

Short Form Certificate Policy



Australian Government

Medicare Australia

Medicare Australia Site Certificates Communities of Interest Certificate Policy v 2.2

(5 Year Duration)

June 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, 2601

Contact (for any matters concerning this document)

National Manager
 EClaiming and eHealth
 PO Box 1001 Tuggeranong DC ACT 2901
 AUSTRALIA

Version History

Doc Version	Status	Date of Issue	Issue By	Comments
1.0	DRAFT	15 Sept 2006	Stephen Wilson	Initial draft derived from Medicare Own
1.1	DRAFT	19 Sept 2006	Stephen Wilson	Changes after internal team review before legal review
1.2	DRAFT	10 OCTOBER 2006	LYNN DU MOULIN	OLC review and amendments; changes to omit references to 'online claiming'; CP to apply to site certificates without limitation as to Medicare Australia programs approved to be accessible by practices using the site certificate.
1.3	DRAFT	12 October 2006	John Brewer, Lynn Du Moulin, Michael Tindall	Accepted and modified OLC suggestions and developed draft for final OLC review and edit definition of practice
1.4	Final	20 OCTOBER 2006	Lynn Du Moulin John Brewer	OLC review; edit to definition of practice Changes Accepted as new version 1.4 and as final
1.5	Draft	14 November 2006	Michael Tindall	Redraft to include DHS communities of interest
1.5	Draft	16 November 2006	Lynn Du Moulin	Revision and redraft to: <ul style="list-style-type: none"> • Include Human Services Col and other Cols in the Medicare Australia Health Sector PKI; • Identify and separate legal entity (practice /organisation) from the site (location); • Related amendments
1.5	Final	20 November	John Brewer	Accepted all draft changes by Lynn and

		2006		Michael and make 1.5 final version
1.6	Draft	1 May 2008	P Sorensen	Revised Draft 2008
1.7	Draft	20 May 2008	P Sorensen	Revised after comments from Lynn Du Moulin
1.8	Draft	13 June 2008	P Sorensen	Revised after comments from Lynn Du Moulin
1.9	Draft	16 June 2008	P Sorensen	Revised to include liability references
1.9.1	Draft	13 April 2009	J Wong	Added HPI-O
1.9.2	Draft	July 2009	M Mynott	Revised to update terminology and HI references.
1.9.3	Draft	April 2010	P Sorensen	AGIMO Feedback to be Included
1.9.2	Draft	June 2010	J Hunt	Changed HPI-O in Certificate profile to Location ID, removed wording 'containing HPI-O number' from 2.6.2
1.9.4	Draft	18 August 2010	Lynn Du Moulin	Accepted Sorensen / Hunt amendments Revised CP to refer to Seed Organisation sites in the Healthcare Identifier Service
1.9.5	Draft Final	20 August 2010	Lynn Du Moulin	Review Sorensen comments on 18 August 2010 draft Accept amendments Accept OID change (Wong) to 1.6.1.2 and made OID changes in Part 6
1.9.5	Draft final	23 August 2010	Paul Sorensen	Review and accept changes; minor amendments
v.2.0	FINAL	23-24 August 2010	Lynn Du Moulin	Accept amendments and final review
v.2.1	Draft final	27 May 2011	Lynn Du Moulin	Revise CP to include Contracted Service Providers (<i>Healthcare Identifiers Act 2010</i>)
v.2.2	FINAL	30 June 2011	Lynn Du Moulin and DLA Piper	Revise CP to include Contracted Service Providers (<i>Healthcare Identifiers Act 2010</i>) plus final review from DLA Piper.

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

 General Manager
 Health eBusiness Division
 Medicare Australia

Date: _____

Introduction

This is the Certificate Policy for Site (previously known as Location) Certificates issued to practices and entities known to Medicare Australia (for example, government departments and agencies and health and welfare services providers). It enables them to conduct secure transactions and data exchange with Medicare Australia and other parties in relation to programs authorised or approved by Medicare Australia or within an entity's Community of Interest recognised by Medicare Australia.

