

# Short Form Certificate Policy



**Australian Government**

---

**Medicare Australia**

**Medicare Australia online claiming for PBS  
Community of Interest (CoI)  
for Site Certificates issued by the  
Medicare Australia Organisation Certification  
Authority (Medicare Australia OCA) v2.7**

---

**6 October 2006**

**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:**

Medicare Australia  
Locked Bag 6666  
Tuggeranong DC ACT 2901  
AUSTRALIA

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

\_\_\_\_\_ Date: \_\_\_\_\_  
General Manager or nominee, Information Technology and Services Division, Medicare Australia  
Representative

## Introduction

This document is the Certificate Policy (CP) for Medicare Australia Relationship Certificates (Site Certificates) issued to Approved Pharmacies at pharmacy locations in the online claiming for PBS Community of Interest, which is within the Pharmaceutical Benefits Branch (PBB) of Medicare Australia.

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

This online claiming for PBS CP (CP) should be read in conjunction with the Medicare Australia Organisation Certification Authority Certification Practice Statement (Medicare Australia OCA CPS).

The commencement date for this CP is: 1 September 2006.

## Terminology

**online claiming for PBS Site Certificate** means the certificate issued under this Medicare Australia online claiming for PBS 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' in this CP. The Certificate will be a soft certificate.

**PBB** means Pharmaceutical Benefits Branch 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 the online claiming for PBS Community of Interest.

## 1. INTRODUCTION

### 1.1 PKI Participants

Refer to the Medicare Australia OCA CPS at cl.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 Certificate Authority (Medicare Australia OCA).

Refer to the Medicare Australia Organisation Certification Authority Practice Statement (Medicare Australia OCA CPS) for further information on the applicable practices and procedures for Certificates issued under this CP.

#### **1.1.2. Relationship Organisation**

Medicare Australia 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.

The ROU has responsibilities in the CoI to manage Subscribers and the CoI.

The PBB is a ROU for the online claiming for PBS CoI.

#### **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.

Certificate Controllers may not be located within the PBB of Medicare Australia. Certificate Controllers are Medicare Australia personnel who may be located outside of the PBB

#### **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 CoI and are located within the PBB.

ROUOs within the online claiming for PBB CoI 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 online claiming for PBS, PBB 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 PBB.

The personnel providing these services to PBB in relation to online claiming for PBS are deemed to be ROUOs for the purposes of this CP. All references to ROUOs in this CP may be to personnel located within PBB or those located in the EBusiness Service Centre (or other service provider to PBB) who provide services under this CP to PBB.

#### **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*.

To become an Approved Pharmacy, a pharmacy makes an application to Medicare Australia. Approvals are given by Medicare Australia officers who are the delegates of the Secretary of the Department of Health and Ageing, holding delegations under the *National Act 1953* to grant approvals.

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 *online claiming for PBS Pharmacy Application and Terms and Conditions*.

The Subscriber is bound to the terms and conditions set out in the *online claiming for PBS Pharmacy Application and Terms and Conditions* by signing the Application that is part of the terms and conditions.

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.

#### **1.1.4. Relying Parties**

Relying Parties under this CP are any Approved Pharmacies who recognise the authority of Medicare Australia for transactions between Medicare Australia and the Approved Pharmacy.

There is no Relying Party Agreement under this CP.

Parties relying on certificates issued under this CP and who do not have a written agreement with Medicare Australia relating to transactions undertaken with 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 used to encrypt transactions to Medicare Australia from Approved Pharmacies and to Approved Pharmacies from Medicare Australia.

#### **1.2.2 Prohibited Certificate Use**

Key Pairs and Certificates issued under this CP should not to be used for transactions with any party other than Medicare Australia.

Where a Subscriber uses the Certificate for transactions with any party other than Medicare Australia, the Subscriber does so at the Subscriber's own risk.

### **1.3 Definitions and Acronyms**

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

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

### **2.1 Naming of Subjects**

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

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

The Subscribers (Approved Pharmacies) under this CP are identified and authenticated at registration through:

- a) the application process to be approved as an Approved Pharmacy;
- b) on approval as an Approved Pharmacy, allocation of an Approval Number, and
- c) the application process to participate in online claiming for PBS.

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

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

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

Note: all certificate renewals under this CP involve re-keying.

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

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

- a) has its approval as an Approved Pharmacy revoked; or
- b) is de-registered or cancelled from online claiming for PBS.

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

An Approved Pharmacy whose approval as an Approved Pharmacy is under suspension will not be able to undertake online claiming for PBS with Medicare Australia.

## **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.

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

The person(s) in relation to the pharmacy approval number is responsible for registration for online claiming for PBS.

The ROUO is responsible for registering the application for the Certificate for online claiming for PBS for the Approved Pharmacy.

The Certificate for an Approved Pharmacy shall be generated by two Certificate Controllers at two standard Certificate Controllers' workstations In accordance with the Medicare Australia OCA CPS.

#### **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's (Approved Pharmacy's) electronic transactions with Medicare Australia for online claiming for PBS.

Each Private Key associated with a Certificate issued under this CP is always associated with the Approved Pharmacy registered with online claiming for PBS, 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 the accredited software on instruction from the ROUOs for the online claiming for PBS CoI.

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

A passphrase to access the keys and Certificates will also be generated and posted separately to the nominated certificate holder for the Approved Pharmacy.

