

# Short Form Certificate Policy



**Australian Government**

---

**Medicare Australia**

## **Medicare Australia Community of Interest Certificate Policy for Healthcare Individual Certificates v 2.1**

**(5 Year Duration)**

**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 Services 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

## Version History

Doc Version	Status	Date of Issue	Issue By	Comments
1.0	DRAFT	15 Sept 2006	Stephen Wilson	Initial draft based on Online Claiming Site CP
1.1	DRAFT	19 Sept 2006	Stephen Wilson	Changes after internal team review before legal review
1.2	DRAFT	4 October 2006	Lynn Du Moulin	OLC review and amendments; change of title to 'Registered Medicare Australia Provider'
1.3	DRAFT	13 October 2006	John Brewer, Lynn Du Moulin, Michael Tindall	Consolidation of comments JB, MT LDM. OLC Review
1.4	Final	20 October 2006	Lynn Du Moulin John Brewer Lynn Du Moulin  John Brewer	OLC review Changes accepted as final OLC review: cl.2.2 (d) and (e) comments Cl.2.2 (d) and (e)
1.4	Final	23 October 2006	Lynn Du Moulin	John Brewer changes accepted
1.5	Final	22 November 2006	John Brewer	clause 2.2; 1st para, last full line - delete "the" before Medicare Australia
1.6		May 2007		Approved by Nic van den Berg
1.7	Draft	1 May 20078	P Sorensen	Revised Draft (incl changes for 5 yr certs)
1.8	Draft	20 May 2008	P Sorensen	Revised after comments from Lynn Du

				Moulin
1.9	Draft	13 June 2008	P Sorensen	Revised after further comments from Lynn Du Moulin
1.9.1	Draft	16 June 2008	P Sorensen	Revised to include liability references
1.9.2	Draft	13 April 2009	J Wong	Added HPI-I
1.9.3	Draft	July 2009	M Mynott	Revised to include 'Healthcare' reference
1.9.4	Draft	April 2010	P Sorensen	AGIMO Feedback to be Included
1.9.5	Draft	April 2010	J Hunt	Changed HPI-I Certificate profile to Location ID, removed wording 'containing HPI-I number from Section 6 field 2.6.2.
1.9.6 v.x1	Draft	15 August 2010	Lynn Du Moulin	Review and revision to identify all Individuals in scope for the Individual Cofl.
1.9.6 v.x1	Draft	19 August 2010	Paul Sorensen John Wong	Review amendments Amendment to OID
1.9.6	Draft final	19 August 2010	Lynn Du Moulin	Review and accept amendments
1.9.6	Draft Final	20 August 2010	Paul Sorensen John Wong	Review of amendments
2.0	FINAL	20 August 2010	Lynn Du Moulin	Final review
2.00		21 March 2011 and 20 May 2011	Lynn Du Moulin	Amendment to include Contracted Service Provider Officer (CSP Officer) as a Medicare Australia Healthcare Individual for the purposes of the <i>Healthcare Identifiers Act 2010</i> .
2.00	FINAL	23 May 2011	Lynn Du Moulin	Final including CSPOs
2.1	FINAL	27 MAY 2010	Lynn Du Moulin	Revise CP to Include Contracted Service Providers ( <i>Healthcare Identifiers Act 2010</i> )

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

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

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

## Introduction

This is the Certificate Policy for Healthcare individual certificates to be provided to Medicare Australia Healthcare Individuals, including:

- providers
- allied health providers
- aged care providers
- other Healthcare individuals and related personnel (including responsible officers authorised as such under the *Healthcare Identifiers Act 2010*), and
- Contracted Service Provider Officers (CSP officers) who are approved as such by a contracted service provider authorised in accordance with the *Healthcare Identifiers Act 2010*.

who are either known to Medicare Australia or have been identified through appropriate EOI requirements.

This CP should be read in conjunction with the:

- Medicare Australia Root Certification Authority Certification Practice Statement (RCA CPS)
- Medicare Australia Root Certification Authority Certificate Policy (RCA CP).
- Medicare Australia Organisation Certification Authority Certification Practice Statement (Medicare Australia OCA CPS).

## Terminology

**Medicare Australia Healthcare Individual Certificate** means an individual Certificate issued under this CP to a Healthcare Individual who is registered with, or known to, Medicare Australia through application and / or relationship.

