



**Australian Government**

---

**Medicare Australia**

**Medicare Australia Root Certification  
Authority (Medicare Australia RCA)  
Certificate Policy (CP) Ver 2.6**

---

**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

**Table 1: Version History**

<b>Doc Version</b>	<b>Status</b>	<b>Date of Issue</b>	<b>Comments</b>
1.0	Draft	14 August 2006	First discussion draft, based on Short Form template.
1.1	Draft	15 August 2006	Amendment to the Certificate Profile, terminology, CP OID and references to the MARCA CPS and MAOCA CPS.
1.2	Draft	16 August 2006	References to the CPS.
1.3	DRAFT	24 August 2006	Review and amendment to the clauses of the CP
1.4	DRAFT	30 August 2006	Revisions to include amendments to fit with penultimate draft of RCA CPS
1.5	Draft	4 September 2006	Accepted most changes; included cross references to Key Signing Ceremony
1.6	FINAL	4 SEPTEMBER	Accepted changes, minor edits to cl.1.3, final proof-read.
1.9	FINAL	8 SEPTEMBER 2006	NUMBER CHANGE TO 1.9 FINAL TO MATCH OID

1.91	FINAL	18 September 2006	Amendments to reflect change in PMA
1.92	Draft	May 2008	Gatekeeper Accreditation under the Relationship Organisation model.
1.93	Draft	June 2008	Amendments after consultations with Legals and Technical teams.
1.94	Draft	June 2008	Amendments after consultations with Legals 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	November 2008	Amendments after review by the Gatekeeper Competent Authority and further review by Medicare Australia.
1.97	Draft	February 2010	Amendment to section 9.8 Limitations of Liability
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	25 October 2010	Updates following legal review
2.2	Draft	28 Feb 2011	Minor updates
2.3	Draft	8 March 2011	Further updates following legal Review
2.4	Draft	April 2011	Updates following AGIMO Review
2.5	Draft	May 2011	Updates following AGIMO Review
2.6	Draft	May 2011	Updates approved by AGIMO

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

\_\_\_\_\_

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

General Manager, Health eBusiness Division

Medicare Australia

# Contents

<b>1.</b>	<b>INTRODUCTION .....</b>	<b>1</b>
1.1	OVERVIEW .....	1
1.2	MEDICARE AUSTRALIA ROOT CERTIFICATION AUTHORITY CERTIFICATE POLICY IDENTIFICATION.....	3
1.3	PKI PARTICIPANTS.....	3
1.4	CERTIFICATE USAGE .....	7
1.5	POLICY ADMINISTRATION.....	7
1.6	DEFINITIONS AND ACRONYMS.....	8
<b>2.</b>	<b>PUBLICATION AND REPOSITORY RESPONSIBILITIES .....</b>	<b>9</b>
2.1	REPOSITORIES .....	9
2.2	PUBLICATION OF CERTIFICATE INFORMATION.....	9
2.3	FREQUENCY OF PUBLICATION .....	10
2.4	ACCESS CONTROL .....	10
<b>3.</b>	<b>IDENTIFICATION AND AUTHENTICATION .....</b>	<b>11</b>
3.1	NAMING .....	11
3.2	INITIAL IDENTITY VALIDATION .....	11
3.3	IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS.....	11
3.4	REVOCAION REQUESTS .....	11
<b>4.</b>	<b>CERTIFICATE MANAGEMENT LIFE-CYCLE .....</b>	<b>12</b>
4.1	CERTIFICATE APPLICATION .....	12
4.2	CERTIFICATE APPLICATION PROCESSING.....	12
4.3	CERTIFICATE ISSUANCE .....	12
4.4	CERTIFICATE ACCEPTANCE.....	12
4.5	KEY AND CERTIFICATE USAGE .....	12
4.6	CERTIFICATE RENEWAL .....	12
4.7	CERTIFICATE RE-KEY .....	12
4.8	CERTIFICATE MODIFICATION.....	13
4.9	CERTIFICATE REVOCATION .....	13

