**Short Form Certificate Policy**

****

**Australian Government Department of Human Services Community of Interest Certificate Policy for Individual Certificates for Healthcare Provider Individuals via data source (HPI-DS) for Healthcare Identifiers Service (HI Service) v 1.2**

**(5 year duration)**

**January 2016**

**Ownership of intellectual property rights in this publication**

Unless otherwise noted, copyright (and any other intellectual property rights, if any) in this publication is owned by the Commonwealth of Australia (referred to below as the Commonwealth).

**Creative Commons licence**

With the exception of the Coat of Arms and the Australian Government Department of Human Services logo, this publication is licensed under a Creative Commons Attribution 3.0 Australia Licence.



Creative Commons Attribution 3.0 Australia Licence is a standard form license agreement that allows you to copy, distribute, transmit and adapt this publication provided that you attribute the work. A summary of the licence terms is available from creativecommons.org/licenses/by/3.0/au/

The full licence terms are available from [creativecommons.org/licenses/by/3.0/au/legalcode](http://creativecommons.org/licenses/by/3.0/au/legalcode)

The Commonwealth’s preference is that you attribute this publication (and any material sourced from it) using the following wording:

*Source: Licensed from the Commonwealth of Australia under a Creative Commons Attribution 3.0 Australia Licence.*

*The Commonwealth of Australia does not necessarily endorse the content of this publication.*

Requests for information about this licence should be sent to:

The Manager

External Communication Branch

Human Services Portfolio Communication Division

PO Box 7788

Canberra BC, ACT, 2610

**Use of the Coat of Arms**

The terms under which the Coat of Arms can be used are set out on the Department of the Prime Minister and Cabinet [website.](http://www.dpmc.gov.au/pmc/about-pmc/core-priorities/guidelines-and-procedures-other-agencies)

**Contact (for any other 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 Department of Human Services Policy Management Authority.

**Background**

This is the Certificate Policy (CP) for Individual Certificates to be provided to persons authorised under the *Healthcare Identifiers Act 2010* to register for an individual healthcare provider (HPI-I) identifier (however described) in accordance with their roles in the Healthcare Identifiers Service (HI Service) under the *Healthcare Identifiers Act 2010* .

Such individuals include healthcare provider individuals—those individual healthcare providers (however described) who are:

* known to and identified by a data source as an individual healthcare provider
* the data source is identified and authorised as a data source under subsection 12(2) (or other relevant section/s) of the *Healthcare Identifiers Act 2010* and/or the Healthcare Identifiers Regulations 2010
* the individuals are identified to the Australian Government Department of Human Services as healthcare provider individuals by that identified and authorised data source, and
* who are then known as HPI-DS to Human Services in its role as the service operator of the HI Service.

The *Healthcare Identifiers Act 2010* and the National Partnership Agreement signed by the COAG jurisdictions in November 2009 provide that Human Services be appointed the service operator for the HI Service.

This CP should be read in conjunction with the:

* Root Certification Authority Certification Practice Statement (RCA CPS)
* Root Certification Authority Certificate Policy (RCA CP), and
* Organisation Certification Authority Certification Practice Statement (OCA CPS).

**Terminology**

Please refer to the documents listed below for definitions relevant to this CP.

In this CP, the order of priority for determining the meaning of a specific term is:

1. *Healthcare Identifiers Act 2010* ([comlaw.gov.au](http://www.comlaw.gov.au)).

2. Healthcare Identifiers Regulations 2010 ([comlaw.gov.au](http://www.comlaw.gov.au)).

4. National Partnership Agreement 2009 (the COAG agreement) ([coag.gov.au](http://www.coag.gov.au)).

5. the Healthcare Identifiers Glossary of Terms and Conditions ([nehta.gov.au/get-started-with-ehealth](http://www.nehta.gov.au/get-started-with-ehealth/)).

