

**Australian Government Department of Human Services Root Certification Authority Certificate Policy**

Version 2.8

**March 2017**

**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/](http://www.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 [dpmc.gov.au/government/commonwealth-coat-arms](https://www.dpmc.gov.au/government/commonwealth-coat-arms)

Copyright © 2017 Commonwealth of Australia Page 2

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

National Manager

Payment and Claiming Branch

Health Service Delivery 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.

**Version History**

**Table 1: Version History**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Doc**  **Version** | **Status** | **Date of Issue** | **Issue By** | **Comments** |
| 1.0 | Draft | 14 August 2006 | Stephen  Wilson | First discussion draft, based on Short Form template. |
| 1.1 | Draft | 15 August 2006 | Patrick Tang | Amendment to the Certificate Profile, terminology, CP OID and references to the MARCA CPS and MAOCA CPS. |
| 1.2 | Draft | 16 August 2006 | Robert Parker | References to the CPS. |
| 1.3 | DRAFT | 24 August 2006 | Lynn Du  Moulin | Review and amendment to the clauses of the CP |
| 1.4 | DRAFT | 30 August 2006 | Lynn Du  Moulin | Revisions to include amendments to fit with penultimate draft of RCA CPS |
| 1.5 | Draft | 4 September  2006 | Stephen  Wilson | Accepted most changes; included cross references to Key Signing Ceremony |
| 1.6 | FINAL | 4 SEPTEMBER | Lynn Du  Moulin | Accepted changes, minor edits to cl.1.3, final proof-read. |
| 1.9 | FINAL | 8 SEPTEMBER  2006 | LYNN  DUMOULIN | NUMBER CHANGE TO 1.9 FINAL TO  MATCH OID |
| 1.91 | FINAL | 18 September  2006 | Lynn Du  Moulin | Amendments to reflect change in PMA |
| 1.92 | Draft | May 2008 | Lee Mansfield | Gatekeeper Accreditation under the Relationship Organisation model. |
| 1.93 | Draft | June 2008 | Lee Mansfield | Amendments after consultations with Lynn Du Moulin and Paul Sorensen from Medicare Australia. |
| 1.94 | Draft | June 2008 | Lee Mansfield | Amendments after consultations with Lynn Du Moulin and Paul Sorensen from Medicare Australia.  Release version to AGIMO for comments. |
| 1.95 | Draft | July 2008 | Lee Mansfield | Amendments after review by the  Gatekeeper Competent Authority. |
| 1.96 | Draft | November  2008 | Paul Sorensen | Amendments after review by the Gatekeeper Competent Authority and further review by Medicare Australia. |
| 1.97 | Draft | February 2010 | Paul Sorensen | Amendment to section 9.8 Limitations of Liability |
| 1.98 | Draft | April 2010 | Paul Sorensen | AGIMO Amendments included |
| 1.99 | Draft | May 2010 | Paul Sorensen | AGIMO Changes included following meeting with Drew Andison & further feedback from Rekha Kattera 4 June 2010 |
| 2.0 | Final | July 2010 | Paul Sorensen | Further AGIMO changes included |
| 2.0 | Final | August 2010 | Lynn Du  Moulin | Final review |
| 2.0 | Final | 18 August 2010 | Paul Sorensen | Final review & clearance for independent legal review |
| 2.1 | Draft | 25 October  2010 | Paul Sorensen | Updates following legal review |
| 2.2 | Draft | 28 Feb 2011 | Paul Sorensen | Minor updates |
| 2.3 | Draft | 8 March 2011 | Lynn Du  Moulin | Further updates following legal Review |
| 2.4 | Draft | April 2011 | Paul Sorensen | Updates following AGIMO Review |
| 2.5 | Draft | May 2011 | Paul Sorensen | Updates following AGIMO Review |
| 2.6 | Draft | May 2011 | Paul Sorensen | Updates approved by AGIMO |
| 2.7 | Final | December  2016 | John Wong | Initial version reflecting changes in the  Gatekeeper PKI Framework version 3.1 |
| 2.8 | Draft | March 2017 | John Wong | Relocation of the Verizon Data Centre and the CA infrastructure. |
| 2.8 | Final | May 2017 | John Wong | Final review & clearance |

