

# Short Form Certificate Policy



**Australian Government**

---

**Medicare Australia**

## **Medicare Australia – Site Certificates for Pharmacy & PBS Community of Interest Certificate Policy v2.9.8**

**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, Media, Marketing and Communications Branch, Medicare Australia National Office, PO Box 1001 Tuggeranong DC ACT 2901.

### Contact:

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

### Version History

Doc Version	Status	Date of Issue	Issue By	Comments
2.8	Final	21 February 2007	Lynn Du Moulin	Approved version released to Medicare Australia Intranet site
2.9	Draft	1 May 2007	P Sorensen	Revised Draft (incl changes for 5 yr certs)
2.9.1	Draft	20 May 2008	P Sorensen	Revised after comments from Lynn Du Moulin
2.9.2	Draft	13 June 2008	P Sorensen	Revised after further comments from Lynn Du Moulin
2.9.3	Draft	16 June 2008	P Sorensen	Revised to include liability references
2.9.4	Draft	July 2009	M Mynott	Revised to clearly reflect Site Certificate requirements.
2.9.5	Draft	March 2010	M Mynott	Added HPI-O
2.9.6	Draft	April 2010	P Sorensen	AGIMO feedback to be included
2.9.7	Draft	June 2010	J Hunt	Changed HPI-O in Certificate profile to Location ID, removed wording 'containing HPI-O number' from 2.6.2
2.9.8	FINAL	30 June 2011	DLA Piper	Final review

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

\_\_\_\_\_  
General Manager  
Health e-Business Division  
Medicare Australia

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

## **Introduction-**

This document is the Certificate Policy (CP) for Site Certificates for Pharmacy and PBS (Site Certificates) issued to the Community of Interest of Approved Pharmacies at pharmacy locations.

The document is structured and numbered according to the *Gatekeeper Short Form Certificate Policy Template*.

This Certificate Policy (CP) should be read in conjunction with the:

- Medicare Australia Root Certificate 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 Certificates for Pharmacy and PBS** means the certificate issued under this Medicare Australia Certificate Policy by the Medicare Australia Organisation Certification Authority (Medicare Australia OCA) in accordance with the processes and procedures under the Medicare Australia OCA CPS. It is referred to as a 'Certificate' or 'Site Certificate' in this CP. The Certificate will be a soft certificate.

**PBPB** means Pharmaceutical Benefits Programs Branch (however described) of Medicare Australia.

**PBS** means the Pharmaceutical Benefits Scheme established under the *National Health Act 1953* (Commonwealth).

## Certificate Policy Clauses

### CP Identification

Certificates issued under this CP shall bear the Policy OID:

#### 1.2.36.174030967.1.3.1.2

(where “174030967” is the last 9 digits of Medicare Australia’s ABN)

**Note:** Any OID prefixed by the numbers “1.2.36.174030967.1.3” will pertain to this Community of Interest.

## 1. INTRODUCTION

### 1.1 PKI Participants

Refer to the Medicare Australia OCA CPS at clause 1.3 for further information on Health Sector 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 Certificate 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) for further information on the 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 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 the Col.

The PBPB is a ROU for the PBS 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 and Certificate Requestors**

Relationship Organisation Unit Operators (ROUOs) are Medicare Australia personnel. ROUOs may be located within the online claiming for PBS Col and are located within the PBPB.

ROUOs within the online claiming for PBPB 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.

For PBS, PBPB has services provided to it by the eBusiness Service Centre in Medicare Australia. For the purposes of receiving applications for online claiming for PBS and requesting certificates from the Certificate Controllers, the eBusiness Services Centre provides ROU and ROUO services to PBPB.

### **1.1.6. Subscribers**

Each Subscriber under this CP is a business entity known to Medicare Australia as an Approved Pharmacy (**Approved Pharmacy**).

Each Subscriber under this CP must be an Approved Pharmacy, approved in accordance with the requirements of the *National Health Act 1953*.

Approved Pharmacies must make a written application to Medicare Australia to participate in online claiming for PBS using the *online claiming for PBS Participation Application and Terms and Conditions*.

There is a Subscriber agreement under this CP, known as the *Medicare Australia Site Certificate Terms and Conditions*.

A person, who is authorised by the entity, 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 his or her first transaction using the Site Certificates and Keys.

For the purposes of this CP, Approved Pharmacy includes a pharmacy that has made a valid application for approval and is awaiting approval as an Approved Pharmacy.

