

Short Form Certificate Policy



Australian Government

Medicare Australia

**Medicare Australia Community of Interest
Certificate Policy for Individual Certificates
for Healthcare Provider Individuals via data
source (HPI-DS) for Healthcare Identifiers
Service (HI Service) v 1.0**

(5 Year Duration)

August 2010

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

Version History

Doc Version	Status	Date of Issue	Issue By	Comments
Draft v.1	First Draft	25 June 2010	Lynn Du Moulin	Initial draft based on Medicare Australia Community of Interest Certificate Policy for Healthcare Individual Certificates v 1.9.5 (5 Year Duration)
Draft v.2	First draft	29 June 2010	Paul Sorensen	Amendments to initial draft
Draft v.3	2 nd draft	4 August 2010	Lynn Du Moulin	
Draft v.4	2 nd draft	12 August 2010	Paul Sorensen and Rob Hunter	Amendments to drafts 2 and 3
Draft v .5	3 rd draft	15 August 2010	Lynn Du Moulin	Accepted previous amendments Redraft to reflect that this CP is for Individual Certificates for HPI-Is known to Medicare Australia via data sources (also referred to as Trusted Data Sources (TDS) in accordance with the <i>Healthcare Identifiers Act 2010</i> (Cth)
Draft v.6	4 th draft	16 August 2010	Paul Sorensen and Rob Hunter	Amendments to draft 5
Draft v.7	Draft final	16 August 2010	Lynn Du Moulin Paul Sorensen	Accept amendments
Final v.1.0	Final	18 August 2010	Lynn Du Moulin	Final for PMA

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

General Manager
Health eBusiness Division

Introduction

This is the Certificate Policy for Individual Certificates to be provided to persons authorised under the *Healthcare Identifiers Act 2010* (Cth) to register for an individual healthcare provider (HPI) identifier (however described) in accordance with their roles in the Healthcare Identifiers Service (HI service) under the *Healthcare Identifiers Act 2010* (Cth).

Such individuals include:

- Healthcare Provider Individuals, being those individual healthcare providers (however described) who are known to and identified by a data source as an individual healthcare provider, and
- the data source is identified and authorised as a data source under subsection 12(2) (or other relevant section(s)) of the *Healthcare Identifiers Act 2010* and / or the Healthcare Identifiers Regulations 2010, and
- the individuals are identified to Medicare Australia as Healthcare Provider Individuals by that identified and authorised data source

and who are then known as HPI-DS to Medicare Australia in its role as service operator of the HI Service.

The *Healthcare Identifiers Act 2010* (Cth) and the National Partnership Agreement signed by the COAG jurisdictions in November 2009 provide that Medicare Australia be appointed the service operator for the HI Service.

This CP should be read in conjunction with the :

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

Terminology

Please refer to the documents listed below for definitions relevant to this CP.

In this CP, the order of priority for determining the meaning of a specific term is:

1. *Healthcare Identifiers Act 2010* (Cth) (<http://www.comlaw.gov.au>)
2. Healthcare Identifiers Regulations 2010 (Cth) (<http://www.comlaw.gov.au>)

3. Health Practitioner Regulations National Law Act 2009 / 2010 (known as National Law) of each State and Territory and related Commonwealth Acts and Regulations (<http://www.ahpra.gov.au/en/Legislation-and-Publications/Legislation.aspx>)
4. National Partnership Agreement 2009 (the COAG agreement)
5. the Healthcare Identifiers Service Glossary of Terms and Conditions
<http://www.nehta.gov.au/connecting-australia/healthcare-identifiers>
6. Medicare Australia PKI Gatekeeper documents, including the Medicare Australia Health Sector PKI Glossary
(<http://www.medicareaustralia.gov.au/provider/business/online/register/policy.jsp>)

Individual Certificate for Healthcare Provider Individual identified by an identified and authorised data source means an Individual Certificate issued by Medicare Australia under this CP to an Individual who is registered with, or known to, Medicare Australia in its role as the service operator of the HI Service.