Copyright © 2017 Commonwealth of Australia Page 4

**Contents**

[1 Introduction 8](#_Toc76255)

[1.1 Background 8](#_Toc76256)

[1.2 Document name and identification 8](#_Toc76257)

[1.3 PKI participants 10](#_Toc76258)

[1.4 Certificate usage 12](#_Toc76259)

[1.5 Policy administration 12](#_Toc76260)

[1.6 Definitions and acronyms 14](#_Toc76261)

[2 Publication and repository responsibilities 15](#_Toc76262)

[2.1 Repositories 15](#_Toc76263)

[2.2 Publication of certification information 15](#_Toc76264)

[2.3 Time or frequency of publication 16](#_Toc76265)

[2.4 Access controls on repositories 16](#_Toc76266)

[3 Identification and authentication 17](#_Toc76267)

[3.1 Naming 17](#_Toc76268)

[3.2 Initial identity validation 17](#_Toc76269)

[3.3 Identification and authentication for re-key requests 17](#_Toc76270)

[3.4 Identification and authentication for revocation request 17](#_Toc76271)

[4 Certificate life-cycle operational requirements 18](#_Toc76272)

[4.1 Certificate application 18](#_Toc76273)

[4.2 Certificate application processing 18](#_Toc76274)

[4.3 Certificate issuance 18](#_Toc76275)

[4.4 Certificate acceptance 18](#_Toc76276)

[4.5 Key pair and certificate usage 18](#_Toc76277)

[4.6 Certificate renewal 18](#_Toc76278)

[4.7 Certificate re-key 18](#_Toc76279)

[4.8 Certificate modification 19](#_Toc76280)

[4.9 Certificate revocation and suspension 19](#_Toc76281)

[4.10 Certificate status services 19](#_Toc76282)

[4.11 End of subscription 19](#_Toc76283)

[4.12 Key escrow and recovery 20](#_Toc76284)

[5 Facility, management and operational controls 21](#_Toc76285)

[5.1 Physical controls 21](#_Toc76286)

[5.2 Procedural controls 21](#_Toc76287)

[5.3 Personnel controls 22](#_Toc76288)

[5.4 Audit logging procedures 22](#_Toc76289)

[5.5 Records archival 22](#_Toc76290)

[5.6 Key changeover 23](#_Toc76291)

[5.7 Compromise and disaster recovery 23](#_Toc76292)

[5.8 CA or RA termination 23](#_Toc76293)

[6 Technical security controls 24](#_Toc76294)

[6.1 Key pair generation and installation 24](#_Toc76295)

[6.2 Private key protection and cryptographic module engineering controls 25](#_Toc76296)

[6.3 Other aspects of key pair management 26](#_Toc76297)

[6.4 Activation data 27](#_Toc76298)

[6.5 Computer security controls 27](#_Toc76299)

[6.6 Life-cycle technical controls 27](#_Toc76300)

[6.7 Network security controls 28](#_Toc76301)

[6.8 Time-stamping 28](#_Toc76302)

[7 Certificate, CRL and OCSP profiles 29](#_Toc76303)

[7.1 Root CA certificate 29](#_Toc76304)

[7.2 Organisation CA certificate 34](#_Toc76305)

[8 Compliance audit and other assessments 40](#_Toc76306)

[8.1 Frequency or circumstances of assessments 40](#_Toc76307)

[8.2 Identity/qualifications of assessor 40](#_Toc76308)

[8.3 Assessor’s relationship to assessed entity 40](#_Toc76309)

[8.4 Topics covered by assessment 40](#_Toc76310)

[8.5 Actions taken as a result of deficiency 40](#_Toc76311)

