



**Australian Government**

**Medicare Australia**

PO 02

SecureNet-HeSA Gatekeeper Health PKI –  
Health Organisation Certification  
Authority  
Certification Practice Statement V.3.0

This work is copyright. You may download, display, print and re produce this material in unaltered form only (retaining this notice) for your personal, non-commercial use or use within your organisation. Apart from any use as permitted under the Copyright Act 1968, all other rights are reserved. Requests and enquiries concerning reproduction and rights should be addressed to The Manager, Media, Communications and Government Relations Branch, Medicare Australia National Office, PO Box 1001 Tuggeranong DC ACT 2901 or posted at [www.medicareaustralia.gov.au](http://www.medicareaustralia.gov.au).

Copyright © Commonwealth of Australia 2005.

The information contained in this Document is intended for Medicare Australia Personnel, those persons named as Recipients, and Subscribers and Relying Parties using Certificates within the SecureNet-HeSA Gatekeeper Health Public Key Infrastructure (Health PKI).

**Contact:**

**Mailing address:**  
Registration Authority Manager  
Medicare Australia  
Locked Bag 6666  
Tuggeranong DC ACT 2901  
AUSTRALIA

**Glossary:**

Definitions are provided in the *Health PKI Glossary version 3*, which is available at the RA's Website ([www.hesa.gov.au](http://www.hesa.gov.au)).

This Document has been Authorised by the Medicare Australia Policy Management Authority (Medicare Australia PMA):

\_\_\_\_\_ Date: \_\_\_\_\_  
General Manager or nominee, Information Technology and Services Division, Medicare Australia Representative

# Table of Contents

1	Introduction .....	6
1.1	Overview.....	6
1.1.1	Overview of SecureNet-HeSA Gatekeeper Health Public Key Infrastructure (Health PKI) .....	6
1.2	References .....	6
1.2.2	Key Documents .....	7
1.2.2.1	Policy Documents and Subscriber Agreement .....	7
1.2.2.2	Root Certification Authority-issued Certificate Policy (RCA-issued CP) .....	8
1.2.2.3	Priority of Documents .....	8
1.2.2.4	Glossary .....	8
1.2.3	Certificates issued under this OCA CPS.....	8
1.3	Identification .....	8
1.3.1	X.500 Object Identifier hierarchy .....	8
1.3.2	Standards.....	8
1.4	Community and Applicability .....	9
1.4.1	Certification Authorities .....	9
1.4.1.1	RCA .....	9
1.4.1.2	OCA .....	9
1.4.2	RA .....	9
1.4.3	End Entities .....	9
1.4.4	Applicability .....	9
1.4.5	Policy authorities .....	9
1.5	Contact Details.....	9
1.5.1	Specification administration organisation .....	9
1.5.2	Contact person .....	9
1.5.3	Person determining CPS suitability for the policy .....	10
2	General Provisions.....	11
2.6	Publication and repository.....	12
2.6.1	Publication of information.....	12
2.6.2	Frequency of publication .....	12
2.6.3	Access Controls .....	12
2.6.4	Repositories .....	12
2.7	Compliance Audit .....	12
2.7.1	Frequency of entity compliance audit .....	12
2.7.2	Identity/qualifications of auditor .....	13
2.7.3	Auditor's relationship to audited party.....	13
2.7.4	Topics covered by audit .....	13
2.7.5	Actions taken as a result of deficiency.....	13
2.7.6	Communication of results.....	13
2.8	Confidentiality.....	13
2.9	Intellectual Property Rights .....	14
3	Identification and Authentication .....	15
4	Operational Requirements .....	16
4.5	Security Audit procedures.....	16
4.5.1	Types of event recorded .....	16
4.5.2	Frequency of processing log .....	16
4.5.3	Retention period of audit log .....	16
4.5.4	Protection of audit log .....	17
4.5.5	Audit log backup procedures.....	17
4.5.6	Audit collection system (internal vs external) .....	17
4.5.7	Notification to event-causing subject .....	17
4.5.8	Vulnerability assessments .....	17

4.6	Records Archival.....	17
4.6.1	Types of event recorded .....	17
4.6.2	Retention period for archive .....	17
4.6.2.1	Secure maintenance of Keys.....	17
4.6.2.2	Secure maintenance of Certificates.....	17
4.6.2.3	Term of archive maintenance.....	17
4.6.3	Protection of archive .....	18
4.6.4	Archive backup procedures.....	18
4.6.5	Requirements for time-stamping of records .....	18
4.6.6	Archive collection system (internal or external) .....	18
4.6.7	Procedures to obtain and verify archive information.....	18
4.7	Key changeover .....	18
4.8	Compromise and Disaster Recovery .....	19
4.8.1	Computing resources, software and/or data are corrupted .....	19
4.8.2	Entity Public Key is Revoked.....	19
4.8.3	Entity Private Key is Compromised .....	19
4.8.4	Secure facility after a natural or other type of disaster .....	19
4.9	OCA and RA Termination .....	19
4.9.1	RA programmed termination .....	20
4.9.2	RA non-programmed termination .....	20
5	Physical, procedural, and Personnel security controls.....	21
5.1	Physical Controls .....	21
5.1.1	Site location and construction.....	21
5.1.2	Physical access.....	21
5.1.3	Power and air conditioning .....	21
5.1.4	Water exposures.....	21
5.1.5	Fire prevention and protection .....	21
5.1.6	Media storage .....	21
5.1.7	Waste disposal .....	21
5.1.8	Off-site backup.....	22
5.2	Procedural Controls.....	22
5.2.1	Trusted roles.....	22
5.2.2	Number of persons required per task.....	22
5.2.3	Identification and Authentication for each role.....	22
5.3	Personnel Controls.....	22
5.3.1	Background, qualifications, experience and clearance requirements .....	22
5.3.2	Background check procedures .....	23
5.3.3	Training requirements .....	23
5.3.4	Retraining frequency and requirements.....	23
5.3.5	Job rotation frequency and sequence .....	23
5.3.6	Sanctions for unauthorised actions .....	23
5.3.7	Contracting Personnel requirements .....	23
5.3.8	Documentation supplied to Personnel .....	23
6	Technical Security Controls.....	25
6.1	Key Pair Generation and Installation.....	25
6.1.1	Key pair generation.....	25
6.1.2	Private Key delivery to Entity.....	25
6.1.3	Public Key delivery to Certificate issuer .....	25
6.1.4	OCA Public Key delivery to users .....	25
6.1.5	Key sizes.....	25
6.1.6	Public Key parameters generation .....	25
6.1.7	Parameter quality checking .....	26
6.1.8	Hardware/software Key generation.....	26
6.1.9	Key usage purposes (as per X.509 v3 usage field) .....	26
6.2	Private Key Protection.....	26
6.2.1	Standards for cryptographic module .....	26
6.2.2	Private Key (n out of m) multi-person control .....	26
6.2.3	Private Key escrow.....	26
6.2.4	Private Key backup .....	26
6.2.5	Private Key Archival .....	26
6.2.6	Private Key entry into cryptographic module .....	26
6.2.7	Method of activating Private Key .....	26
6.2.8	Method of deactivating Private Key.....	26

