**Short Form Certificate Policy**

****

**Medicare Australia Community of Interest**

**Certificate Policy for Healthcare Individual Certificates v 2.2**

**(5 Year Duration)**

**April 2013**

Copyright © 2010 Commonwealth of Australia Page 1

Medicare Australia Community of Interest Certificate Policy for Healthcare Individual Certificates v 2.2 - April 2013

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.

**Contact (for any matters concerning this document)**

National Manager

eClaiming Branch

Health eBusiness Division Department of Human Services

PO Box 7788, Canberra BC ACT 2610

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

Copyright © 2010 Commonwealth of Australia Page 2

Medicare Australia Community of Interest Certificate Policy for Healthcare Individual Certificates v 2.2 - April 2013

**Introduction**

This is the Certificate Policy for Healthcare individual certificates to be provided to Medicare Australia Healthcare Individuals, including:

* providers
* allied health providers
* aged care providers
* other Healthcare individuals and related personnel (including responsible officers authorised as such under the *Healthcare Identifiers* *Act 2010*), and
* Contracted Service Provider Officers (CSP officers) who are approved as such by a contracted service provider authorised in accordance with the *Healthcare Identifiers Act 2010*.

who are either known to Medicare Australia [1](#page3) or have been identified through appropriate EOI requirements.

This CP should be read in conjunction with the:

* Medicare Australia Root Certification Authority Certification Practice Statement (RCA CPS)
* Medicare Australia Root Certification Authority Certificate Policy (RCA

CP).

* Medicare Australia Organisation Certification Authority Certification

Practice Statement (Medicare Australia OCA CPS).

**Terminology**

**eHealth Record System** means the Personally Controlled Electronic HealthRecords system established under the *Personally Controlled Electronic* *Health Records Act 2012* (Cth).

**Medicare Australia Healthcare Individual Certificate** means an individual

Certificate issued under this CP to a Healthcare Individual who is registered with, or known to, Medicare Australia through application and / or relationship.

1 Medicare Australia is now integrated into the Department of Human Services by virtue of the Human Services Legislation Amendment Act 2011. The effect of item 99 of Schedule 1 to the Human Services Legislation Amendment Act 2011 is to provide that where there is a reference to "Medicare Australia" in the Health Sector PKI documents, that reference is read as a reference to the Department of Human Services.

Copyright © 2010 Commonwealth of Australia Page 3

Medicare Australia Community of Interest Certificate Policy for Healthcare Individual Certificates v 2.2 - April 2013

Some Healthcare Individuals will, at registration, be issued with a registration number (however described) by Medicare Australia, for example, healthcare providers.

Other Healthcare Individuals will be known to Medicare Australia through:

* Medicare Australia program applications and/or relationships (for example, aged care providers)
* Its role as service operator of the HI Service, in accordance with the *Healthcare Identifiers Act 2010* (Cth) and the National Partnership

Agreement 2009 (the COAG Agreement). Such Healthcare individuals include, for example:

1. Healthcare Provider Individuals (HPIs) (who are not otherwise known to Medicare Australia through Medicare Australia program applications)
2. those persons who are identified as Responsible Officers under the *Healthcare Identifiers Act 2010* (Cth), and
3. those persons identified as Contracted Service Provider Officers by a contracted service provider authorised as a contracted service provider in accordance with the provisions of the

*Healthcare Identifiers Act 2010.*

Copyright © 2010 Commonwealth of Australia Page 4

Medicare Australia Community of Interest Certificate Policy for Healthcare Individual Certificates v 2.2 - April 2013

**Certificate Policy Clauses**

**CP Identification**

Certificates issued under this CP shall bear the Policy OID:

**1.2.36.174030967.1.5.1.2**

(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 Medicare Australia Healthcare Individuals.

The certificates are provided on a Secure Token to Subscribers.

The meaning of a Medicare Australia Healthcare Individual Certificate

(Healthcare Individual 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 Healthcare Individual) has either been issued with a Medicare Australia registration number (however described) or otherwise is known to Medicare Australia through application and / or relationship.

A Certificate does not verify or represent that the Certificate Subject is a particular individual.

The Relationship Organisation for this CP is Medicare Australia or, in the case of Healthcare Individuals who are Responsible Officers in accordance with that role as set out in the *Healthcare Identifiers Act 2010* (Cth) or who are

Contracted Service Provider Officers under that *Healthcare Identifiers Act* *2010*, Medicare Australia as the Healthcare Identifier (HI) Service serviceoperator as appointed under the *Healthcare Identifiers Act 2010* (Cth),

The Relationship Organisation Unit (ROU) is either the program area in Medicare Australia responsible for undertaking the Application registration or the relevant area within Medicare Australia operating as the HI Service service operator.