---

4.10	CERTIFICATE STATUS SERVICES.....	13
4.11	END OF SUBSCRIPTION.....	13
4.12	KEY ESCROW AND RECOVERY.....	14
<b>5.</b>	<b>FACILITY MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS .....</b>	<b>15</b>
5.1	PHYSICAL SECURITY CONTROLS .....	15
5.2	PROCEDURAL CONTROLS.....	15
5.3	PERSONNEL SECURITY CONTROLS.....	16
5.4	AUDIT LOGGING PROCEDURES.....	17
5.5	RECORDS ARCHIVAL .....	17
5.6	KEY CHANGEOVER.....	17
5.7	COMPROMISE AND DISASTER RECOVERY.....	17
5.8	HEALTH SECTOR PKI TERMINATION.....	18
<b>6.</b>	<b>TECHNICAL SECURITY CONTROLS .....</b>	<b>19</b>
6.1	KEY PAIR GENERATION AND INSTALLATION .....	19
6.2	PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS .....	20
6.3	OTHER ASPECTS OF KEY PAIR MANAGEMENT .....	21
6.4	ACTIVATION DATA .....	22
6.5	COMPUTER SECURITY CONTROLS.....	22
6.6	LIFE CYCLE SECURITY CONTROLS .....	22
6.7	NETWORK SECURITY CONTROLS.....	23
6.8	TIME-STAMPING .....	23
<b>7.</b>	<b>CERTIFICATE AND CRL PROFILES .....</b>	<b>24</b>
7.1	CERTIFICATE PROFILE .....	24
7.2	CERTIFICATE REVOCATION LIST PROFILE.....	26
7.3	ONLINE CERTIFICATE STATUS PROTOCOL PROFILE .....	27
<b>8.</b>	<b>COMPLIANCE AUDIT AND OTHER ASSESSMENT .....</b>	<b>28</b>
8.1	FREQUENCY OF ENTITY COMPLIANCE AUDIT .....	28
8.2	IDENTITY / QUALIFICATIONS OF AUDITOR .....	28
8.3	AUDITOR'S RELATIONSHIP TO MEDICARE AUSTRALIA RCA.....	28

8.4	TOPICS COVERED BY AUDIT .....	28
8.5	ACTIONS TAKEN AS A RESULT OF DEFICIENCY .....	28
8.6	COMMUNICATION OF RESULTS .....	28
<b>9.</b>	<b>OTHER BUSINESS AND LEGAL MATTERS .....</b>	<b>29</b>
9.1	FEEES .....	29
9.2	FINANCIAL RESPONSIBILITY .....	29
9.3	CONFIDENTIALITY OF BUSINESS INFORMATION.....	29
9.4	PRIVACY OF PERSONAL INFORMATION.....	30
9.5	INTELLECTUAL PROPERTY RIGHTS.....	31
9.6	REPRESENTATIONS AND WARRANTIES.....	32
9.7	DISCLAIMERS OF WARRANTIES .....	32
9.8	LIMITATIONS OF LIABILITY .....	33
9.9	INDEMNITIES .....	33
9.10	TERM AND TERMINATION .....	33
9.11	INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS.....	34
9.12	AMENDMENTS .....	35
9.13	DISPUTE RESOLUTION PROCEDURES .....	35
9.14	GOVERNING LAW .....	37
9.15	COMPLIANCE WITH APPLICABLE LAW .....	37
9.16	MISCELLANEOUS PROVISIONS.....	37
<b>ANNEX A</b>	<b>MEDICARE AUSTRALIA PKI WEBSITE.....</b>	<b>38</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 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 CP 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 CP,
- 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 Practice Statement (Medicare Australia RCA CPS), 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 Policy**

This Medicare Australia RCA CP 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 OCA CPs, then

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

#### **1.1.1.4. Documentation**

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

- this Medicare Australia RCA CP,
- the Medicare Australia RCA CPS,
- 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 Policy Identification**

### **1.2.1. Medicare Australia RCA CP 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).

Certificates issued under this CP shall bear the Policy OID:

#### **1.2.36.174030967.2.1.1**

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

## **1.3 PKI Participants**

This Medicare Australia RCA CP is applicable to:

- the Medicare Australia RCA,
- any subordinate Medicare Australia OCA (e.g. the Medicare Australia OCA),

- Medicare Australia and Verizon Australia Pty Ltd staff responsible for the issuance of Certificates to Subscribers,
- 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 CP.

### **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 CP, 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 with 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.

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

The Medicare Australia RCA performs the functions listed in section 1.3.1.2 of the Medicare Australia RCA CPS.

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

The Medicare Australia RCA obligations are listed in section 1.3.1.3 of the Medicare Australia RCA CPS.

#### **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 within 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 Medicare Australia OCA Keys, used to sign Certificates is 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 are 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.

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 CP.

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

OCAs operating under the Health Sector PKI hierarchy perform the functions listed in section 1.3.1.5 of the Medicare Australia RCA CPS.

Medicare Australia OCA is an OCA of the Medicare Australia RCA.

### **1.3.1.6. OCA Obligations**

An OCA's (e.g. the Medicare Australia OCA) obligations are listed in section 1.3.1.6 of the Medicare Australia RCA CPS.

### **1.3.2. Registration Authorities and Certificate Issuance**

This Medicare Australia RCA CP does not include information on Registration Authorities (RAs) or certificate issuance. Information about certificate issuance for the Health Sector PKI is included in section 1.3.2 of the Medicare Australia OCA CPS. The Medicare Australia OCA CPS is available at [www.medicareaustralia.com.au](http://www.medicareaustralia.com.au).

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. Subscribers**

Subscribers of the Medicare Australia RCA are OCAs that apply to be issued with Certificates within the Health Sector PKI hierarchy managed by Medicare Australia.

#### **1.3.3.1. Applicants**

An applicant is a third party who wishes to become a 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 CP are listed in section 1.3.3.2 of the Medicare Australia RCA CPS.

