



**Australian Government**

---

**Medicare Australia**

**Medicare Australia Root Certification  
Authority (Medicare Australia RCA)  
Certification Practice Statement (CPS)  
Ver 2.5**

---

**Medicare Australia**

**May 2011**

## Copyright Notice:

This document contains information protected by copyright. © Commonwealth of Australia

This work is copyright. You may download, display, print and reproduce 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, External Communication Branch, Human Service Portfolio Communication Division,  
PO Box 7788, Canberra BC, ACT, 2610.

### Contact (for any other matters concerning this document)

National Manager

eClaiming and eHealth

PO Box 1001 Tuggeranong DC ACT 2901

Email: [ehealth.mca@medicareaustralia.gov.au](mailto:ehealth.mca@medicareaustralia.gov.au)

**Table 1: Version History**

Doc Version	Status	Date of Issue	Comments
0.1	DRAFT	16 August 2006	Initial draft for internal review.
0.2	DRAFT	21 August 2006	Accept/delete formatting to make it more readable, all fields' macros are also removed and replaced with the actual text.
0.3	DRAFT	25 August 2006	Revision of draft, including inserting Part 9 information from OCA CPS
0.4	DRAFT	29/08/2006	Acceptance of v.03 amendments; further revisions to consolidate information on Client CAs; revise information on termination and other amendments to ensure this CPS links with the OCA CPS and the RCA CP.
0.5	Draft	30/08/2006	Acceptance and review of changes
0.6	Draft	01/09/2006	Amendments re references to CoIs; deletion of settled comments; amendments to Part 9.
1.0	FINAL	5/09/2006	Acceptance of edits; deletion of comments as per meeting. Minor edits / tidy up
1.9	FINAL	8 SEPTEMBER 2006	NUMBER CHANGE TO 1.9 FINAL TO MATCH OID
1.9	FINAL	18 Sept 2006	Amendments to change PMA membership
1.91	Final	20 November 2006	Deletion of reference to the IT Security Manager in 5.2.4

			Other minor grammatical amendments
1.92	Draft	May 2008	Gatekeeper Accreditation under the Relationship Organisation model.
1.93	Draft	June 2008	Amendments after consultations with Legal and Technical teams.
1.94	Draft	June 2008	Amendments after consultations with Legal and Technical teams. Release version to AGIMO for comments.
1.95	Draft	July 2008	Amendments after review by the Gatekeeper Competent Authority.
1.96	Draft	November2008	Amendments after review by the Gatekeeper Competent Authority and further review by Medicare Australia.
1.97	Draft	February 2010	Updated References
1.98	Draft	April 2010	AGIMO Amendments included
1.99	Draft	May 2010	AGIMO Changes included following meeting.
2.0	Final	July 2010	Further AGIMO changes included
2.0	Final	August 2010	Final review
2.0	Final	18 August 2010	Final review & clearance for independent legal review
2.1	Draft	27 October 2010	Updates following Legal Review
2.2	Draft	28 February 2011	Update adjustments
2.3	Draft	9 March 2011	Update adjustments following Legal Review
2.4	Draft	April 2011	Update adjustments following AGIMO Review
2.5	Draft	May 2011	Update adjustments following AGIMO Review and approved by AGIMO.

This Document has been authorised by the Medicare Australia Policy Management Authority:

\_\_\_\_\_  
 General Manager, Health eBusiness Division  
 Medicare Australia

Date: \_\_\_\_\_

## Contents

<b>1.</b>	<b>INTRODUCTION .....</b>	<b>1</b>
1.1	OVERVIEW .....	1
1.2	MEDICARE AUSTRALIA ROOT CERTIFICATION AUTHORITY CERTIFICATE PRACTICE STATEMENT IDENTIFICATION	3
1.3	HEALTH SECTOR PKI PARTICIPANTS .....	4
1.4	CERTIFICATE USAGE .....	12
1.5	POLICY ADMINISTRATION.....	12
1.6	DEFINITIONS AND ACRONYMS.....	14
<b>2.</b>	<b>PUBLICATION AND REPOSITORY RESPONSIBILITIES .....</b>	<b>15</b>
2.1	REPOSITORIES .....	15
2.2	PUBLICATION OF CERTIFICATE INFORMATION.....	15
2.3	FREQUENCY OF PUBLICATION .....	16
2.4	ACCESS CONTROL .....	16
<b>3.</b>	<b>IDENTIFICATION AND AUTHENTICATION .....</b>	<b>17</b>
3.1	NAMING .....	17
3.2	INITIAL IDENTITY VALIDATION .....	17
3.3	IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS.....	17
3.4	REVOCATION REQUESTS .....	17
<b>4.</b>	<b>CERTIFICATE MANAGEMENT LIFE-CYCLE .....</b>	<b>18</b>
4.1	CERTIFICATE MANAGEMENT PROCESS .....	18
<b>5.</b>	<b>FACILITY MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS .....</b>	<b>19</b>
5.1	PHYSICAL SECURITY CONTROLS .....	19
5.2	PROCEDURAL CONTROLS .....	20
5.3	PERSONNEL SECURITY CONTROLS.....	22
5.4	AUDIT LOGGING PROCEDURES .....	24
5.5	RECORDS ARCHIVAL .....	25
5.6	KEY CHANGEOVER.....	27
5.7	COMPROMISE AND DISASTER RECOVERY.....	27

5.8	HEALTH SECTOR PKI TERMINATION.....	28
<b>6.</b>	<b>TECHNICAL SECURITY CONTROLS .....</b>	<b>29</b>
6.1	KEY PAIR GENERATION AND INSTALLATION .....	29
6.2	PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS .....	30
6.3	OTHER ASPECTS OF KEY PAIR MANAGEMENT .....	32
6.4	ACTIVATION DATA .....	32
6.5	COMPUTER SECURITY CONTROLS.....	32
6.6	LIFE CYCLE SECURITY CONTROLS .....	33
6.7	NETWORK SECURITY CONTROLS.....	33
6.8	TIME-STAMPING .....	33
<b>7.</b>	<b>CERTIFICATE AND CRL PROFILES .....</b>	<b>34</b>
7.1	CERTIFICATE PROFILE .....	34
7.2	CERTIFICATE REVOCATION LIST PROFILE.....	35
7.3	ONLINE CERTIFICATE STATUS PROTOCOL PROFILE .....	35
<b>8.</b>	<b>COMPLIANCE AUDIT AND OTHER ASSESSMENT .....</b>	<b>36</b>
8.1	FREQUENCY OF ENTITY COMPLIANCE AUDIT .....	36
8.2	IDENTITY / QUALIFICATIONS OF AUDITOR .....	36
8.3	AUDITOR'S RELATIONSHIP TO MEDICARE AUSTRALIA RCA.....	36
8.4	TOPICS COVERED BY AUDIT .....	36
8.5	ACTIONS TAKEN AS A RESULT OF DEFICIENCY .....	37
8.6	COMMUNICATION OF RESULTS .....	37
<b>9.</b>	<b>OTHER BUSINESS AND LEGAL MATTERS .....</b>	<b>38</b>
9.1	FEEES .....	38
9.2	FINANCIAL RESPONSIBILITY .....	38
9.3	CONFIDENTIALITY OF BUSINESS INFORMATION.....	38
9.4	PRIVACY OF PERSONAL INFORMATION.....	38
9.5	INTELLECTUAL PROPERTY RIGHTS.....	39
9.6	REPRESENTATIONS AND WARRANTIES.....	39
9.7	DISCLAIMERS OF WARRANTIES .....	39

9.8	LIMITATIONS OF LIABILITY .....	39
9.9	INDEMNITIES .....	39
9.10	TERM AND TERMINATION .....	39
9.11	INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS .....	39
9.12	AMENDMENTS .....	39
9.13	DISPUTE RESOLUTION PROCEDURES .....	40
9.14	GOVERNING LAW .....	40
9.15	COMPLIANCE WITH APPLICABLE LAW .....	40
9.16	MISCELLANEOUS PROVISIONS .....	40
<b>ANNEX A</b>	<b>MEDICARE AUSTRALIA PKI WEBSITE .....</b>	<b>41</b>
<b>ANNEX B</b>	<b>MEDICARE AUSTRALIA COMMUNITIES OF INTEREST .....</b>	<b>42</b>

## 1. Introduction

The commencement date of this Medicare Australia Root Certification Authority Certificate Policy (Medicare Australia RCA CP) is the date the Memorandum of Agreement (MOA) is signed by the Department of Finance and Deregulation and the Medicare Australia Policy Management Authority (Medicare Australia PMA).