6. PKI gatekeeper documents, including the Department of Human Services Public Key Infrastructure (PKI) glossary ([humanservices.gov.au/health-professionals/services/public-key-infrastructure/public-key-infrastructure-policy-documents](http://www.humanservices.gov.au/health-professionals/services/public-key-infrastructure/public-key-infrastructure-policy-documents) ).

**My Health Record system** means the My Health Record system established under the *My Health Records Act 2012*.

**Individual Certificate for Healthcare Provider Individual identified by an identified and authorised data source** means an Individual Certificate issued by Human Services under this CP to an Individual who is registered with, or known to, Human Services in its role as the service operator of the HI Service.

Individuals issued with an Individual Certificate for Healthcare Provider Individual identified by an authorised data source (HPI-DS) will, at registration with the HI Service, be recorded with their identifying Healthcare Provider Individual Identifier (however described) as issued by the data source that provides the identifier (and other information) to Human Services in its role as the service operator of the HI Service.

**Certificate Policy Clauses**

**CP Identification**

Certificates issued under this CP shall bear the Policy OID:

**1.2.36.174030967.1.7.1.1**

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.

1. **Introduction**

This is the CP for individual certificates provided by Human Services as service operator of the Healthcare Identifiers Service (HI Service) to individuals who are assigned healthcare provider individual roles by an authorised data source, and who are known in the HI Service and registered by Human Services in accordance with its role as the service operator of the HI service.

Such individuals are known as healthcare provider individuals via data source (HPI-DS) and are Subscribers for the purposes of the CP.

The certificates are provided on a secure token to Subscribers.

The meaning of an individual certificate for the Healthcare Identifier Service (HI Service) issued by Human Services 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 HI Service Healthcare Provider Individual via data source (HPI-DS)) has been issued with a registration number (however described) by a data source and through this registration with the data source is known to Human Services in its role as the service operator of the HI Service, 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 Human Services as the service operator for the HI Service.

The Relationship Organisation Unit (ROU) is the HI Service operator area in Human Services responsible for undertaking the Application registration.

The Relationship Organisation Unit Operators (ROUOs) are Human Services staff working in the ROU.

**1.1 PKI Participants**

**1.1.1 Certification Authority**

All certificates issued under this CP shall be produced by the Department of Human Services Organisation Certification Authority (Human Services OCA).

For more information on applicable practices and procedures for certificates issued under this CP, refer to the OCA CPS and the Organisation Certification Authority Certificate Policy (OCA CP) located at [[humanservices.gov.au/pki](http://www.humanservices.gov.au/health-professionals/services/public-key-infrastructure/public-key-infrastructure-policy-documents)](http://www.medicareaustralia.gov.au)

**1.1.2 Relationship Organisation**

Human Services, as service operator of the HI Service, is the Relationship Organisation (Human Services RO) in the Health Sector PKI.

**1.1.3 Relationship Organisation Unit**

There is a separately identified Relationship Organisation Unit (ROU) within the Human Services RO for the HI Service Community of Interest (CoI) for Healthcare Individual Providers via data source (HPI-DS) in the Health Sector PKI operated by Human Services.

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

**1.1.4 Certificate Controllers**

Certificate Controllers are Human Services RO staff with responsibilities for managing Certificates.

All Certificate Controllers operating under this CP are duly authorised representatives of Human Services.

**1.1.5 Relationship Organisation Unit Operators**

Relationship Organisation Unit Operators (ROUOs) are Human Services staff within the Human Services HI Service CoI.

ROUOs within the Human Services HI Service CoI are not Certificate Controllers.

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

**1.1.6 Subscribers**

Subscribers under this CP include Healthcare Provider Individuals via data source as identified and defined under the *Healthcare Identifiers Act 2010* by a data source that is identified and authorised as a data source under the *Healthcare Identifiers Act 2010* and the Healthcare Identifiers Regulations 2010.

1. A Subscriber under this CP will be an individual who is registered and allocated a number—for example, a registration number (however described)—by an identified and authorised data source, in accordance with the National Law (*Health Practitioner Regulation National Law Act 2009*), and
2. will be identified to Human Services as the service operator of the HI Service by that data source.