Some Healthcare Individuals will, at registration, be issued with a registration number (however described) by Medicare Australia, for example, healthcare providers.

Other Healthcare Individuals will be known to Medicare Australia through:

- Medicare Australia program applications and/or relationships (for example, aged care providers)
- Its role as service operator of the HI Service, in accordance with the *Healthcare Identifiers Act 2010* (Cth) and the National Partnership Agreement 2009 (the COAG Agreement). Such Healthcare individuals include, for example:

- Healthcare Provider Individuals (HPIs) (who are not otherwise known to Medicare Australia through Medicare Australia program applications)
- those persons who are identified as Responsible Officers under the *Healthcare Identifiers Act 2010* (Cth), and
- those persons identified as Contracted Service Provider Officers by a contracted service provider authorised as a contracted service provider in accordance with the provisions of the *Healthcare Identifiers Act 2010*.

## **Certificate Policy Clauses**

### **CP Identification**

Certificates issued under this CP shall bear the Policy OID:

#### **1.2.36.174030967.1.5.1.2**

(where “174030967” is the last 9 digits of Medicare Australia’s Australian Business Number).

### **1. INTRODUCTION**

This is the Certificate Policy for individual certificates to be provided to Medicare Australia Healthcare Individuals.

The certificates are provided on a Secure Token to Subscribers.

The meaning of a Medicare Australia Healthcare Individual Certificate (Healthcare Individual Certificate) issued in this way is nothing more and nothing less than a statement expressed in a digital format of the fact that the certificate Subject (the Medicare Australia Healthcare Individual) has either been issued with a Medicare Australia registration number (however described) or otherwise is known to Medicare Australia through application and / or relationship.

The Relationship Organisation for this CP is Medicare Australia or, in the case of Healthcare Individuals who are Responsible Officers in accordance with that role as set out in the *Healthcare Identifiers Act 2010* (Cth) or who are Contracted Service Provider Officers under that *Healthcare Identifiers Act 2010*, Medicare Australia as the Healthcare Identifier (HI) Service service operator as appointed under the *Healthcare Identifiers Act 2010* (Cth),

The Relationship Organisation Unit (ROU) is either the program area in Medicare Australia responsible for undertaking the Application registration or the relevant area within Medicare Australia operating as the HI Service service operator.

The Relationship Organisation Unit Operators (ROUOs) are Medicare Australia personnel working in the ROU or the HI Service service operator area responsible for undertaking the Application registration of the Responsible Officers and of Contracted Service Provider Officers.

#### **1.1 PKI Participants**

##### **1.1.1 Certification Authority**

All Certificates issued under this CP shall be produced by the Medicare Australia Organisation Certification Authority (Medicare Australia OCA).

Refer to the Medicare Australia Root Certification Authority Certification Practice Statement (Medicare Australia RCA CPS), the Medicare Australia Certification

Authority Certificate Policy (Medicare Australia RCA CP) and the Medicare Australia Organisation Certification Authority Certification Practice Statement (Medicare Australia OCA CPS) for further information on applicable practices and procedures for Certificates issued under this CP, located at [www.medicareaustralia.gov.au](http://www.medicareaustralia.gov.au).

### **1.1.2. Relationship Organisation**

Medicare Australia, or Medicare Australia as the HI Service service operator, is the Relationship Organisation (Medicare Australia RO) in the Health Sector PKI.

### **1.1.3. Relationship Organisation Unit**

There are separately identified Relationship Organisation Units (ROUs) within the Medicare Australia RO, usually one ROU for each Community of Interest (Col) in the Health Sector PKI operated by Medicare Australia.

The ROU has responsibilities in the Col in managing the Subscribers in that Col.

### **1.1.4 Certificate Controllers**

Certificate Controllers are Medicare Australia RO personnel with responsibilities for management of Certificates.

All Certificate Controllers operating under this CP are duly authorised representatives of Medicare Australia.

### **1.1.5 Relationship Organisation Unit Operators**

Relationship Organisation Unit Operators (ROUOs) are Medicare Australia personnel within the Registered Medicare Australia Individual Col.

ROUOs within the Registered Medicare Australia Individual Col are not Certificate Controllers.

ROUOs operate in accordance with the processes and procedures set out in the Medicare Australia OCA CPS and this CP.