This Medicare Australia RCA CP is written in accordance with RFC3647 "Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework", and outlines the rules applying to and scope of use of Health Sector Public Key Infrastructure (Health Sector PKI) Certificates.

### 1.1 Overview

#### 1.1.1. General

In general, a PKI consists of a hierarchy of Trusted Elements and Subscribers. In the Health Sector PKI, the hierarchy of Trusted Elements comprises the Medicare Australia Root Certification Authority (Medicare Australia RCA), Organisation Certification Authorities (OCAs) (e.g. the Medicare Australia OCA) and End User-Subscribers.

The Health Sector PKI is designed and operated to comply with the broad strategic direction of existing international standards and Gatekeeper Criteria and Policies for the establishment and operations of a PKI.

The Health Sector PKI supports the creation and use of Key pairs and of Public Key Certificates. Key pairs and Public Key Certificates are used in the provision of Health Sector PKI certificate services that include but are not limited to:

- Authentication services (authentication, integrity and non-repudiation), and
- Confidentiality services.

##### 1.1.1.1. Common Elements

This Medicare Australia RCA CPS covers the common practices and procedures that apply to the entire Health Sector PKI Hierarchies operated by Medicare Australia.

These common elements include:

- the use of Evaluated Products for any of the security-critical cryptographic operations,
- the separation of registration and certification operations, with CA operations and registration operations generally being performed on a remote site managed and operated by the Medicare Australia Relationship Organisation (RO or a third party,

- the application of tiered security comprising prevention, detection and considered response,
- the employment of trustworthy personnel who have been independently vetted to the HIGHLY PROTECTED security level,
- the application of rigorous change control processes to ensure no change is introduced without due consideration of all its possible security impacts, and
- the institution of a continuous cycle of internal and external audits to ensure a high level of operational integrity is always maintained.

### **1.1.1.2. Relationship between the Certificate Practice Statements and Certificate Policies**

The full set of practices, procedures, terms and conditions relating to a particular Certificate can be determined by reading:

- this Medicare Australia RCA CPS,
- the Medicare Australia Organisation Certification Authority Certificate Practice Statement (Medicare Australia OCA CPS) or the CPS for other OCAs within the Health Sector PKI Hierarchy,
- the Medicare Australia Root Certification Authority Certificate Policy (Medicare Australia RCA CP), and
- the Certificate Policy (CP) for the PKI Community of Interest (CoI) that the Certificate is issued under.

### **1.1.1.3. Medicare Australia Root Certification Authority Certificate Practice Statement**

This Medicare Australia RCA CPS relates to:

- the self-signed Medicare Australia RCA authentication and confidentiality Certificates which the Medicare Australia RCA issues to itself, and
- the authentication and confidentiality Certificates signed by the Medicare Australia RCA and issued to OCAs within the Health Sector PKI Hierarchy (e.g. the Medicare Australia OCA).

If there is any conflict between the provisions in relevant CPS and CPs, the following order of precedence of documents will apply:

- the CP for the PKI CoI that the Certificate was issued under, then

- other Health Sector PKI or relevant OCA CPs, then
- the Medicare Australia OCA CPS or other Health Sector PKI OCA CPSs, then
- the Medicare Australia RCA CP, then
- this Medicare Australia RCA CPS.

#### **1.1.1.4. Documentation**

Medicare Australia conducts its Medicare Australia RCA role in accordance with the following public documents:

- this Medicare Australia RCA CPS,
- the Medicare Australia RCA CP,
- the Medicare Australia OCA CPS,
- the relevant Certificate Policy the Certificates are issued under,
- the Health Sector PKI Glossary,
- Gatekeeper (Public Key Infrastructure) Criteria and Policies, and
- COMMERCIAL-IN-CONFIDENCE or HIGHLY PROTECTED documents which are not publicly available.

## **1.2 Medicare Australia Root Certification Authority Certificate Practice Statement Identification**

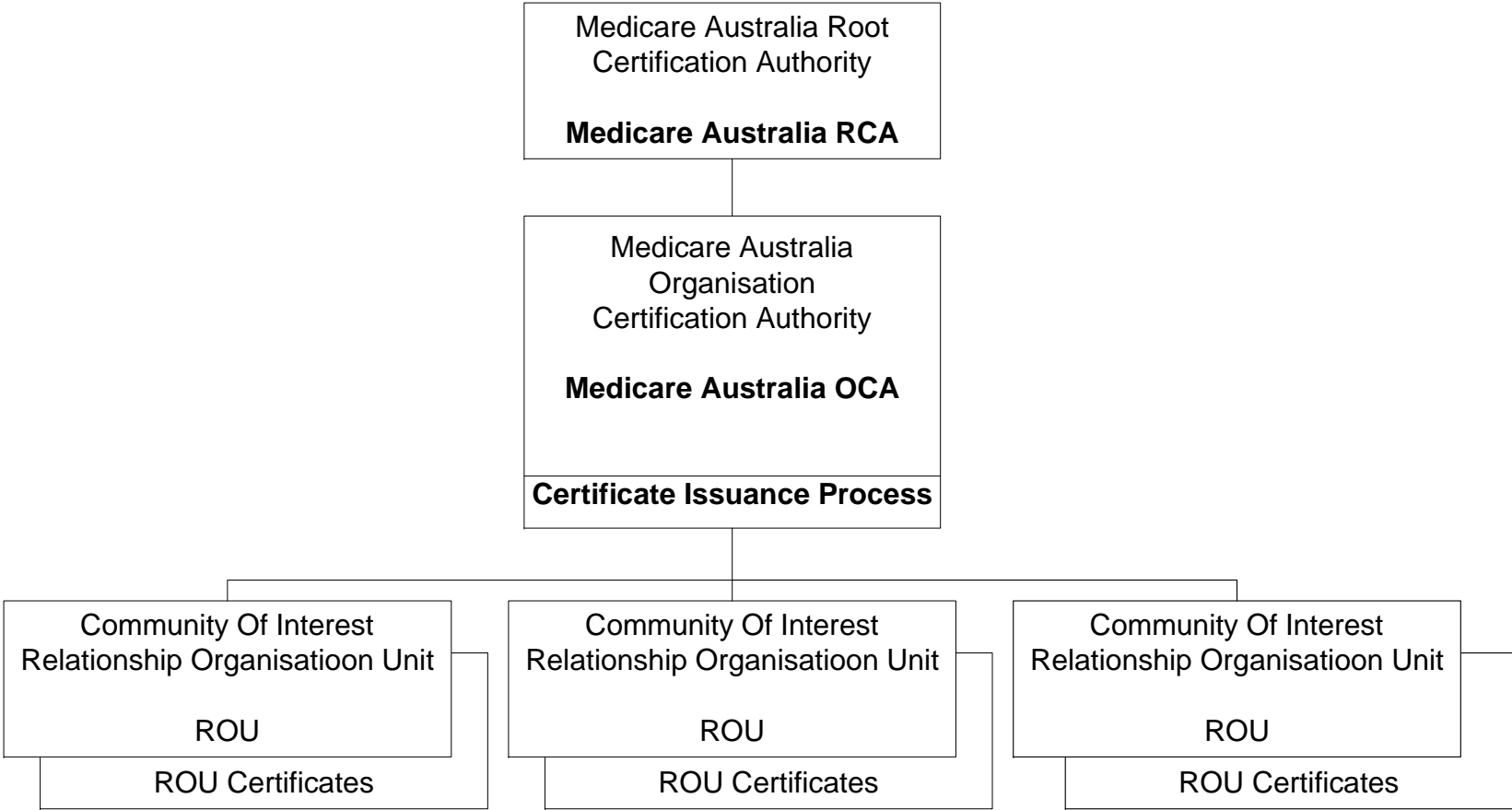
### **1.2.1. Medicare Australia RCA CPS Identification**

Specified elements under the Health Sector PKI have been assigned an X.500 Object Identifier (OID). The authority for issuing an OID is the Medicare Australia Policy Management Authority (Medicare Australia PMA).

An OID is not applicable to this CPS.

The Medicare Australia RCA CPS is published on [www.medicareaustralia.gov.au](http://www.medicareaustralia.gov.au) website.

**1.3 Health Sector PKI Participants**



This Medicare Australia RCA CPS is applicable to:

- the Medicare Australia RCA,
- any subordinate Medicare Australia OCA (e.g. the Medicare Australia OCA),
- Medicare Australia Relationship Organisation Unit Operators (Medicare Australia ROUOs) approved to operate within the Health Sector PKI hierarchy, and
- Relying Parties and End User-Subscribers registered for Health Sector PKI Keys and Certificates issued under the CP for the Subscribers' PKI CoI and supported by this CPS.