The Subscriber (the HPI-DS) is since known to Human Services in its role as the service operator of the HI Service and is able to be included in the HPI-DS CoI as a subscriber for an Individual Certificate for HPI-DS under this CP.

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

**1.1.7 Relying Parties**

Relying Parties under this CP are:

1. Human Services, as HI Service operator and receiver of transactions secured using the HI Service Individual Keys and Certificates.
2. Individuals assigned a healthcare identifier as a healthcare provider organisation or a healthcare provider individual, in accordance with and as authorised by the *Healthcare Identifiers Act 2010* and Healthcare Identifier Regulations 2010 and who transact with the HI Service and Relying Parties using the Individual Keys and Certificates.
3. Individuals assigned a registration number as a Responsible Officer (RO) or an Organisation Maintenance Officer (OMO) in accordance with and as authorised by the *Healthcare Identifiers Act 2010* and Healthcare Identifier Regulations 2010 and who transact with the HI Services and Relying Parties using the Individual Keys and Certificates.
4. The System Operator of the My Health Record system appointed under section 14 of the *My Health Records Act 2012*.

There is no Relying Party Agreement under this CP**.**

Parties who rely on Certificates issued under this CP and undertake transactions that are not authorised or approved by the *Healthcare Identifiers Act 2010*, the Healthcare Identifiers Regulations 2010, rely on such Certificates at their own risk. Parties who rely on Certificates issued under this CP and who do not have a written agreement with Human Services or authorisation through a notice published at [humanservices.gov.au/pki](http://www.humanservices.gov.au/pki) (specifying authorised usage relating to a transaction type), and since undertake transactions that are not authorised or approved by Human Services in its role as the service operator of the HI Service, rely on such certificates at their own risk.

**1.2 Certificate Use**

* + 1. **Appropriate Certificate Use**

Key Pairs and certificates issued under this CP are to be used by individuals for conducting transactions with:

* Human Services as the service operator of the HI Service
* the system operator of the My Health Record system, or
* other individuals or entities as authorised or approved by the *Healthcare Identifiers Act 2010* and Healthcare Identifiers Regulations 2010.

**1.2.2 Prohibited Certificate Uses**

There are no prohibited certificate uses.

Use of certificates outside of the Human Services Relationship Organisation CoIs for the HI Service is not supported.

Parties using Individual Certificates for any transaction other than an authorised or approved transaction do so at their own risk.

* + 1. **Definitions and Acronyms**

Definitions and acronyms are in the:

* *Healthcare Identifiers Act 2010*
* Healthcare Identifiers Regulations 2010
* Healthcare Identifiers Glossary
* Department of Human Services Public Key Infrastructure (PKI) glossary ([humanservices.gov.au/health-professionals/services/public-key-infrastructure/public-key-infrastructure-policy-documents](http://www.humanservices.gov.au/health-professionals/services/public-key-infrastructure/public-key-infrastructure-policy-documents?utm_id=9))

**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) as a Healthcare Provider Individual via data source (HPI-DS) according to Human Services, in its role as the service operator of the HI Service, application and registration processes for HI Service Individuals.

**2.2 Identification and authentication of the Subscriber at registration**

Subscribers under this CP will be identified and authenticated, at the time of their application for registration (however described), as a Healthcare Provider Individual via data source (HPI-DS) by Human Services in its role as the service operator of the HI Service, in accordance with trusted practices that may include, but not be limited to:

1. receipt of data from data sources, identified and authorised as data sources by the *Healthcare Identifiers Act 2010* or the Healthcare Identifier Regulations 2010 and the National Law (*Health Practitioner Regulation National Law Act 2009*)
2. receipt of applications for registration as a Healthcare Provider Individual via data source (HPI-DS)
3. assessment of applications and associated documents
4. processing and administering in accordance with the *Healthcare Identifiers Act 2010* and the Healthcare Identifiers Regulations 2010
5. association with NEHTA and the Department of Health (DoH) (where required)
6. allocation of HPI-DS Individual Certificate registration number(s) (where required) and registration on Human Services and HI Service systems (however described) and where required.