### **1.1.6. Subscribers**

Subscribers under this CP include:

- (a) a Healthcare Individual who is currently registered with, and in some cases, allocated a number (for example, provider number(s)) by, Medicare Australia or is known to Medicare Australia), or
- (b) a Healthcare Individual who is employed in the Health Sector, and who has provided EOI commensurate with Medicare Australia requirements

- (c) a Responsible Officer whose role is established under the *Healthcare Identifiers Act 2010* and who is, at the time of registration with the Medicare Australia RO for a Healthcare Individual Certificate, registered with, and allocated a number by, Medicare Australia as HI Service service operator and is known to Medicare Australia.
- (d) a Contracted Service Provider Officer who has authority to act for the contracted service provider authorised as such in accordance with the *Healthcare Identifiers Act 2010*.

There is a Subscriber agreement under this CP, known as the *Individual Keys and Certificates Certificate Terms and Conditions of Use*.

The Subscriber is bound by these terms and conditions when the Subscriber conducts his or her first transaction using the Individual Keys and Certificates issued under this CP.

#### **1.1.7. Relying Parties**

Relying Parties under this CP are:

- a) Medicare Australia, as receiver of transactions secured using the Individual keys and Certificates;
- b) Healthcare Individuals conducting transactions with other Individuals or entities as authorised or approved by Medicare Australia;
- c) Healthcare Providers who have authorised a contracted service provider, represented by a Contracted Service Provider Officer, to provide services in accordance with the *Healthcare Identifiers Act 2010*.

There is no Relying Party Agreement under this CP.

Parties who rely on Certificates issued under this CP and who do not have a written agreement with Medicare Australia or authorisation via a notice published at [www.medicareaustralia.gov.au](http://www.medicareaustralia.gov.au) (specifying authorised usage relating to a transaction type), and therefore undertake transactions that are not authorised or approved by Medicare Australia, rely on such certificates at their own risk.

## **1.2 Certificate Use**

### **1.2.1 Appropriate Certificate Use**

Key Pairs and Certificates issued under this CP are to be used by Healthcare Individuals conducting transactions with Medicare Australia or other Individuals or entities as authorised or approved by Medicare Australia.

### **1.2.2 Prohibited Certificate Uses**

There are no prohibited certificate uses.

Parties using Individual Certificates for any transaction other than an authorised or approved transaction with Medicare Australia or an approved transaction between parties so authorised under the *Healthcare Identifiers Act 2010*, do so at their own risk.

### **1.3 Definitions and Acronyms**

Definitions and Acronyms are in the:

- Medicare Australia Health Sector PKI Glossary at (<http://www.medicareaustralia.gov.au/provider/business/online/register/policy.jsp>).
- *Healthcare Identifiers Act 2010*
- The Healthcare Identifiers Regulations 2010
- The Healthcare Identifiers Glossary

## **2. IDENTIFICATION AND AUTHENTICATION OF USERS**

### **2.1 Naming of Subscribers**

Subscribers (termed 'Certificate Subjects' in the x.509 definition) under this CP shall be named (and the uniqueness of their names shall be assured) according to Medicare Australia application and registration processes for Healthcare Individuals.

### **2.2 Identification and authentication of the Subscriber at registration**

Subscribers (Healthcare Individuals) under this CP will be identified and authenticated at the time of their application for registration (however described) as a Healthcare Individual by Medicare Australia in accordance with trusted practices that may include, but not be limited to:

- a) receipt of applications for registration as a Healthcare Individual or a Responsible Officer or as a Contracted Service Provider Officer;
- b) assessment of Applications and associated documents;
- c) processing in association with the Department of Health and Ageing (DoHA) (where required);
- d) allocation of number(s) (where required) and registration on Medicare Australia systems (however described);

Where a Medicare Australia Healthcare Individual wishes to access Medicare Australia programs using his/her Certificate, Medicare Australia reserves the right to require that the Medicare Australia Healthcare Individual enters into terms and conditions for participation in that program.

Any such program terms and conditions are separate from the *Individual Keys and Certificates Terms and Conditions of Use*.

### **2.3 Identification and authentication of the Subscriber at renewal**

Subscribers (Medicare Australia Healthcare Individuals) under this CP shall be identified and authenticated and the Certificate renewed provided that the Medicare Australia Healthcare Individual's registration or other status with Medicare Australia and / or the HI Service (Medicare Australia as HI Service service operator), has not changed.

