



Australian Government

Medicare Australia

**Medicare Australia Organisation
Certification Authority (Medicare
Australia OCA) Certification Practice
Statement (CPS) Ver 2.4**

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

Doc Version	Status	Date of Issue	Comments
0.8.	Draft	02/02/2006	Initial re-draft.
0.9	Final	13/02/2006	Incorporated feedback from 0.8.1 and submit for Medicare Australia PMA approval.
0.10		25/06/2006	Incorporate feedback from Legal.
0.11		25/06/2006	Incorporate further feedback from MA
0.12		27/06/2006	Changing document title to better reflect that the OCA (Medicare Australia Human Services CA) is owned by Medicare Australia
0.13		07/07/2006	Update the document to reflect the new ownership of the RCA and Section 9 of this document.
0.14		10/07/2006	Update the document to reflect the new sub CA name.
0.15	Draft	7/8/06	Make consistent all terminology under new Gatekeeper Health Sector PKI Framework
0.16	Draft	8/8/06	Review and update references
0.17	Draft	11/8/06	Edit and revise to update terminology and content

0.18	Draft	15/8/06	Updated to reflect consistency between Health Sector PKI entity names, and include relationship diagram
0.19	Draft	16/08/2006	Minor format editing.
0.20	Draft	18/08/2006	Review of edits and acceptance of edits to Part 5.3 in v0.19; review and revision for parts 5.4 and following parts
0.21	draft	23/08/2006	Format editing.
0.22	draft	25/08/2006	Final draft
0.23	Draft	28/08/2006	Transfer of Part 9 substantive content to the Medicare Australia RCA CPS; insert 'see reference' to Part 9 the RCA CPS in this OCA CPS. Review of previous edits and acceptance / amendment as required.
0.24	Draft	29/08/2006	Further amendments to link this CPS with RCA CPS; addition of clauses on OCA functions and obligations;
0.25	Draft	4/09/2006	Review of changes to date
1.0	FINAL	4/09/2006	Review, delete comments, amendments to Pt 9 to reflect changes in RCA CPS; minor edits, final proofread
1.9	FINAL	8/09/2006	NUMBER CHANGE TO 1.9 TO MATCH OID
	Final	18/09/2006	Amendment to reflect changes to PMA
1.91	Final	October – November 2006	Deletion of reference to the IT Security Manager in 5.2.3 Amendments to grammar/phrasing/typos etc
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	Updated References
1.98	Draft	February 2010	AGIMO Feedback Included
1.99	Draft	May 2010	AGIMO Changes included following meeting with AGIMO.
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	29 October 2010	Updates following legal review
2.2	Draft	28 Feb 2011	Minor Updates
2.3	Draft	May 2011	Updates following AGIMO review
2.4	Draft	May 2011	Updates approved by AGIMO

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

 General Manager, Health eBusiness Division
 Medicare Australia

Date: _____

Contents

1	INTRODUCTION	1
1.1	OVERVIEW	1
1.2	MEDICARE AUSTRALIA ORGANISATION CERTIFICATION AUTHORITY CERTIFICATE PRACTICE STATEMENT AND IDENTIFICATION	2
1.3	HEALTH SECTOR PKI PARTICIPANTS	3
1.4	CERTIFICATE USAGE	7
1.5	POLICY ADMINISTRATION	7
1.6	DEFINITIONS AND ACRONYMS	7
2	PUBLICATION AND REPOSITORY RESPONSIBILITIES	8
2.1	REPOSITORIES	8
2.2	PUBLICATION OF CERTIFICATE INFORMATION	8
2.3	FREQUENCY OF PUBLICATION	9
2.4	ACCESS CONTROLS ON REPOSITORIES	9
3	IDENTIFICATION AND AUTHENTICATION	10
3.1	NAMING	10
3.2	INITIAL IDENTITY VALIDATION	10
3.3	IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS	10
3.4	REVOCATION REQUESTS	10
4	CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS	11
5	MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS	12
5.1	PHYSICAL SECURITY CONTROLS	12
5.2	PROCEDURAL CONTROLS	12
5.3	PERSONNEL SECURITY CONTROLS	12
5.4	AUDIT LOGGING PROCEDURES	12
5.5	RECORDS ARCHIVAL	12
5.6	KEY CHANGEOVER	13
5.7	COMPROMISE AND DISASTER RECOVERY	14
5.8	MEDICARE AUSTRALIA OCA TERMINATION	14