The Relationship Organisation Unit Operators (ROUOs) are Medicare

Australia personnel working in the ROU or the HI Service service operator area responsible for undertaking the Application registration of the

Responsible Officers and of Contracted Service Provider Officers.

**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).

Copyright © 2010 Commonwealth of Australia Page 5

Medicare Australia Community of Interest Certificate Policy for Healthcare Individual Certificates v 2.2 - April 2013

Refer to the Medicare Australia Root Certification Authority Certification Practice Statement (Medicare Australia RCA CPS), the Medicare Australia 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 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.

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

**1.1.5 Relationship Organisation Unit Operators**

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

ROUOs within the Registered Medicare Australia Individual 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**

Subscribers under this CP include:

1. a Healthcare Individual who is currently registered with, and in some cases, allocated a number (for example, provider number(s)) by, Medicare Australia or is known to Medicare Australia), or

Copyright © 2010 Commonwealth of Australia Page 6

Medicare Australia Community of Interest Certificate Policy for Healthcare Individual Certificates v 2.2 - April 2013

1. a Healthcare Individual who is employed in the Health Sector, and who has provided EOI commensurate with Medicare Australia requirements
2. a Responsible Officer whose role is established under the

*Healthcare Identifiers Act 2010* and who is, at the time ofregistration with the Medicare Australia RO for a Healthcare Individual Certificate, registered with, and allocated a number by, Medicare Australia as HI Service service operator and is known to

Medicare Australia.

1. a Contracted Service Provider Officer who has authority to act for the contracted service provider authorised as such in accordance with the *Healthcare Identifiers Act 2010*.

There is a Subscriber agreement under this CP, known as the *Individual Keys* *and Certificates 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 Individual Keys and Certificates issued under this CP.

**1.1.7. Relying Parties**

Relying Parties under this CP are:

1. Medicare Australia, as receiver of transactions secured using the Individual keys and Certificates;
2. Healthcare Individuals conducting transactions with other

Individuals or entities as authorised or approved by Medicare

Australia;

1. Healthcare Providers who have authorised a contracted service provider, represented by a Contracted Service Provider Officer, to provide services in accordance with the *Healthcare Identifiers Act* *2010.*
2. The System Operator of the eHealth Record System appointed under section 14 of the *Personally Controlled Electronic Health* *Records Act 2012* (Cth).

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 (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.

Copyright © 2010 Commonwealth of Australia Page 7

Medicare Australia Community of Interest Certificate Policy for Healthcare Individual Certificates v 2.2 - April 2013

1. **Certificate Use**

**1.2.1 Appropriate Certificate Use**

Key Pairs and Certificates issued under this CP are to be used by Healthcare

Individuals conducting transactions with Medicare Australia, the System Operator of the eHealth Record System or other Individuals or entities as 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 or an approved transaction between parties so authorised under the *Healthcare Identifiers Act* *2010*, do so at their own risk.

1. **Definitions and Acronyms**

Definitions and Acronyms are in the:

* + Medicare Australia Health Sector PKI Glossary at (http://www.medicareaustralia.gov.au/provider/business/online/register/ policy.jsp).
	+ *Healthcare Identifiers Act 2010*
	+ The Healthcare Identifiers Regulations 2010
	+ The Healthcare Identifiers Glossary
1. **IDENTIFICATION AND AUTHENTICATION OF USERS**
2. **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 Medicare Australia application and registration processes for

Healthcare Individuals.

1. **Identification and authentication of the Subscriber at registration**

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

1. receipt of applications for registration as a Healthcare Individual or a Responsible Officer or as a Contracted Service Provider Officer;
2. assessment of Applications and associated documents;

Copyright © 2010 Commonwealth of Australia Page 8

Medicare Australia Community of Interest Certificate Policy for Healthcare Individual Certificates v 2.2 - April 2013

1. processing in association with the Department of Health and Ageing (DoHA) (where required);
2. allocation of number(s) (where required) and registration on

Medicare Australia systems (however described);

Where a Medicare Australia Healthcare Individual wishes to access Medicare

Australia programs using his/her Certificate, Medicare Australia reserves the right to require that the Medicare Australia Healthcare Individual enters into terms and conditions for participation in that program.