Annex B details the Medicare Australia Community of Interest Relationship Organisation Units.

### **1.3.1. Health Sector PKI Certification Authorities**

#### **1.3.1.1. Medicare Australia RCA Overview**

The Medicare Australia RCA is the highest point of trust within the Health Sector PKI CoI. All other OCAs entities in the Medicare Australia RCA Hierarchy rely on this point of trust.

The Medicare Australia RCA generates and signs its own Certificate and certifies the Certificates of its OCAs subordinate to the Medicare Australia RCA, e.g. the Medicare Australia OCA. In this CPS, these OCAs (including the Medicare Australia OCA) are referred to as "OCAs".

The Medicare Australia RCA is accessed via a single Root Certification Authority Operator (RCAO) which is used solely for the purpose of creating subordinate OCA Certificates (e.g. the Medicare Australia OCA Certificate). The Key length of the Medicare Australia RCA Signing Key, used to sign Certificates, is as determined by a relevant certificate profile.

Generation of the Medicare Australia RCA's Keys is performed on Trustworthy Systems using Evaluated Products in a physically secure facility.

The Medicare Australia RCA resides at a Secure Facility and is usually switched off except when required to create a new OCA or CRL.

#### **1.3.1.2. Medicare Australia RCA Functions**

The Medicare Australia RCA performs the following functions:

- generates its own Keys and issues a self signed Certificate using software listed on the Defence Signals Directorate (DSD) Evaluated Products List (EPL),
- issues to itself a self-signed Certificate binding itself to its own Public Key,
- publishes the Medicare Australia RCA Hash on the Healthcare Public Directory,

- administers the registration of OCAs in accordance with the Certificate registration process described in this CPS,
- generates and issue OCA Certificates only on receipt of properly formatted and verified Certificate Requests,
- ensures, at the time a OCA Certificate is issued to a OCA, that:
  - the OCA Certificate Information (i.e. information needed to complete an OCA Certificate as required by the Certificate Profile) is accurate,
  - the OCA Certificate contains all the elements required by the Certificate Profile (i.e. the specification of the fields to be included in a OCA Certificate and the contents of each), and
  - the OCA is in possession or control of the Private Key corresponding to the Public Key included in the OCA Certificate,
- issues Certificates that are factually correct from the information known to the Medicare Australia RCA at the time of issue and are free from data entry errors,
- receives suspension and revocation requests and take appropriate action,
- make reasonable enquiries in accordance with the arrangements agreed with OCAs to determine the validity of compromises and suspected compromises of Private Keys at any subordinate level the Medicare Australia RCA deems warranted in its chain of trust,
- promptly notifies an OCA in the event that the Medicare Australia RCA initiates revocation of an OCA Certificate(s),
- provides Relying Parties access to:
  - Certificate information published in the Healthcare Public Directory, and
  - the Public Keys associated with operational Certificates listed in the Healthcare Public Directory,
- if appropriate, to issue a new OCA Certificate to an OCA whose Keys have been compromised, or are suspected to have been compromised, after receiving a properly formatted and verified request from the OCA for a new OCA Certificate,
- facilitates the conduct of annual audits by Medicare Australia PMA-authorized external auditors,
- when the Medicare Australia RCA generates Key Pairs, ensures that each Key Pair can work as an operable pair of cryptographic Keys,

- revokes an OCA Certificate as required by, and in accordance with, this Medicare Australia RCA CPS,
- registers the revocation of the OCA Certificate so that this information is readily available to a Relying Party,
- administers the registration of the subordinate Medicare Australia OCA in accordance with the Certificated registration process described in this CPS,
- issues to the subordinate Medicare Australia OCA signed Certificates binding the subordinate Medicare Australia OCA to its Public Keys,
- publishes and certifies Public Keys and associated Certificates of the subordinate Medicare Australia OCA on a Healthcare Public Directory when requested to do so,
- operates in accordance with documented operational practice, and
- publishes this Medicare Australia RCA CPS and the Medicare Australia RCA CP at [www.medicareaustralia.gov.au](http://www.medicareaustralia.gov.au).

### **1.3.1.3. Medicare Australia RCA Obligations**

The Medicare Australia RCA obligations are:

- to comply with all Gatekeeper Policies and Criteria, including the Gatekeeper Core Obligations Policy and Medicare Australia's Gatekeeper Approved Documents,
- to comply with applicable laws,
- to maintain this Medicare Australia RCA CPS and Medicare Australia RCA CP,
- to comply with, and ensure that its personnel and contractors comply with, the conditions and obligations set out in this Medicare Australia RCA CPS and the policies set out in the Medicare Australia RCA CP, and
- to advise OCAs of their obligations under this Medicare Australia RCA CPS and the Medicare Australia RCA CP and make accessible a copy of these documents to each OCA.

### **1.3.1.4. Organisation Certification Authorities (OCAs) Overview**

Organisation Certification Authorities (OCAs) are immediately subordinate to the Medicare Australia RCA in the Health Sector PKI hierarchy. The primary purpose of such a subordinate OCA (e.g. the Medicare Australia OCA) is to provide Certificates and certificate management services to Relying Parties and Subscribers who are subordinate to the OCA in the Health Sector PKI.

OCAs subordinate to the Medicare Australia RCA include:

- the Medicare Australia OCA that provides Certificate management services for:
  - PKI CoI within Medicare Australia, and
  - Australian Government Agencies who do not wish to operate their own Certification Authority for certification services for that Agency's CoIs.
- Other OCAs that may be included as OCAs subordinate to the Medicare Australia RCA in the Health Sector PKI hierarchy.

The Key length of a Medicare Australia OCA Keys used to sign Certificates are determined by the relevant certificate profile. However, unless otherwise stated, the minimum Key length for a Medicare Australia OCA is 2048 bits.

Generation of Medicare Australia OCA Keys is performed on Trustworthy Systems using Evaluated Products in a physically secure facility.

The functions and obligations of OCAs, as a CA within the Health Sector PKI hierarchy, are dealt with in the CP under which the OCA issues Certificates to members of a PKI CoI subordinate to that OCA.

The functions and obligations of an OCA when acting in the role of a Subscriber are set out at 1.3.3 of this Medicare Australia RCA CPS.

The functions and obligations of an OCA when acting in the role of a Relying Party are set out at 1.3.4 of this Medicare Australia RCA CPS.

#### **1.3.1.5. Organisation Certification Authorities (OCAs) Functions**

OCAs operating under the Health Sector PKI hierarchy perform the following functions:

- generate their own Keys,
- submit their Public Keys together with digitally signed certification requests to the Medicare Australia RCA, and
- publish their OCA CPS, the OCA CP or each CP for the PKI CoI under which they issue Certificates on a nominated web site specified within the OCA CPS.

On the receipt of authenticated digitally signed Certificate requests from authorised ROUOs, OCAs will:

- issue Certificates in accordance with this Medicare Australia RCA CPS, the Medicare Australia RCA CP, their OCA CPS, their OCA CP (where one is required) and the CP for the PKI CoI that

the Certificates are issued under for:

- Subscriber ROUOs, and
  - End User-Subscribers,
- publish issued Certificates in the Healthcare Public Directory where there is permission from the PKI CoI to do so,
- to generate and issue Certificates only on receipt of properly formatted and verified Certificate Requests,
- to ensure, at the time a Certificate is issued to a End-User Subscriber, that:
  - the Certificate Information (i.e. information needed to complete a Certificate as required by the Certificate Profile) is factually correct and accurate,
  - the Certificate contains all the elements required by the Certificate Profile (i.e. the specification of the fields to be included in a Certificate and the contents of each), and
  - the Certificate is in possession or control of the Private Key corresponding to the Public Key included in the Certificate,
- to receive suspension and revocation requests and take appropriate action,
- revoke Certificates on receipt of authenticated digitally signed revocation requests,
- post revoked Certificates in the Healthcare Public Directory,
- to make reasonable enquiries in accordance with the arrangements agreed with each PKI CoI to determine the validity of compromises and suspected compromises of Private Keys at any subordinate level the Medicare Australia RCA deems warranted in its chain of trust,
- to promptly notify the Registration Organisation Unit (ROU) for a PKI CoI in the event that the Medicare Australia RCA initiates revocation of the OCAs Certificate(s), and
- to revoke a Certificate as required by, and in accordance with this Medicare Australia RCA CPS.