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

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

### **1.3.4. Other participants**

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

### **1.3.4.1. 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**

The Medicare Australia RCA Certificate may only be used to sign its own certificate, any OCA (including the Medicare Australia OCA) Certificates or RCA operational personnel Certificates.

See Section 1.2.1 of the relevant Col CP that the Certificate is issued under for the appropriate use.

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

The Medicare Australia RCA Certificate cannot directly sign end users/Subscribers Certificates.

See Section 1.2.2 of the relevant Col CP that the Certificate is issued under for the prohibited use.

## **1.5 Policy Administration**

### **1.5.1. Document Administration**

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

The Medicare Australia PMA:

- approves changes to this CP, Medicare Australia RCA CPS 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) or certificate issuance process with the Medicare Australia RCA CPS, this Medicare Australia RCA CP, 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 but which must be consistent with this CP and RCA 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 CP, the Medicare Australia RCA CPS 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 CP**

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

The Medicare Australia PMA determines whether or not the Medicare Australia RCA CPS provides suitable support for this 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 and its 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) or [www.certificates-australia.com.au](http://www.certificates-australia.com.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 CP 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 CP, 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 programmatically. Technical details are at [www.medicareaustralia.gov.au](http://www.medicareaustralia.gov.au) and [www.certificates-australia.com.au](http://www.certificates-australia.com.au).

The Healthcare Public Directory is available 7 days a week, 24 hours a day (except for scheduled outages).

### 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 Certificate is published on Medicare Australia's website, [www.medicareaustralia.gov.au](http://www.medicareaustralia.gov.au) and [www.certificates-australia.com.au](http://www.certificates-australia.com.au).

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

This Medicare Australia RCA CP is published electronically at the website, [www.medicareaustralia.gov.au](http://www.medicareaustralia.gov.au) and [www.certificates-australia.com.au](http://www.certificates-australia.com.au).

Formal notification of changes to this Medicare Australia RCA CP 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 CP. Interested parties are responsible for retrieving amendments when a revised and / or amended Medicare Australia RCA CP is posted to the website.

## **2.3 Frequency of Publication**

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

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

#### **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 and Medicare Australia RCA CP 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 CP, the Medicare Australia RCA CPS or the CPS 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 CoI CP the Certificates were issued under.

#### 3.1 Naming

Subscribers under this CP are OCAs for the Medicare Australia RCA.

Subscribers are termed 'Certificate Subjects' in the x.509 definition.

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

#### 3.2 Initial Identity Validation

For the purposes of the Health Sector PKI, the Subscribers (Certificate Subjects) under this CP are identified and authenticated through the CA Key Signing Ceremony. Information on this process is not publicly available.

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

Subscribers under this CP shall be identified and authenticated and the Certificates renewed using the same process as the identification and authentication process at registration.

Note: all certificate renewals under this CP involve re-keying.

#### 3.4 Revocation Requests

Revocation of Certificates under this CP shall only be requested by the Medicare Australia PMA or Medicare Australia IT Security Manager/Advisor or nominee with the same or higher security clearance.

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

### **4.1 Certificate Application**

Upon approval from the Medicare Australia PMA, the Medicare Australia RCA is authorised to sign OCA Certificates.

### **4.2 Certificate Application Processing**

Medicare Australia RCA and Medicare Australia OCA Certificate Application processing are undertaken during the CA Key Signing Ceremony. Information on this process is not publicly available.

### **4.3 Certificate Issuance**

Certificates are issued at the CA Key Signing Ceremony and are held within the certificate creation facility and are not exposed externally to this facility. Information on this process is not publicly available.

### **4.4 Certificate Acceptance**

Medicare Australia RCA and Medicare Australia OCA Certificate Application processing are undertaken during the CA Key Signing Ceremony. Information on this process is not publicly available.

### **4.5 Key and Certificate Usage**

The Medicare Australia RCA Key will only be used to sign Medicare Australia OCA Certificates.

#### **4.5.1. Key Pair Generation and Installation**

Key pair generation and installation (that is, the CA Key Signing Ceremony) for the Medicare Australia RCA and for OCAs signed by the Medicare Australia RCA are documented in the Verizon Australia Pty Ltd *SEC1 Security Profile* (this document is not publicly available).

### **4.6 Certificate Renewal**

Certificates issued under this CP will need to be renewed in the event of expiry of the certificates or as a result of unforeseen circumstances that may occur. They will be renewed by repeating the CA Key Signing Ceremony.

The relevant Col CP the Certificate was issued under will document the certificate renewal activities.

### **4.7 Certificate Re-key**

Certificate re-key is not supported for the Medicare Australia RCA.

The relevant Col CP the Certificate was issued under will document if Certificate re-key is supported within the Col.

## **4.8 Certificate Modification**

Certificate modification is not supported for the Medicare Australia RCA.

The relevant Col CP the Certificate was issued under will document if Certificate modification is supported within the Col.

## **4.9 Certificate Revocation**

Certificates issued under this CP shall be revoked in the event of loss, destruction or theft of the RCA Private Key.