6.2.9	Method of destroying Private Key .....	27
6.3	Other Aspects of Key Pair Management.....	27
6.3.1	Public Key archival.....	27
6.3.2	Usage periods for the Public Keys and Private Keys.....	27
6.4	Activation Data .....	27
6.4.1	Activation data generation and installation .....	27
6.4.2	Activation data protection .....	27
6.4.3	Other aspects of activation data.....	27
6.5	Computer Security Controls .....	27
6.5.1	Specific computer security technical requirements .....	27
6.5.2	Computer security rating .....	28
6.6	Life cycle technical controls.....	28
6.6.1	System development controls.....	28
6.6.2	Security management controls.....	28
6.6.3	Life cycle security ratings.....	28
6.7	Network security controls .....	28
6.8	Cryptographic module engineering controls .....	28
7	Certificate and CRL Profiles .....	29
7.1	Certificate Profile .....	29
7.1.1	Version number .....	29
7.1.2	Certificate extension(s).....	30
7.1.3	Algorithm object identifiers .....	31
7.1.4	Name forms .....	31
7.1.5	Name constraints.....	31
7.1.6	Certificate Policy Object Identifier.....	31
7.1.7	Usage of policy constraints extension.....	31
7.1.8	Policy Qualifiers syntax and semantics .....	31
7.1.9	Processing semantics for the critical Certificate Policy extension .....	31
7.2	CRL Profile.....	31
7.2.1	Version number(s) .....	31
7.2.2	CRL and CRL entry extensions .....	31
8	Specification Administration.....	32
8.1	Specification change procedures .....	32
8.2	Publication and notification policies .....	32
8.3	Approved Document approval procedures .....	32

# 1 Introduction

## 1.1 Overview

### 1.1.1 Overview of SecureNet-HeSA Gatekeeper Health Public Key Infrastructure (Health PKI)

1. The SecureNet-HeSA Gatekeeper Health Public Key Infrastructure (Health PKI) facilitates electronic connectivity within the Australian Health Sector. The RA's Website ([www.hesa.gov.au](http://www.hesa.gov.au)) provides additional information about Health PKI.
2. In general, a PKI consists of a hierarchy of trusted elements and End Entities. In Health PKI the hierarchy of trusted elements comprises:
  - a) the Root Certification Authority (RCA);
  - b) the Health Organisation Certification Authority (OCA); and
  - c) the Medicare Australia Extended Services Registration Authority (RA).
3. Both the RCA and the OCA are operated by Cybertrust Australia Pty Ltd using the name SecureNet. All references to the SecureNet entity throughout this Document refer to the Cybertrust Australia Pty Ltd entity, operating the RCA and/or the OCA in the name of SecureNet.
4. End Entities are Subscribers and Relying Parties. For information about the roles played by these Parties, please refer to clause 1.4 of this Document.
5. The RCA, OCA and RA in Health PKI (refer to clause 1.4 of this Document) are Gatekeeper Accredited. The criteria for Gatekeeper Accreditation are found at [www.gatekeeper.gov.au](http://www.gatekeeper.gov.au).
6. For further information, refer to the Certificate Policies (CPs) under which Healthcare Individual and Healthcare Location Certificates are issued.

## 1.2 References

- |    |                             |   |
|----|-----------------------------|---|
| 1. | <i>ACSI_33</i>              | Defence Signals Directorate, ACSI 33 – Australian Government Information and Communications Technology Security Manual                              |
| 2. | <i>RA_Operations_Manual</i> | AD 02 - SecureNet-HeSA Gatekeeper Health Public Key Infrastructure - Registration Authority Operations Manual version 3                             |
| 3. | <i>Subscriber_Agreement</i> | CO 01 - SecureNet-HeSA Gatekeeper Health Public Key Infrastructure - Subscriber (Healthcare Individual and Healthcare Location) Agreement version 3 |

4.	<i>Individual_CP</i>	PO 01 - SecureNet-HeSA Gatekeeper Health Public Key Infrastructure – Subscriber (Healthcare Individual) Certificate Policy version 3 (Type1 Grade2)
5.	<i>Location_CP</i>	PO 01 - SecureNet-HeSA Gatekeeper Health Public Key Infrastructure – Subscriber (Healthcare Location) Certificate Policy version 3 (Type2 Grade2)
6.	<i>OCA_CPS</i> <b>(this Document)</b>	PO 02 - SecureNet-HeSA Gatekeeper Health Public Key Infrastructure – Health Organisation Certification Authority Certification Practice Statement version 3
7.	<i>RCA_CPS</i>	Root Certification Authority Certification Practice Statement version 3
8.	<i>RA_Security_Policy</i>	SE 01 - SecureNet-HeSA Gatekeeper Health Public Key Infrastructure - Registration Authority Protective Security Policy version 3
9.	<i>RA_DRP_BCP</i>	SE 03 - SecureNet-HeSA Gatekeeper Health Public Key Infrastructure - Registration Authority Disaster Recovery Plan and Business Continuity Plan version 3
10.	<i>RA_Security_Plan</i>	SE 04 - SecureNet-HeSA Gatekeeper Health Public Key Infrastructure - Registration Authority Protective Security Plan version 3
11.	<i>RCA_Issued_CP</i>	PO 01 - SecureNet Gatekeeper Root Certification Authority issued Certificate Policy version 1