#### **1.3.1.6. OCA Obligations**

An OCA's (e.g. the Medicare Australia OCA) obligations are:

- to comply with all Gatekeeper Policies and Criteria, including the Gatekeeper Core Obligations Policy and Medicare Australia's Gatekeeper Approved Documents,

- to comply with applicable laws,
- to maintain their OCA CPS and the relevant CPs for each COI,
- to comply with, and ensure that its personnel and contractors comply with, the conditions and obligations set out in this Medicare Australia RCA CPS and the practices set out in the Medicare Australia RCA CP,
- to advise End User-Subscribers of their obligations under this Medicare Australia RCA CPS, the Medicare Australia RCA CP, their OCA CPS and the CP relevant to that CoI and make copies accessible to each End User-Subscriber, and
- when requested by the Medicare Australia PMA, manage the conduct of audits performed on the OCA, the certificate issuance process and ROUs.

### **1.3.2. Registration Authorities**

This Medicare Australia RCA CPS does not include information on Registration Authorities (RAs). Information about RAs in the Health Sector PKI is included in the relevant OCA CPS. The Medicare Australia OCA CPS is available at [www.medicareaustralia.com.au](http://www.medicareaustralia.com.au).

### **1.3.3. Subscribers**

Subscribers of the Medicare Australia RCA are OCAs that apply to have their Certificates signed by the Medicare Australia RCA within the Health Sector PKI hierarchy managed by Medicare Australia.

The Medicare Australia RCA is responsible for checking Evidence of Identity (EOI) and collecting registration information for and about subordinate Medicare Australia OCAs only.

#### **1.3.3.1. Applicants**

An applicant is a third party who wishes to become an Medicare Australia OCA subordinate to the Medicare Australia RCA within the Health Sector PKI hierarchy.

Prior to a certificate being issued, the applicant must apply to the Medicare Australia RCA to be a subordinate Medicare Australia OCA and be issued a signed Certificate binding the OCA Public Keys with the signed Certificate.

#### **1.3.3.2. OCA Subscribers to Medicare Australia RCA**

The obligations of OCAs, when acting as Subscribers under this Medicare Australia RCA CPS and the Medicare Australia RCA CP, are:

- to comply with the provisions of this Medicare Australia RCA CPS and the Medicare Australia RCA CP,
- to comply with and maintain their own Medicare Australia Gatekeeper Approved Documents,
- to comply with applicable laws,
- to maintain an OCA Policy Management Authority (OCA PMA) with the authority to represent the OCA Relationship Organisation (OCA RO) in matters relating to the OCA,
- to ensure that all information provided to the Medicare Australia RCA in relation to their Key Pairs and Certificates is true and complete,
- to ensure that their own Key Pairs are operable pairs of cryptographic Keys which meet the requirements of their own and the Medicare Australia RCA Key Management Plan,
- to keep their Private Keys secret,
- to promptly notify the Medicare Australia RCA in the event that the OCA's Keys have been compromised, or are suspected of having been compromised,
- to cooperate with compliance audits conducted by the Medicare Australia PMA for the Medicare Australia RCA,
- to immediately notify the Medicare Australia RCA if the OCA:
  - has an adverse audit finding made against it, or
  - has any other change to their Registration Information, or any other information provided to the Medicare Australia RCA,
- to use Trustworthy Systems in which:
  - only authorised personnel can make entries and changes,
  - information can be checked for authenticity, and
  - any technical changes compromising security are apparent to the operator,
- to employ personnel who possess the expert knowledge, experience, and qualifications necessary for the provision of certification services, and who have undergone the required security clearances for the position,
- to apply administrative and management procedures which are appropriate for the activities being carried out,
- to enter into appropriate agreements with their own Subscribers and Relying Parties which clearly outline End Entity obligations, including any terms and conditions required by the Gatekeeper Competent Authority for Subscriber agreements, and

- to obtain appropriate insurance to cover the risk of liability for damages flowing from its provision of certification services.

The issuance of Certificates to End User-Subscribers is outside the scope of this Medicare Australia RCA CPS.

The obligations of End User-Subscribers are set out in the CPS and CPs for the PKI CoI under which the End User-Subscriber's certificate was issued.

### **1.3.4. Relying Parties**

There are no Relying Parties for the RCA CPS as there are no end-user subscribers.

Relying Parties for each ROU PKI CoI under an OCA are identified in the CP under which that particular ROU's PKI CoI Certificates are issued.

### **1.3.5. Other Participants**

There are no other participants in the Health Sector PKI Relationship Certificate model operated by Medicare Australia.

#### **1.3.5.1. End User-Subscribers**

The Medicare Australia RCA does not issue Certificates to End User-Subscribers and does not check EOI or collect registration information from End User-Subscribers.

## **1.4 Certificate Usage**

### **1.4.1. Appropriate Certificate Use**

See Section 1.4.1 of the Medicare Australia RCA CP or section 1.2 of the CP that Certificates are issued under.

### **1.4.2. Prohibited Certificate Uses**

See Section 1.4.2 of the Medicare Australia RCA CP or section 1.2 of the CP that Certificates are issued under.

## **1.5 Policy Administration**

### **1.5.1. Document Administration**

This Medicare Australia RCA CPS is administered and approved by the Medicare Australia PMA.

The Medicare Australia PMA:

- approves changes to this CPS, Medicare Australia RCA CP and other Documents,

- approves any OCA CP and CPS, including any changes to those documents, and
- manages compliance by an OCA and its RA(s) with this CPS, any OCA CPS, the CP the Certificate was issued under, and other Documents.

OCA's may operate an OCA Policy Management Authority (OCA PMA). An OCA's PMA is responsible for the creation and internal approval of policies which are unique to the operation of that OCA and are consistent with the RCA CP/CPS.

The OCA's PMA performs the following functions:

- formulates and gives internal approval to new policy and policy changes within the OCA policy domain, and
- submits new or changed policies to the Medicare Australia PMA for approval.

## **1.5.2. Contact Persons**

### **1.5.2.1. Policy Management Authority**

The contact details for the Medicare Australia PMA are:

National Manager

eClaiming and eHealth

PO Box 1001 Tuggeranong DC ACT 2901

Email: [ehealth.mca@medicareaustralia.gov.au](mailto:ehealth.mca@medicareaustralia.gov.au)

The contact person can provide copies of, or access to, this Medicare Australia RCA CPS, the Medicare Australia RCA CP and answer questions relating to the policy, practices and procedures described in these documents.

### **1.5.3. CPS Suitability and CPS and CP Approval Procedures for the Medicare Australia RCA Certificate Policy**

The Medicare Australia PMA reviews all documents to ensure that the practices documented in this Medicare Australia RCA CPS fulfil the requirements defined in the relying Medicare Australia RCA CP.

The Medicare Australia PMA determines whether or not this Medicare Australia RCA CPS provides suitable support for the Medicare Australia RCA CP.

The Medicare Australia PMA approves all Medicare Australia RCA CPS and Medicare Australia RCA CP changes and modifications.

All new applications for Subscribers as an OCA or RA under the Medicare Australia RCA will be vetted by the Medicare Australia PMA and if satisfactory, will be approved by the Medicare Australia PMA.

## 1.6 Definitions and Acronyms

Please refer to the Medicare Australia Healthcare Sector PKI Glossary at [www.medicareaustralia.gov.au](http://www.medicareaustralia.gov.au) and the Gatekeeper PKI Framework Glossary at [www.gatekeeper.gov.au/](http://www.gatekeeper.gov.au/) for a list of Definitions and Acronyms.

## 2. Publication and Repository Responsibilities

### 2.1 Repositories

The repository for all Public Key Certificates issued under this Medicare Australia RCA CPS is the Healthcare Public Directory.

The Healthcare Public Directory provides information about Active, Revoked and Expired Certificates issued under the respective CP(s) for each ROU's PKI CoI, OCAs or the Medicare Australia RCA.

Note that Certificate suspension is not supported under the Relationship Certificate model as operated by Medicare Australia in this Health Sector PKI.

Changes in the status of Certificates issued under this Medicare Australia RCA CPS, including Revocation and Expiry of Certificates will be published in the Healthcare Public Directory by the Medicare Australia RCA.

The Healthcare Public Directory:

- does not publish reasons why a Certificate has been Revoked,
- only publishes information already contained in the Certificate, and
- only publishes information pertaining to a given PKI CoI when the responsible RO and ROU have agreed to publication.

The Healthcare Public Directory is accessible from [www.certificates-australia.com.au](http://www.certificates-australia.com.au). Technical details are at [www.medicareaustralia.gov.au](http://www.medicareaustralia.gov.au).