The relevant Col CP the Certificate was issued under will document Certificate revocation within the Col.

## **4.10 Certificate Status Services**

### **4.10.1. Operational Characteristics**

The Medicare Australia internet web site ([www.medicareaustralia.gov.au](http://www.medicareaustralia.gov.au).) provides details of all current PKI policies pertaining to the Medicare Australia RCA and OCA. This will include certificate policies for each community of interest operating under the Medicare Australia RO.

Verizon Australia Pty Ltd currently manages the Medicare CA and the bulk issuance of subscriber Certificates. The Verizon Australia internet website ([www.certificates-australia.com.au](http://www.certificates-australia.com.au)) provides:

- (a) All valid Medicare Australia PKI certificates, and
- (b) The most up to date CRL.

Once a Certificate is revoked, the CA will write the Certificate serial number to the CRL. While the Certificate is revoked immediately after the CA processes the revocation request, any end user checking the validity of the Certificate will not be able to detect the revocation until the next refreshed CRL posting.

### **4.10.2. Service Availability**

The Certificate Revocation List (CRL) is available 24 x 7 at [www.certificates-australia.com.au](http://www.certificates-australia.com.au).

### **4.10.3. Optional Features**

Optional features for Certificates are listed within the Col CP the Certificate was issued under.

## **4.11 End of Subscription**

Certificates are terminated when they are revoked or have expired.

## **4.12 Key Escrow and Recovery**

Key Escrow is not supported by the Medicare Australia RCA.

## **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 Gatekeeper Accredited CA facility operated to the level of HIGHLY PROTECTED as defined in the Australian Government Information and Communications Technology Security Manual (ISM) and certified by a member of the Physical Security Evaluation Panel listed on the Gatekeeper website. The Gatekeeper Accredited CA 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 and is described in section 5.1.2 of the Medicare Australia RCA CPS.

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

This is described in section 5.1.3 of the Medicare Australia RCA CPS.

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

This is described in section 5.1.4 of the Medicare Australia RCA CPS.

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

This is described in section 5.1.5 of the Medicare Australia RCA CPS.

#### **5.1.6. Media Storage**

This is described in section 5.1.6 of the Medicare Australia RCA CPS.

#### **5.1.7. Waste Disposal**

This is described in section 5.1.7 of the Medicare Australia RCA CPS.

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

This is described in section 5.1.8 of the Medicare Australia RCA CPS.

### **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). These people must hold a security clearance commensurate with the appropriate security level required for the position of trust.

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 *SEC 1 Security Profile* (this document is not a public document).

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

This is described in section 5.2.2 of the Medicare Australia RCA CPS and in the Verizon Australia Pty Ltd *SEC1 Security Profile* (this document is not a public document).

### **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 Verizon Australia Pty Ltd *SEC1 Security Profile* (this document is not a public document).

### **5.2.4. Roles requiring separation of duties**

This is described in section 5.2.4 of the Medicare Australia RCA CPS and in the Verizon Australia Pty Ltd *SEC1 Security Profile* (this document is not a public document).

## **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**

This is described in section 5.3.2 of the Medicare Australia RCA CPS and in the Verizon Australia Pty Ltd *SEC1 Security Profile* (this document is not a public document).

### **5.3.3. Training requirements**

This is described in section 5.3.3 of the Medicare Australia RCA CPS and in the Verizon Australia Pty Ltd *SEC1 Security Profile* (this document is not a public document).

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

This is described in section 5.3.4 of the Medicare Australia RCA CPS and in the Verizon Australia Pty Ltd *SEC1 Security Profile* (this document is not a public document).

### **5.3.5. Sanctions for unauthorised actions**

This is described in section 5.3.5 of the Medicare Australia RCA CPS and in the Verizon Australia Pty Ltd *SEC1 Security Profile* (this document is not a public document).

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

This is described in section 5.3.6 of the Medicare Australia RCA CPS and in the Verizon Australia Pty Ltd *SEC1 Security Profile* (this document is not a public document).

### **5.3.7. Documentation supplied to personnel**

This is described in section 5.3.7 of the Medicare Australia RCA CPS and in the Verizon Australia Pty Ltd *SEC1 Security Profile* (this document is not a public document).

## **5.4 Audit Logging Procedures**

This is described in section 5.4 of the Medicare Australia RCA CPS and in the Verizon Australia Pty Ltd *SEC1 Security Profile* (this document is not a public document).

## **5.5 Records Archival**

This is described in section 5.5 of the Medicare Australia RCA CPS and in the Verizon Australia Pty Ltd *SEC1 Security Profile* (this document is not a public document).

## **5.6 Key Changeover**

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

This is described in section 5.6 of the Medicare Australia RCA CPS and in the Verizon Australia Pty Ltd *SEC1 Security Profile* (this document is not a public document).

## **5.7 Compromise and Disaster Recovery**

This is described in section 5.7 of the Medicare Australia RCA CPS and in section 7 in the Medicare Australia Certification Authority Annex Documents (this document is not a public document).