6	TECHNICAL SECURITY CONTROLS	15
6.1	KEY PAIR GENERATION AND INSTALLATION	15
6.2	PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS	16
6.3	OTHER ASPECTS OF KEY PAIR MANAGEMENT	17
6.4	ACTIVATION DATA	17
6.5	COMPUTER SECURITY CONTROLS	18
6.6	LIFE CYCLE SECURITY CONTROLS	18
6.7	NETWORK SECURITY CONTROLS	18
6.8	TIME-STAMPING	18
7	CERTIFICATE AND CRL PROFILES	19
7.1	CERTIFICATE PROFILE	19
7.2	CERTIFICATE REVOCATION LIST PROFILE	19
7.3	ONLINE CERTIFICATE STATUS PROTOCOL PROFILE	20
8	COMPLIANCE AUDIT AND OTHER ASSESSMENT	21
8.1	FREQUENCY OF ENTITY COMPLIANCE AUDIT	21
8.2	IDENTITY / QUALIFICATIONS OF AUDITOR	21
8.3	AUDITOR'S RELATIONSHIP TO ASSESSED PARTY	21
8.4	TOPICS COVERED BY AUDIT	21
8.5	ACTIONS TAKEN AS A RESULT OF DEFICIENCY	21
8.6	COMMUNICATION OF RESULTS	22
9	OTHER BUSINESS AND LEGAL MATTERS	23
9.1	FEEES	23
9.2	FINANCIAL RESPONSIBILITY	23
9.3	CONFIDENTIALITY OF BUSINESS INFORMATION	23
9.4	PRIVACY OF PERSONAL INFORMATION	23
9.5	INTELLECTUAL PROPERTY RIGHTS	24
9.6	REPRESENTATIONS AND WARRANTIES	24
9.7	DISCLAIMERS OF WARRANTIES	24
9.8	LIMITATIONS OF LIABILITY	24

9.9	INDEMNITIES	24
9.10	TERM AND TERMINATION	24
9.11	INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS	24
9.12	AMENDMENTS	24
9.13	DISPUTE RESOLUTION PROCEDURES	25
9.14	GOVERNING LAW	25
9.15	COMPLIANCE WITH APPLICABLE LAW	25
9.16	MISCELLANEOUS PROVISIONS.....	25
APPENDIX A	MEDICARE AUSTRALIA PKI WEBSITE	26

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

Medicare Australia, has established a Health Sector Public Key Infrastructure (Health Sector PKI) comprising Certification Authorities and Medicare Australia Relationship Organisation Units (Medicare Australia ROU) (known as Communities of Interest (CoIs) within the Relationship Certificate model) aligned with Medicare Australia's business programs.

Medicare Australia will use this infrastructure to support business needs for the health and welfare sector. The Medicare Australia website (www.medicareaustralia.gov.au) provides additional information about Medicare Australia's Relationship Certificate model.

1.1.1 Hierarchy of trusted elements

The hierarchy of trusted elements comprises:

- the Medicare Australia Root Certification Authority (Medicare Australia RCA),
- the Medicare Australia Organisation Certification Authority (Medicare Australia OCA),
- the Medicare Australia certificate issuance process, including emergency issuance and certificate management policies and procedures, and
- a number of web-based Relationship Organisation Unit Operator (ROUO) workstations dedicated to that ROU's CoI participating in the Relationship Certificate model of the Health Sector PKI.

End Entities are the Subscribers and Relying Parties within each ROU CoI.

This Medicare Australia OCA CPS governs all Relationship Certificates issued by the Medicare Australia OCA on request from each Medicare Australia ROU for that ROU's CoI.

For further information on each ROU and its CoI and the Relationship Certificates applicable to that CoI, refer to the Medicare Australia ROU's CoI Certificate Policy (CP) under which that ROU's CoI Relationship Certificates are issued.