## 1.2.2 Key Documents

### 1.2.2.1 Policy Documents and Subscriber Agreement

1. Key policy Documents for Health PKI are this *OCA\_CPS* the Certificate Policy Documents (the *Individual\_CP* and the *Location\_CP*) and the *Subscriber\_Agreement*. These Documents can be accessed via the RA's Website ([www.hesa.gov.au](http://www.hesa.gov.au)).
2. This *OCA\_CPS* describes the practices of the OCA and the RA relevant to Health PKI.
3. The Certificate Policy (CP) Documents outline the policies that sit behind the Individual and Location Certificates issued under Health PKI, and provide obligation and liability information.
4. If the RA issues an Applicant with Individual and/or Location Keys and Certificates, the relevant *Subscriber\_Agreement* forms a contract between the Applicant, the RA and the OCA in relation to the possession and use of the Individual and/or Location Keys and Certificates.

#### **1.2.2.2 Root Certification Authority-issued Certificate Policy (RCA-issued CP)**

1. The RCA practices set out in the *RCA\_Issued\_CP* apply to the OCA as if they were repeated in this *OCA\_CPS*.

#### **1.2.2.3 Priority of Documents**

1. If there is any conflict between provisions in key policy Documents, the following order of precedence applies:
  - a) the CP the Certificates are issued under (*Individual\_CP* or *Location\_CP*); then
  - b) the related *Subscriber\_Agreement* (Individual or Location Agreement); then
  - c) this *OCA\_CPS*; then
  - d) the *RCA\_Issued\_CP*.
2. If there is any conflict between the provisions set out in this *OCA\_CPS* and the provisions of the *RCA\_Issued\_CP* incorporated by clause 1.1.2.2, the provisions set out in this *OCA\_CPS* will prevail.

#### **1.2.2.4 Glossary**

1. Key policy Documents should be read in conjunction with *Health PKI Glossary version 3* which contains definitions (either words or terms). Definitions used throughout this *OCA\_CPS* commence with capital letters. The *Health PKI Glossary version 3* is located at the RA's Website.

#### **1.2.3 Certificates issued under this OCA CPS**

1. For information on Certificate types and Policy Qualifiers, please refer to the CP the Certificates are issued under.

### **1.3 Identification**

#### **1.3.1 X.500 Object Identifier hierarchy**

1. Specified elements under Health PKI have been assigned an X.500 Object Identifier (OID). The authority for issuing OIDs is the SecureNet Policy Management Authority (SecureNet PMA).
2. OIDs are not applicable to this *OCA\_CPS*.

#### **1.3.2 Standards**

1. This *OCA\_CPS* is based on RFC 2527, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, IETF PKIX RFC2527, by S. Chokhani and W. Ford, March 1999.
2. However, in some instances, that guideline does not provide adequate definition. In such cases, this *OCA\_CPS* will differ from the guideline insofar as is necessary for clarity only.

## **1.4 Community and Applicability**

### **1.4.1 Certification Authorities**

#### **1.4.1.1 RCA**

1. Cybertrust Australia Pty Ltd operates the RCA in Health PKI. The RCA issues the Certificates that bind itself and the OCA to its Public Keys and is the highest point of trust in Health PKI. Refer to the *RCA\_Issued\_CP* and the *RCA\_CPS* on the RCA's Website at [www.certificates-australia.com.au](http://www.certificates-australia.com.au) for contact details and further information about functions.

#### **1.4.1.2 OCA**

1. Cybertrust Australia Pty Ltd operates the OCA in Health PKI. The OCA generates, signs and issues the Certificates that bind the RA to its Public Keys, and does the same for Subscribers in response to Certificate requests that come from the RA. For further details on the role and obligations of OCA, refer to clauses 2 and 4 of the relevant CP.

#### **1.4.2 RA**

1. Medicare Australia is the Registration Authority that provides Registration services to the OCA in Health PKI. The RA is a Gatekeeper Extended Services RA, and as such conducts Evidence of Identity (EOI) checks, requests the OCA to generate Certificates and undertakes a range of other functions associated with the management of Keys and Certificates for Health PKI. For further details on the role and obligations of RA, refer to clauses 2 - 4 of the relevant CP.

#### **1.4.3 End Entities**

1. Refer to clause 1 of the CP the Certificates are issued under.

#### **1.4.4 Applicability**

1. Refer to clause 1 of the CP the Certificates are issued under.

#### **1.4.5 Policy authorities**

1. Refer to clauses 1 and 8 of the CP the Certificates are issued under.

## **1.5 Contact Details**

### **1.5.1 Specification administration organisation**

1. This *OCA\_CPS* is administered by the Medicare Australia Policy Management Authority (Medicare Australia PMA) and approved by the SecureNet Policy Management Authority (SecureNet PMA) and the Competent Authority. For further information refer to clauses 1 and 8 of the CP the Certificates are issued under.

### **1.5.2 Contact person**

1. Enquiries or other communications about this *OCA\_CPS* should be addressed to:

Registration Authority Manager  
Medicare Australia  
Locked Bag 6666  
Tuggeranong DC ACT 2901  
AUSTRALIA

**1.5.3 Person determining CPS suitability for the policy**

1. Refer to clauses 1 and 8 of the CP the Certificates are issued under.

## 2 General Provisions

1. Clauses 2.1 to 2.5 are designed to explain the roles and responsibilities of key Parties in Health PKI, for example:
  - a) Obligations
    - i) OCA obligations
    - ii) RA obligations
    - iii) Subscriber obligations
    - iv) Other Subscriber obligations
    - v) Relying Party obligations
    - vi) Repository obligations
  - b) Liability
    - i) OCA liability
    - ii) RA liability
    - iii) Subscriber liability
    - iv) Relying Party liability
    - v) Liability of the Commonwealth
    - vi) Limited warranties
    - vii) Contribution
    - viii) Duty to mitigate
    - ix) Indemnity from Subscriber
    - x) Indemnity from Relying Party
    - xi) Limit on liability
  - c) Financial responsibility
    - i) Indemnification by Relying Parties
    - ii) Fiduciary relationships
    - iii) Administrative processes
  - d) Interpretation and Enforcement
    - i) Governing law
    - ii) Severability, survival, merger, notice
    - iii) Dispute resolution procedures
  - e) Fees
    - i) Certificate issuance or Re-key fees
    - ii) Certificate access fees
    - iii) Revocation or status information Access fees
    - iv) Fees for other services such as policy information
    - v) Refund policy

2. For further information, refer to clauses 2.1 - 2.5 of the CP the Certificates are issued under.

## **2.6 Publication and repository**

Note: The OCA practices set out in clause 2 of the *RCA\_CPS* apply to the OCA.