This CP should be read in conjunction with the:

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

Terminology

Site Certificate means a Certificate issued under this CP.

Site means:

- a) the physical location of any practice registered by Medicare Australia as a Medicare Australia program or service as eligible for Medicare Australia Site Certificates under this CP. The practice may be referred to as a Registered Medicare Australia Practice or healthcare practice and includes Pharmacies* and aged care providers, or
- b) any site of an entity, where that entity:
 - is recognised by Medicare Australia as being a member of a Medicare Australia recognised Community of Interest. For example, that entity is a seed organisation or a Contracted Service Provider (CSP) and recognised as such under the *Healthcare Identifiers Act 2010*; and
 - is known to Medicare Australia and Medicare Australia is the Relationship Organisation.

The commonly used term 'Location Certificate' has the same meaning as Site Certificate.

*Pharmacies who participate in online claiming for PBS will normally be issued with a site certificate under the *Pharmacy and PBS Community of Interest Site Certificate Certificate Policy*.

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>)

Certificate Policy Clauses

CP Identification

Certificates issued under this CP shall bear the Policy OID:

1.2.36.174030967.1.6.1.2

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

1. INTRODUCTION

This is the Certificate Policy (CP) for Site Certificates provided by Medicare Australia as the Relationship Organisation (Medicare Australia RO) for practices and entities (however described and defined) who wish to undertake secure electronic transmissions at Sites:

- with Medicare Australia, and /or
- to access data held by Medicare Australia; and / or
- with Medicare Australia as service operator of the Healthcare Identifiers (HI) Service; and / or
- with Relying Parties within the Medicare Australia RO Communities of Interest (Cols); and / or
- within this Site Certificate CP Col.

Such Sites are known as Medicare Australia RO Sites and are Subscribers for the purposes of this CP.

The Site Certificates are provided on a CD to Subscribers who are responsible for uploading the Certificates onto the Subscriber’s client operating system.

The meaning of a Medicare Australia Site 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 Site) is:

- (a) known to Medicare Australia through Application and / or relationship;
- (b) issued with a HI Service registration number in the case of a seed organisation;
- (c) is identified as a Contracted Service Provider (CSP) in accordance with the *Healthcare Identifiers Act 2010*; or
- (d) is otherwise known to Medicare Australia in its role as the service operator of the HI Service.

The Relationship Organisation Units (ROU) are:

- a program area(s) in Medicare Australia responsible for programs accessible by Sites using Site Certificates; and
- Medicare Australia, in its role as the Healthcare Identifiers Service (HI Service) service operator, appointed as HI Service operator under the *Healthcare Identifiers Act 2010*.

The Relationship Organisation Unit Operators (ROUOs) are:

- Medicare Australia personnel who accept and manage the registration of practices or other entities for Site Certificates;
- personnel in Medicare Australia acting in its role as service operator of the HI Service who accept and manage registration of seed organisations for Site Certificates;
- authorised personnel (known as Responsible Officers under the *Healthcare Identifiers Act 2010*) of entities who are members of the HI Service Community of Interest who accept and manage the registration of seed organisations identified as such under the *Healthcare Identifiers Act 2010*; or
- those authorised under the *Healthcare Identifiers Act 2010* to identify Contracted Service Providers for the purposes set out in the *Healthcare Identifiers Act 2010*, from time to time.

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), Medicare Australia Root 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.

1.1.2. Relationship Organisation

Medicare Australia or Medicare Australia as the HI 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 (CoI) in the Health Sector PKI operated by Medicare Australia. For example, the various program areas in Medicare Australia are the ROUs for the participating sites, such as Medicare provider sites, ACIR sites, hospital sites etc.

There is a separate ROU within the Medicare Australia RO for the HI Service Community of Interest (Col) for seed organisation sites 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) who are Medicare Australia personnel within the relevant program Col are located within Medicare Australia.

ROUOs who are authorised personnel of an entity within a relevant Col are located within that entity. Authorised personnel may include Responsible Officers, identified as such by Application and / or registration and so identified in accordance with the *Healthcare Identifiers Act 2010*.