1.1.2 Documentation

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

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

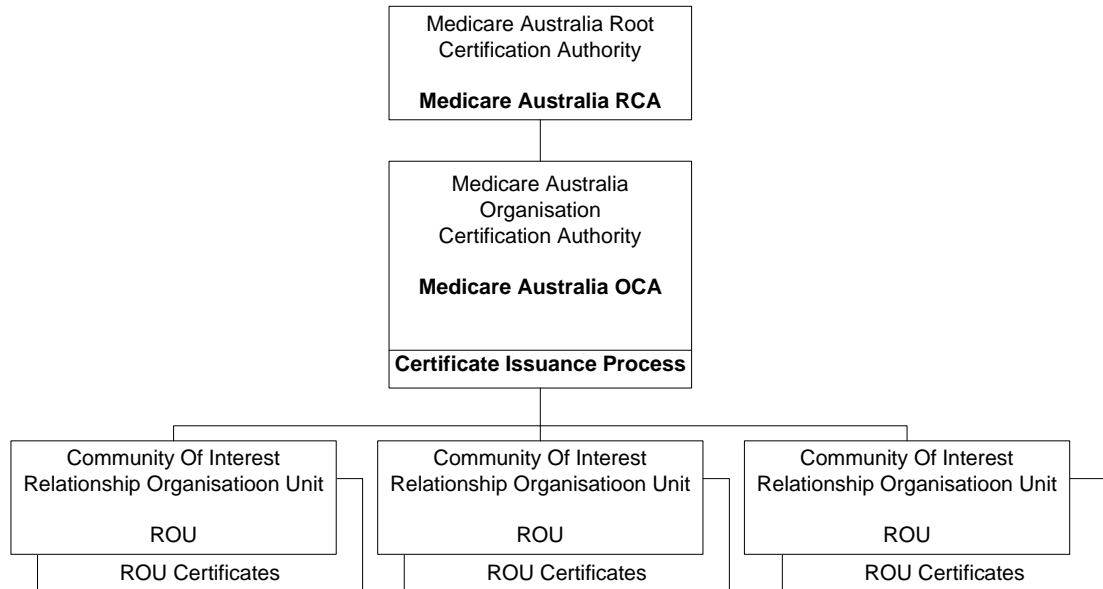
1.2 Medicare Australia Organisation Certification Authority Certificate Practice Statement and Identification

OIDs are not applicable to this Medicare Australia OCA CPS.

This Medicare Australia OCA CPS is published on www.medicareaustralia.gov.au.

Certificates supported by this Medicare Australia OCA CPS will contain the Uniform Resource Identifier (URI) in the CPS pointer qualifier field of the Certificate Policies extension.

1.3 Health Sector PKI Participants



1.3.1 Certification Authorities

1.3.1.1 Medicare Australia Root Certification Authority (Medicare Australia RCA)

The Medicare Australia Root Certification Authority (Medicare Australia RCA) is the trust anchor for all Medicare Australia ROU Cols.

The Medicare Australia RCA issues and signs its own certificate.

The Medicare Australia RCA is owned by Medicare Australia. The Medicare Australia RCA is hosted and operated by Verizon Australia Pty Ltd (ABN 62 081 001 194) on behalf of Medicare Australia.

1.3.1.2 Medicare Australia Organisation Certification Authority (Medicare Australia OCA)

The Medicare Australia Organisation Certification Authority (Medicare Australia OCA) is immediately subordinate to the Medicare Australia RCA in the Health Sector PKI hierarchy. The Medicare Australia OCA manages all Relationship Certificates in the Health Sector PKI Relationship Organisation/Col model operated by Medicare Australia.

The primary purpose of the Medicare Australia OCA is to generate Certificates and to perform other certificate management services in response to requests from authorised Medicare Australia staff (ROUOs) for the CoIs.

The Medicare Australia OCA is owned by Medicare Australia. The Medicare Australia OCA is hosted and operated by Verizon Australia Pty Ltd on behalf of Medicare Australia.

The Medicare Australia OCA is also an OCA under the Medicare Australia RCA. Further information on OCAs is at 1.3.1.4 of the Medicare Australia RCA CPS.