Note that the passphrase must be posted to the certificate holder.

On receipt of these P12 files, it is the responsibility of the Subscriber or the authorised agent of the Subscriber to install the keys and certificates into the intended environment.

### **3.3. Certificate renewal**

Certificates issued under this CP shall be renewed automatically by the authorised officer of PBB of Medicare Australia provided the status of the Subject (Approved Pharmacy) is unchanged. Refer to cl.2.3 for details of identification and authentication at renewal.

### **3.4. Certificate revocation**

Certificates issued under this CP shall be revoked under the following circumstances:

- after loss, destruction or theft of the private key;
- in the event of de-registration or cancellation by the ROUO of PBB of Medicare Australia of the Approved Pharmacy's participation in online claiming for PBS:

---

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

- where the Approved Pharmacy fails to comply with this CP and the Medicare Australia OCA CPS, or
- where 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 private key, to enable revocation to be requested in a timely manner.

ROUOs and Certificate Controllers must comply with the Medicare Australia OCA CPS, any Medicare Australia and any PBB business continuity and disaster recovery plan in revoking Certificates in response to a request from an Approved Pharmacy.

### **3.5 Certificate status services**

#### **3.5.1 Operational characteristics**

No stipulation.

#### **3.5.2 Service availability**

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

#### **3.5.3 Optional features**

No stipulation.

## **4. REGISTRATION OPERATIONAL CONTROLS**

Under this CP, Relationship Organisation Unit Operators (ROUOs) must process applications for Certificates by Approved Pharmacies in accordance with the business rules for online claiming for PBS and other written administrative procedures (where applicable).

### **4.1 Personnel controls**

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

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 Medicare Australia's 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**

Refer to cl.4.4 of the Medicare Australia OCA CPS for details of the business continuity of the RO (Medicare Australia).

#### **4.5 ROU termination or transfer**

The ROU (that is PBB) may be terminated, or its business responsibilities transferred, by a decision of the Commonwealth government, the relevant Minister, the Secretary to a Department or the Chief Executive Officer of Medicare Australia.

#### **4.6 ROUO 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 PBB of Medicare Australia.

PBB 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. CERTIFICATE, CRL AND OCSP PROFILES

### 5.1 Certificate profile – Medicare Australia Online Claiming for 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. 2 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))	<Trading Name <Locality>>	M	
1.6.6. Common Name (CN)	<Trading Name <Locality> :RA Number	M	
1.7. Subject Public Key Info	RSA Public Key of 1024 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	1.2.36.174030967.1.3.1.2		

Field	Content	Mandatory	Critical*
2.5.1.1. Policy Qualifier ID	User Notice		
2.5.1.2. User Notice	Certificates issued under this CP must 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	
2.7. 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	<a href="http://www.certificates-australia.com.au/cgi-bin/getcrl_health.pl?DN=cn%3DMedicare%20Australia%20Organisation%20Certification%20Authority%2Co%3DMedicare%20Australia%2Cc%3DAU">http://www.certificates-australia.com.au/cgi-bin/getcrl_health.pl?DN=cn%3DMedicare%20Australia%20Organisation%20Certification%20Authority%2Co%3DMedicare%20Australia%2Cc%3DAU</a>		Non-Critical
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	
3.0.3 Generic IA5 String: RA Number (OID=1.2.36.73665175.1.10009)	< RA Number >	M	

## 5.2 Certificate profile – Medicare Australia Online Claiming for 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, 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			

<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 – online claiming for PBS Community of Interest  
v2.7

Field	Content	Mandatory	Critical*
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. 2 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))	<Trading Name <Locality>>	M	
1.6.6. Common Name (CN)	<Trading Name <Locality> :RA Number	M	
1.7. Subject Public Key Info	RSA Public Key of 1024bits.	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 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	
2.7. Basic Constraints			Critical
2.7.1. Subject Type	Not CA		
2.7.2. Path Length Constraint	Not present		
2.8. Authority Information Access			
2.8.1. Access Description	Not present		
2.8.1.1. Access Method	On-line Certificate Status Protocol (1.3.6.1.5.5.7.4.1)		Non-Critical
2.8.1.2. Alternative Name	URL= <a href="http://ocsp.certificates-australia.com.au/maoca.pkx">http://ocsp.certificates-australia.com.au/maoca.pkx</a>		
2.9 CRL Distribution Point			
2.9.1 URL	<a href="http://www.certificates-australia.com.au/cgi-">http://www.certificates-australia.com.au/cgi-</a>		Non-Critical

Field	Content	Mandatory	Critical*
	<a href="bin/getcrl_health.pl?DN=cn%3DMedicare%20Australia%20Organisation%20Certification%20Authority%2Co%3DMedicare%20Australia%2Cc%3DAU">bin/getcrl_health.pl?DN=cn%3DMedicare%20Australia%20Organisation%20Certification%20Authority%2Co%3DMedicare%20Australia%2Cc%3DAU</a>		
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	
3.0.3 Generic IA5 String: RA Number (OID=1.2.36.73665175.1.10009)	< RA Number >	M	

### 5.3 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		

### 5.4 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	

<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 – online claiming for PBS Community of Interest  
v2.7

Field	Content	Mandatory	Critical*
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- 1024 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			N/A
2.7.1. Subject Type	End Entity		
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)			