Any such program terms and conditions are separate from the *Individual Keys* *and Certificates Terms and Conditions of Use.*

1. **Identification and authentication of the Subscriber at renewal**

Subscribers (Medicare Australia Healthcare Individuals) under this CP shall be identified and authenticated and the Certificate renewed provided that the Medicare Australia Healthcare Individual’s registration or other status with

Medicare Australia and / or the HI Service (Medicare Australia as HI Service service operator), has not changed.

1. **Identification and authentication of revocation request**

Revocation of certificates under this CP shall only be requested in writing by:

1. ROUOs in the event that the Subscriber becomes ineligible to remain as a Medicare Australia Healthcare Individual; or
2. The Subscriber; or
3. Certificate Controllers.
4. **CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS**
5. **Certificate creation**

**3.1.1. Enrolment process and responsibilities**

Medicare Australia may consider that the Healthcare Individual be enrolled for Certificates by Certificate Controllers on the basis of:

1. being known to Medicare Australia as a Medicare Australia Healthcare Individual either through:
	1. a Medicare Australia program registration (eg Aged Care provider)

Copyright © 2010 Commonwealth of Australia Page 9

Medicare Australia Community of Interest Certificate Policy for Healthcare Individual Certificates v 2.2 - April 2013

* + 1. being currently registered with Medicare Australia, and in some cases, allocated a number (for example, provider number(s)).
	1. Receipt of a certificate application together with EOI commensurate with Medicare Australia requirements.
	2. an individual’s role as a Responsible Officer which is established under the *Healthcare Identifiers Act 2010* and who provides EOI commensurate with Medicare Australia requirements, and is registered with, and allocated a number by, Medicare Australia as HI Service service operator.
	3. an individual’s role as a Contracted Service Provider Officer where the contracted service provider is authorised as such in accordance with the *Healthcare Identifiers Act 2010* and who provides EOI commensurate with Medicare Australia requirements, and is registered with, and allocated a number by Medicare Australia, as HI Service service operator.
1. **Publication of the certificate by the CA**

Certificates issued under this CP will be published in the Healthcare Public

Directory

Revocation status of Certificates issued under this CP will be published in the Healthcare Public Directory.

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

**3.2.1 Key pair generation and installation**

All Subscriber key pairs under this CP shall be generated by Certificate Controllers using accredited software.

The signing key & encryption key shall be stored and dispatched on a secure token. A PIC (personal identification code) to access the keys and Certificates will also be generated and dispatched separately.

1. **Certificate renewal**

Refer to clause 2.3 for details of identification and authentication.

1. **Certificate revocation**

Certificates issued under this CP may be revoked by Medicare Australia in its absolute discretion, including but not limited to:

a) after loss, destruction or theft of the Certificate;

Copyright © 2010 Commonwealth of Australia Page 10

Medicare Australia Community of Interest Certificate Policy for Healthcare Individual Certificates v 2.2 - April 2013

1. in the event of Medicare Australia Healthcare Individual’s de-registration (however described);
2. in the event the Medicare Australia Healthcare Individual’s Provider Number(s) or other numbers are cancelled by Medicare

Australia.

**3.5** **Certificate status services**

**3.5.1 Operational characteristics**

Refer to Section 4.10.1 of the Medicare Australia RCA CP.

**3.5.2 Service availability**

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

**3.5.3 Optional features**

Not applicable.

1. **REGISTRATION OPERATIONAL CONTROLS**
2. **Personnel controls**

All Certificate Controllers under this CP shall be authorised representatives of

Medicare Australia or Medicare Australia as the service operator for the HI

Service (in relation to Responsible Officers and Contracted Service Provider Officers).

1. **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.

1. **Physical controls**

Certificate requests will be processed by Medicare Australia Certificate

Controllers in accordance with the security provisions of the Medicare Australia OCA CPS.

1. **Business continuity of the Relationship Organisation**

The Department of Human Services (the Relationship Organisation under this CP) is a department of state of the Commonwealth of Australia and forms part of the Commonwealth.

Changes in legislation or government policy will provide for business continuity of the RO in accordance with policy as determined by the

Copyright © 2010 Commonwealth of Australia Page 11

Medicare Australia Community of Interest Certificate Policy for Healthcare Individual Certificates v 2.2 - April 2013

government and implemented in accordance with Commonwealth Machinery of Government (MOG) requirements.

1. **Relationship Organisation termination**

Changes in legislation or government policy will provide for termination of Department of Human Services as the RO under this CP and for a replacement agency as the successor RO in accordance with policy as determined by the government, if required.

