detail the lock up procedures for the beginning and end of shifts.
- Describe daily alarm checks.

5.2.6 **Emergency destruction procedures**

Describe the procedures for the emergency destruction of classified material.

5.2.7 **Incident management**

Describe the procedures for managing incidents of a security nature.

5.3 **Personnel Security Controls**

5.3.1 **Facility Security Officer**

Describe the roles and responsibilities of the Facility Security Officer (FSO) or Information Technology Security Advisor (ITSA).
5.3.2 Training requirements
Describe the
- training requirements for staff;
- retraining frequency and requirements; and
- employment rotation frequency and sequence.

5.3.3 Documentation
- describe confidentiality provisions (i.e. non-disclosure agreements) to which employees are subject. May refer to organisation employment policy; and
- identify which of the Gatekeeper Approved Documents are supplied to which positions in the organisation.

5.3.4 Separation
Describe the procedures for separation of personnel from the organisation.

5.4 Audit Logging Procedures
Describe the event logging and audit systems implemented for the purpose of maintaining a secure environment. Elements should include:
- types of events recorded;
- frequency with which audit logs are processed or audited;
- period for which audit logs are kept;
- protection of audit logs;
- who can view audit logs;
- protection against modification of audit log;
- protection against deletion of audit log;
- audit log back up procedures;
- whether the audit log accumulation system is internal or external to the entity;
- whether the subject who caused an audit event to occur is notified of the audit action; and
- vulnerability assessments.

Reference to SEC1 should be made to address event logging and audit systems that are to be implemented for the purpose of maintaining a secure environment.
5.5 Records Archival

Describe the general records archival (or records retention) policies and procedures including reference to the following:

- types of events recorded;
- retention period for archives;
- protection of archives - physical and electronic;
- who can view the archived items;
- protection against modification of archived items;
- protection against deletion of archived items;
- archive backup and recovery procedures;
- requirements for time-stamping of records;
- whether the archive collection system is internal or external; and
- procedures to obtain and verify archive information.

Reference to SEC1 should be made to address record archival issues that are to be implemented for the purpose of maintaining a secure environment.

5.6 Compromise and Disaster Recovery

Reference to the Disaster Recovery and Business Continuity Plan and the Security Profile (SEC1) is required to:

- describe the overall management responsibilities including process and recovery procedure references;
- state who is responsible for providing details of corrective action to be taken and other protective actions;
- detail the frequency with which disaster recovery exercises will be conducted;
- describe immediate actions to be taken in the event of a disaster; and
- state who are permitted to authorise a desktop disaster recovery exercise.
5.7 CA Termination

Describe the procedures relating to termination and for termination notification, including the identity of the custodian of CA archival records. (Note: this section should correspond to requirements in the Gatekeeper Head Agreement.)

6. TECHNICAL SECURITY CONTROLS

- Describe the security measures taken to protect cryptographic keys and activation data (e.g. PINs, passwords, or manually held key shares).
- Provide details of the constraints on repositories.
- Define other technical security controls on repositories.

This section should also describe other technical security controls used to securely perform the functions of key generation, user authentication, Certificate registration, Certificate revocation, audit, and archival. Technical controls include life-cycle security controls (including software development environment security, trusted software development methodology) and operational security controls.

Note: care should be taken in drafting this section to avoid duplication with SEC1 and to ensure that the security classification of the Operations Manual is not raised to a level that precludes access by relevant staff.

6.1 Subscriber Key Pair Generation and Installation

Identify the position responsible for generating the Public and Private Key Pairs.

6.1.1 Private Key delivery to Subscriber

- Detail controls implemented to ensure the secrecy of the Private Key(s).
- Provide details on trusted channels used for the issue of the Keys if the Keys are not delivered to the Subscriber in person.

6.1.2 Public Key delivery to Certificate issuer

If the Public Key is to be delivered to the Certificate issuer (if the CA is not the issuer), an online transfer complying with IETF RFC 2510 (PKI Certificate Management Protocols) using Evaluated Products, or equally secure non-electronic means, should be used. Details of these procedures are to be provided here.
6.1.3 Public Key delivery to Relying Parties

Detail the processes involved and the person(s) responsible in the delivery of the Public Key to Relying Parties.

6.1.4 Hardware/software Key generation

Describe any hardware/software Key generation processes.

6.1.5 Key renewal/changeover

Describe the procedures to provide a new Public Key to users. This should also provide brief details of changeover of Keys.

6.2 Private Key Protection

Describe how Private Keys are secured and who is responsible for this.

6.2.1 Private Key (n out of m) multi-person control

State the number of individuals (including positions) required to perform the task (n out of m rule).