[8.6 Communication of results 40](#_Toc76312)

[9 Other business and legal matters 41](#_Toc76313)

[9.1 Fees 41](#_Toc76314)

[9.2 Financial responsibility 41](#_Toc76315)

[9.3 Confidentiality of business information 41](#_Toc76316)

[9.4 Privacy of personal information 41](#_Toc76317)

[9.5 Intellectual property rights 42](#_Toc76318)

[9.6 Representations and warranties 43](#_Toc76319)

[9.7 Disclaimers of warranties 44](#_Toc76320)

[9.8 Limitations of liability 44](#_Toc76321)

[9.9 Indemnities 45](#_Toc76322)

[9.10 Term and termination 45](#_Toc76323)

[9.11 Individual notices and communications with participants 45](#_Toc76324)

[9.12 Amendments 46](#_Toc76325)

[9.13 Dispute resolution provisions 47](#_Toc76326)

[9.14 Governing law 48](#_Toc76327)

[9.15 Compliance with applicable law 48](#_Toc76328)

[9.16 Miscellaneous provisions 48](#_Toc76329)

[9.17 Other provisions 48](#_Toc76330)

# 1 Introduction

The commencement date of this Human Services Root Certification Authority Certificate Policy (Human Services RCA CP) is the date the Memorandum of Agreement (MOA) is signed by the Digital Transformation Agency (DTA) and the Department of Human Services (Human Services).

This Human Services RCA CP is written in accordance with RFC3647 ‘Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework’, and outlines the rules applying to and scope of use of Healthcare Network Public Key Infrastructure (Healthcare Network PKI) certificates.

### 1.1 Background

In general, a Public Key Infrastructure (PKI) consists of a hierarchy of Trusted Elements and

Subscribers. In the Healthcare Network PKI, the hierarchy of trusted elements comprises the Human Services Root Certification Authority (Human Services RCA), Organisation Certification Authorities (OCAs) (e.g. the Human Services OCA) and End User-Subscribers.

The Healthcare Network PKI is designed and operated to comply with the broad strategic direction of existing international standards for the establishment and operations of a PKI.

The Healthcare Network PKI supports the creation and use of key pairs and of public key certificates. Key pairs and public key certificates are used in the provision of Healthcare Network PKI certificate services that include but are not limited to:

 Authentication services (authentication, integrity and non-repudiation), and  Confidentiality services.

### 1.2 Document name and identification

1.2.1 Human Services RCA CP identification

Specified elements under the Healthcare Network PKI have been assigned an X.500 Object Identifier

(OID). The authority for issuing an OID is the Human Services Policy Management Authority (Human Services PMA).

Certificates issued under this CP shall bear the policy OID:

**1.2.36.174030967.1.2.2.1**

The Human Services RCA CPS is published on [humanservices.gov.au](http://www.humanservices.gov.au/)

1.2.2 Common elements

This Human Services RCA CP sets out the functions and obligations of PKI participants in the

Healthcare Network PKI. The Human Services Root Certification Authority Certification Practice Statement (Human Services RCA CPS) covers the common practices and procedures that apply to the entire Healthcare Network PKI Hierarchies operated by Human Services.

These common elements include:

* the use of Evaluated Products for any of the security-critical cryptographic operations
* the separation of registration and certification operations, with Certification Authority (CA) operations and registration operations generally being performed on a remote site managed and operated by the Human Services Registration Authority (RA) or a third party
* the application of tiered security comprising prevention, detection and considered response
* the employment of trustworthy personnel who have been independently vetted to the PROTECTED Negative Vetting 1 security level
* the application of rigorous change control processes to ensure no change is introduced without due consideration of all its possible security impacts, and
* the institution of a continuous cycle of internal and external audits to ensure a high level of operational integrity is always maintained.