1. **OTHER BUSINESS AND LEGAL MATTERS**
2. **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.

1. L E G AL MATTE R S

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:

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:

* 1. 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
	2. the carrying out or omitting to carry out, any activity related to the Gatekeeper accreditation process.
1. **Indemnities**

Indemnities are not provided between parties in the Health Sector PKI to which this CP applies.

Copyright © 2010 Commonwealth of Australia Page 12

Medicare Australia Community of Interest Certificate Policy for Healthcare Individual Certificates v 2.2 - April 2013

**6. CERTIFICATE, CRL AND OCSP PROFILES**

**6.1 Certificate profile – Registered Medicare Australia Healthcare Individual Encipherment Certificate**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Field** |  |  |  | **Content** | **Mandatory** | **Critical\*** |  |
| 1. | X.509v1 Field |  |  |  |  | N/A |  |
|  | 1.1. | Version |  |  | V3 | M |  |  |
|  | 1.2. | Serial Number |  | A positive integer that uniquely identifies the | M |  |  |
|  |  |  |  |  | Certificate. |  |  |  |
|  | 1.3. | Signature Algorithm |  | SHA-1 RSA, | M |  |  |
|  |  |  |  |  | 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 |  |  |
|  |  | 1.4.3 | Common Name (CN) | Medicare Australia Organisation Certification | M |  |  |
|  |  |  |  |  | Authority |  |  |  |
|  | 1.5. | Validity |  |  |  |  |  |  |
|  |  | 1.5.1. | Not Before | The date that the Certificate is valid from (system | M |  |  |
|  |  |  |  |  | time at certificate issuance). |  |  |  |
|  |  |  |  |  | YYMMDDHHMMSSZ encoded as UTCTime for |  |  |  |
|  |  |  |  |  | dates up to 2049 and encoded as |  |  |  |
|  |  |  |  |  | GeneralizedTime for dates in 2050 or later. |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  | 1.5.2. | Not After |  | The date that the Certificate is valid until. 5 years | M |  |  |
|  |  |  |  |  | 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 |  |  |  |
|  | 1.6. | Subject |  |  |  |  |  |  |
|  |  | 1.6.1. | Country (C) | AU | M |  |  |
|  |  | 1.6.2. | State (St) |  | <STATE> | M |  |  |
|  |  | 1.6.3. | Organization (O) | <Health> | O |  |  |
|  |  | 1.6.4. | Common Name (CN) | <First Middle Last Name> :RA Number | M |  |  |
|  | 1.7. Subject Public Key Info | RSA Public Key of 2048 bits. | M |  |  |
|  |  |  |  |  |  |  |
| 2. | X.509v3 Extensions |  |  |  |  |  |
|  | 2.1. | Authority Key Identifier |  | M | Non- |  |
|  |  |  |  |  |  | Critical |  |
|  |  | 2.1.1. | Key Identifier | SHA-1 hash (60 bits) of the Issuer's public key. |  |  |
|  |  | 2.1.2. | AuthorityCertIssuer | Not present |  |  |  |
|  |  | 2.1.3. |  |  | Not present |  |  |  |
|  |  | AuthorityCertSerialNumber |  |  |  |  |
|  | 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 | Not Selected |  |  |  |
|  |  | Signature |  |  |  |  |  |
|  |  | 2.3.7. | CRL Signature | Not Selected |  |  |  |
|  | 2.4. | Extended Key Usage | Not applicable |  | Non- |  |
|  |  |  |  |  |  |  | Critical |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | Non- |  |
|  | 2.5. | Certificate Policies |  |  |  |  |
|  |  |  |  |  |  | Critical |  |
|  |  | 2.5.1. | Policy Identifier | 1.2.36.174030967.1.5.1.2 |  |  |
|  |  | 2.5.1.1. | Policy | User Notice |  |  |  |
|  |  |  | Qualifier ID |  |  |  |  |
|  |  | 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- |  |

Copyright © 2010 Commonwealth of Australia Page 13

Medicare Australia Community of Interest Certificate Policy for Healthcare Individual Certificates v 2.2 - April 2013