1.3.1.3 Medicare Australia OCA Functions

The Medicare Australia OCA, operating under the Health Sector PKI hierarchy, performs the following functions:

- generates its own Keys,
- submits its Public Keys together with digitally signed certification requests to the Medicare Australia RCA,
- publishes this Medicare Australia OCA CPS and each CP for the CoI under which they issue Certificates at www.medicareaustralia.gov.au.

On the receipt of authenticated requests, the Medicare Australia OCA will:

- issue Certificates in accordance with this Medicare Australia OCA CPS and the CP for the CoI that the Certificates are issued under for:
 - ROUOs for that CoI, and
 - End User-Subscribers within that CoI.
- publish issued Certificates in the Healthcare Public Directory where there is permission from the CoI to do so,
- generate and issue CoI Certificates to Subscribers only on receipt of properly formatted and verified Certificate Requests,
- ensure, at the time a CoI Certificate is issued to a Subscriber, that:
 - the Subscriber's CoI Certificate Information (i.e. information needed to complete a Subscriber's Certificate as required by the CoI Certificate Profile) is factually correct and accurate,

- the Subscriber's Certificate contains all the elements required by the Certificate Profile (i.e. the specification of the fields to be included in a Subscriber's Certificate and the contents of each), and
- the Subscriber is in possession or control of the Private Key corresponding to the Public Key included in the Certificate,
- receive revocation requests and take appropriate action,
- revoke Certificates on receipt of authenticated digitally signed revocation requests,
- post revoked Certificates in the Healthcare Public Directory,
- make reasonable enquiries in accordance with the arrangements agreed with CoIs 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 notify a CoI participant in the event that the Medicare Australia RCA initiates revocation of the Medicare Australia OCA's Certificate, and
- revoke a Certificate within a CoI as required by, and in accordance with, this Medicare Australia OCA CPS and the CP for the CoI under which the Certificate was issued.

1.3.1.4 Medicare Australia OCA Obligations

The Medicare Australia OCA's obligations are:

- to comply with all Gatekeeper Approved Documents, Gatekeeper Policies and Criteria including the Gatekeeper Core Obligations Policy,
- to comply with applicable laws,
- to maintain this Medicare Australia OCA CPS, and the relevant CoI CPs,
- to comply with, and ensure that its personnel and contractors comply with, the conditions and obligations set out in this Medicare Australia OCA CPS,
- to comply with, and ensure that its personnel and contractors comply with, the conditions and obligations set out in the Medicare Australia RCA CPS and the practices set out in the Medicare Australia RCA CP,
- to advise CoIs of their obligations under this Medicare Australia OCA CPS, and the CP relevant to that CoI and make copies accessible to each CoI,

- to manage and conduct audits of the Medicare Australia OCA and CoIs' ROUs when requested by the Medicare Australia PMA.

1.3.2 Relationship Organisation Unit Certificate Issuance Process

Medicare Australia operates the certificate issuance process to provide a registration service to the Medicare Australia OCA. Medicare Australia staff (ROUOs) request the Medicare Australia OCA to generate the Certificate. Certificates are issued in either a once a business day batch method or per individual request as required.

Medicare Australia staff (ROUOs) also undertake a range of other functions associated with the management of Keys and Certificates for the Relationship Certificate model in the Health Sector PKI, such as certificate revocation.

There are two separate categories of authorised persons involved in the registration of an application for Relationship Certificates.

The Certificate Controller is an authorised officer of Medicare Australia and is responsible for:

- operating the Medicare Australia Certificate issuance process,
- correlating the required information to request bulk issuance of Certificates from the Medicare Australia OCA, and
- issuing Certificates in response to requests from ROUOs.

The CA Operator is an employee of Verizon Australia Pty Ltd supplying CA management services. They are responsible for the:

- transmission of the correlated bulk issuance files received from Medicare Australia to the Medicare Australia OCA, and
- transferring the subsequent Certificates for shipping to the Subscribers.

1.3.3 Subscribers

Subscribers for Medicare Australia Relationship Certificates in the Health Sector PKI are members of a defined ROU's CoI. Each CoI is represented by a ROU.

For details of Subscribers for each ROU CoI, refer to the Certificate Policy (CP) the Certificate was issued under for that ROU's CoI.