## **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 Col participants in a timely manner.

## **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 Defence Signals Directorate (DSD) Evaluated Products Lists (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 self-generated by the OCA and do not require delivery.

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

This is described in section 6.1.3 of the Medicare Australia RCA CPS and in the Verizon Australia Pty Ltd *SEC1 Security Profile* (this document is not a public document).

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

The Medicare Australia RCA 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)**

The Medicare Australia RCA Key will only be used to sign OCA Certificates.

## **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 operated by Verizon Australia Pty Ltd.

### **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 transferred into and from the module.

### **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.

### **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**

This is described in section 6.2.10 of the Medicare Australia RCA CPS and in the Verizon Australia Pty Ltd *SEC1 Security Profile* (this document is not a public document).

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

No Stipulation.

## **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 Records Archival set out at 5.5 in the RCA CPS.

### **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 are specified in the OCA CP or OCA CPS.

## **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 detail their system development controls in the Verizon Australia Pty Ltd *SEC1 Security Profile* (this document is not publicly available).

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

Medicare Australia CAs detail their security management controls 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 has 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

Field	Content	Mandatory	Critical*	
1. X.509v1 Field			N/A	
1.1. Version	V3	M		
1.2. Serial Number	Unique value assigned by the Issuing CA	M		
1.3. Signature Algorithm	SHA-1 with RSA Encryption	M		
1.4. Issuer Distinguished Name	(self-signed)	M		
1.4.1. Country (C)	AU	M		
1.4.2. Organisation (O)	GOV	M		
1.4.3. Organisational Unit (OU)	Medicare Australia	M		
1.4.4. Common Name (CN)	Medicare Australia Root Certification Authority	M		
1.5. Validity	20 years			
1.5.1. Not Before		M		
1.5.2. Not After		M		
1.6. Subject				
1.6.1. Country (C)	AU	M		
1.6.2. Organisation (O)	GOV	M		
1.6.3. Organisational Unit (OU)	Medicare Australia	M		
1.6.4. Common Name (CN)	Medicare Australia Root Certification Authority	M		
1.7. Subject Public Key Info	Public Key encoded in accordance with RFC2459 & PKCS#1  Key length 2048 bits	M		
2. X.509v3 Extensions				
2.1. Authority Key Identifier		M		Non-Critical
2.1.1. Key Identifier	SHA-1 hash (60 bits) of the Issuer's public key.			
2.1.2. AuthorityCertIssuer	Not present			
2.1.3. AuthorityCertSerialNumber	Not present			

Field	Content	Mandatory	Critical*
2.2. Subject Key Identifier	SHA-1 hash (60 bits) of the Subject's public key.	M	Non-Critical
2.3. Key Usage		M	Critical
2.3.1. Digital Signature	SET		
2.3.2. Non Repudiation	SET		
2.3.3. Key Encipherment	SET		
2.3.4. Data Encipherment	SET		
2.3.5. Key Agreement	SET		
2.3.6. Certificate Signing	SET		
2.3.7. Off-line CRL signing	SET		
2.3.8. CRL Signing	SET		
2.4. Extended Key Usage	Not applicable		Non-Critical
2.5. Certificate Policies			Non-Critical
2.5.1. Policy Identifier			
2.5.1.1. Policy Identifier	1.2.36.174030967.2.1.1 (OID of the CP)		
2.5.1.2. CPS Pointer	<a href="http://www.medicareaustralia.gov.au/">http://www.medicareaustralia.gov.au/</a>		
2.5.1.3. Policy Qualifier ID	User Notice		
2.5.1.4. Notice Text	"Certificates under this policy are issued by the Medicare Australia Root CA to itself and to CAs subordinate to the Medicare Australia Root CA"		
2.6. Basic Constraints			Critical
2.6.1. Subject Type	CA		
2.6.2. Path Length Constraint	none		

### 7.1.1. Version Number(s)

Certificates issued by the Medicare Australia RCA are X.509 version 3.

## 7.1.2. Certificate Extensions

Certificate extensions are used by the Medicare Australia RCA Certificates and are listed in the certificate profile presented in section 7.1.

## 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 (Medicare Australia) and subject name (Medicare Australia) fields respectively.

## 7.1.5. Name Constraints

Anonymous names are not supported by the Medicare Australia RCA.

## 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 section 1.2 of this CP.

## 7.1.7. Usage of Policy Constraints Extension

The Medicare Australia RCA supports the use of the Policy Constraints extension.

## 7.1.8. Policy Qualifiers Syntax and Semantics

The Medicare Australia RCA supports the use of syntax and semantics policy qualifiers.