6.2.2 Private key backup

If Subscriber Private Key back-ups are held, they should be secured at a level at least equivalent to the CA Private Key. If utilised:

- describe the processes required to perform this task;
- identify the back-up agent;
- describe the form in which Keys are backed-up; and
- describe the security controls on the back-up system.

6.2.3 Private Key archival

If Subscriber Private Key archives are held, they should be secured at a level at least equivalent to the CA Private Key. If utilised:

- describe the processes required to perform this task;
- identify the archival agent;
- describe what form Keys are archived; and
- describe the security controls on the archival system.
6.2.4  Private key transfer into or from a cryptographic module

Private Keys not generated by the end entity's cryptographic module should be delivered via an online transfer meeting the IETF RFC 2510 (PKI Certificate Management Protocols) using Evaluated Products or equally secure non-electronic means. Identify the position responsible for entering the Private Keys in the cryptographic module, and in what form the Private Keys are entered and stored in the module.

6.2.5  Method of activating the Private Key

- Identify the position responsible for activating or using Private Keys and describe the method of activating the Private Key.
- Describe how end entity authentication to the cryptographic module to activate the Private Key is achieved.

6.2.6  Method of deactivating the Private Key

- Identify the position responsible for deactivating Private Keys and describe the method of deactivating the Private Key.
- Describe how the Private Key is cleared from memory before it is deactivated.

6.2.7  Method of destroying the Private Key

- Identify the position responsible for destroying Private Keys and describe the method of destroying the Private Key.
- Describe when Keys are destroyed, how they are cleared from memory before it is de-activated, and made irrecoverable on any storage media, in particular before any possible reuse.

6.3  Other Aspects of Key Pair Management

6.3.1  Public Key archival

If utilised, describe how the Public Key is archived and by what designated position within the organisation.

6.4  Activation Data

Activation data refers to data values other than Keys that are required to operate cryptographic module and that need to be secured. Protection of activation data potentially needs to be considered.
6.4.1 Activation data generation and installation

- Identify which position generates the activation data;
- Describe how the activation data is provided securely to Key Holders;
- Identify the parameters for the activation date; and
- Identify the hardware and software used to generate the activation data.

6.4.2 Activation data protection

- Identify standards with which the module used to generate activation data complies where appropriate.
- Discuss if the activation data is under multi-person control.
- Discuss if the activation data is escrowed; backed-up or archived; identify the escrow/back-up/archival agent; in what form are keys escrowed/backed-up/archived; and what are the security controls on the escrow/back-up/archival system.

6.5 Life Cycle Technical Controls

Reference to the SEC1 should be made to address system development controls and security management controls.

6.5.1 System development controls

- Describe the security controls in relation to the development environment, development facility and development personnel.
- Describe controls in relation to:
  - configuration management security during product maintenance;
  - software engineering practices; and
  - software development methodology.
- Describe use of failsafe design and implementation techniques.
- Describe use of trusted products and systems that have been evaluated.

6.5.2 Security management controls

Describe the system configuration management procedures used for installing and modifying systems, including the methods used to verify the authenticity and integrity of software when first loaded on a system and staff responsible for this.
6.6 Network Security Controls

Describe the method of logging successful and unsuccessful attempts to communicate with the CA and the person(s) responsible for logging this information.

7 CERTIFICATE, CRL AND OCSP PROFILES

7.1 CRL Management and Distribution Advice

Describe the arrangements for posting and hosting the CRL, including feedback provided to the client.

8 COMPLIANCE AUDITS AND OTHER ASSESSMENTS

This section should describe:

- the frequency of audits - noting that Gatekeeper requires an annual Compliance Audit of Accredited/Recognised Service Providers;
- the identity/qualifications of the auditor - ensure no conflicts of interest;
- a list of topics to be addressed/covered under the audit;
- actions to be taken as a result of a deficiency found during audit; and
- audit results:
  - with whom they are shared (e.g. CA, RA, KCO, TRO, RO and/or end entities);
  - who communicates these results (e.g., entity being audited or auditor); and
  - how the results are communicated.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Confidentiality of Information

Indicate adherence to the Privacy Act 1988 (Cth) and Gatekeeper privacy requirements and describe the process and procedures relating to:

- types of information that must be kept confidential by the CA;
- how this information will be secured;
- types of information that are not considered confidential;
- who is to be informed of reasons for revocation of Certificates;
- policy on release of information to law enforcement officials;
- information that can be revealed as part of civil discovery;
- conditions upon which CA may disclose upon owner’s request; and
- any other circumstances under which confidential information may be disclosed.

Note that CRL and OCSP are not the only means available to a CA to make available lists of revoked Digital Certificates. Whichever means is selected, the key principle is that information is made available in a manner accessible by all potential Relying Parties using standard protocols and technologies.