### **2.6.1 Publication of information**

1. This *OCA\_CPS* is published electronically in PDF format on the RA's Website.
2. Notices to Subscribers about RA services may also be published on the RA's Website. Refer to clause 2.4 of the relevant CP for more detailed information about Notice types and publication channels.

### **2.6.2 Frequency of publication**

1. Newly Gatekeeper Approved versions of this *OCA\_CPS* are published promptly.
2. For further information, refer to clause 2.6.2 of the CP the Certificates are issued under.

### **2.6.3 Access Controls**

1. There are no Access Controls on reading this *OCA\_CPS* on the RA's Website.
2. For further information, refer to clause 2.6.3 of the CP the Certificates are issued under.

### **2.6.4 Repositories**

1. The Healthcare Public Directory can be Accessed from the OCA and RA Websites.
2. For further information, refer to clause 2.6.4 of the CP the Certificates are issued under.

## **2.7 Compliance Audit**

Note: The OCA practices set out in clause 8 of the *RCA\_CPS* apply to the OCA.

### **2.7.1 Frequency of entity compliance audit**

1. The RA will undergo an annual Gatekeeper Compliance Audit Program as required by the Gatekeeper MOA between Medicare Australia and Finance.
2. The Registration Authority Operations Manager (RAOM) will ensure regular internal audits of the RA processes and Records occur on no less than an annual basis. In addition, an internal compliance audit will be conducted after any disaster recovery and/or business continuity exercise.

### **2.7.2 Identity/qualifications of auditor**

1. External audits will be conducted by a Finance-approved Authorised Auditor.
2. Internal audits will be conducted by a qualified physical and logical security auditor.

### **2.7.3 Auditor's relationship to audited party**

1. External auditors will be organisationally independent of the RA and shall not have any current or planned financial, legal, or other relationship that could result in a conflict of interest during the period of the audit.
2. Internal auditors will be organisationally independent of the RA's operations.

### **2.7.4 Topics covered by audit**

1. The areas to be audited for both external and internal audits include but are not limited to:
  - a) physical security;
  - b) documentation and processes;
  - c) vetting of operational Personnel;
  - d) technology;
  - e) privacy; and
  - f) financial viability.

### **2.7.5 Actions taken as a result of deficiency**

1. The results of the audit will be provided to the Registration Authority Manager (RAM) and recorded in the RA audit log. The RAM is responsible for addressing any serious deficiencies in a timely manner.
2. When irregularities are found after an internal audit of the RA, the RAM shall promptly oversee or implement appropriate corrective action.

### **2.7.6 Communication of results**

1. External audit results will be communicated to the Competent Authority, the SecureNet PMA, the Health PMA and the RA. The Competent Authority will make an assessment of the Audit Report and identify any remedial action required.

## **2.8 Confidentiality**

1. Clause 2.8 sets out Confidentiality requirements, for example:
  - a) Types of information to be kept Confidential;
  - b) Types of information not considered Confidential;
  - c) Disclosure of Certificate Revocation / Suspension information;
  - d) Release to law enforcement officials;

- e) Release as part of civil discovery;
  - f) Disclosure upon owner's request; and
  - g) Other information release circumstances.
2. Refer to clause 2.8 of the CP the Certificates were issued under.
  3. For further information, refer to the RA's Privacy Policy on its Website.

## **2.9 Intellectual Property Rights**

1. Refer to clause 2.9 of the CP the Certificates were issued under.

### **3 Identification and Authentication**

1. Clause 3 is designed to explain the process that Applicants (for Location Certificates, this includes the Duly Authorised Officer) go through to Authenticate themselves and Register for Individual Keys and Certificates, for example:
  - a) initial Registration;
  - b) routine Re-key;
  - c) Re-key after Revocation; and
  - d) Revocation requests.
2. For further information, refer to clause 3 of the CP the Certificates were issued under.

## 4 Operational Requirements

1. Clauses 4.1 to 4.4 are designed to explain what the RA does to Register Applicants, for example:
  - a) Certificate Application;
  - b) Certificate issuance;
  - c) Certificate acceptance; and
  - d) Certificate Suspension and Revocation.
2. For further information, refer to clauses 4.1 to 4.4 of the CP the Certificates were issued under.

### 4.5 Security Audit procedures

Note: The OCA practices set out in clause 5.4 of the *RCA\_CPS* apply to the OCA.

1. It is a requirement of Gatekeeper Accreditation for the RCA, OCA and RA to maintain Records and Archives of information pertaining to their respective activities under this *OCA\_CPS*.
2. Sufficient Records and Archives of information relating to the operation of that entity will be retained to enable a proper audit to be conducted in accordance with the requirements of this *OCA\_CPS*.

#### 4.5.1 Types of event recorded

1. The minimum audit records to be kept include all:
  - a) Registration Records;
  - b) Key generation Records;
  - c) Certificate generation requests;
  - d) Certificate issuance Records, including CRLs;
  - e) Audit Records including security related events;
  - f) Revocation Records;
  - g) Suspension Records; and
  - h) Reinstatement Records.

#### 4.5.2 Frequency of processing log

1. Audit logs are processed on a daily, weekly, monthly and annual basis.

#### 4.5.3 Retention period of audit log

1. Audit logs are maintained on-site prior to archiving. Archived logs are retained for a period of seven years.

#### **4.5.4 Protection of audit log**

1. RA audit logs are stored in a B-class safe located in the RA's Secure Operations Room prior to archiving. Archived RA audit logs are stored in a B-class safe at a secure off-site location.