1.3.4 Relying Parties

Relying Parties for each ROU CoI are identified in the CP under which that particular ROU's 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.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Use

The appropriate Certificate use for each ROU's CoI Certificate is set out in the CP under which that particular Certificate was issued.

1.4.2 Prohibited Certificate Uses

The prohibited Certificate use for each ROU's CoI Certificate is set out in the CP under which that particular Certificate was issued.

1.5 Policy Administration

1.5.1 Organization Administering the Document

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

1.5.2 Contact Person

The person to contact in relation to this Medicare Australia OCA CPS is:

National Manager

eClaiming and eHealth

PO Box 1001 Tuggeranong DC ACT 2901

Email: ehealth.mca@medicareaustralia.gov.au

The contact person can provide copies of, or access to, this Medicare Australia OCA CPS and associated CPs for ROUs' CoIs and answer questions relating to the policy, practices and procedures described in these documents.

1.5.3 Persons Determining CPS Suitability for the Relying Party Certificate Policies

The Medicare Australia PMA reviews all documents to ensure that the practices documented in the Medicare Australia OCA CPS fulfil the requirements specified in each ROU CoI and any other relying CP.

1.6 Definitions and Acronyms

Definitions and acronyms are set out in the Medicare Australia Health Sector PKI Glossary, as amended from time to time. The Glossary is located at <http://www.medicareaustralia.gov.au>.

2 Publication and Repository Responsibilities

2.1 Repositories

The repository for all Public Key Certificates issued under this Medicare Australia OCA 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 CoI.

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 OCA CPS, including Revocation and Expiry of Certificates will be published in the Healthcare Public Directory by the Medicare Australia OCA.

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 CoI, when the responsible RO and ROU have agreed to publication.

The Healthcare Public Directory is accessible programmatically from www.certificates-australia.com.au/. Technical details are at www.medicareaustralia.gov.au.

The Healthcare Public Directory is substantially available 7 days a week, 24 hours a day.

2.2 Publication of Certificate Information

2.2.1 Publication of Medicare Australia OCA 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 this Medicare Australia OCA Certificate and Medicare Australia RCA Certificate is published at www.certificates-australia.com.au.

2.2.2 Publication of Policy and Practice Information

This Medicare Australia OCA CPS is published electronically at the website, www.medicareaustralia.gov.au.

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

Notification of changes will be provided on Medicare Australia's website, www.medicareaustralia.gov.au. This notification method uses a "pull" model. Interested parties are responsible to exercise due care and check, on a regular basis, the Medicare Australia website to review and monitor any changes in the

Medicare Australia OCA CPS. Interested parties are responsible for retrieving amendments when a revised and/or amended Medicare Australia OCA CPS is posted to the website.

2.3 Frequency of Publication

New and revised approved versions of this Medicare Australia OCA CPS are published promptly at www.medicareaustralia.gov.au.

2.4 Access Controls on Repositories

There are no access controls on the reading of this Medicare Australia OCA CPS or the associated CP(s) for the ROU CoIs on the Medicare Australia web sites on which these documents are published.

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 on naming, refer to Section 2 of the CP that the Certificates were issued under.

3.2 Initial Identity Validation

For further information on the initial identity validation, refer to section 2 in the CP that the Certificates were issued under.

3.3 Identification and Authentication for Re-key Requests

For further information on identification and authentication for re-key requests, refer to section 2 of the CP that the Certificates were issued under.

3.4 Revocation Requests

For further information on identification and authentication for revocation requests, refer to section 2.4 of the Community of Interest (CoI) CP that the Certificates were issued under.

4 Certificate Life-Cycle Operational Requirements

Further information on Certificate life-cycle operational requirements is set out in Section 4 of the Certificate Policy under which an ROU CoI Certificate was issued.

5 Management, Operational, and Physical Controls

5.1 Physical Security Controls

Section 5.1 of the Medicare Australia RCA CPS and the Verizon Australia Pty Ltd *SEC1 Security Profile* details the physical security controls for both the Medicare Australia RCA and Medicare Australia OCA. (The *SEC1 Security Profile* is not publicly available.)