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Field** |  |  |  | **Content** | **Mandatory** | **Critical\*** |
|  | 2.6.1. | rfc822Name | <email address> | O | 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 | On-line Certificate Status Protocol |  | Non- |
|  |  | Method |  | (1.3.6.1.5.5.7.4.1) |  | Critical |
|  | 2.8.1.2. | Alternative | URL=http://ocsp.certificates- |  |  |
|  |  | Name |  | australia.com.au/maoca.pkx |  |  |
| 2.9 CRL Distribution Point |  |  |  |  |
|  | 2.9.1 URL |  | http://www.certificates- |  | Non- |
|  |  |  |  | australia.com.au/general/cert\_search\_health.shtml |  | Critical |
|  |  |  |  |  |
|  | 3.0 Other Fields - Generic2 |  |  |  |
|  | 3.0.1 | Generic IA5 String: | < RA Number > | M |  |
|  |  | RA Number |  |  |  |  |
|  |  | (OID=1.2.36.73665175.1.10 |  |  |  |
|  |  | 009) |  |  |  |  |
|  | 3.0.2 | Generic IA5 String: | < Provider Stem Number > | O |  |
|  |  | Provider Stem Number |  |  |  |
|  |  | (OID=1.2.36.174030967.0.2) |  |  |  |
|  | 3.0.3 | Generic IA5 String: | < Prescriber Number > | O |  |
|  |  | Prescriber Number |  |  |  |
|  |  | (OID=1.2.36.174030967.0.3) |  |  |  |
|  | 3.0.4 | Generic IA5 String: | < Healthcare Provider Identifier > | O |  |
|  |  | Healthcare Provider |  |  |  |
|  |  | Identifier |  |  |  |  |
|  |  | (OID=1.2.36.174030967.0.4) |  |  |  |
|  | 3.0.5 | Generic IA5 String: | < Medicare Identifier > | O |  |
|  |  | Medicare Identifier |  |  |  |
|  |  | (OID=1.2.36.174030967.0.5) |  |  |  |

**6.2 Certificate profile – Registered Medicare Australia Healthcare Individual Signing Certificate**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Field** |  |  |  | **Content** | **Mandatory** | **Critical\*** |
| 1. | X.509v1 Field |  |  |  |  | N/A |
|  | 1.1. | Version |  |  | V3 | M |  |
|  | 1.2. | Serial Number | A positive integer that uniquely identifies the | M |  |
|  |  |  |  |  | Certificate. |  |  |
|  | 1.3. | Signature Algorithm | SHA-1 RSA, | M |  |
|  |  |  |  |  | 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 | M |  |
|  |  |  |  |  | Authority |  |  |
|  | 1.5. | Validity |  |  |  |  |  |
|  |  | 1.5.1. | Not Before | The date that the Certificate is valid from (system | M |  |
|  |  |  |  |  | time at certificate issuance). |  |  |
|  |  |  |  |  | YYMMDDHHMMSSZ encoded as UTCTime for |  |  |
|  |  |  |  |  | dates up to 2049 and encoded as |  |  |
|  |  |  |  |  | GeneralizedTime for dates in 2050 or later. |  |  |
|  |  | 1.5.2. | Not After | The date that the Certificate is valid until. 5 years | M |  |
|  |  |  |  |  | from Start Validity, i.e. certificate issuance. |  |  |
|  |  |  |  |  |  |  |  |

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

Copyright © 2010 Commonwealth of Australia Page 14

Medicare Australia Community of Interest Certificate Policy for Healthcare Individual Certificates v 2.2 - April 2013