The Healthcare Public Directory is substantially available 7 days a week, 24 hours a day (except for designated system maintenance periods)

### 2.2 Publication of Certificate Information

#### 2.2.1. Publication of Medicare Australia RCA Information

Certificates and their corresponding hash values are published to the Healthcare Public Directory when the Certificate is generated. In addition, the hash value of the Medicare Australia RCA and Medicare Australia RCA CA Certificate is published on Medicare Australia's website, [www.medicareaustralia.gov.au](http://www.medicareaustralia.gov.au).

#### 2.2.2. Publication of Policy and Practice Information

This Medicare Australia RCA CPS is published electronically at the website, [www.medicareaustralia.gov.au](http://www.medicareaustralia.gov.au).

Formal notification of changes to this Medicare Australia RCA CPS will not be given to any entities.

Notification of changes will be provided on Medicare Australia's website, [www.medicareaustralia.gov.au](http://www.medicareaustralia.gov.au). This notification method uses a "pull" model. Interested parties must exercise due care and check, on a regular basis, the Medicare Australia website to review and monitor any changes in the Medicare Australia RCA CPS. Interested parties are responsible for retrieving amendments when a revised and / or amended Medicare Australia RCA CPS is posted to the website.

## **2.3 Frequency of Publication**

### **2.3.1. Frequency of Publication of this CPS**

New and revised approved versions of this Medicare Australia RCA CPS are published promptly at [www.medicareaustralia.gov.au](http://www.medicareaustralia.gov.au).

#### **2.3.1.1. Publication by OCAs**

All OCAs within the Health Sector PKI hierarchy must publish the current approved version of the Medicare Australia RCA CPS on the web site(s) on which they publish their OCA CPS and any CPs that Certificates are issued under.

## **2.4 Access Control**

There are no access controls on the reading of this Medicare Australia RCA CPS, the Medicare Australia RCA CP or the CPS and CP for the Medicare Australia OCA or any associated OCA CPS and CPs on the web sites nominated for publication.

### **3. Identification and Authentication**

This Section 3 sets out the process that Applicants go through to authenticate themselves and register for Health Sector PKI Keys and Certificates, for example:

- initial Registration,
- routine Re-key,
- Re-key after Revocation, and
- Revocation requests.

For further information, refer to Section 2 of the CP the Certificates were issued under.

#### **3.1 Naming**

For further information, refer to Section 3 of the Medicare Australia RCA CP or section 2 of the CP that the Certificates were issued under.

#### **3.2 Initial Identity Validation**

For further information, refer to Section 3 of the Medicare Australia RCA CP or section 2 of the CP that the Certificates were issued under.

#### **3.3 Identification and Authentication for Re-key Requests**

For further information, refer to Section 3 of the Medicare Australia RCA CP or section 2 of the CP that the Certificates were issued under.

#### **3.4 Revocation Requests**

Refer to Section 3.4 of the RCA CP.

## **4. Certificate Management Life-Cycle**

### **4.1 Certificate Management Process**

Section 4 sets out Medicare Australia RCA processes to maintain the Certificate Management Process within the Health Sector PKI, and includes, for example:

- Certificate generation,
- Certificate operational use,
- Certificate expiry, and
- Certificate archive.

For further information, refer to Section 4 of the Medicare Australia RCA CP or Section 3 of the CP that the Certificates were issued under.

## **5. Facility Management, Operational, and Physical Controls**

### **5.1 Physical Security Controls**

#### **5.1.1. Site Location and Construction**

The Medicare Australia RCA is housed in a Secure Facility operated to the level of HIGHLY PROTECTED as defined in the Australian Government ICT Security Manual (ISM), and certified by a member of the Physical Security Evaluation Panel listed on the Gatekeeper website. The Secure Facility is staffed on a 24 x 7 basis.

#### **5.1.2. Physical Access**

The Medicare Australia PMA decides the physical security access requirements for the Health Sector PKI.

The Medicare Australia RCA is housed in a no-lone zone, meaning that two people must always be present for operations carried out at the Medicare Australia RCA.

Physical access to servers is controlled through procedural control of keys for the C-Class cabinets housing the servers.

#### **5.1.3. Power and Air Conditioning**

All Secure Facilities are 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.

The Secure Facility has an air conditioning system which controls temperature and humidity. Backup air conditioning units are provided for the no lone zones (i.e. the CA room).

#### **5.1.4. Water Exposures**

The Secure Facility is protected against water exposure by being located on built in raised floors of a building that is not in a flood zone.

#### **5.1.5. Fire Prevention and Protection**

The Secure Facility is subject to normal Verizon Australia Pty Ltd fire prevention and protection procedures.

Early detection of smoke in the Secure Facility is assured through the use of an extremely sensitive VESDA (Very Early Smoke Detection Apparatus) smoke detection system which continuously samples air from under the computer room floor and from the computer room itself. On detection of an unacceptably high level of smoke in the sampled air, the VESDA unit triggers a non-toxic gas fire suppression system.

In addition to this automatic fire suppression system, suitable fire extinguishers are maintained in the secure operating area.

The Secure Facility's proximity swipe-card system supports emergency evacuation procedures to cater for environmental hazards such as fire, natural disasters and structural collapse.

### **5.1.6. Media Storage**

All magnetic media containing sensitive Health Sector PKI information, including backup media, is stored in containers, cabinets or safes with fire protection capabilities which are located either within the secure operating area or in a secure off-site storage area.

No Medicare Australia Health Sector PKI documents may be removed from the Secure Facility without approval from the Medicare Australia PMA. All removals must be recorded in the appropriate register, for example the Classified Media Register.

### **5.1.7. Waste Disposal**

#### **Waste Disposal at the Secure Facility**

Paper documents and magnetic media containing any Private Keys or commercially sensitive or Confidential Information are securely disposed of by:

- in the case of magnetic media:
  - physical damage to, or complete destruction of the asset, or
  - the use of an approved utility to wipe or overwrite magnetic media, and
- in the case of printed material, cross-cut shredding.

All disposal actions will be undertaken in a manner that is compliant with the ISM.

### **5.1.8. Off-Site Backup**

An approved secure site that is certified by a member of the Physical Security Evaluation Panel listed on the Gatekeeper website is used for the storage and retention of off-site backup software and data. The off-site storage:

- has appropriate levels of physical security in place, and
- may be accessed on a 24 x 7 basis by authorised personnel for the purposes of retrieving software and data.

## **5.2 Procedural Controls**

### **5.2.1. Trusted Roles**

The Health Sector PKI contains a number of designated 'positions of trust'. These positions underpin the secure and reliable operation of the Health Sector PKI, and as such must be filled by competent and

trustworthy people (although the same person may fill several positions of trust) who have undergone the required security clearances for the position.

The general principle is that any role providing an opportunity to compromise Private Key material or impact on the certificate life cycle must be a trusted role. Further details are set out in the Verizon Australia Pty Ltd *SEC1 Security Profile* (this document is not a public document).

### **5.2.2. Number of Persons Required Per Task**

Multi-person control is used where the requirement is to provide enhanced security and checks and balances over Health Sector PKI operations. In particular:

- the appropriate Security Manager always remains separate from the Health Sector PKI System Operators in order to provide an independent third party when reviewing and auditing Health Sector PKI Operations,
- logical access controls for Health Sector PKI operations personnel have been implemented to ensure that no one person can access a single machine and therefore the sensitive information contained on those machines,
- the CA Operators are broken into the following 2 groups,  
**Group 1** - has access to the logon passphrase for cryptographic elements, and  
**Group 2** - has access to the logon database applications, and
- any task requiring the creation, backup or import into a database of a Health Sector PKI component Private Key takes place in a no-lone zone and therefore involves two trusted persons, one performing the function and the second person fulfilling a security monitoring role.

### **5.2.3. Identification and Authentication for each Role**

Each Health Sector PKI operations personnel has a separate account so all operations can be traced to an individual.

Details for emergency account access to Health Sector PKI infrastructure are specified in the Verizon Australia Pty Ltd *SEC1 Security Profile* (this document is not a public document).

### **5.2.4. Roles Requiring Separation of Duties**

To enhance security of the Health Sector PKI the following roles are to be undertaken by different personnel:

- the Health Sector PKI hosting facility Security Administrator will normally remain separate from the Health Sector PKI System Operators in order to provide an independent review

of audit logs unless in exceptional circumstances (i.e. personnel issues whereby integrity of the Health Sector PKI service being operated could be breached).