#### **4.5.5 Audit log backup procedures**

1. The RA has established and maintains a detailed backup procedure for audit logs which is documented in the *RA\_Security\_Plan* (this Document is not publicly available).

#### **4.5.6 Audit collection system (internal vs external)**

1. The RA audit collection system is a combination of automated and manual processes performed by the operating system running the UniCERT software, the UniCERT software itself, and by operational Personnel. The audit mechanisms and procedures used are documented in the *RA\_Security\_Plan* (this Document is not publicly available).

#### **4.5.7 Notification to event-causing subject**

1. RA Operations Personnel notify the RAOM when a process or action causes a critical security event or discrepancy.

#### **4.5.8 Vulnerability assessments**

1. Protective Security Risk Reviews have been completed for the RA. These Protective Security Risk Reviews cover the overarching Risks and Threats that may impact RA operations.

### **4.6 Records Archival**

Note: The OCA practices set out in clause 5.5 of the *RCA\_CPS* apply to the OCA.

#### **4.6.1 Types of event recorded**

1. The following information is archived by the RA:
  - a) Audit logs (refer to clause 4.5.1 of this *OCA\_CPS*);
  - b) Certificate request information; and
  - c) Complete back up registers.

#### **4.6.2 Retention period for archive**

##### **4.6.2.1 Secure maintenance of Keys**

1. The RA does not make or retain copies of Public or Private Keys.

##### **4.6.2.2 Secure maintenance of Certificates**

1. The RA does not make or retain copies of Certificates.

##### **4.6.2.3 Term of archive maintenance**

1. Archives are retained for a period of seven years in accordance with National Archives of Australia requirements.

#### **4.6.3 Protection of archive**

1. Archive media are protected by physical security.

#### **4.6.4 Archive backup procedures**

1. Archive backup procedures have been established to ensure complete restoration of current service or verification. Details are specified in the *RA\_DRP\_BCP*, the *RA\_Security\_Plan* and the *RA\_Operations\_Manual* (these Documents are not publicly available).

#### **4.6.5 Requirements for time-stamping of records**

1. All automatically generated logs are time-stamped using the system clock of the computer on which they are generated. Manually generated Records record the date of occurrence, but may not record the time.

#### **4.6.6 Archive collection system (internal or external)**

1. Archiving is performed by the operations staff delegated with the responsibility for doing so. Detailed procedures for backups, archiving and storage are set out in the *RA\_Security\_Plan* and the *RA\_Operations\_Manual* (these Documents are not publicly available).

#### **4.6.7 Procedures to obtain and verify archive information**

1. The integrity of the Archives is verified in accordance with the criteria set out in the *RA\_Security\_Plan* as follows:
  - a) annually at the time of the programmed security audit;
  - b) at any time when a full security audit is required; and
  - c) at the time the Archive is prepared.

### **4.7 Key changeover**

Note: The OCA practices set out in clause 5.6 of the *RCA\_CPS* apply to the OCA.

1. The RCA, OCA and RA Key changeovers will be affected in such a manner as to cause minimal disruption to Subscribers.
2. The RCA and OCA shall each obtain a new Authentication Key Pair a minimum of two years prior to the expiry of the Certificate associated with their respective current Private Authentication Key, and then commence signing new Certificates with the new Private Authentication Key.
3. During this changeover period until the expiry of the Certificate associated with the current RCA or OCA Private Authentication Key, both Authentication Public Keys in the associated Certificate will be in use and shall be published in the Healthcare Public Directory.
4. The RCA, OCA and RA are committed to:

- a) ensuring that Key changeover causes minimal disruption to Subscribers; and
- b) providing Subscribers with reasonable Notice of planned Key changeover.

## **4.8 Compromise and Disaster Recovery**

Note: The OCA practices set out in clause 5.7 of the *RCA\_CPS* apply to the OCA.

1. It is a requirement of Gatekeeper Accreditation for the RA to maintain a Disaster Recovery and Business Continuity Plan (*RA\_DRP\_BCP*). This plan, although not publicly available, will be made available to those persons responsible for conducting security audits and to the Finance approved Authorised Auditor conducting the annual external audit.

### **4.8.1 Computing resources, software and/or data are corrupted**

1. Directions for managing service restoration in the event of a corruption of computing resources, software and/or data are provided in the *RA\_Operations\_Manual* and the *RA\_DRP\_BCP* (these Documents are not publicly available).

### **4.8.2 Entity Public Key is Revoked**

1. In the situation that the RA's Public Key is Revoked, for whatever reason, the procedures outlined for RA termination will be followed. Details are provided in the *RA\_DRP\_BCP* (this Document is not publicly available).

### **4.8.3 Entity Private Key is Compromised**

1. In the situation that the RA's Private Key is Compromised, for whatever reason, the procedures outlined for RA termination would be followed. Details are provided in the *RA\_DRP\_BCP* (this Document is not publicly available).

### **4.8.4 Secure facility after a natural or other type of disaster**

1. Actions to be taken in order to restore core business operation as quickly as practicable following fire, strikes or similar events are provided in the *RA\_DRP\_BCP* (this Document is not publicly available).

## **4.9 OCA and RA Termination**

Note: The OCA practices set out in clause 5.8 of the *RCA\_CPS* apply to the OCA.

1. This clause 4.9 applies if the RCA, the OCA or the RA intend to, or become aware that they are likely to, cease providing services which are necessary for the continuance of Health PKI.
2. The RCA, the OCA or the RA will give as much Notice as possible of the relevant circumstances, and the actions they propose to take for key Parties in Health PKI and Subscribers.

3. In such situations, all key Parties will co-operate with each other in order to minimise the Risk of disruption to any services described in this *OCA\_CPS*.
4. If any Personal Information or Confidential Information needs to be transferred from one key Party to another, all key Parties involved will do so in accordance with the appropriate privacy legislation in force at the time.

