

Short Form Certificate Policy



Australian Government

Medicare Australia

**Registered Medicare Australia Provider Community
of Interest (CoI) Certificate Policy (CP)
for Individual Certificates issued under the
Medicare Australia Organisation Certification
Authority (Medicare Australia OCA)**

v1.5

November 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 Services Division, Medicare Australia

Introduction

This is the Certificate Policy for individual certificates to be provided to Registered Medicare Australia Providers. The certificates will be provided on a Secure Token (known as the Health Professional Card) and provided to Registered Medicare Australia Providers.

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

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

Terminology

Registered Medicare Australia Provider Certificate means a Certificate issued under this CP to a provider (however described) who is registered with Medicare Australia and has, at registration, been issued with a number or numbers by Medicare Australia.

Certificate Policy Clauses

CP Identification

Certificates issued under this CP shall bear the Policy OID:

1.2.36.174030967.1.5.1.1

(where "174030967" is the last 9 digits of Medicare Australia's Australian Business Number).

1. INTRODUCTION

This is the Certificate Policy for individual certificates to be provided to Registered Medicare Australia Providers. The certificates will be provided on a Secure Token (known as the Health Professional Card) and provided to Registered Medicare Australia Providers.

The meaning of a Registered Medicare Australia Provider Individual Certificate (Provider 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 Registered Medicare Australia Provider) has been issued with a Registered Medicare Australia Provider Number (however described).

The Relationship Organisation for this CP is Medicare Australia. The Relationship Organisation Unit (ROU) is the program area in Medicare Australia responsible for provider registration. The Relationship Organisation Unit Operators (ROUOs) are Medicare Australia personnel working in the ROU.

1.1 PKI Participants

1.1.1 Certification Authority

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

Refer to the Medicare Australia Organisation Certification Authority Practice Statement (Medicare Australia OCA CPS) for further information on 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 (Col) in the Health Sector PKI operated by Medicare Australia.

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

1.1.4 Certificate Controllers

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

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

1.1.5 Relationship Organisation Unit Operators

Relationship Organisation Unit Operators (ROUOs) are Medicare Australia personnel within the Registered Medicare Australia Provider CoI.

ROUOs within the Registered Medicare Australia Provider 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.

1.1.6. Subscribers

Each Subscriber under this CP is a healthcare professional who is currently registered with, and allocated provider number(s) by, Medicare Australia and is known to Medicare Australia as a Registered Medicare Australia Provider (**Registered Medicare Australia Provider**).

There is a Subscriber agreement under this CP, known as the *Health Professional Card (Registered Medicare Australia Provider Individual Keys and Certificates) Terms and Conditions of Use*.

The Subscriber is bound by these terms and conditions when the Subscriber conducts his or her first transaction with Medicare Australia using the Keys and Certificates on his or her Health Professional Card.

1.1.7. Relying Parties

Relying Parties under this CP are:

- a) Medicare Australia, as receiver of transactions secured using the Individual keys and Certificates of the Registered Medicare Australia Provider;
- b) Registered Medicare Australia Providers conducting transactions with other Registered Medicare Australia Providers or third parties, as authorised or approved by Medicare Australia.

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 relating to transactions undertaken with Medicare Australia or who 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 Registered Medicare Australia Providers to secure transactions with Medicare Australia, other Registered Medicare Australia Providers and third parties for programs and services authorised or approved by Medicare Australia.

1.2.2 Prohibited Certificate Uses

There are no prohibited certificate uses. Parties using Individual Certificates for any transaction other than an authorised or approved transaction with Medicare Australia 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.

2. IDENTIFICATION AND AUTHENTICATION OF USERS

2.1 Naming of Subscribers

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

2.2 Identification and authentication of the Subscriber at registration

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

- a) receipt of applications for Provider Numbers;
- b) assessment of applications and associated documents;
- c) processing in association with the Department of Health and Ageing (DoHA) (where required);
- d) allocation of Provider Number(s) and registration on the Provider Directory System (PDS);
- e) where required, be linked to speciality codes to allow access to Medicare benefits. Note that allocation of a Provider Number does not give access to Medicare benefits: for example, restricted doctors have Provider Numbers but do not have access to Medicare benefits.

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

Any such program terms and conditions are separate from the *Health Professional Card (Registered Medicare Australia Provider Individual Keys and Certificates) Terms and Conditions of Use*.

2.3 Identification and authentication of the Subscriber at renewal

Subscribers (Registered Medicare Australia Providers) under this CP shall be identified and authenticated and the Certificate renewed automatically provided that:

- a) the healthcare professional is a Registered Medicare Australia Provider;
- b) the Registered Medicare Australia Provider's registration status with Medicare Australia 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:

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

3. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

3.1. Certificate creation

3.1.1. Enrolment process and responsibilities

Where a healthcare professional is a Registered Medicare Australia Provider, he/she may be enrolled automatically for Certificates by Certificate Controllers on the basis of registration as a Registered Medicare Australia Provider.

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

The Subscriber Key Pairs and Certificates issued under this CP shall be generated by an approved process.