### **1.1.7. Relying Parties**

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

In relation to entities known to Medicare Australia and who are in a recognised Medicare Australia Col, the Relying Party under this CP is the other entity in the Col who is the receiver of transactions secured using the Site Certificates.

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 Sites conducting secure transactions with Medicare Australia for programs and services authorised or approved by Medicare Australia.

### **1.2.2 Prohibited Certificate Use**

There are no prohibited certificate uses. Parties using the Site Certificates for any transaction other than transactions authorised or approved by Medicare Australia do so at their own risk.

## **1.3 Definitions and Acronyms**

Definitions and Acronyms are in the *Health Sector PKI Glossary* at [www.medicareaustralia.gov.au/pki](http://www.medicareaustralia.gov.au/pki)

## **2 IDENTIFICATION AND AUTHENTICATION OF SUBJECTS**

### **2.1 Naming of Subjects**

Subscribers (are termed 'Certificate Subjects' in the x.509 definition and referred to in this CP as Approved Pharmacies) under this CP shall be named (and the uniqueness of their names shall be assured) according to Medicare Australia's registration process.

### **2.2 Identification and authentication of Subscribers at registration**

Subscribers (Approved Pharmacies) under this CP will be identified and authenticated at the time of their application for registration through:

- a) the application process to be approved as an Approved Pharmacy; and
- b) on approval as an Approved Pharmacy, and allocation of an approval number.

The approval of a pharmacy as an Approved Pharmacy involves the completion of an application form and referral to the Australian Community Pharmacy Authority for assessment. The assessment and subsequent approval by Medicare Australia establishes the identity of the Approved Pharmacy and authenticates it for participating in the Pharmaceutical Benefits Scheme.

## **2.3 Identification and authentication of Subscribers at renewal**

Subscribers (Approved Pharmacies) under this CP shall be identified and authenticated and the Certificate renewed provided that:

- a) the pharmacy is an Approved Pharmacy; and
- b) the Approved Pharmacy's registration status has not changed.

The renewal of Pharmacies involves the completion of an application form and referral to the Australian Community Pharmacy Authority for assessment. The assessment and subsequent approval by Medicare Australia establishes the identify of the Pharmacy and authenticates them for continued participation in the Pharmaceutical Benefits Scheme.

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

Revocation of certificates under this CP shall only be requested in writing by Certificate Controllers and / or ROUOs of the online claiming for PBS Col, when an Approved Pharmacy either:

- has its approval as an Approved Pharmacy revoked; or
- by the Subscriber by written notice.

.Where an Approved Pharmacy has its approval suspended, the Certificate shall remain valid for the period the Approval Pharmacy's approval is under suspension, provided the Certificate does not expire during the Approved Pharmacy's suspension as an Approved Pharmacy.

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

### **3.1. Certificate creation**

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

Enrolment and registration is the responsibility of the ROUOs and the Certificate Controllers.

Applications to participate in online claiming for PBS is the responsibility of the person(s) associated with the approval number for the Approved Pharmacy.

Approved Pharmacies are enrolled automatically for Site Certificates for Pharmacy and PBS when they register with online claiming for PBS by completing and signing the *online claiming for PBS Pharmacy Application and Terms and Conditions*

The ROUO is responsible for registering the application for the Site Certificate for the Approved Pharmacy.

#### **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 also be published in the Healthcare Public Directory.

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

Key Pairs and Certificates issued under this CP must only be used in connection with each Subscriber.

Each Certificate issued under this CP is always associated with the Approved Pharmacy, and must never be used outside of that context.

#### **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 and Certificate shall be stored in a password protected PKCS#12 (P12 file) separate to the encryption key and Certificate. These P12 files (including the trust chain) will be stored in electronic medium<sup>1</sup> and distributed as instructed by the ROUO.

A passphrase to access the keys and Certificates will be generated and distributed separately to the Subscriber.

### **3.3. Certificate renewal**

Certificates issued under this CP shall be renewed automatically by the authorised officer of PBPB of Medicare Australia provided the status of the Subscriber is unchanged. Refer to clause 2.3 for details of identification and authentication at renewal.

### **3.4. Certificate revocation**

Certificates issued under this CP shall 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 Approved Pharmacy fails to comply with this CP and the Medicare Australia OCA CPS; or
- c) in the event the Approved Pharmacy's approval as an Approved Pharmacy is revoked.