### **2.4 Identification and authentication of revocation request**

Revocation of certificates under this CP shall only be requested in writing by:

- a) ROUOs in the event that the Subscriber becomes ineligible to remain as a Medicare Australia Healthcare Individual; or
- b) The Subscriber; or
- c) Certificate Controllers.

## **3. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS**

### **3.1. Certificate creation**

#### **3.1.1. Enrolment process and responsibilities**

Medicare Australia may consider that the Healthcare Individual be enrolled for Certificates by Certificate Controllers on the basis of:

- (a) being known to Medicare Australia as a Medicare Australia Healthcare Individual either through:
  - i. a Medicare Australia program registration (eg Aged Care provider)
  - ii. being currently registered with Medicare Australia, and in some cases, allocated a number (for example, provider number(s)).
- (b) Receipt of a certificate application together with EOI commensurate with Medicare Australia requirements.
- (c) an individual's role as a Responsible Officer which is established under the *Healthcare Identifiers Act 2010* and who provides EOI commensurate with Medicare Australia requirements, and is registered with, and allocated a number by, Medicare Australia as HI Service service operator.

- (d) an individual's role as a Contracted Service Provider Officer where the contracted service provider is authorised as such in accordance with the *Healthcare Identifiers Act 2010* and who provides EOI commensurate with Medicare Australia requirements, and is registered with, and allocated a number by Medicare Australia, as HI Service service operator.

### **3.1.2. Publication of the certificate by the CA**

Certificates issued under this CP will be published in the Healthcare Public Directory

Revocation status of Certificates issued under this CP will be published in the Healthcare Public Directory.

## **3.2. Key Pair and Certificate Usage**

### **3.2.1 Key pair generation and installation**

All Subscriber key pairs under this CP shall be generated by Certificate Controllers using accredited software.

The signing key & encryption key shall be stored and dispatched on a secure token. A PIC (personal identification code) to access the keys and Certificates will also be generated and dispatched separately.

### **3.3. Certificate renewal**

Refer to clause 2.3 for details of identification and authentication.

### **3.4. Certificate revocation**

Certificates issued under this CP may be revoked by Medicare Australia in its absolute discretion, including but not limited to:

- a) after loss, destruction or theft of the Certificate;
- b) in the event of Medicare Australia Healthcare Individual's de-registration (however described);
- c) in the event the Medicare Australia Healthcare Individual's Provider Number(s) or other numbers are cancelled by Medicare Australia.

## **3.5 Certificate status services**

### **3.5.1 Operational characteristics**

Refer to Section 4.10.1 of the Medicare Australia RCA CP.

### **3.5.2 Service availability**

Service availability for the Certificate Revocation List (CRL) is substantially 24 x 7 at [www.certificates-australia.com.au](http://www.certificates-australia.com.au).

### **3.5.3 Optional features**

Not applicable.

## **4. REGISTRATION OPERATIONAL CONTROLS**

### **4.1 Personnel controls**

All Certificate Controllers under this CP shall be authorised representatives of Medicare Australia or Medicare Australia as the service operator for the HI Service (in relation to Responsible Officers and Contracted Service Provider Officers).

### **4.2 Logical and Technological controls**

Certificate requests will be processed by the authorised Certificate Controllers of Medicare Australia in accordance with the security provisions of the Medicare Australia OCA CPS.

### **4.3 Physical controls**

Certificate requests will be processed by Medicare Australia Certificate Controllers in accordance with the security provisions of the Medicare Australia OCA CPS.

### **4.4 Business continuity of the Relationship Organisation**

Medicare Australia (the Relationship Organisation under this CP) is a statutory agency established under the *Medicare Australia Act 1973*. Its continuation depends on continuance in force of the *Medicare Australia Act 1973* or by other Acts of the Commonwealth Parliament made pursuant to government policy.

Changes in legislation or government policy will provide for business continuity of the RO in accordance with policy as determined by the government and implemented in accordance with Commonwealth Machinery of Government (MOG) requirements.

### **4.5 Relationship Organisation termination**

Medicare Australia is a statutory agency established under the *Medicare Australia Act 1973*. Its termination or change of entity status can only be through amendment to the *Medicare Australia Act 1973* or by other Acts of the Commonwealth Parliament made pursuant to changes in government policy.