Individuals issued with an Individual Certificate for Healthcare Provider Individual identified by an authorised data source (HPI-DS), will at registration with the HI Service, be recorded with their identifying Healthcare Provider Individual Identifier (however described) as issued by the data source that provides the identifier (and other information) to Medicare Australia as the HI Service service operator.

Certificate Policy Clauses

CP Identification

Certificates issued under this CP shall bear the Policy OID:

1.2.36.174030967.1.7.1.1

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

1. INTRODUCTION

This is the Certificate Policy (CP) for individual certificates provided by Medicare Australia as service operator of the Healthcare Identifiers Service (HI Service) to individuals who are assigned Healthcare Provider Individual roles by an authorised data source and who are known in the HI Service and registered by the HI Service service operator in the HI Service in accordance with that role.

Such individuals are known as Healthcare Provider Individuals via data source (HPIDS) and are Subscribers for the purposes of the CP.

The certificates are provided on a Secure Token to Subscribers.

The meaning of an Individual Certificate for the Healthcare Identifier Service (HI Service) issued by Medicare Australia 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 HI Service Healthcare Provider Individual via data source (HPIDS)) has been issued with a registration number (however described) by a data source and through this registration with the data source is known to Medicare Australia in its role as the service operator of the HI Service, through Application and / or relationship.

The Relationship Organisation (RO) for this CP is Medicare Australia as the service operator for the HI Service.

The Relationship Organisation Unit (ROU) is the HI Service service operator area in Medicare Australia responsible for undertaking the Application registration.

The Relationship Organisation Unit Operators (ROUOs) are Medicare Australia personnel working in the ROU.

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 Organisation Certification Authority Certification Practice Statement (Medicare Australia OCA CPS) and the Medicare Australia

Organisation Certification Authority Certificate Policy (Medicare Australia OCA CP) for further information on applicable practices and procedures for Certificates issued under this CP, located at www.medicareaustralia.gov.au.

1.1.2. Relationship Organisation

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

1.1.3. Relationship Organisation Unit

There is a separately identified Relationship Organisation Unit (ROU) within the Medicare Australia RO for the HI Service Community of Interest (Col) for Healthcare Individual Providers via data source (HPIDS) 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 Medicare Australia HI Service Col.

ROUOs within the Medicare Australia HI Service Col are not Certificate Controllers.

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

1.1.6. Subscribers

Subscribers under this CP include Healthcare Provider Individuals via data source as identified and defined under the *Healthcare Identifiers Act 2010* by a data source that is identified and authorised as a data source under the *Healthcare Identifiers Act 2010* and the Healthcare Identifiers Regulations 2010.

- a) A Subscriber under this CP will be an Individual who is registered and allocated a number (for example, a registration number (however described)) by an identified and authorised data source, in accordance with the National Law (Health Practitioner Regulation National Law Act 2009, and

- b) will be identified to Medicare Australia as the service operator of the HI Service by that data source.

The Subscriber (the HPI-DS) is therefore known to Medicare Australia in Medicare Australia's role as the HI Service service operator for the HI Service and is able to be included in the HPI-DS Community of Interest (CofI) as a Subscriber for an Individual Certificate for HPI-DS under this CP.

There is a Subscriber agreement under this CP, known as the *Individual Keys and Certificates 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 HI Service operator and receiver of transactions secured using the HI Service Individual Keys and Certificates.
- b) Individuals assigned a healthcare identifier as a healthcare provider organisation or a healthcare provider individual, in accordance with and as authorised by the *Healthcare Identifiers Act 2010* and Healthcare Identifier Regulations 2010 and who transact with the HI Service and Relying Parties using the Individual Keys and Certificates.
- c) Individuals assigned a registration number as a Responsible Officer (RO) or an Organisation Maintenance Officer (OMO) in accordance with and as authorised by the *Healthcare Identifiers Act 2010* and Healthcare Identifier Regulations 2010 and who transact with the HI Services and Relying Parties using the Individual Keys and Certificates.