#### **4.9.1 RA programmed termination**

1. A programmed termination will arise where there is a termination of the RA for default or for convenience (for example, termination of its own services or end of relevant contracts or any other type of termination that is not a non-programmed termination). Termination for convenience by the RA will be a RA programmed termination.
2. If Medicare Australia intends to implement a RA programmed termination:
  - a) it will give not less than 3 months Notice in writing to the Gatekeeper Competent Authority and the OCA of its intention to terminate its business operations in a programmed manner; and
  - b) it will use its best endeavours to facilitate the transfer in a secure and trustworthy manner all records to a replacement RA.

#### **4.9.2 RA non-programmed termination**

1. A non-programmed termination will arise where pursuant to a law (Commonwealth, State or Territory) it is illegal for the RA to continue the business operations of the RA.
2. The OCA and RA will promptly use their best endeavours to facilitate the transfer, in a secure and trustworthy manner, subject to approval by the Gatekeeper Competent Authority, of all Records held by the RA to a replacement RA or if no replacement RA can be promptly located, the OCA will accept the transfer of the RA Records that contain the private information concerning the Subscribers.
3. For the purposes of this clause 4.9.2, Records include but are not limited to:
  - a) Registration Records;
  - b) Key generation Records;
  - c) Certificate generation requests;
  - d) Audit records including security related events;
  - e) Suspension Records; and
  - f) Revocation Records.

# 5 Physical, procedural, and Personnel security controls

Note: The OCA practices set out in clause 5 of the *RCA\_CPS* apply to the OCA.

## 5.1 Physical Controls

### 5.1.1 Site location and construction

1. The Secure RA Operations Room is a secure facility that meets the standards set by Commonwealth Protective Security Manual and *ACSI\_33*.

### 5.1.2 Physical access

1. Only Vetted Personnel and visitors under the constant supervision of these Vetted Personnel are permitted entry to the RA secure operations room. Access is controlled via magnetic swipe cards and an entry log is maintained. All visitors are required to sign a visitors' log.

### 5.1.3 Power and air conditioning

1. The Secure RA Operations Room is connected to a standard power supply. All critical components are connected to uninterruptible power supply (UPS) units, to prevent abnormal shutdown in the event of a power failure.
2. The operations and server rooms have air conditioning systems that control temperature and humidity. The server room air-conditioning system is an independent unit.

### 5.1.4 Water exposures

1. The Secure RA Operations Room is protected against water exposure by being located above ground floor level.

### 5.1.5 Fire prevention and protection

1. The Secure RA Operations Room and all other areas of the RA's premises are fitted with hard-wired smoke detectors. A fire extinguisher is located in the Secure RA Operations Room.

### 5.1.6 Media storage

1. All magnetic media containing sensitive RA information, including backup media, are stored in containers, cabinets or safes which are located either within the Secure RA Operations Room or in a secure off-site storage area.

### 5.1.7 Waste disposal

1. Magnetic media containing classified material is securely disposed of by either physical destruction or by being wiped or overwritten using an approved utility.

2. Printed material is securely disposed of by being shredded using a B-Class shredder housed within the Secure RA Operations Room.

### **5.1.8 Off-site backup**

1. A weekly backup of the RA's operations is securely stored off-site.
2. The off-site storage facility has appropriate levels of security in place and may be accessed by Authorised Personnel for the purposes of retrieving software and data.

## **5.2 Procedural Controls**

### **5.2.1 Trusted roles**

1. RA operational responsibilities are shared by multiple roles and individuals to ensure that one person acting alone cannot circumvent the security of the system.
2. All positions held within the Secure RA Operations Room are positions of trust. Personnel placed in positions of trust are expected to display a high level of trustworthiness, integrity and professional conduct in their roles.
3. The following roles have been established:
  - a) Registration Authority Manager (RAM)
  - b) Registration Authority Operations Manager (RAOM)
  - c) Facility Security Officer (FSO)
  - d) System Administrator
  - e) Registration Authority Officer (RAO)
4. The process for maintaining separation of roles is defined in the *RA\_Security\_Plan* (this Document is not publicly available).

### **5.2.2 Number of persons required per task**

1. Duties surrounding registration, Key generation and Certificate collection are shared. Key generation cannot be performed by a RAO without the RAOM's involvement.

### **5.2.3 Identification and Authentication for each role**

1. Personnel performing trusted roles are Authenticated to the system prior to Access. Access Authorisation is controlled by the System Administrator.

## **5.3 Personnel Controls**

### **5.3.1 Background, qualifications, experience and clearance requirements**

1. The recruitment and selection practices for RA Personnel shall take into account the background, qualifications, experience and clearance requirements of each position, which are then compared against the profiles of potential candidates.

### **5.3.2 Background check procedures**

1. All RA Personnel Authorised to enter the Secure RA Operations Room are Vetted by an Australian Security Vetting service to the Highly Protected level.

### **5.3.3 Training requirements**

1. All RA operational Personnel are trained in:
  - a) basic PKI concepts;
  - b) security awareness;
  - c) disaster recovery and business continuity processes;
  - d) UniCERT software;
  - e) RA systems;
  - f) Audit review;
  - g) identifying paper signatures;
  - h) privacy considerations; and
  - i) documented RA procedures.

### **5.3.4 Retraining frequency and requirements**

1. Continuation training will be conducted at least every twelve months. Additional training may be provided following an upgrade to the UniCERT software or the RA system as a whole or as required.

### **5.3.5 Job rotation frequency and sequence**

1. Jobs within the Secure RA Operations Room are rotated on a daily or weekly basis as instructed by the RAOM.

### **5.3.6 Sanctions for unauthorised actions**

1. Unauthorised actions by RA Personnel are submitted to appropriate authorities including, but not limited to, the RAM.
2. Sanctions for unauthorised actions by RA Personnel are specified in the *RA\_Security\_Policy* and shall include disciplinary actions up to and including immediate termination of the employment of the offending Personnel.

### **5.3.7 Contracting Personnel requirements**

1. RA operational Personnel may be contractors who are appointed in writing and who are given written notification of the terms and conditions of their position.