## **5.3 Personnel Security Controls**

### **5.3.1. Background, Qualifications, Experience and Clearance Requirements**

All Health Sector PKI operations personnel (excluding Relationship Organisation Unit Operators (ROUOs)) require a HIGHLY PROTECTED clearance prior to being granted access to Medicare Australia RCA Trusted Elements.

### **5.3.2. Background Check Procedures**

The Health Sector PKI security clearance process will follow the guidelines of the Commonwealth Protective Security Policy Framework (PSPF).

### **5.3.3. Training Requirements**

A formal training program, founded on competency-based training principles is in place.

The Health Sector PKI operation centre Team Leader is responsible for ensuring that new and inexperienced personnel are appropriately trained and supervised.

All Health Sector PKI operational personnel are trained in:

- basic Health Sector PKI concepts,
- the use and operation of the Health Sector PKI software,
- the Verizon Australia Pty Ltd PKI hosting facility procedures,
- computer security awareness and procedures, and
- the meaning and effect of this Medicare Australia RCA CPS and the Medicare Australia RCA CP.

### **5.3.4. Retraining Frequency and Requirements**

The introduction of any new security procedure or major software release will be accompanied by a corresponding education program for personnel affected by the changes to ensure that they are aware of their new responsibilities.

Remedial training is completed when recommended by audit findings and / or recommendations.

### **5.3.5. Sanctions for Unauthorised Actions**

Where personnel are found to have seriously misused the resources to which they have been granted access, these actions shall be documented and passed to Medicare Australia or Verizon Australia Pty Ltd as appropriate for determination in accordance with the relevant Commonwealth legislation.

Sanctions against contract personnel of Medicare Australia or Verizon Australia Pty Ltd shall be in accordance with the terms and conditions of their relevant contract with Medicare Australia or Verizon Australia Pty Ltd.

Depending on the nature of the actions sanctions may range from counselling and/or suspension of access rights, through to dismissal and/or legal action.

Criminal sanctions apply for contravention of relevant legislation, for example the *Crimes Act 1914* (Commonwealth), and the *Public Services Act 1999* (Commonwealth).

Prohibited actions in the Health Sector PKI include (but are not limited to):

- connecting private computers, computer peripherals, or computer software to the Health Sector PKI network,
- installing unauthorised software (including copyright infringed items). All software installations must be in accordance with the requirements of Health Sector PKI policies and the documented change management procedures,
- using Health Sector PKI systems for unauthorised purposes,
- having diagnostic tools (capable of testing or breaking security resident in any system) on their machines, and
- changing the configuration of any Health Sector PKI hardware or software without approval of the Verizon Australia Pty Ltd PKI Security Administrator and the Medicare Australia PMA.

### **5.3.6. Contracted Personnel – Management and Responsibilities**

For all contractors employed in positions of trust within the Health Sector PKI in any capacity, their rights and obligations and all terms and conditions of service will be as per the contract between the contractor and Medicare Australia or other applicable contract.

Casual Health Sector PKI personnel and third party users who are not already covered by an existing contract including confidentiality clauses will be required to sign a Confidentiality Deed before being granted limited access to information processing facilities. The need for the party to enter into the Confidentiality Deed is at the discretion of Medicare Australia.

Contractors in breach of security obligations may be guilty of certain criminal offences, for example offences relating to computers, offences relating to espionage and official secrets and offences against the Government, as set out in the *Crimes Act 1914* (Commonwealth) and other Commonwealth legislation.

### **5.3.7. Documentation Supplied to Personnel**

All Health Sector PKI operational personnel have access to the following documentation:

- all relevant hardware and software documentation,
- application manuals where appropriate,
- policy documents, including this CPS, and
- operational and procedure documents, including this Medicare Australia RCA CPS, Health Sector PKI operating procedures and OCA and certificate issuance operating procedures, as appropriate.

Note: the Health Sector PKI is largely composed of commercial-off-the-shelf products. Software documentation is therefore widely available to Health Sector PKI personnel.

General documents relating to the operation of the Health Sector PKI such as this Medicare Australia RCA CPS and Medicare Australia RCA CP are available to Medicare Australia personnel, for example through publication on the Medicare Australia intranet or to the public through the Medicare Australia website [www.medicareaustralia.gov.au](http://www.medicareaustralia.gov.au).

## **5.4 Audit Logging Procedures**

Medicare Australia will maintain Records and Archives of information for the activities of the Medicare Australia RCA and the Medicare OCA as required by the *Archives Act 1983* (Commonwealth).

Contracted service providers for the CAs and / or certificate issuance process will be contractually bound to comply with the *Archives Act 1983*.

### **5.4.1.1. Types of Events Recorded**

The minimum audit records to be kept include all:

- registration records,
- Key generation records,
- certificate generation requests,
- certificate issuance records, including Certificate Revocation Lists (CRLs),
- audit records including security related events, and

- revocation records.

#### **5.4.1.2. Frequency of Processing Log**

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

#### **5.4.1.3. Retention Period of Audit Log**

Audit logs are maintained on site prior to archiving for a maximum period of three months and then transferred to the off-site archive facility. Archived logs are retained for a period of seven years (from the date of archival).

#### **5.4.1.4. Protection of Audit Log**

Medicare Australia RCA audit logs are stored in a B-class safe located in the Secure Operations Room prior to archiving. Audit logs are signed using a Private Key specifically generated for this purpose. Audit log signatures can be verified using the Certificate associated with the Audit log Private Key.

Archived Health Sector PKI audit logs are stored in a secure off-site facility that is certified by a member of the Physical Security Evaluation Panel listed on the Gatekeeper website.

#### **5.4.1.5. Audit log Backup Procedures**

A detailed backup procedure for audit logs has been established and maintained and is documented in the Verizon Australia Pty Ltd *SEC1 Security Profile* (this document is not publicly available).

#### **5.4.1.6. Audit Collection System (Internal vs. External)**

The Medicare Australia RCA audit collection system for the Medicare Australia RCA 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 Verizon Australia Pty Ltd *SEC1 Security Profile* (this document is not publicly available).

#### **5.4.1.7. Notification to Event-causing Subject**

Operations personnel notify the Medicare Australia PMA chair when a process or action causes a critical security event or discrepancy. The Medicare Australia PMA shall notify the Gatekeeper Competent Authority.

### **5.5 Records Archival**

#### **5.5.1. Types of Event Recorded**

The following information is archived by the Medicare Australia RCA:

- Audit logs (refer to 5.4 of this Document),

- Certificate request information, and
- Complete back up registers.

Each CA or RA or certificate issuance entity in the Health Sector PKI Hierarchy is required to maintain an archive of relevant records.

## **5.5.2. Retention Period for Archive**

### **5.5.2.1. Secure Maintenance of Keys**

Medicare Australia retains copies of the Public and Private Keys of the Medicare Australia RCA and subordinate OCAs in a Secure Facility.

### **5.5.2.2. Secure Maintenance of Certificates**

Medicare Australia retains copies of the Public and Private Certificates of the Medicare Australia RCA and subordinate OCAs in a Secure Facility.

### **5.5.2.3. Term of Archive Maintenance**

Archives are retained for a period of seven years from date of generation in accordance with the requirements of the *Archives Act 1983* (Commonwealth).

## **5.5.3. Protection of Archive**

Archive media is protected by physical security and cryptographic protection commensurate with the security classification of the contents and in accordance with relevant provisions of the PSPF.

## **5.5.4. Archive Backup Procedures**

Archive backup procedures have been established to ensure complete restoration of current service or verification. Details are specified in the Verizon Australia Pty Ltd *SEC1 Security Profile* (this document is not publicly available).

## **5.5.5. Requirements for Time-stamping of Records**

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.

## **5.5.6. Archive Collection System (Internal or External)**

Archiving is performed by operations personnel delegated with the responsibility for doing so. Detailed procedures for backups, archiving and storage are set out in the Verizon Australia Pty Ltd *SEC1 Security Profile* (this document is not publicly available).

### **5.5.7. Procedures to Obtain and Verify Archive Information**

The integrity of the Archives is verified in accordance with the criteria set out in the Verizon Australia Pty Ltd *SEC1 Security Profile* (this document is not publicly available).

## **5.6 Key Changeover**

Key changeover will be affected in such a manner as to cause minimal disruption to Subscribers and End User-Subscribers.

OAs 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.

During this changeover period until the expiry of the Certificate associated with the current Health Sector PKI Private Authentication Key, both Authentication Public Keys in the associated Certificate will be in use and published in the Healthcare Public Directory.

The Health Sector PKI is committed to:

- ensuring that Key changeover causes minimal disruption to Subscribers, and
- providing Subscribers with reasonable notice of planned Key changeover.