5.2 Procedural Controls

Section 5.2 of the Medicare Australia RCA CPS and the Verizon Australia Pty Ltd *SEC1 Security Profile* details the procedural controls for both the Medicare Australia RCA and Medicare Australia OCA. (The *SEC1 Security Profile* is not publicly available.)

5.3 Personnel Security Controls

Section 5.3 of the Medicare Australia RCA CPS and the Verizon Australia Pty Ltd *SEC1 Security Profile* details the personal security controls for both the Medicare Australia RCA and Medicare Australia OCA. (The *SEC1 Security Profile* is not publicly available.)

5.4 Audit Logging Procedures

Section 5.4 of the Medicare Australia RCA CPS and the Verizon Australia Pty Ltd *SEC1 Security Profile* details the audit logging procedures for both the Medicare Australia RCA and Medicare Australia OCA. (The *SEC1 Security Profile* is not publicly available.)

5.5 Records Archival

5.5.1 Types of Event Recorded

The following information is archived by the Medicare Australia OCA:

- Audit logs (refer to 5.4 of the Medicare Australia RCA CPS),
- Certificate request information, and
- Complete back up registers.

5.5.2 Retention Period for Archive

5.5.2.1 Secure Maintenance of Keys

The Medicare Australia OCA does not make or retain copies of Public or Private Keys.

5.5.2.2 Secure Maintenance of Certificates

The Medicare Australia OCA does not make or retain copies of Certificates.

5.5.2.3 Term of Archive Maintenance

Archives are retained for a period of seven years in accordance with *Archives Act 1983* (Commonwealth).

5.5.3 Protection of Archive

Archive media are protected by physical security commensurate with the security classification of the contents, and in accordance with relevant provisions of the Commonwealth Protective Security Policy Framework (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* and the *OP1 Operations Manual* (these documents are 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) as follows:

- annually at the time of the programmed security audit,
- at any time when a full security audit is required, and
- at the time the Archive is prepared.

5.6 Key Changeover

Key changeovers will be affected in such a manner as to cause minimal disruption to Subscribers.

The Medicare Australia RCA and Medicare Australia OCA shall each obtain a new Authentication Key Pair a minimum of two years prior to the expiry of the Certificate associated with their respective current Private Authentication Key. Both the Medicare Australia RCA and the Medicare Australia OCA must 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 Medicare Australia RCA or Medicare Australia OCA Private Authentication Key, both Authentication Public Keys in the associated Certificate will be in use and must be published in the Healthcare Public Directory.

The Medicare Australia RCA and Medicare Australia OCA are 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 OCA. 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 OCA.

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 *OP1 Operations Manual*, *SEC1 Security Profile*, and the *Disaster Recovery and Business Continuity Plan* (these documents are not publicly available).

5.7.3 Entity Private Key Compromise Procedures

In the situation that a Private Key is compromised, for whatever reason, the procedures outlined for CA termination will be followed. Details are provided in Verizon Australia Pty Ltd *SEC1 Security Profile* (this document is not publicly available).

5.7.4 Business Continuity Capabilities after a Disaster

Actions to be taken in order to restore core business operation as quickly as practicable following fire, strikes or similar events are provided in *Disaster Recovery and Business Continuity Plan* for Medicare Australia Health Sector PKI (this document is not publicly available).

5.8 Medicare Australia OCA Termination

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

If the Medicare Australia OCA 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

The Medicare Australia OCA Key pairs are generated by the OCA itself using software listed on the Defence Signals Directorate (DSD) Evaluated Products List (EPL), equipment and processes. Following this a properly formatted and verified certificate request is forwarded to the RCA.

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

6.1.2 Private Key Delivery to Subscriber

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

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

6.1.3 Public Key Delivery to Certificate issuer

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

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

6.1.4 CA Public Key Delivery to Relying Parties

The Medicare Australia OCA Public Keys are made available to End User-Subscribers and Relying Parties via the Medicare Australia publicly accessible Repository (www.certificates-australia.com.au).

6.1.5 Key Sizes

The Medicare Australia OCA Key strength is 2048 bits in length.

Subscriber Keys are a minimum of 1024 bits in length.