ROUOs within any Col are not Certificate Controllers in accordance with clause 1.1.4 of this CP.

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

1.1.6. Subscribers

All Subscribers for Site Certificates shall be either:

- practices registered with a Medicare Australia program and known to Medicare Australia as such according to an application for participation in a Medicare Australia program;
- an entity which is known to Medicare Australia by Application and / or registration and is therefore a member of a recognised Medicare Australia Community of Interest; or
- an entity identified as a Contracted Service Provider (CSP) in accordance with the *Healthcare Identifiers Act 2010*.

A person, who is authorised by a practice or entity to bind the practice or entity, or the Responsible Officer of a seed organisation, must enter into the Subscriber agreement for a Site Certificate which is known as the *Medicare Australia Site Certificate Terms and Conditions of Use*.

The Subscriber is bound by these terms and conditions when the Subscriber conducts their first transaction using the Site Certificate and Keys.

1.1.7. Relying Parties

In relation to the Medicare Australia program COIs, the Relying Party under this CP is Medicare Australia, as receiver of transactions secured using the Site Certificates.

Relying Parties under this CP are:

- a) Medicare Australia, as receiver of transactions secured using the Site Certificates and Keys.
- b) practices and entities known to Medicare Australia and who are in a recognised Medicare Australia RO Col, being the other practice or entity in the Col which conducts and receives transactions secured using the Site Certificates and Keys.
- c) individuals who are recognised Medicare Australia RO Individuals and who receive and conduct transactions secured using the Site Certificates and Keys in conjunction with their Individual Certificates and Keys.

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 Medicare Australia as the RO or, where relevant, by the *Healthcare Identifiers Act 2010* and 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, rely on such certificates at their own risk.

1.2 Certificate Use

1.2.1 Appropriate Certificate Uses

Key Pairs and Certificates issued under this CP are to be used by Sites conducting transactions with Medicare Australia for programs and services authorised or approved by Medicare Australia and where relevant, the *Healthcare Identifiers Act 2010* and Healthcare Identifier Regulations 2010

1.2.2 Prohibited Certificate Uses

There are no prohibited certificate uses.

Use of Site Certificates outside the Medicare Australia RO Cols is not supported.

Parties using Site 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 will be named (and the uniqueness of their names will be assured) according to Medicare Australia through its relationship with the Subscriber. This may include the name by which Medicare Australia has recognised the entity as a member of a Col or the name under which the entity is registered as a Subscriber.

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 as a Site by Medicare Australia in accordance with trusted practices that may include, but not be limited to:

- a) Medicare Australia ROUs responsible for registering practices for Medicare Australia programs and services; and / or
- b) In each Col, the entity's ROU responsible for registering that entity for a Site Certificate.

2.3 Identification and authentication of the Subscriber at renewal

Subscribers under this CP shall be identified and authenticated and the Certificate renewed provided that:

- if the Site is a registered Medicare Australia practice, its registration status with the relevant ROU has not changed, or
- if the Site is an entity recognised by Medicare Australia in a Medicare Australia Col, Medicare Australia is satisfied that its registration 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:

- ROUOs in the event that the Subscriber becomes ineligible to remain as a registered Medicare Australia practice or entity recognised by Medicare Australia as a member of a Medicare Australia Col; or
- the Subscriber; or
- Certificate Controllers.

3. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

3.1. Certificate creation

3.1.1. Enrolment process and responsibilities

Where a Site is a registered Medicare Australia practice, the Site may be enrolled for Certificates by Certificate Controllers on the basis of that registration.

Where a Site is not a registered Medicare Australia practice, the Site may apply to the relevant ROU for the Col of the Medicare Australia program or service to be registered for that program or service and to be enrolled for Site Certificates when registration as a registered Medicare Australia practice occurs on the basis of that registration.

Where a Site is not a registered Medicare Australia practice, the Site, being a member of a Medicare Australia Col and responsible for that Site, may apply to the Medicare Australia RO Certificate Controllers to be enrolled for Site Certificates.