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Field** |  |  |  |  | **Content** | **Mandatory** | **Critical\*** |  |
|  |  |  |  |  |  | YYMMDDHHMMSSZ encoded as UTCTime for |  |  |  |
|  |  |  |  |  |  | dates up to 2049 and encoded as |  |  |  |
|  |  |  |  |  |  | GeneralizedTime for dates in 2050 or later |  |  |  |
|  | 1.6. | Subject |  |  |  |  |  |  |
|  |  | 1.6.1. | Country (C) | AU | M |  |  |
|  |  | 1.6.2. | State (St) |  |  | <STATE> | M |  |  |
|  |  | 1.6.4. | Organization (O) | <Health> | O |  |  |
|  |  | 1.6.6. | Common Name (CN) | <First Middle Last Name> :RA Number | M |  |  |
|  | 1.7. Subject Public Key Info | RSA Public Key of 2048 bits. | M |  |  |
|  |  |  |  |  |  |  |  |
| 2. | X.509v3 Extensions |  |  |  |  |  |  |
|  | 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 | Not Selected |  |  |  |
|  |  |  | Signature |  |  |  |  |  |  |
|  |  | 2.3.7. | CRL Signature | Not Selected |  |  |  |
|  | 2.4. | Extended Key Usage | Not applicable |  | Non- |  |
|  |  |  |  |  |  |  |  | Critical |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | Non- |  |
|  | 2.5. | Certificate Policies |  |  |  |  |  |
|  |  |  |  |  |  |  | Critical |  |
|  |  | 2.5.1. | Policy Identifier | 1.2.36.174030967.1.5.1.2 |  |  |
|  |  | 2.5.1.1. | Policy | User Notice |  |  |  |
|  |  |  | Qualifier ID |  |  |  |  |
|  |  | 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 | On-line Certificate Status Protocol |  | Non- |  |
|  |  |  | Method |  |  | (1.3.6.1.5.5.7.4.1) |  | Critical |  |
|  |  | 2.8.1.2. | Alternative | URL=http://ocsp.certificates- |  |  |  |
|  |  |  | Name |  |  | australia.com.au/maoca.pkx |  |  |  |
|  | 2.9 CRL Distribution Point |  |  |  |  |  |  |
|  |  | 2.9.1 URL |  |  | http://www.certificates- |  | Non- |  |
|  |  |  |  |  |  | australia.com.au/general/cert\_search\_health.shtml |  | Critical |  |
|  |  |  |  |  |  |  |  |
|  |  | 3.0 Other Fields - Generic3 |  |  |  |  |
|  |  | 3.0.1 | Generic IA5 String: | < RA Number > | O |  |  |
|  |  |  | RA Number |  |  |  |  |  |  |
|  |  |  | (OID=1.2.36.73665175.1.10 |  |  |  |  |
|  |  |  | 009) |  |  |  |  |  |  |
|  |  | 3.0.2 | Generic IA5 String: | < Provider Stem Number > | O |  |  |
|  |  |  | Provider Stem Number |  |  |  |  |

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

Copyright © 2010 Commonwealth of Australia Page 15

Medicare Australia Community of Interest Certificate Policy for Healthcare Individual Certificates v 2.2 - April 2013

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Field** |  | **Content** | **Mandatory** | **Critical\*** |
|  | (OID=1.2.36.174030967.0.2) |  |  |  |
| 3.0.3 | Generic IA5 String: | < Prescriber Number > | O |  |
|  | Prescriber Number |  |  |  |
|  | (OID=1.2.36.174030967.0.3) |  |  |  |
| 3.0.4 | Generic IA5 String: | < Healthcare Provider Identifier > | O |  |
|  | Healthcare Provider |  |  |  |
|  | Identifier |  |  |  |
|  | (OID=1.2.36.174030967.0.4) |  |  |  |
| 3.0.5 | Generic IA5 String: | < Medicare Identifier > | O |  |
|  | Medicare Identifier |  |  |  |
|  | (OID=1.2.36.174030967.0.5) |  |  |  |

**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 |  | M |  |
|  |  | Certification Authority |  |  |  |
| 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 |  |  |  |

Copyright © 2010 Commonwealth of Australia Page 16

Medicare Australia Community of Interest Certificate Policy for Healthcare Individual Certificates v 2.2 - April 2013

**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 |  | M |  |  |
|  |  |  |  |  |  | Issuing CA |  |  |  |  |
|  |  | 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 |  | M |  |  |
|  |  |  |  |  |  | Certification Authority |  |  |  |  |
|  |  | 1.5. | Validity |  |  | 5 years |  |  |  |  |
|  |  |  | 1.5.1. | Not Before |  | Issue date |  | M |  |  |
|  |  |  | 1.5.2. | Not After |  | Expiry date |  | M |  |  |

1. 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 | M |
|  |  | Responder |  |
| 1.7. Subject Public Key Info | Public Key encoded in accordance | M |
|  |  | with RFC2459 & PKCS#1- 2048 bits |  |

1. X.509v3 Extensions

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 2.1. | Authority Key Identifier | SHA-1 hash (60 bits) of the Issuer’s | M | Non- |  |
|  |  |  | public key |  | 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 | M | Non- |  |
|  |  |  | public key |  | 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 |  |  |

1. Certificate Policies

|  |  |  |
| --- | --- | --- |
| 2.5.1. | Policy Identifier | Not present |
| 2.5.1.1. | Policy Qualifier | Not present |
|  |  | ID |  |
| 2.5.1.2. | User Notice | Not present |

1. 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 |  |

1. Basic Constraints

|  |  |  |  |
| --- | --- | --- | --- |
| 2.7.1. | Subject Type | End Entity | N/A |
| 2.7.2. | Path Length Constraint | Not present |  |

1. 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) |  |  |  |  |

Copyright © 2010 Commonwealth of Australia Page 17