The Approved Pharmacy must promptly notify Medicare Australia of the possible loss, destruction or theft of the Site Certificate, to enable revocation to be processed in a timely manner.

ROUOs and Certificate Controllers may take into account the Medicare Australia OCA CPS, any Medicare Australia and any PBPB business continuity and disaster recovery plan in considering whether to revoke Certificates in response to a request from an Approved Pharmacy.

### **3.5 Certificate status services**

---

<sup>1</sup> 'electronic medium' includes, CD or other medium in which data can be stored electronically.

### **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**

Under this CP, Relationship Organisation Unit Operators (ROUOs) must process applications for Certificates by Approved Pharmacies and other written administrative procedures (where applicable).

### **4.1 Personnel controls**

All ROUOs under this CP shall be authorised officers of the PBPB of Medicare Australia for the purposes of providing services under this CP to PBPB.

ROUOs under this CP are not Registration Authority Officers (RAOs) under a Gatekeeper accredited PKI.

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

ROUOs will communicate Certificate requests to Certificate Controllers 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 ROU termination or transfer**

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 ROU through the PBPB and provide for a replacement agency as the successor ROU in accordance with policy as determined by the government and implemented in accordance with legislation passed by the Commonwealth Parliament.

## **4.6 ROU Termination**

An ROUO is terminated through:

- termination of the ROUO's employment with Medicare Australia; or
- termination of the ROUO's representation as a ROUO by the PBPB of Medicare Australia.

PBPB of Medicare Australia must ensure that the person who has ceased to be an ROUO cannot make certificate requests or carry out ROUO functions.

## **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/pki](http://www.medicareaustralia.gov.au/pki).

### **5.2 Legal Matters**

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

#### **5.2.1 Limitation 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 – Medicare Australia Site Certificate for Pharmacy & PBS 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. Locality (L)	<Suburb Name>	M	
1.6.4. Organization (O)	<Trading Name <Locality>>	M	
1.6.5. Organisation Unit (OU)	<Organisational 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			Non-Critical
2.1. Authority Key Identifier		M	
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	
2.3. Key Usage		M	
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

Medicare Australia Gatekeeper Short Form CP – Site Certificates for Pharmacy & PBS Community of Interest v2.9.8

Field	Content	Mandatory	Critical*
2.5. Certificate Policies			Non-Critical
2.5.1. Policy Identifier	1.2.36.174030967.1.3.1.2		
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			Critical
2.7.1. Subject Type	Not CA		
2.7.2. Path Length Constraint	Not present		
2.8. Authority Information Access			Non-Critical
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)		
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			Non-Critical
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>		
3.0 Other Fields - Generic <sup>2</sup>			
3.0.1 Generic IA5 String: "Pharmacy Approval Number" (OID=1.2.36.174030967.1.3.2.1)	<Pharmacy Approval number >	O	
3.0.4 Generic IA5 String: Location ID (OID=1.2.36.174030967.1.6.2.1) <<check>>	<Location ID >	O	
3.0.3 Generic IA5 String: RA Number (OID=1.2.36.73665175.1.10009)	< RA Number >	M	

## 6.2 Certificate profile – Medicare Australia Site Certificate for Pharmacy & PBS 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,	M	

<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.

Medicare Australia Gatekeeper Short Form CP – Site Certificates for Pharmacy & PBS Community of Interest v2.9.8

Field	Content	Mandatory	Critical*
	SHA-1 hashing algorithm using the RSA signing algorithm.		
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 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))	<Organisational 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	1.2.36.174030967.1.3.1.2		
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	

Medicare Australia Gatekeeper Short Form CP – Site Certificates for Pharmacy & PBS Community of Interest v2.9.8

Field	Content	Mandatory	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>3</sup>			
3.0.1 Generic IA5 String: "Pharmacy Approval Number" (OID=1.2.36.174030967.1.3.2.1)	<Pharmacy Approval number >	O	
3.0.4 Generic IA5 String: Location ID (OID=1.2.36.174030967.1.6.2.1) <<check>>	< Location ID >	O	
3.0.3 Generic IA5 String: RA Number (OID=1.2.36.73665175.1.10009)	< RA Number >	M	

### 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		

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

Medicare Australia Gatekeeper Short Form CP – Site Certificates for Pharmacy & PBS Community of Interest v2.9.8

---

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)			