All applications are the responsibility of the Site through its authorised contact person (however described). A Responsible Officer will be the Authorised contact person for a seed organisation, in accordance with the *Healthcare Identifiers Act 2010*.

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 and Certificates issued under this CP shall be generated by a Certificate Controller using accredited software.

The signing key and encryption key shall be stored in a password protected PKCS#12 file separate from the encryption key and Certificate. These PKCS#12 files are stored in electronic medium¹ and distributed as instructed by the ROUO.

A PIC (Personal Identification Code) to access the keys and Certificates will be generated and distributed separately to the Subscriber.

3.3. Certificate renewal

Certificates issued under this CP may be renewed automatically by the Certificate Controllers. This is at the discretion of Medicare Australia.

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 Site Certificate;
- b) in the event the site (however described) is de-registered, whether in relation to participation in any Medicare Australia program or not;
- c) in the event any approvals (however described) relating to the Site are cancelled by Medicare Australia;
- d) in the event any Site identification number(s) (however described) are cancelled by Medicare Australia or other organisation or body authorised to cancel such number(s); or
- e) in the event the Site ceases to exist or be recognised by Medicare Australia or ceases to be a member of a Medicare Australia RO Col.

¹ 'electronic medium' includes CD or other medium in which data can be stored electronically.

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.

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 – Site 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). YYMMDDHHMSSZ 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. YYMMDDHHMSSZ 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. Locality (L)	<Suburb Name>	M	
1.6.4. Organization (O)	<Trading Name <Locality>>	M	
1.6.5. Organisation Unit (OU)	<Organisation Unit <Locality>>	O	
1.6.6. Common Name (CN)	<Trading Name <Locality>> :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	1.2.36.174030967.1.6.1.2		
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.		

Field	Content	Mandatory	Critical*
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.pfx		
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=1.2.36.73665175.1.10009)	< RA Number >	M	
3.0.2 Generic IA5 String: Healthcare Provider Identifier (OID=1.2.36.17403096 7.0.4)	< Healthcare Provider Identifier >	O	
3.0.3 Generic IA5 String: Medicare Identifier (OID=1.2.36.17403096 7.0.5)	< Medicare Identifier >	O	
3.0.4 Generic IA5 String: Location ID (OID=1.2.36.17403096 7.1.6.2.1)	< Location ID >	O	
3.0.5 Generic IA5 String: Pharmacy Approval Number (OID=1.2.36.17403096 7.0.6)	< Pharmacy Approval Number >	O	

6.2 Certificate profile –Site 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	

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

Medicare Australia Short Form CP – Medicare Australia Site Certificate CP v2.2 (including seed organisations) and CSPs

Field	Content	Mandatory	Critical*
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	
1.6.3. Locality (L)	<Suburb Name>	M	
1.6.4. Organization (O)	<Trading Name <Locality>>	M	
1.6.5. Organisation Unit (OU)	<Organisation Unit <Locality>>	O	
1.6.6. Common Name (CN)	<Trading Name <Locality>> :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	NOT 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	1.2.36.174030967.1.6.1.2		
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-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.ppk		
2.9 CRL Distribution Point			
2.9.1 URL	http://www.certificates-australia.com.au/general/cert_search_health.shtml		Non-Critical

Field	Content	Mandatory	Critical*
3.0 Other Fields - Generic ³			
3.0.1 Generic IA5 String: RA Number (OID=1.2.36.73665175.1.10 009)	< RA Number >	M	
3.0.2 Generic IA5 String: Healthcare Provider Identifier (OID=1.2.36.174030967.0.4)	< Healthcare Provider Identifier >	O	
3.0.3 Generic IA5 String: Medicare Identifier (OID=1.2.36.174030967.0.5)	< Medicare Identifier >	O	
3.0.4 Generic IA5 String: Location ID (OID=1.2.36.174030967.1.6 .2.1)	< Location ID >	O	
3.0.4 Generic IA5 String: Pharmacy Approval Number (OID=1.2.36.174030967.0.6)	< Pharmacy Approval Number >	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		

³ These Certificate extension OID references are expected to be common to all CoI Certificate Policies, and may have applicability to this CoI.

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)			