## 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

Field	Content	Mandatory	Critical*
1. X.509v1 Field			N/A
1.1. Version	V2	M	
1.2. Signature Algorithm	sha1RSA	M	
1.3. Issuer Distinguished Name		M	
1.3.1. Country (C)	AU	M	
1.3.2. Organization (O)	GOV	M	

Field	Content	Mandatory	Critical*
1.3.3. Organisational Unit (OU)	Medicare Australia		
1.3.4. Common Name (CN)	Medicare Australia Root Certification Authority	M	
1.4 Validity		M	
1.4.1 Effective Date			
1.4.2 Next Update			
1.5 CRL Number		M	
2. X.509v3 Extensions			
2.1. Authority Key Identifier		M	Non-Critical
2.1.1. Key Identifier	SHA-1 hash (60 bits) of the Issuer's public key		

### 7.2.1. Version Number(s)

The Medicare Australia RCA supports 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 as shown in the CRL profile presented in section 7.2.

## 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 OCA is reflected within the relevant OCA 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**

This is described in section 8.3 of the Medicare Australia RCA CPS and in the Verizon Australia Pty Ltd *SEC1 Security Profile* (this document is not a public document).

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

This is described in section 8.4 of the Medicare Australia RCA CPS and in the Verizon Australia Pty Ltd *SEC1 Security Profile* (this document is not a public document).

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

This is described in section 8.5 of the Medicare Australia RCA CPS and in the Verizon Australia Pty Ltd *SEC1 Security Profile* (this document is not a public document).

### **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 CP.

#### **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 CP.

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

#### **9.3.1. Scope of Confidential Information**

For further information, refer to the Medicare Australia Health Sector PKI Privacy Policy on its website [www.medicareaustralia.gov.au](http://www.medicareaustralia.gov.au).

### **9.3.2. Information Not Within the Scope of Confidential Information**

For further information, refer to the Medicare Australia Health Sector PKI Privacy Policy on its website [www.medicareaustralia.gov.au](http://www.medicareaustralia.gov.au)

### **9.3.3. Responsibility to Protect Confidential Information**

For further information, refer to the Medicare Australia Health Sector PKI Privacy Policy on its website [www.medicareaustralia.gov.au](http://www.medicareaustralia.gov.au).

## **9.4 Privacy of Personal Information**

For further information, refer to the Medicare Australia Health Sector PKI Privacy Policy on its website [www.medicareaustralia.gov.au](http://www.medicareaustralia.gov.au).

### **9.4.1. Privacy Plan**

For further information, refer to the Medicare Australia Health Sector PKI Privacy Policy on its website [www.medicareaustralia.gov.au](http://www.medicareaustralia.gov.au).

### **9.4.2. Information Treated as Private**

For further information, refer to the Medicare Australia Health Sector PKI Privacy Policy on its website [www.medicareaustralia.gov.au](http://www.medicareaustralia.gov.au).

### **9.4.3. Information not treated as private**

For further information, refer to the Medicare Australia Health Sector PKI Privacy Policy on its website [www.medicareaustralia.gov.au](http://www.medicareaustralia.gov.au).

### **9.4.4. Responsibility to Protect Private Information**

For further information, refer to the Medicare Australia Health Sector PKI Privacy Policy on its website [www.medicareaustralia.gov.au](http://www.medicareaustralia.gov.au).

### **9.4.5. Notice and Consent to Use Private Information**

For further information, refer to the Medicare Australia Health Sector PKI Privacy Policy on its website [www.medicareaustralia.gov.au](http://www.medicareaustralia.gov.au).

### **9.4.6. Disclosure Pursuant to Judicial or Administrative Process**

Verizon and / or Medicare Australia will comply, where required by a court of law or a tribunal, in accordance with the Rules of that Court or the procedures of that Tribunal and with the Legal Services Directions (Commonwealth).

### **9.4.7. Other Information Disclosure Circumstances**

For further information, refer to the Medicare Australia Health Sector PKI Privacy Policy on its website [www.medicareaustralia.gov.au](http://www.medicareaustralia.gov.au).

## **9.5 Intellectual Property Rights**

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

Medicare Australia Materials include, but are not limited to:

- a) the Medicare Australia RCA Certificate and Keys,
- b) this Medicare Australia RCA CP,
- c) the Medicare Australia RCA CPS,
- d) the Medicare Australia OCA Certificate and Keys,
- e) the Medicare Australia OCA CP,
- f) the Medicare Australia OCA CPS,
- g) the contents of the Healthcare Public Directory,
- h) any other data or database created by Medicare Australia, the Medicare Australia RCA, the Medicare Australia OCA, the Card Management System or Medicare Australia's contractors and subcontractors for the purposes of the Health Sector PKI,
- i) all Certificate Policies for all ROU CoIs,
- j) all Applications and Terms and Conditions between Medicare Australia and the Subscribers in Medicare Australia ROUs' CoI, and
- k) All other Documents owned by Medicare Australia and published on the Medicare Australia website ([www.medicareaustralia.gov.au](http://www.medicareaustralia.gov.au)) for the purposes of the Health Sector PKI.

Intellectual Property Rights in Medicare Australia Materials and in any modifications or enhancements made to Medicare Australia Materials remain, or are from the date of creation, the property of the Medicare Australia.