Changes in legislation or government policy will provide for termination of Medicare Australia as the RO and for a replacement agency as the successor RO in accordance with policy as determined by the government and

implemented in accordance with legislation passed by the Commonwealth Parliament.

## **5. OTHER BUSINESS AND LEGAL MATTERS**

### **5.1 Other Business**

For information on other business (for example fees, confidentiality, privacy, intellectual property, representations and warranties and disclaimers of warranties), refer to section 9 and subsections 9.1 - 9.7 of the Medicare Australia Root Certification Authority (RCA) Certificate Policy (CP) at [www.medicareaustralia.gov.au](http://www.medicareaustralia.gov.au).

### **5.2 LEGAL MATTERS**

For information on legal matters, refer to section 9 (Other Business and Legal Matters) of the Medicare Australia Root Certification Authority (RCA) Certificate Policy (CP) at [www.medicareaustralia.gov.au](http://www.medicareaustralia.gov.au)

#### **5.2.1 Limitations of Liability**

For information on limitation of liabilities and indemnities, refer to section 9 and subsection 9.8 (Limitations of Liability) of the Medicare Australia Root Certification Authority (RCA) Certificate Policy (CP) at [www.medicareaustralia.gov.au](http://www.medicareaustralia.gov.au)

Paragraph 9.8.1 of the Medicare Australia RCA CP provides:

##### **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.

#### **5.2.2 Indemnities**

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

## 6. CERTIFICATE, CRL AND OCSP PROFILES

### 6.1 Certificate profile – Registered Medicare Australia Healthcare Individual Encipherment Certificate

Field	Content	Mandatory	Critical*
1. X.509v1 Field			N/A
1.1. Version	V3	M	
1.2. Serial Number	A positive integer that uniquely identifies the Certificate.	M	
1.3. Signature Algorithm	SHA-1 RSA, SHA-1 hashing algorithm using the RSA signing algorithm.	M	
1.4. Issuer Distinguished Name		M	
1.4.1. Country (C)	AU	M	
1.4.2. Organization (O)	GOV	M	
1.4.3. Organization Unit (OU)	Medicare Australia	M	
1.4.3. Common Name (CN)	Medicare Australia Organisation Certification Authority	M	
1.5. Validity			
1.5.1. Not Before	The date that the Certificate is valid from (system time at certificate issuance). YYMMDDHHMMSSZ encoded as UTCTime for dates up to 2049 and encoded as GeneralizedTime for dates in 2050 or later.	M	
1.5.2. Not After	The date that the Certificate is valid until. 5 years from Start Validity, i.e. certificate issuance. YYMMDDHHMMSSZ encoded as UTCTime for dates up to 2049 and encoded as GeneralizedTime for dates in 2050 or later	M	
1.6. Subject			
1.6.1. Country (C)	AU	M	
1.6.2. State (St)	<STATE>	M	
1.6.3. Organization (O)	<Health>	O	
1.6.4. Common Name (CN)	<First Middle Last Name> :RA Number	M	
1.7. Subject Public Key Info	RSA Public Key of 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		
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	NOT SET		
2.3.2. Non Repudiation	NOT SET		
2.3.3. Key Encipherment	SET		
2.3.4. Data Encipherment	NOT SET		
2.3.5. Key Agreement	NOT SET		
2.3.6. Key Certificate Signature	Not Selected		
2.3.7. CRL Signature	Not Selected		
2.4. Extended Key Usage	Not applicable		Non-Critical
2.5. Certificate Policies			Non-Critical
2.5.1. Policy Identifier	1.2.36.174030967.1.5.1.2		
2.5.1.1. Policy Qualifier ID	User Notice		
2.5.1.2. User Notice	Certificates issued under this CP must only be relied on by entities within the Community of Interest, unless otherwise agreed, and not for purposes other than those permitted by this CP.		
2.5.1.3. Policy Qualifier ID	CPS URI		
2.5.1.4. CPS URI	http://www.medicareaustralia.gov.au/		
2.6. Subject Alternate Names			Non-