### **5.3.8 Documentation supplied to Personnel**

1. RA operational Personnel shall have Access to the following documentation:
  - a) all relevant hardware and software documentation;
  - b) the Approved Documents for the RA;
  - c) all CPs relating to Health PKI; and

d) this *OCA\_CPS*.

## 6 Technical Security Controls

Note: The OCA practices set out in clause 6 of the *RCA\_CPS* apply to the OCA.

### 6.1 Key Pair Generation and Installation

#### 6.1.1 Key pair generation

1. Keys for Subscribers are generated by the RA.

#### 6.1.2 Private Key delivery to Entity

1. The RA arranges for the delivery of Keys to Subscribers in a secure manner:
  - a) the inactive Keys are delivered to the Subscriber by standard post to the address recorded during the Application process;
  - b) the Subscriber is required to fax back confirmation that the Keys have been received;
  - c) the RA compares the signature on the fax to that recorded on the original *Subscriber\_Agreement*;
  - d) if satisfied that the signatures have been made by the same person, the RA delivers the associated Personal Identification Code (PIC) to the RA's eBusiness Service Centre, ready for retrieval by the Subscriber;
  - e) the Subscriber is required to telephone the RA's eBusiness Service Centre and correctly quote their Secret Identifier and relevant reference number (Application or Re-key). Correctly quoted information will result in the PIC being given to the Subscriber by telephone. Incorrectly quoted information will result in the PIC being delivered to the Subscriber by standard post, to the address recorded during the Application process.

#### 6.1.3 Public Key delivery to Certificate issuer

1. Using a product listed on the Evaluated Products List, the RA securely delivers Subscriber Public Keys to the OCA for signing.

#### 6.1.4 OCA Public Key delivery to users

1. Using a product listed on the Evaluated Products List, the OCA securely delivers Subscriber Public Keys to the RA for distribution to Subscribers.

#### 6.1.5 Key sizes

1. Subscriber Keys are 1024 bits in length.

#### 6.1.6 Public Key parameters generation

1. The parameters used to create Public Keys for Subscribers are generated using a product listed on the Evaluated Products List.

### **6.1.7 Parameter quality checking**

1. Parameter quality checking is ensured through the use of a product listed on the Evaluated Products List.

### **6.1.8 Hardware/software Key generation**

1. Quality of Key generation is ensured through the use of a product listed on the Evaluated Products List.

### **6.1.9 Key usage purposes (as per X.509 v3 usage field)**

1. Keys will be used for the purposes and in the manner described in clause 1 of the CP under which the Certificates are issued.

## **6.2 Private Key Protection**

### **6.2.1 Standards for cryptographic module**

1. Cryptographic modules used in Health PKI are listed on the Evaluated Products List.

### **6.2.2 Private Key (n out of m) multi-person control**

1. OCA and RA Private Keys are not under 'n out of m' multi-person control.

### **6.2.3 Private Key escrow**

1. Private Key escrow is not supported.

### **6.2.4 Private Key backup**

1. The Private Keys of the OCA are stored in Encrypted files and are backed up under further Encryption with backup copies maintained on-site and in secure off-site storage.
2. Private Key backup is not provided for Subscribers.

### **6.2.5 Private Key Archival**

1. Private Keys of the OCA are not Archived.
2. Private Key Archival is not provided for Subscribers.

### **6.2.6 Private Key entry into cryptographic module**

1. When a Cryptographic module is used, the Private Key of the OCA is generated and retained in the module in an Encrypted format. It will be Decrypted only at the time at which it is being used.

### **6.2.7 Method of activating Private Key**

1. The Private Keys of the OCA and Subscribers are activated by Cryptographic software following the successful completion of a login process that validates an Authorised User.

### **6.2.8 Method of deactivating Private Key**

1. The *SEO4 - Registration Authority Protective Security Plan* details what Personnel are Authorised to deactivate Private Keys and in what manner. This Document is not publicly available.

### **6.2.9 Method of destroying Private Key**

1. Media containing Subscriber Private Keys are securely destroyed by, in the case of:
  - a) floppy disks – destruction by disintegration or burning; or
  - b) hard disks – Sanitisation by overwriting in accordance with *ACSI\_33*; or
  - c) other media – in accordance with recommendations in *ACSI\_33*.
2. Media containing a Private Key of the OCA will be securely disposed of by Sanitisation by overwriting (where feasible), then supervised physical destruction in accordance with *ACSI\_33*.

## **6.3 Other Aspects of Key Pair Management**

### **6.3.1 Public Key archival**

1. At the expiration of the OCA Public Key, the Public Key will be archived for seven years in accordance with the Australian National Archives Policy.
2. Further information on records archival is at clause 4.6 of this *OCA\_CPS*.

### **6.3.2 Usage periods for the Public Keys and Private Keys**

1. The usage period for the OCA Public and Private Keys is four years.
2. The usage period for Subscriber Public and Private Keys is two years.

## **6.4 Activation Data**

### **6.4.1 Activation data generation and installation**

1. No activation data other than Access Control mechanisms is required to operate Cryptographic modules.

### **6.4.2 Activation data protection**

1. No activation data other than Access Control mechanisms is required to operate Cryptographic modules.

### **6.4.3 Other aspects of activation data**

1. No activation data other than Access Control mechanisms is required to operate Cryptographic modules.

## **6.5 Computer Security Controls**

### **6.5.1 Specific computer security technical requirements**

1. The RA details its computer security technical requirements in its *SEO4 Protective Security Plan*. This plan is required for Gatekeeper Accreditation and is not publicly available.

## **6.5.2 Computer security rating**

1. The RA details its computer security rating in its *SEO4 – Registration Authority Protective Security Plan*. This plan is required for Gatekeeper Accreditation and is not publicly available.

## **6.6 Life cycle technical controls**

### **6.6.1 System development controls**

1. The RCA OCA and RA detail their system development controls in their respective *SEO4 – Registration Authority Protective Security Plans*. These plans are required for Gatekeeper Accreditation and are not publicly available.

### **6.6.2 Security management controls**

1. The RAs details its security management controls in its *SEO4 – Registration Authority Protective Security Plan*. This plan is required for Gatekeeper Accreditation and is not publicly available.