3.3. Certificate renewal

Certificates issued under this CP shall be renewed automatically provided the status of the Registered Medicare Australia Provider has not changed.

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 Card;
- b) in the event of Registered Medicare Australia Provider's de-registration (however described);
- c) in the event the Registered Medicare Australia Provider's Provider Number(s) are cancelled by Medicare Australia.

3.5 Certificate status services

3.5.1 Operational characteristics

Details of Operational Characteristics are not provided.

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

Details of Operational Features are not provided.

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

As Medicare Australia (the Relationship Organisation under this CP) is a statutory agency 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.

4.5 Relationship Organisation termination

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

5. CERTIFICATE, CRL AND OCSP PROFILES

5.1 Certificate profile – Registered Medicare Australia Provider 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. Organization (O)	<Health>	O	
1.6.4. Common Name (CN)	<First Middle Last Name> :RA Number	M	
1.7. Subject Public Key Info	RSA Public Key of 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	1.2.36.174030967.1.5.1.1		
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		

Field	Content	Mandatory	Critical*
2.5.1.4. CPS URI	http://www.medicareaustralia.gov.au/		
2.6. Subject Alternate Names			Non-Critical
2.6.1. rfc822Name	<email address>	O	
2.7. 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/cgi-bin/getcrl_health.pl?DN=cn%3DMedicare%20Australia%20Organisation%20Certification%20Authority%2Co%3DMedicare%20Australia%2Cc%3DAU		Non-Critical
3.0 Other Fields - Generic ¹			
3.0.1 Generic IA5 String: RA Number (OID=1.2.36.73665175.1.10009)	< RA Number >	M	
3.0.2 Generic IA5 String: Provider Stem Number (OID=1.2.36.174030967.0.2)	< Provider Stem Number >	O	
3.0.3 Generic IA5 String: Prescriber Number (OID=1.2.36.174030967.0.3)	< Prescriber Number >	O	
3.0.4 Generic IA5 String: Healthcare Provider Identifier (OID=1.2.36.174030967.0.4)	< Healthcare Provider Identifier >	O	
3.0.5 Generic IA5 String: Medicare Identifier (OID=1.2.36.174030967.0.5)	< Medicare Identifier >	O	

5.2 Certificate profile – Registered Medicare Australia Provider Signing Certificate

Field	Content	Mandatory	Critical*
1. X.509v1 Field			N/A
1.1. Version	V3	M	
1.2. Serial Number	A positive integer that uniquely identifies the Certificate.	M	
1.3. Signature Algorithm	SHA-1 RSA, SHA-1 hashing algorithm using the RSA signing algorithm.	M	
1.4. Issuer Distinguished Name		M	
1.4.1. Country (C)	AU	M	
1.4.2. Organization (O)	Medicare Australia	M	
1.4.3. Organization Unit (OU)	Medicare Australia	M	
1.4.4. Common Name (CN)	Medicare Australia Organisation Certification Authority	M	
1.5. Validity			
1.5.1. Not Before		M	

The date that the Certificate is valid from (system time at certificate issuance).
YYMMDDHHMMSSZ encoded as
UTCTime for dates up to 2049 and

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

Field	Content	Mandatory	Critical*
	encoded as GeneralizedTime for dates in 2050 or later.		
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	
1.6.4. Organization (O)	<Health>	O	
1.6.6. Common Name (CN)	<First Middle Last Name> :RA Number	M	
1.7. Subject Public Key Info	RSA Public Key of 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	SET		
2.3.2. Non Repudiation	SET		
2.3.3. Key Encipherment	NOT SET		
2.3.4. Data Encipherment	NOT SET		
2.3.5. Key Agreement	NOT SET		
2.3.6. Key Certificate Signature	Not Selected		
2.3.7. CRL Signature	Not Selected		
2.4. Extended Key Usage	Not applicable		Non-Critical
2.5. Certificate Policies			Non-Critical
2.5.1. Policy Identifier	1.2.36.174030967.1.5.1.1		
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.pcx		
2.9 CRL Distribution Point			
2.9.1 URL	http://www.certificates-australia.com.au/cgi-bin/getcrl_health.pl?DN=cn%3DMedicare%20Australia%20Organisation%20Certification%20Authority%2Co%3DMedicare%20Australia%2Cc%3DAU		Non-Critical
3.0 Other Fields - Generic ²			

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

Field	Content	Mandatory	Critical*
3.0.1 Generic IA5 String: RA Number (OID=1.2.36.73665175.1.10009)	< RA Number >	M	
3.0.2 Generic IA5 String: Provider Stem Number (OID=1.2.36.174030967.0.2)	< Provider Stem Number >	O	
3.0.3 Generic IA5 String: Prescriber Number (OID=1.2.36.174030967.0.3)	< Prescriber Number >	O	
3.0.4 Generic IA5 String: Healthcare Provider Identifier (OID=1.2.36.174030967.0.4)	< Healthcare Provider Identifier >	O	
3.0.5 Generic IA5 String: Medicare Identifier (OID=1.2.36.174030967.0.5)	< Medicare Identifier >	O	

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	
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	

Field	Content	Mandatory	Critical*
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			
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)			