1.2.3 Relationship between the certification practice statements and certificate policies

The full set of practices, procedures, terms and conditions relating to a particular certificate can be determined by reading:

* this Human Services RCA CP
* the Human Services Organisation Certification Authority Certification Practice Statement (Human Services OCA CPS) or the CPS for other OCAs within the Healthcare Network PKI Hierarchy
* the Human Services RCA CPS, and
* the Certificate Policy (CP) for the PKI Community of Interest (CoI) that the certificate is issued under.

1.2.4 Human Services Root Certification Authority Certificate Policy This Human Services RCA CP relates to:

* the self-signed Human Services RCA authentication and confidentiality certificates which the Human Services RCA issues to itself, and
* the authentication and confidentiality certificates signed by the Human Services RCA and issued to OCAs within the Healthcare Network PKI Hierarchy (e.g. the Human Services OCA).

If there is any conflict between the provisions in relevant CPS and CPs, the following order of precedence of documents will apply:

* the CP for the PKI CoI that the certificate was issued under, then
* other Healthcare Network PKI OCA CPs, then
* the Human Services OCA CPS or other Healthcare Network PKI OCA CPSs, then  this Human Services RCA CP, then  the Human Services RCA CPS.

1.2.5 DTA Gatekeeper PKI Framework Documentation

Human Services conducts its Human Services RCA role in accordance with the DTA PKI Gatekeeper Framework and the following documents:

* this Human Services RCA CP
* the Human Services RCA CPS
* the Human Services OCA CPS
* the relevant certificate policy the certificates are issued under
* the Healthcare Network PKI Glossary,
* Gatekeeper (Public Key Infrastructure) criteria and policies, and
* For Official Use Only (**FOUO**), Sensitive or PROTECTED documents which are not publicly available.

### 1.3 PKI participants

This Human Services RCA CP is applicable to:

* the Human Services RCA
* any subordinate Human Services OCA (e.g. the Human Services OCA)
* Human Services and Human Services contracted PKI Service Provider’s staff responsible for the issuance of certificates to Subscribers
* Human Services Registration Organisation Unit Operators (Human Services ROUOs) approved to operate within the Healthcare Network PKI hierarchy, and
* Relying parties and End User-Subscribers registered for Healthcare Network PKI keys and certificates issued under the CP for the Subscribers’ PKI CoI and supported by this CP.

1.3.1 Certification authorities

*1.3.1.1 Human Services RCA overview*

The Human Services RCA is the highest point of trust within the Healthcare Network PKI CoI. All other OCAs entities in the Human Services RCA Hierarchy rely on this point of trust.

The Human Services RCA generates and signs its own certificate and certifies the certificates of its subordinate OCAs, e.g. the Human Services OCA. In this CP, these OCAs (including the Human Services OCA) are referred to as ‘OCAs’.

The Human Services RCA is accessed via a single Root Certification Authority Operator (RCAO) which is used solely for the purpose of creating subordinate OCA certificates (e.g. the Human Services OCA certificate). The key length of the Human Services RCA Signing Key, used to sign certificates, is as determined by a relevant certificate profile. However, unless otherwise stated, the minimum key length for a Human Services RCA is 2048 bits.

Generation of the Human Services RCA’s keys is performed with trustworthy systems using evaluated products in a physically secure facility.

The Human Services RCA resides at a Secure Facility and is usually switched off except when required to create a new OCA.

*1.3.1.2 Human Services RCA functions*

The Human Services RCA performs the functions listed in section 1.3.1.2 of the Human Services RCA CPS.

*1.3.1.3 Human Services RCA obligations*

The Human Services RCA obligations are listed in section 1.3.1.3 of the Human Services RCA CPS.

*1.3.1.4 Human Services OCA overview*

Organisation Certification Authorities (OCAs) are immediately subordinate to the Human Services RCA in the Healthcare Network PKI hierarchy. The primary purpose of such a subordinate OCA (e.g. the Human Services OCA) is to provide certificates and certificate management services to relying parties and Subscribers within in the Healthcare Network PKI.