**2.3 Identification and authentication of the Subscriber at renewal**

Subscribers (HPI-DS) under this CP shall be identified and authenticated and the Certificate renewed provided that:

1. the HPI-DS registration or other status with the relevant data source has not changed
2. the HPI-DS registration or other status with the HI Service has not changed, and
3. Human Services, as service operator of the HI Service, is satisfied that such registration or other status has not changed.

**2.4 Identification and authentication of revocation request**

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

a) ROUOs in the event that the Subscriber becomes ineligible to remain as a HPI-DS, 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 an individual is a HPI-DS and identified as such by operation of the:

* the *Healthcare Identifiers Act 2010*
* the Healthcare Identifier Regulations 2010, or
* the National Law (*Health Practitioner Regulation National Law Act 2009*).

Human Services may consider that the individual be enrolled for Certificates by Certificate Controllers on the basis of being known to Human Services, in its role as the service operator of the HI Service, as a HPI-DS.

**3.1.2. Publication of the certificate by the CA**

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

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

**3.2. Key Pair and Certificate Usage**

**3.2.1 Key pair generation and installation**

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

The signing key and encryption key shall be stored and dispatched on a secure token. A Personal Identification Code (PIC)) to access the Keys and Certificates will also be generated and dispatched separately.

**3.3 Certificate renewal**

\Refer to clause 2.3 for details of identification and authentication.

**3.4. Certificate revocation**

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

1. after loss, destruction or theft of the Certificate
2. in the event of the HPI-DS’s de-registration for HI Service purposes (however described)
3. in the event the HPI-DS’s registration number(s) or other numbers (where applicable) are cancelled by Human Services.

**3.5 Certificate status services**

**3.5.1 Operational characteristics**

Refer to Section 4.10.1 of the RCA CP.

**3.5.2 Service availability**

Service availability for the Certificate Revocation List (CRL) is substantially 24 hours a day, seven days a week at [certificates-australia.com.au](http://www.certificates-australia.com.au/)

**3.5.3 Optional features**

Not applicable.

**4. Registration Operational Controls**

**4.1 Staff controls**

All Certificate Controllers under this CP shall be authorised representatives of Human Services operating as the service operator for the HI Service.

**4.2 Logical and Technological controls**

Certificate requests will be processed by the authorised Certificate Controllers of Human Services in accordance with the security provisions of the OCA CPS.

**4.3 Physical controls**

Certificate requests will be processed by Human Services Certificate Controllers in accordance with the security provisions of the OCA CPS.

**4.4 Business continuity of the Relationship Organisation**

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

**4.5 Relationship Organisation termination**

Changes in legislation or government policy will provide for termination 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.

**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 RCA CP at [humanservices.gov.au/pki](http://www.humanservices.gov.au/health-professionals/services/public-key-infrastructure/public-key-infrastructure-policy-documents?utm_id=9)

**5.2 Legal matters**

For information on legal matters, refer to section 9 (Other Business and Legal Matters) of the RCA CP at [humanservices.gov.au/pki](http://www.humanservices.gov.au/health-professionals/services/public-key-infrastructure/public-key-infrastructure-policy-documents?utm_id=9)

**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 RCA CP at [humanservices.gov.au/pki](http://www.humanservices.gov.au/pki)

Paragraph 9.8.1 of the 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:

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.