Field	Content	Mandatory	Critical*
2.6.1. rfc822Name	<email address>	O	Critical
2.6.2. uniformResourceIdentifier	<Uniform Resource Identifier>	O	
2.7. Basic Constraints			
2.7.1. Subject Type	Not CA		Critical
2.7.2. Path Length Constraint	Not present		
2.8. Authority Information Access			
2.8.1. Access Description	Not present		
2.8.1.1. Access Method	On-line Certificate Status Protocol (1.3.6.1.5.5.7.4.1)		Non-Critical
2.8.1.2. Alternative Name	URL=http://ocsp.certificates-australia.com.au/maoca.pkx		
2.9 CRL Distribution Point			
2.9.1 URL	http://www.certificates-australia.com.au/general/cert_search_health.shtml		Non-Critical
3.0 Other Fields - Generic <sup>1</sup>			
3.0.1 Generic IA5 String: RA Number (OID=1.2.36.73665175.1.10009)	< RA Number >	M	
3.0.2 Generic IA5 String: Provider Stem Number (OID=1.2.36.174030967.0.2)	< Provider Stem Number >	O	
3.0.3 Generic IA5 String: Prescriber Number (OID=1.2.36.174030967.0.3)	< Prescriber Number >	O	
3.0.4 Generic IA5 String: Healthcare Provider Identifier (OID=1.2.36.174030967.0.4)	< Healthcare Provider Identifier >	O	
3.0.5 Generic IA5 String: Medicare Identifier (OID=1.2.36.174030967.0.5)	< Medicare Identifier >	O	

## 6.2 Certificate profile – Registered Medicare Australia Healthcare Individual Signing Certificate

Field	Content	Mandatory	Critical*
1. X.509v1 Field			N/A
1.1. Version	V3	M	
1.2. Serial Number	A positive integer that uniquely identifies the Certificate.	M	
1.3. Signature Algorithm	SHA-1 RSA, SHA-1 hashing algorithm using the RSA signing algorithm.	M	
1.4. Issuer Distinguished Name		M	
1.4.1. Country (C)	AU	M	
1.4.2. Organization (O)	GOV	M	
1.4.3. Organization Unit (OU)	Medicare Australia	M	
1.4.4. Common Name (CN)	Medicare Australia Organisation Certification Authority	M	
1.5. Validity			
1.5.1. Not Before	The date that the Certificate is valid from (system time at certificate issuance). YYMMDDHHMMSSZ encoded as UTCTime for dates up to 2049 and encoded as GeneralizedTime for dates in 2050 or later.	M	
1.5.2. Not After	The date that the Certificate is valid until. 5 years	M	

<sup>1</sup> These Certificate extension OID references are expected to be common to all CoI Certificate Policies, and may have applicability to this CoI.

Field	Content	Mandatory	Critical*
	from Start Validity, i.e. certificate issuance. YYMMDDHHMMSSZ encoded as UTCTime for dates up to 2049 and encoded as GeneralizedTime for dates in 2050 or later		
1.6. Subject			
1.6.1. Country (C)	AU	M	
1.6.2. State (St)	<STATE>	M	
1.6.4. Organization (O)	<Health>	O	
1.6.6. Common Name (CN)	<First Middle Last Name> :RA Number	M	
1.7. Subject Public Key Info	RSA Public Key of 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		
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	NOT SET		
2.3.4. Data Encipherment	NOT SET		
2.3.5. Key Agreement	NOT SET		
2.3.6. Key Certificate Signature	Not Selected		
2.3.7. CRL Signature	Not Selected		
2.4. Extended Key Usage	Not applicable		Non-Critical
2.5. Certificate Policies			Non-Critical
2.5.1. Policy Identifier	1.2.36.174030967.1.5.1.2		
2.5.1.1. Policy Qualifier ID	User Notice		
2.5.1.2. User Notice	Certificates issued under this CP must only be relied on by entities within the Community of Interest, unless otherwise agreed, and not for purposes other than those permitted by this CP.		
2.5.1.3. Policy Qualifier ID	CPS URI		
2.5.1.4. CPS URI	<a href="http://www.medicareaustralia.gov.au/">http://www.medicareaustralia.gov.au/</a>		
2.6. Subject Alternate Names			Non-Critical
2.6.1. rfc822Name	<email address>	O	
2.6.2. uniformResourceIdentifier	<Uniform Resource Identifier>	O	
2.7. Basic Constraints			
2.7.1. Subject Type	Not CA		Critical
2.7.2. Path Length Constraint	Not present		
2.8. Authority Information Access			
2.8.1. Access Description	Not present		
2.8.1.1. Access Method	On-line Certificate Status Protocol (1.3.6.1.5.5.7.4.1)		Non-Critical
2.8.1.2. Alternative Name	URL= <a href="http://ocsp.certificates-australia.com.au/maoca.pkx">http://ocsp.certificates-australia.com.au/maoca.pkx</a>		
2.9 CRL Distribution Point			
2.9.1 URL	<a href="http://www.certificates-australia.com.au/general/cert_search_health.shtml">http://www.certificates-australia.com.au/general/cert_search_health.shtml</a>		Non-Critical
3.0 Other Fields - Generic <sup>2</sup>			
3.0.1 Generic IA5 String: RA Number (OID=1.2.36.73665175.1.10.009)	< RA Number >	O	
3.0.2 Generic IA5 String:	< Provider Stem Number >	O	