### **6.6.3 Life cycle security ratings**

1. The RA details its life cycle security ratings in its *SEO4 – Registration Authority Protective Security Plan*. This plan is required for Gatekeeper Accreditation and is not publicly available.

## **6.7 Network security controls**

1. The RA has undertaken a *SEO2 – Registration Authority Protective Security Risk Review* which identifies and addresses all high or significant life cycle security Threats. This Document is required for Gatekeeper Accreditation and is not publicly available.

## **6.8 Cryptographic module engineering controls**

1. Any change to a Cryptographic module requires re-evaluation by DSD or its agent.

## 7 Certificate and CRL Profiles

### 7.1 Certificate Profile

Note: The OCA practices set out in clause 7 of the *RCA\_CPS* apply to the OCA.

#### 7.1.1 Version number

Field	Value
Version	V3
Serial Number	A positive integer that uniquely identifies the Certificate.
Signature Algorithm	SHA-1 RSA, SHA-1 hashing algorithm using the RSA signing algorithm.
Issuer	The X.500 distinguished name of the OCA cn= SecureNet OCA o= SecureNet c= AU
Validity (From)	The date that the Certificate is valid from. YYMMDDHHMMSSZ encoded as UTCTime for dates up to 2049 and encoded as GeneralizedTime for dates in 2050 or later.
Validity (To)	The date that the Certificate is valid until. YYMMDDHHMMSSZ encoded as UTCTime for dates up to 2049 and encoded as GeneralizedTime for dates in 2050 or later
Subject	The X.500 Distinguished Name of the person who is to hold this Certificate. Example: C=AU, ST=NSW, CN= John A Smith :5402869084
Certificate Policies	Individual Certificate Policy OID: 1.2.36.73665175.1.0.101.2 Location Certificate Policy OID: 1.2.36.73665175.1.0.101.3 CPS URL: <a href="http://www.cybertrust.com">www.cybertrust.com</a> <sup>1</sup> Certificates issued under the Individual (or Location) CP must only be relied upon by Individual and/or Location Subscribers who have been issued Individual and/or Location Certificates for secure online Health-related messages and not for purposes other than those permitted by the related CP.

---

<sup>1</sup> Prior to September 2003, Cybertrust Australia Pty Ltd was known as and traded under the name SecureNet Limited. As a result, certificates issued prior to August 2004 have a CPS URL of [www.securenet.com.au](http://www.securenet.com.au)

Field	Value
Public Key	The public key which in this system will be in the RSA form. RSA (1024 bits) The public key expressed in hexadecimal: <u>Example:</u> 3081 8902 8181 00A6 FD51 35E3 639D 4A92 E05A 991E 8660 1AF2 152F BBD1 F2C2 53FE 1F22 80F6 B255 8D25 1798 F336 7E92 B460 5D55 E958 324E DE66 F19B 5275 5A9B 1359 2DBD B482 C234 76DC 6C08 6A8E C491 1377 5D24 9743 C74A 43AA 1AFC D6EA 7460 OCD0 C1D0 57F3 OCA90 9707 9F9C 3F31 2B1C 6CF9 DC4E 642D D5AE 8863 89E5 9710 9A41 1F40 86E0 8A0E 2240 BD02 0301 0001
Key Usage	Describes how the Certificate can be used. In this example the Certificate is to be used only for digital signature verification. Digital Signature Non Repudiation
Authority Key Identifier	0100 followed by the least significant 60 bits of the SHA-1 hash of the Issuer's public key. 4xxx xxxx xxxx xxxx
Subject Key Identifier	0100 followed by the least significant 60 bits of the SHA-1 hash of the Subject's public key. <u>Example:</u> 4E2D 8D95 F63F 1551
Subject Alternative Name	RFC822 <a href="mailto:john.citizen@aaa.com.au">Name=john.citizen@aaa.com.au</a> (Example only)
CRL Distribution Point	Not applicable.
Signature Algorithm	Defines the algorithm that is used to generate the signature. SHA-1
Signature	The SHA-1 hash of the Certificate. <u>Example:</u> 9789 BDEB 1AA7 3BB9 7CD2 A68D FA8C C99B E501 B257

### 7.1.2 Certificate extension(s)

1. Private Extensions	
Field	Value
OID of RA Registration Number	The RA Registration number. A ten digit field. <u>Example:</u>

extension	5402869084
OID of Authority Info Access extension	Not applicable.

### **7.1.3 Algorithm object identifiers**

1. OIDs are not allocated to algorithms in Health PKI.

### **7.1.4 Name forms**

1. Certificates issued under Health PKI contain the full X.500 Distinguished Name of the Certificate issuer and Certificate subject in the issuer name and subject name fields respectively.

### **7.1.5 Name constraints**

1. Anonymous names are not supported.

### **7.1.6 Certificate Policy Object Identifier**

1. The OID of the Individual and Location CPs is carried in the standard extension field of issued X.509 Certificates and is published in clause 1.2 of the relevant CP.

### **7.1.7 Usage of policy constraints extension**

1. Not applicable.

### **7.1.8 Policy Qualifiers syntax and semantics**

1. The OCA supports the use of syntax and semantics Policy Qualifiers.

### **7.1.9 Processing semantics for the critical Certificate Policy extension**

1. The X.509 Certificate Profile complies with the Australian Standard X.509 profile.

## **7.2 CRL Profile**

### **7.2.1 Version number(s)**

1. The OCA supports the use of X.509 Version 2 CRLs.

### **7.2.2 CRL and CRL entry extensions**

1. The OCA supports the use of X.509 Version 2 CRL entry extensions.

## **8 Specification Administration**

### **8.1 Specification change procedures**

1. Three policy approval authorities are relevant to this *OCA\_CPS* and related CP Documents:
  - a) the Competent Authority;
  - b) the SecureNet Policy Management Authority (SecureNet PMA); and
  - c) the Health Policy Management Authority (Health PMA).
2. Further information can be found in the CP under which the Certificates were issued.

### **8.2 Publication and notification policies**

1. Refer to the CP under which the Certificates were issued.

### **8.3 Approved Document approval procedures**

1. Refer to the CP under which the Certificates were issued.