OCAs subordinate to the Human Services RCA include:

* the Human Services OCA that provides certificate management services for:
  + PKI CoI within Human Services, and
  + Australian Government Agencies who do not wish to operate their own Certification Authority for certification services for that Agency’s CoIs.
* other OCAs that may be included as OCAs subordinate to the Human Services RCA in the Healthcare Network PKI hierarchy.

The key length of Human Services OCA keys, used to sign certificates is determined by the relevant certificate profile. However, unless otherwise stated, the minimum key length for a Human Services OCA is 2048 bits.

Generation of Human Services OCA keys are performed on trustworthy systems using evaluated products in a physically secure facility.

The functions and obligations of OCAs, as a CA within the Healthcare Network PKI hierarchy, are dealt with in the CP under which the OCA issues certificates to members of a PKI CoI.

*1.3.1.5 Human Services OCA functions*

OCAs operating under the Healthcare Network PKI hierarchy perform the functions listed in section 1.3.1.5 of the Human Services OCA CPS.

Human Services OCA is an OCA of the Human Services RCA.

*1.3.1.6 Human Services OCA obligations*

An OCA’s (e.g. the Human Services OCA) obligations are listed in section 1.3.1.6 of the Human Services OCA CPS.

1.3.2 Registration authorities

This Human Services RCA CP does not include information on Registration Authorities (RAs) or certificate issuance. Information about certificate issuance for the Healthcare Network PKI is included in section 1.3.2 of the Human Services OCA CPS. The Human Services OCA CPS is available at [humanservices.com.au](http://www.humanservices.gov.au/)

The Human Services RCA is responsible for checking Evidence of Identity (EOI) and collecting registration information for and about subordinate OCAs only.

1.3.3 Subscribers

Subscribers of the Human Services RCA are OCAs that apply to be issued with certificates within the Healthcare Network PKI hierarchy managed by Human Services.

*1.3.3.1 Applicants*

An applicant is a third party who wishes to become a Human Services OCA subordinate to the Human Services RCA within the Healthcare Network PKI hierarchy.

Prior to a certificate being issued, the applicant must apply to the Human Services RCA to be a subordinate Human Services OCA and be issued a signed certificate binding the OCA public keys with the signed certificate.

*1.3.3.2 OCA Subscribers to Human Services RCA*

The obligations of OCAs, when acting as Subscribers under this Human Services RCA CP are listed in section 1.3.3.2 of the Human Services OCA CPS or in relevant sections of other Healthcare Network PKI OCA CPSs.

The issuance of certificates to End User-Subscribers is outside the scope of this Human Services RCA CP.

The obligations of End User-Subscribers are set out in the Human Services OCA CPS and CP for the PKI CoI under which the End User-Subscriber’s certificate was issued.

1.3.4 Relying parties

Relying parties and End User-Subscribers registered for Healthcare Network PKI keys and certificates issued under the CP for the Subscribers’ PKI CoI are supported by this CP.

*1.3.4.1 Other participants*

There are no other participants in the Healthcare Network PKI Registration certificate model operated by Human Services.

*1.3.4.2 End User-Subscribers*

The Human Services RCA does not issue certificates to End User-Subscribers and does not check EOI or collect registration information from End User-Subscribers.

### 1.4 Certificate usage

1.4.1 Appropriate certificate use

The Human Services RCA certificate may only be used to sign its own certificate, any OCA (including the Human Services OCA) certificates or RCA operational personnel certificates.

1.4.2 Prohibited certificate uses

The Human Services RCA certificate cannot directly sign end users/Subscribers certificates.

### 1.5 Policy administration

1.5.1 Organisation administering the document

This Human Services RCA CP is administered by the Human Services.

The Human Services PMA:

* approves changes to this CP, Human Services RCA CPS and other documents
* approves any OCA CP and CPS, including any changes to those documents, and
* manages compliance by an OCA and its RA(s) or certificate issuance process with the Human Services RCA CPS, this Human Services RCA CP, any OCA CPS, the CP the certificate was issued under, and other documents.