6.1.6 Public Key Parameters Generation

The parameters used to create Public Keys for Subscribers are generated using a product listed on the Defence Signals Directorate (DSD) Evaluated Products List (EPL). Parameter quality checking is ensured through the use of a product listed on the EPL.

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

Medicare Australia OCA 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 CoI CP under which the Certificate was issued.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

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

6.2.2 Private Key (m of n) Multi-person Control

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

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 OCA are stored in encrypted files and are backed up under further encryption with backup copies maintained on-site and in secure off-site storage.

Private Key backup is not provided for Subscribers.

6.2.5 Private Key Archival

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

Private Key Archival is not provided for Subscribers.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

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

6.2.7 Private Key Storage on a Cryptographic Module

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

6.2.8 Method of Activating Private Key

The Private Keys of the Medicare Australia OCA and Subscribers 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 Australian Government Information and Communication Technology Security Manual (ISM), or
- other media – in accordance with recommendations in ISM.

Media containing a Private Key of the Medicare Australia OCA will be securely disposed of by sanitisation by overwriting (where feasible), then by supervised physical destruction in accordance with 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, as it is currently not used in the Health Sector PKI: 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 Health Sector PKI Public Directory for the life of the Certificate.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

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

- Authentication Private and Public Keys – ten (10) years,
- Confidentiality Public Key – ten (10) years,
- Confidentiality Private Key – no expiry.

The usage period for Subscriber Public and Private Keys is documented in the applicable CoI CP.

6.4 Activation Data

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 OCA computer security technical requirements are detailed in the Verizon Australia Pty Ltd *SEC1 Security Profile* (this document is not publicly available).

6.5.2 Computer Security Rating

Medicare Australia computer security rating is detailed 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 system development controls are detailed in the Verizon Australia *SEC1 Security Profile* (this document is not publicly available).

6.6.2 Security Management Controls

Medicare Australia 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

Medicare Australia life cycle security ratings are detailed 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* which identifies and addresses all high or significant life cycle Security Threats. This is not publicly available.

6.8 Time-stamping

Time stamping is carried out as required using evaluated products.

7 Certificate and CRL Profiles

7.1 Certificate Profile

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

7.1.1 Version Number(s)

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

7.1.2 Certificate extensions

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

7.1.6 Certificate Policy Object Identifier

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

7.1.7 Usage of Policy Constraints Extension

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

7.1.8 Policy Qualifiers Syntax and Semantics

The Medicare Australia OCA supports the use of syntax and semantics Policy Qualifiers. For this information, please refer to the CoI 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 International Standard X.509 profile.

7.2 Certificate Revocation List Profile

7.2.1 Version Number(s)

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

7.2.2 CRL and CRL Entry Extensions

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

7.3 Online Certificate Status Protocol Profile

7.3.1 Version Numbers (s)

The Medicare Australia OCA may support the use of Online Certificate Status Protocol (OCSP) requests in a limited manner, in so far as OCSP requests need not be digitally signed by the sender.

7.3.2 OCSP Extensions

Dependant on the responder deployed and its configuration, OCSP extensions will be supported by the Medicare Australia OCA.

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 will ensure regular internal audits of Medicare Australia OCA processes occur on no less than an annual basis.

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 Assessed Party

External auditors will be organisationally independent of the Medicare Australia OCA 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 OCA's operations.

8.4 Topics Covered by Audit

The areas to be audited for both external and internal audits include but are not limited to:

- physical security,
- documentation and processes,
- vetting of operational personnel,
- technology,
- privacy, and
- financial viability.

Further criteria are listed in section 8.4 of the Medicare Australia RCA CPS.

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 OCA 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 OCA, 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 OCA CPS.

9.2.3 Warranty Coverage

There is no warranty coverage available for Subscribers or Relying Parties under this 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 OCA CPS applies.

9.10 Term and Termination

9.10.1 Term

The OCA 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 OCA CPS, the Medicare Australia RCA 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

For further information, refer to Section 9.13 of the Medicare Australia RCA CP.

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.

Appendix 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 CoIs,
- 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.

The www.certificates-australia.com.au website also provides, the Health Sector PKI Directory, CA Certificates and their hash values.