## **5.7 Compromise and Disaster Recovery**

### **5.7.1. Incident and Compromise Handling Procedures**

Medicare Australia will maintain a Disaster Recovery and Business Continuity Plan for the Medicare Australia RCA. This plan, although not publicly available, will be made available to those persons responsible for and authorised to, conduct security audits as well as those persons who provide ongoing support for the RCA.

### **5.7.2. Computing Resources, Software, and/or Data are Corrupted**

Directions for managing service restoration in the event of a corruption of computing resources, software and/or data are provided in the Verizon Australia Pty Ltd *OPS1 CA Operations Manual* and *SEC1 Security Profile* (these documents are not publicly available).

### **5.7.3. Entity Private Key Compromise Procedures**

In the situation that the Medicare Australia RCA or the Medicare Australia OCA or any other OCA Private Key is compromised, for whatever reason, the procedures outlined for a termination of the entity whose Private Key was compromised, would be followed. Details for the termination of the entity are provided in the Verizon Australia Pty Ltd *SEC1 Security Profile* (these documents are not publicly available).

The Medicare Australia PMA Chair shall promptly advise the Gatekeeper Competent Authority of any compromise or suspected compromise of any of the Private Keys belonging to any Gatekeeper Accredited CA in the Health Sector PKI hierarchy.

#### **5.7.4. Business Continuity Capabilities after a Disaster**

Actions will be taken in order to restore core business operation as quickly as practicable following fire, strikes or similar events. Details are provided in the Verizon Australia Pty Ltd *SEC1 Security Profile* (this document is not publicly available). Medicare Australia will provide notification of any business outages through a number of channels such as the Medicare Australia's website, [www.medicareaustralia.gov.au](http://www.medicareaustralia.gov.au) or through its client relations helpdesk framework.

### **5.8 Health Sector PKI Termination**

Medicare Australia may terminate the Health Sector PKI at its own discretion or as directed by the Commonwealth government.

If the Health Sector PKI is terminated, details of transition plans and procedures will be provided to Health Sector PKI participants.

## **6. Technical Security Controls**

### **6.1 Key Pair Generation and Installation**

#### **6.1.1. Key Pair Generation**

##### **6.1.1.1. Medicare Australia RCA Key Pair Generation**

Medicare Australia RCA Key pairs are generated and installed by the Medicare Australia RCA using software that is listed on the DSD EPL.

##### **6.1.1.2. Medicare Australia RCA Private Key Pair Generation**

The self-generated Medicare Australia RCA Private Keys do not require delivery.

#### **6.1.2. Private Key Delivery to Organisation Certification Authorities**

OCA Private Keys are generated by the OCA and do not require delivery.

##### **6.1.3. Public Key Delivery to Medicare Australia RCA**

OCA Public Keys are delivered to the Medicare Australia RCA, personally escorted by trusted OCA personnel.

The OCAs PKCS#10 Certificate request must be transferred to the Medicare Australia RCA in a way that ensures that:

- it has not been changed during transit,
- the sender possesses the Private Key that corresponds to the transferred Public Key, and
- the sender of the Public Key is the legitimate user claimed in the certificate application.

##### **6.1.4. Public Key Delivery to Relying Parties**

The CA Public Keys are made available to End User-Subscribers and Relying Parties via the Healthcare Public Directory.

##### **6.1.5. Key Sizes**

The Medicare Australia RCA Key length is 2048 bits.

Subscriber OCA and RA Key strengths are to be minimum 2048 bits in length.

Relying Parties and End User-Subscriber Key strengths are to be minimum length 1024 bits in length.

## **6.1.6. Public Key Parameters Generation and Quality Checking**

### **6.1.6.1. Parameter Generation**

The parameters used to create the Medicare Australia RCA Public Keys are generated by the Medicare Australia RCA.

The parameters used to create the OCA Public Keys are generated by the OCA.

In both cases, the generation of Public Key parameters has been certified in the course of Common Criteria EAL 4 evaluation of the CA products used for Key generation.

### **6.1.6.2. Parameter Checking**

Parameter quality checking (including primality testing for prime numbers where appropriate) has been certified in the course of Common Criteria EAL 4 evaluation of the CA products used for Medicare Australia RCA Key generation.

Parameter quality checking (including primality testing for prime numbers where appropriate) shall have been certified in the course of Common Criteria EAL 4 evaluation of the CA products used for OCA Key generation.

## **6.1.7. Key Usage Purposes (as per X.509 v3 Key Usage Field)**

Medicare Australia RCA Keys will be used for the purposes set out in the Medicare Australia RCA CP.

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

## **6.2 Private Key Protection and Cryptographic Module Engineering Controls**

### **6.2.1. Cryptographic Module Standards and Controls**

If approved by Medicare Australia, Cryptographic modules may be used in the Health Sector PKI.

### **6.2.2. Private Key (n out of m) Multi-person Control**

Medicare Australia RCA Private Keys are not under 'n out of m' multi-person control.

Dual person control shall be present for all operations concerning OCA or Medicare Australia RCA Private Keys.

### **6.2.3. Private Key Escrow**

Private Key escrow is not supported.

#### **6.2.4. Private Key Backup**

The Private Keys of the Medicare Australia RCA are stored in encrypted files and are backed up under further encryption with backup copies maintained on-site and in secure off-site storage.

Private Key backup is not provided for Subscribers.

#### **6.2.5. Private Key Archival**

Private Keys of the Medicare Australia RCA are archived in a Secure Facility.

Private Key Archival is not provided for Subscribers, Relying Parties and End User-Subscribers.

#### **6.2.6. Private Key Transfer into or from a Cryptographic Module**

If a Cryptographic module is used, the Private Key of the OCA or RA 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. Private Key Storage on a Cryptographic Module**

If a Cryptographic module is used, the Private Key of the OCA or RA 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.

#### **6.2.8. Method of Activating Private Key**

The Private Keys of the Medicare Australia RCA and of OCAs are activated by Cryptographic software following the successful completion of a login process that validates an Authorised User.

#### **6.2.9. Method of Deactivating Private Key**

The Verizon Australia Pty Ltd *SEC1 Security Profile* details which personnel are authorised to deactivate Private Keys and in what manner. This Document is not publicly available.

#### **6.2.10. Method of Destroying Private Key**

Media containing Subscriber Private Keys are securely destroyed by, in the case of:

- floppy disks – destruction by disintegration or burning, or
- hard disks – sanitisation by overwriting in accordance with the ISM, or
- other media – in accordance with recommendations in the ISM,

Media containing a Private Key of the Medicare Australia RCA will be securely disposed of by sanitisation by overwriting (where feasible), then supervised physical destruction in accordance with the ISM.

Further detail on Private Key destruction is contained in the Verizon Australia Pty Ltd *SEC1 Security Profile* (this Document is not publicly available).

### **6.2.11. Cryptographic Module Rating**

Cryptographic Module Rating is not specified: refer to 6.2.1.

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

### **6.3.1. Public Key Archival**

The Public Keys are stored in the Healthcare Public Directory for the life of the Certificate.

At the expiration of the Medicare Australia RCA, the Public Key will be archived for seven years in accordance with the Commonwealth *Archives Act 1983*.

### **6.3.2. Certificate Operational Periods and Key Pair Usage Periods**

The Medicare Australia RCA Key Pairs have the following usage periods:

- Authentication Private and Public Keys – twenty (20) years,
- Confidentiality Public Key – twenty (20) years,
- Confidentiality Private Key – no expiry.

Usage periods for OCA Public and Private Keys shall be specified in the OCA CP.

## **6.4 Activation Data**

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

### **6.4.1. Activation Data Generation and Installation**

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

### **6.4.2. Activation Data Protection**

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

### **6.4.3. Other Aspects of Activation Data**

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**

Medicare Australia details its computer security technical requirements in the Verizon Australia Pty Ltd *SEC1 Security Profile* (this document is not publicly available).

## **6.5.2. Computer Security Rating**

Medicare Australia details its computer security rating in the Verizon Australia Pty Ltd *SEC1 Security Profile* (this document is not publicly available).

## **6.6 Life Cycle Security Controls**

### **6.6.1. System Development Controls**

The Medicare Australia RCA and OCA system development controls are detailed in the Verizon Australia Pty Ltd *SEC1 Security Profile* (this document is not publicly available).

### **6.6.2. Security Management Controls**

Medicare Australia CAs security management controls are detailed in the Verizon Australia Pty Ltd *SEC1 Security Profile* (this document is not publicly available).