**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 – Registered Human Services 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 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) | Human Services | M |
| 1.4.3           Common Name (CN) | Human Services 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.           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.           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 | 1.2.36.174030967.1.7.1.1 |  |
| 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 | humanservices.gov.au |  |
| 2.6.      Subject Alternate Names |  |  | Non-Critical |
| 2.6.1.           rfc822Name | <email address> | O |
| 2.6.2.          uniformResourceIdentifier | <Uniform Resource Identifier> | O |  |
| 2.7.      Basic Constraints |  |  |  |
| 2.7.1.           Subject Type | Not CA |  | Critical |
| 2.7.2.           Path Length Constraint | Not present |  |
| 2.8.      Authority Information Access |  |  |  |
| 2.8.1.           Access Description | Not present |  |  |
| 2.8.1.1.                  Access Method | On-line Certificate Status Protocol (1.3.6.1.5.5.7.4.1) |  | Non-Critical |
| 2.8.1.2.                  Alternative Name | URL=http://ocsp.certificates-australia.com.au/maoca.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[[1]](#footnote-2) |  |  |  |
| 3.0.1 Generic IA5 String:  RA Number (OID=1.2.36.73665175.1.10009) | < RA Number > | M |  |

**6.2 Certificate profile – Registered Human Services 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 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) | Human Services | M |
| 1,4,3, Organization Unit (OU) | Human Services | M |
| 1.4.4           Common Name (CN) | Human Services 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 |
| 1.6.4.           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 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 | 1.2.36.174030967.1.7.1.1 |  |
| 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 | humanservices.gov.au |  |
| 2.6.      Subject Alternate Names |  |  | Non-Critical |
| 2.6.1.           rfc822Name | <email address> | O |
| 2.6.2.          uniformResourceIdentifier | <Uniform Resource Identifier> | O |  |
| 2.7.      Basic Constraints |  |  |  |
| 2.7.1.           Subject Type | Not CA |  | Critical |
| 2.7.2.           Path Length Constraint | Not present |  |
| 2.8.      Authority Information Access |  |  |  |
| 2.8.1.           Access Description | Not present |  |  |
| 2.8.1.1.                  Access Method | On-line Certificate Status Protocol (1.3.6.1.5.5.7.4.1) |  | Non-Critical |
| 2.8.1.2.                  Alternative Name | URL=http://ocsp.certificates-australia.com.au/maoca.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[[2]](#footnote-3) |  |  |  |
| 3.0.1 Generic IA5 String:  RA Number (OID=1.2.36.73665175.1.10009) | < RA Number > | O |  |

**6.3 Human Services 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) | Human Services |  |  |
| 1.3.3.           Common Name (CN) | Human Services 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 |  |  |

**6.4 Human Services OCA OCSP Profile**

| **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) | Human Services | M |
| 1.4.4           Common Name (CN) | Human Services Organisation Certification Authority | M |
| 1.5.      Validity |  |  |
| 1.5.1.           Not Before | 5 years | M |
| 1.5.2.           Not After | Expiry date | M |
| 1.6.      Subject |  |  |
| 1.6.1.           Country (C) | AU | M |
| 1.6.4.           Organization (O) | GOV | O |  |
| 1.6.3 Organisation Unit (OU) | Human Services |  |  |
| 1.6.6.           Common Name (CN) | Human Services OCAOCSP Responder | M |  |
| 1.7.      Subject Public Key Info | Public Key encoded in accordance with RFC459 & PKC #1 2048 bites | 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 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 |  |  | Non-Critical |
| 2.5.1.           Policy Identifier | Not present |  |
| 2.5.1.1.                 Policy Qualifier ID | No present |  |
| 2.5.1.2.                  User Notice | Not present |  |
| 2.5.1.3.                 Policy Qualifier ID | CPS URI |  |
| 2.5.1.4.                  User Notice | Not present |  |
| 2.6.      Subject Alternate Names |  |  | Non-Critical |
| 2.6.1.           rfc822Name | NA | O |
| 2.7.      Basic Constraints |  |  |  |
| 2.7.1.           Subject Type | End Entity |  | 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 | Not present |  | Non-Critical |
| 2.8.1.2.                  Alternative Name | Not present |  |
| 3. No check Extension (generic extension) |  |  |  |

1. These Certificate extension OID references are expected to be common to all CoI Certificate Policies, and may have applicability to this CoI. [↑](#footnote-ref-2)
2. These Certificate extension OID references are expected to be common to all CoI Certificate Policies, and may have applicability to this CoI. [↑](#footnote-ref-3)