There is no Relying Party Agreement under this CP.

Parties who rely on Certificates issued under this CP and undertake transactions that are not authorised or approved by the *Healthcare Identifiers Act 2010*, the Healthcare Identifiers Regulations 2010, rely on such Certificates at their own risk.

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/pki specifying authorised usage relating to a transaction type, and therefore undertake transactions that are not authorised or approved by Medicare Australia as HI Service service operator of the HI Service, 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 Individuals using the HI Service to conduct transactions with Medicare Australia as the HI Service service operator or other Individuals or entities as authorised or approved by the *Healthcare Identifiers Act 2010* and Healthcare Identifiers Regulations 2010.

1.2.2 Prohibited Certificate Uses

There are no prohibited certificate uses.

Use of Certificates outside of the Medicare Australia Relationship Organisation Cols for the HI Service is not supported.

Parties using Individual Certificates for any transaction other than an authorised or approved transaction do so at their own risk.

1.3 Definitions and Acronyms

Definitions and Acronyms are in the:

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

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) as an Healthcare Provider Individual via data source (HPI-DS) according to Medicare Australia, as HI Service service operator, application and registration processes for HI Service Individuals.

2.2 Identification and authentication of the Subscriber at registration

Subscribers under this CP will be identified and authenticated, at the time of their application for registration (however described), as an Healthcare Provider Individual via data source (HPI-DS) by Medicare Australia as service operator of the HI Service, in accordance with trusted practices that may include, but not be limited to:

- a) receipt of data from data sources, identified and authorised as data sources by the *Healthcare Identifiers Act 2010* or the Healthcare Identifier Regulations 2010 and the National Law (Health Practitioner Regulation National Law Act 2009)
- b) receipt of Applications for registration as a Healthcare Provider Individual via data source (HPI-DS);
- c) assessment of Applications and associated documents;
- d) processing and administering in accordance with the *Healthcare Identifiers Act 2010* and the Healthcare Identifiers Regulations 2010;
- e) association with NEHTA and the Department of Health and Ageing (DoHA) (where required);
- f) allocation of HPI-DS Individual Certificate registration number(s) (where required) and registration on Medicare Australia and HI Service systems (however described) and where required.

2.3 Identification and authentication of the Subscriber at renewal

Subscribers (HPI-DS) under this CP shall be identified and authenticated and the Certificate renewed provided that:

- a) the HPI-DS registration or other status with the relevant data source has not changed, and
- b) the HPI-DS registration or other status with the HI Service has not changed, and
- c) Medicare Australia, as service operator of the HI Service, is satisfied that such registration or other status 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 HPI-DS; 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

Where an individual is a HPI-DS and identified as such by operation of:

- the *Healthcare Identifiers Act 2010*, and/or
- the Healthcare Identifier Regulations 2010, and/or
- the National Law (Health Practitioner Regulation National Law Act 2009)

Medicare Australia may consider that the individual be enrolled for Certificates by Certificate Controllers on the basis of being known to Medicare Australia (in its role as the HI Service operator) as an HPI-DS.

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 the HPI-DS's de-registration for HI Service purposes (however described);

- c) in the event the HPI-DS's registration number(s) or other numbers (where applicable) 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.

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 operating as the service operator for the HI Service.

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 provide 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.

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

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

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	1.2.36.174030967.1.7.1.1		
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		

Field	Content	Mandatory	Critical*
2.5.1.4. CPS URI	http://www.medicareaustralia.gov.au/		
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=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 ¹			
3.0.1 Generic IA5 String: RA Number (OID=1.2.36.73665175.1.10009)	< RA Number >	M	

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)	Medicare Australia	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 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	
1.6.4. 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			

¹ 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*
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	1.2.36.174030967.1.7.1.1		
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-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= 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 ²			
3.0.1 Generic IA5 String: RA Number (OID=1.2.36.73665175.1.10 009)	< RA Number >	O	

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

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)			