The Medicare Australia RCA, Medicare Australia OCA, Medicare Australia Subscribers and Relying Parties must ensure that Medicare Australia Materials are, to the extent practicable, identified as the property of Medicare Australia (for the Commonwealth) and that Medicare Australia Materials remain at all times free of any lien, charge or other encumbrance of a third Party.

Medicare Australia grants to Subscribers and Relying Parties a revocable, royalty-free, nonexclusive, non-transferable license for the terms of a Subscriber's Certificate, to view, display and use (including downloading, reproducing and printing) Medicare Australia Materials for the purpose of:

- a) participating in the Health Sector PKI, and

- b) understanding their rights and obligations under the Health Sector PKI, including obtaining legal or other advice as necessary.

## **9.6 Representations and Warranties**

### **9.6.1. Commonwealth and Medicare Australia Representations and Warranties**

To the extent permitted by law and notwithstanding any other provision of any Health Sector PKI documents or whether Keys or Certificates are used in a transaction or not, the Commonwealth, its Agencies and Medicare Australia make no representations or warranties to any:

- a) Agency,
- b) CA service provider,
- c) RA service provider,
- d) Subscriber,
- e) Replying Party, or
- f) Other participant.

in relation to their activities or performance of the Health Sector PKI and any services or products associated with, or part of, or used in delivery of the Health Sector PKI.

### **9.6.2. Other Parties Representations and Warranties**

To the extent permitted by law and notwithstanding any other provision of any Health Sector PKI documents or whether Keys or Certificates are used in a transaction or not, Agencies, RA service providers, Subscribers, Relying Parties and other participants (collectively, Other Parties) make no representations or warranties to the:

- a) Commonwealth,
- b) Any Commonwealth Agencies,
- c) Medicare Australia, or
- d) Each other.

in relation to their activities or performance of the Health Sector PKI and any services or products associated with, or part of, or used in delivery of the Health Sector PKI.

## **9.7 Disclaimers of Warranties**

The Commonwealth, its Agencies and Medicare Australia disclaims all warranties, express or implied.

If any warranties or conditions are implied by legislation, then the liability of the Commonwealth, its Agencies and Medicare Australia (and of any of their officers, staff and contractors (including sub-contractors)), for any breach of the condition or warranty is limited to:

- a) re-performing the services to which the warranty applied, or

- b) paying the cost of re-performing those services.

## **9.8 Limitations of Liability**

### **9.8.1. Commonwealth, Agencies and Medicare Australia Liability**

The aggregate liability of the Commonwealth and its Agencies and Medicare Australia (the Parties) to any and all persons concerning all Certificates shall be limited to an amount not to exceed \$50,000 in aggregate for all claims, arising in connection with the Health Sector PKI, including but not limited to:

- a) an entity described in the CP that Certificates are issued under carrying out, or omitting to carry out, any activity described in, or contemplated by, the Documents, and
- b) the carrying out or omitting to carry out, any activity related to the Gatekeeper accreditation process.

## **9.9 Indemnities**

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

## **9.10 Term and Termination**

### **9.10.1. Term**

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

### **9.10.2. Termination**

Medicare Australia may terminate this Health Sector PKI at its own discretion or otherwise as may be required by the Commonwealth government.

Medicare Australia will promptly notify, in accordance with clause 9.11, all OCAs, RAs, Subscribers, Relying Parties, the Gatekeeper Competent Authority and other participants of the intended termination of the Health Sector PKI.

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

The Medicare RCA and the Medicare OCA will, on notification of termination, cease to generate and issue Certificates.

On termination, all Certificates issued under this Medicare Australia RCA CP and under any CP remain in force for any period left of the two-year or five year operative time of the Certificate in accordance with that relevant CP.

The Healthcare Public Directory will be maintained for the period left of all Certificates current at the date of termination.

## 9.11 Individual Notices and Communications with Participants

For the purpose of this clause, a Notice includes a consent, information, Application, request or any other communication provided under or in connection with this Medicare Australia RCA CP.

A Notice to a Party under this Medicare Australia RCA CP is only given or made if it is in writing and distributed in one of the following ways:

- a) delivered or posted to that Party at its postal address, or
- b) emailed to that Party at its email address, or
- c) faxed to that Party at its fax number, or
- d) posted on Medicare Australia website ([www.medicareaustralia.gov.au](http://www.medicareaustralia.gov.au)) in accordance with this clause.

A Notice can only be provided by email where:

- a) the sender and Recipient are holders of current Certificates which have not been Revoked, and
- b) the sender digitally signs the message using the Sender's Private Authentication Key.

A Notice will be issued and posted to the relevant websites when any of the following events occurs:

- a) a new Medicare Australia RCA CP or Medicare Australia CPS is approved,
- b) there is a change or alteration to an existing Medicare Australian CP or Medicare Australia RCA CPS, and/or
- c) any other event which the Medicare Australia RCA deem appropriate.

If a Party gives the other Parties three Business Days Notice of a change of its postal address, fax number or email address, a Notice is only given or made by that other Party if it is delivered, posted, faxed or emailed to the latest postal or email address or fax number.