### **6.6.3. Life Cycle Security Ratings**

Health Sector PKI life cycle security ratings are set out in the Verizon Australia Pty Ltd *SEC1 Security Profile* (this document is not publicly available).

## **6.7 Network Security Controls**

Medicare Australia RCA and OCAs have undertaken a Risk Assessment that is presented in the Medicare Australia Certification Authority Annex Documents. It identifies and addresses all high or significant life cycle Security Threats. These documents are not publicly available.

## **6.8 Time-stamping**

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

## **7. Certificate and CRL Profiles**

### **7.1 Certificate Profile**

For this information, please refer to the RCA CP under which the Certificate was issued.

#### **7.1.1. Version Number(s)**

For this information, please refer to the RCA CP under which the Certificate was issued.

#### **7.1.2. Certificate Extensions**

For this information, please refer to the RCA CP under which the Certificate was issued.

#### **7.1.3. Algorithm Object Identifiers**

OIDs are not allocated to algorithms in the Health Sector PKI.

#### **7.1.4. Name Forms**

Certificates issued under the Health Sector 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**

For this information, please refer to the RCA CP under which the Certificate was issued.

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

The OID of the Medicare Australia RCA CP is carried in the standard extension field of issued X.509 Certificates and is published under CP Identification in the Medicare Australia RCA CP.

#### **7.1.7. Usage of Policy Constraints Extension**

For this information, please refer to the RCA CP under which the Certificate was issued.

#### **7.1.8. Policy Qualifiers Syntax and Semantics**

For this information, please refer to the RCA CP under which the Certificate was issued.

#### **7.1.9. Processing Semantics for the Critical Certificate Policy Extension**

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

## **7.2 Certificate Revocation List Profile**

### **7.2.1. Version Number(s)**

The Medicare Australia RCA supports the use of X.509 Version 2 CRLs.

OAs support the use of X.509 Version 2 CRLs.

### **7.2.2. CRL and CRL Entry Extensions**

The Medicare Australia RCA supports the use of X.509 Version 2 CRL entry extensions.

OAs support the use of X.509 Version 2 CRL entry extensions.

## **7.3 Online Certificate Status Protocol Profile**

Online Certificate Status Protocol (OCSP) is not currently approved by the Medicare Australia PMA for this Medicare Australia RCA. OCSP status for each OA is reflected within the relevant OA CPS.

## **8. Compliance Audit and Other Assessment**

The Medicare Australia PMA will authorise audits for compliance where necessary.

### **8.1 Frequency of Entity Compliance Audit**

The Medicare Australia PMA may conduct regular internal audits of Medicare Australia RCA processes in addition to the annual Gatekeeper audit conducted by a member of the Audit Panel listed on the Gatekeeper website.

### **8.2 Identity / Qualifications of Auditor**

External audits will be conducted by a Medicare Australia-approved Authorised Auditor.

Internal audits will be conducted by a qualified physical and logical security auditor.

### **8.3 Auditor's Relationship to Medicare Australia RCA**

External auditors will be organisationally independent of the Medicare Australia RCA 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.

Internal auditors will be organisationally independent of the Medicare Australia RCA's operations.

### **8.4 Topics Covered by Audit**

The areas of the Medicare Australia RCA to be audited include, but are not limited to:

- compliance with Gatekeeper Approved Documents, Policies, Criteria and processes,
- plans, including but not limited to security, business continuity and disaster recovery plans,
- physical and logical security,
- vetting of operational personnel and personnel management,
- technology,
- data and information management,
- management of Health Sector PKI services, and
- privacy.

## **8.5 Actions Taken as a Result of Deficiency**

The results of the audit will be provided to the Medicare Australia PMA and recorded in the Medicare Australia RCA audit log. The Medicare Australia PMA Chair is responsible for addressing any serious deficiencies in a timely manner.

When irregularities are found after an internal audit of the Medicare Australia RCA, the Medicare Australia PMA Chair shall promptly oversee or implement appropriate corrective action.

## **8.6 Communication of Results**

External audit results will be communicated to the Medicare Australia PMA and also to the Gatekeeper Competent Authority.

## **9. Other Business and Legal Matters**

### **9.1 Fees**

#### **9.1.1. Certificate Issuance or Renewal Fees**

N/A.

#### **9.1.2. Certificate Access Fees**

N/A.

#### **9.1.3. Revocation or Status Information Access Fees**

N/A.

#### **9.1.4. Fees for Other Services**

N/A.

#### **9.1.5. Refund Policy**

N/A.

### **9.2 Financial Responsibility**

#### **9.2.1. Insurance Coverage**

All insurances are the responsibility of each Subscriber.

#### **9.2.2. Other Assets**

Other Assets are not considered under this Medicare Australia RCA CPS.

#### **9.2.3. Insurance or other Warranty Coverage for End Entities**

There is no warranty coverage available for Subscribers or Relying Parties under this Medicare Australia RCA CPS or the Medicare Australia OCA CPS.

### **9.3 Confidentiality of Business Information**

For further information, refer to Section 9.3 of the Medicare Australia RCA CP.

### **9.4 Privacy of Personal Information**

For further information, refer to Section 9.4 of the Medicare Australia RCA CP.

## **9.5 Intellectual Property Rights**

### **9.5.1. Medicare Australia Materials**

For further information, refer to section 9.5 of the Medicare Australia RCA CP.

## **9.6 Representations and Warranties**

For further information, refer to section 9.6 of the Medicare Australia RCA CP.

## **9.7 Disclaimers of Warranties**

For further information, refer to section 9.7 of the Medicare Australia RCA CP.

## **9.8 Limitations of Liability**

For further information, refer to section 9.8 of the Medicare Australia RCA CP.

## **9.9 Indemnities**

Indemnities are not provided between parties in the Health Sector PKI to which this Medicare Australia RCA CPS applies.

## **9.10 Term and Termination**

### **9.10.1. Term**

The RCA CPS will be ongoing. Refer to 9.10.2 of the RCA CP for details as to when it may be terminated.

### **9.10.2. Termination**

For further information, refer to Section 9.10.2 of the Medicare Australia RCA CP.

### **9.10.3. Effect of Termination and Survival**

For further information, refer to Section 9.10.3 of the Medicare Australia RCA CP.

## **9.11 Individual Notices and Communications with Participants**

For further information, refer to Section 9.11 of the Medicare Australia RCA CP.

## **9.12 Amendments**

The policy approval authority for this Medicare Australia RCA CPS, the Medicare Australia OCA CPS and related CP Documents is the Medicare Australia PMA.

### **9.12.1. Procedure for Amendment**

For further information, refer to Section 9.12.1 of the Medicare Australia RCA CP.

### **9.12.2. Notification Mechanism and Period**

For further information, refer to Section 9.12.2 of the Medicare Australia RCA CP.

### **9.12.3. Circumstances under Which OID Must be Changed**

For further information, refer to Section 9.12.3 of the Medicare Australia RCA CP.

## **9.13 Dispute Resolution Procedures**

Refer to section 9.13 of the Medicare Australia RCA CP for further information.

## **9.14 Governing Law**

For further information, refer to Section 9.14 of the Medicare Australia RCA CP.

## **9.15 Compliance with Applicable Law**

For further information, refer to Section 9.15 of the Medicare Australia RCA CP.

## **9.16 Miscellaneous Provisions**

For further information, refer to Section 9.16 of the Medicare Australia RCA CP.

## **Annex A Medicare Australia PKI Website**

The Health Sector PKI uses the following documents and websites for the provision of information to Relying Parties and Subscribers.

- Medicare Australia RCA CPS,
- Medicare Australia RCA CP,
- Medicare Australia OCA CPS,
- CPs for PKI Cols,
- Subscriber Application and Terms and Conditions documents,
- The Health Sector PKI privacy policy, and
- The Medicare Australia Health Sector PKI Glossary.

All documents are located at: [www.medicareaustralia.gov.au](http://www.medicareaustralia.gov.au).

The [www.certificates-australia.com.au](http://www.certificates-australia.com.au) website also provides the Healthcare Sector PKI Directory, CA Certificates and their hash values.

## **Annex B Medicare Australia Communities of Interest**

- Medicare Australia Online Claiming for Pharmacy and PBS
- Medicare Australia Site Certificates
- Medicare Australia Healthcare Individual Certificates
- Medicare Australia Individual Certificates for Healthcare Provider Individuals under the Healthcare Identifiers Service
- Medicare Australia Individual Certificates for an authorised Organisation Maintenance Officer under the Healthcare Identifiers Service
- Medicare Australia Site Certificates for Network Organisations under the Healthcare Identifiers Service