<sup>2</sup> These Certificate extension OID references are expected to be common to all CoI Certificate Policies, and may have applicability to this CoI.

Field	Content	Mandatory	Critical*
3.0.3 Provider Stem Number (OID=1.2.36.174030967.0.2) Generic IA5 String: Prescriber Number (OID=1.2.36.174030967.0.3)	< Prescriber Number >	O	
3.0.4 Generic IA5 String: Healthcare Provider Identifier (OID=1.2.36.174030967.0.4)	< Healthcare Provider Identifier >	O	
3.0.5 Generic IA5 String: Medicare Identifier (OID=1.2.36.174030967.0.5)	< Medicare Identifier >	O	

### 6.3 Medicare Australia OCA CRL 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	
1.3.3. Organisational Unit (OU)	Medicare Australia		
1.3.3. Common Name (CN)	Medicare Australia Organisation 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		

Frequency of issuing	60 minutes		
Grace Period	60 minutes		

## 6.4 Medicare Australia OCA OCSP 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 Signature	M	
1.4. Issuer Distinguished Name		M	
1.4.1. Country (C)	AU	M	
1.4.2. Organization (O)	GOV	M	
1.4.3. Organisational Unit (OU)	Medicare Australia		
1.4.4. Common Name (CN)	Medicare Australia Organisation Certification Authority	M	
1.5. Validity	5 years		
1.5.1. Not Before	Issue date	M	
1.5.2. Not After	Expiry date	M	
1.6. Subject			
1.6.1. Country (C)	AU	M	
1.6.2. Organization (O)	GOV	M	
1.6.3. Organizational Unit (OU)	Medicare Australia		
1.6.4. Common Name (CN)	Medicare Australia OCA OCSP Responder	M	
1.7. Subject Public Key Info	Public Key encoded in accordance with RFC2459 & PKCS#1- 2048 bits	M	
2. X.509v3 Extensions			
2.1. Authority Key Identifier	SHA-1 hash (60 bits) of the Issuer's public key	M	Non-Critical
2.1.1. Key Identifier	The Key Identifier of the Issuer of this Certificate – 60 bit		
2.1.2. AuthorityCertIssuer	Not present		
2.1.3. AuthorityCertSerialNumber	Not present		
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	Not Selected		
2.3.3. Key Encipherment	Not Selected		
2.3.4. Data Encipherment	Not Selected		
2.3.5. Key Agreement	Not Selected		
2.3.6. Key Certificate Signature	Not Selected		
2.3.7. CRL Signature	Not Selected		
2.4. Extended Key Usage			Non-Critical
2.4.1. OCSP Signing	1.3.6.1.5.5.7.3.9		
2.5. Certificate Policies			
2.5.1. Policy Identifier	Not present		
2.5.1.1. Policy Qualifier ID	Not present		
2.5.1.2. User Notice	Not present		
2.5.1.3. Policy Qualifier ID	Not present		
2.5.1.4. User Notice	Not present		
2.6. Subject Alternate Names			Non-Critical
2.6.1. rfc822Name	NA		
2.7. Basic Constraints			
2.7.1. Subject Type	End Entity		N/A
2.7.2. Path Length Constraint	Not present		
2.8. Authority Information Access			
2.8.1. Access Description	Not present		
2.8.1.1. Access Method	Not present		Non-Critical
2.8.1.2. Alternative Name	Not present		
3. No Check Extension (generic extension)			