A Notice is given or made as follows:

- (a) if it is delivered, when it is left at the relevant address,
- (b) if it is sent by post, three Business Days after it is posted (seven days if posted to or from a place outside Australia),
- (c) if it is sent by facsimile, as soon as the sender receives from the sender's facsimile machine a report of an error free transmission to the correct facsimile number,
- (d) if it is sent by email, as soon as the Recipient's host machine receives the Notice and the Digital Signature has been verified and authenticated, and/or
- (e) if it is posted on the Medicare Australia Website ([www.medicareaustralia.gov.au](http://www.medicareaustralia.gov.au)), five Business Days after it is posted.

If a Notice is delivered, or an error free transmission report in relation to it is received, on a day that is not a Business Day, or if on a Business Day, after 5pm on that day in the place of the Party to whom it is sent, it is to be treated as having been given or made at the beginning of the next Business Day.

## **9.12 Amendments**

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

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

Medicare Australia operates the Medicare Australia PMA which is responsible for setting Certificate Policies for the Health Sector PKI operated by Medicare Australia.

The Medicare Australia PMA also gives internal approval to CPs within the Health Sector PKI operated by Medicare Australia.

The Medicare Australia PMA is the General Manager or nominee, Health eBusiness Division, Medicare Australia.

All proposed amendments must be approved by the Medicare Australia PMA.

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

Amended or varied CPS and CPs will be posted at [www.medicareaustralia.gov.au](http://www.medicareaustralia.gov.au) as soon as practicable after approval by the Medicare Australia PMA.

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

Where a change to a CPS or CP is required, the OID of the policy will stay the same. However, a new version number will be allocated by the Medicare Australia PMA on its endorsement of the amended CPS or CP.

A new OID must be given when a new CP is created for a different CoI of Interest.

## **9.13 Dispute Resolution Procedures**

Disputes arising out of the CP the Certificates is issued under shall be resolved using the following processes:

- a) The Parties shall use their best endeavours to resolve any problem that arises by negotiating with each other.

- b) No Party shall resort to court proceedings (except for proceedings necessary to seek an urgent interim relief) in respect of a dispute arising out of or in connection with the CP the Certificate is issued under until the process outlined in this section has been exhausted.
- c) If a problem arises (including a breach or an alleged breach) which is not resolved at the operational level, or is sufficiently serious that it cannot be resolved at the operational level, the Party with the problem shall notify the other Party, and the management representatives of each of the Parties shall endeavour to agree on a resolution.
- d) If the management representatives of each of the Parties fail to reach a solution to the dispute within five Business Days from the date notice of the problem was first given, the Parties may seek to settle the matter by referring the issue for mediation, administered by the Australian Commercial Disputes Centre (ACDC).
- e) The mediation is to be conducted in accordance with the latest version of the ACDC Mediation Guidelines to the extent that such guidelines are not inconsistent with any other provisions of this CP unless the mediation is administered by an organisation other than the ACDC, in which case the mediation is to be conducted in accordance with the current guidelines of that organisation, to the extent that such guidelines are not inconsistent with any other provision of the CP the Certificate is issued under.
- f) In the event that the dispute has not been settled within twenty eight (28) Business Days or other such period as agreed to in writing between the Parties after the appointment of the mediator, the dispute may be submitted to arbitration administered by ACDC and in accordance with their current arbitration guidelines.
- g) The arbitrator shall not be the same person as the mediator.
- h) The Parties will promptly furnish to the arbitrator (imposing appropriate obligations of confidence) all information reasonably requested by the arbitrator relating to the dispute.
- i) If either Party breaches any provision of this section in relation to a dispute, the other Party need not comply with that provision in relation to that same dispute.
- j) Unless prevented by the nature of the dispute, the Parties shall continue to perform in accordance with the CP the Certificate is issued under while attempts are made to resolve the dispute.
- k) The Parties will share equally the fees and expenses of the mediator or the arbitrator, as the case may be.

Disputes relating to any contractual relationship referred to in, or related to the CP the Certificate is issued under, other than disputes relating to a CP, must be resolved in accordance with the contract governing that relationship.

## **9.14 Governing Law**

All CPSs and each CP are governed by, and are to be construed in accordance with, the laws from time to time in force in the Australian Capital Territory.

The Parties agree to submit to the courts having jurisdiction in the Australian Capital Territory.

## **9.15 Compliance with Applicable Law**

In conducting the activities under the CP the Certificates are issued under, all Parties agree to abide by the provisions of all relevant legislation, and the requirements of any Commonwealth, State, Territory or local body.

## **9.16 Miscellaneous Provisions**

Clauses that relate to Intellectual Property Rights, safety, integrity, accuracy of information, Confidentiality, privacy, liability and indemnity will survive the expiration or termination (for whatever reason) of this Medicare Australia RCA CP, the Medicare Australia RCA CPS, the Medicare Australia OCA CPS and the CP the Certificate is issued.

## 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 Health Sector PKI Directory, the Medicare Australia RCA Certificates and their hash values.