OCAs may operate an OCA Policy Management Authority (OCA PMA). An OCA’s PMA is responsible for the creation and internal approval of policies which are unique to the operation of that OCA but which must be consistent with this CP and RCA CPS.

The OCA’s PMA performs the following functions:

* formulates and gives internal approval to new policy and policy changes within the OCA policy domain, and
* submits new or changed policies to the Human Services PMA for approval.

1.5.2 Contact person

*1.5.2.1 Policy management authority*

The contact details for the Human Services PMA are:

National Manager

Payment and Claiming Branch

Health Service Delivery Division

Department of Human Services

PO Box 7788, Canberra BC ACT 2610

The contact person can provide copies of, or access to, this Human Services RCA CP, the Human Services RCA CPS and answer questions relating to the policy, practices and procedures described in these documents.

1.5.3 Persons determining CPS suitability for the relying party certificate policies

All new applications for Subscribers as an OCA and its RA under the Human Services RCA will be vetted by the Human Services PMA and if satisfactory, will be approved by the Human Services PMA.

1.5.4 CPS approval procedures

The Human Services PMA reviews all documents to ensure that the practices documented in the Human Services RCA CPS fulfil the requirements defined in this Human Services RCA CP.

The Human Services PMA determines whether or not the Human Services RCA CPS provides suitable support for this Human Services RCA CP.

The Human Services PMA approves all Human Services RCA CPS changes and modifications.

### 1.6 Definitions and acronyms

Please refer to the Human Services Healthcare Sector PKI Glossary at [humanservices.gov.au](http://www.humanservices.gov.au/) and the Digital Transformation Agency (DTA) - *Identity and Access Management Glossary* at [dta.gov.au](https://www.dta.gov.au/) for a list of definitions, acronyms and related terms.

# 2 Publication and repository responsibilities

### 2.1 Repositories

The repository for all public key certificates issued under this Human Services RCA CP is the Healthcare Public Directory.

The Healthcare Public Directory provides information about active, revoked and expired certificates issued under the respective CP(s) for each Registration Organisation Unit (ROU)’s PKI CoI, OCAs or the Human Services RCA.

Note that certificate suspension is not supported under the Registration certificate model as operated by Human Services in this Healthcare Network PKI.

Changes in the status of certificates issued under this Human Services RCA CP, including Revocation and Expiry of certificates will be published in the Healthcare Public Directory by the Human Services RCA.

The Healthcare Public Directory:

* does not publish reasons why a certificate has been revoked
* only publishes information already contained in the certificate, and
* only publishes information pertaining to a given PKI CoI when the responsible RO and ROU have agreed to publication.

The Healthcare Public Directory is accessible programmatically. Technical details are at [humanservices.gov.au](http://www.humanservices.gov.au/) and [certificates-australia.com.au](http://www.certificates-australia.com.au/)

The Healthcare Public Directory is available 24 hours a day, 7 days a week (except for designated system maintenance periods).

### 2.2 Publication of certification information

2.2.1 Publication of Human Services RCA information

Certificates and their corresponding hash values are published to the Healthcare Public Directory when the certificate is generated. In addition, the hash value of the Human Services RCA and Human Services RCA certificate is published on [certificates-australia.com.au](http://www.certificates-australia.com.au/)

2.2.2 Publication of policy and practice information

This Human Services RCA CP is published electronically at the Human Services website, [humanservices.gov.au](http://www.humanservices.gov.au/)

Formal notification of changes to this Human Services RCA CP will not be given to any entities.

Notification of changes will be provided on the Human Services website, [humanservices.gov.au](http://www.humanservices.gov.au/)

This notification method uses a ‘pull’ model. Interested parties must exercise due care and check, on a regular basis, the Human Services website to review and monitor any changes in the Human Services RCA CP. Interested parties are responsible for retrieving amendments when a revised and/or amended Human Services RCA CP is posted to the website.

### 2.3 Time or frequency of publication

2.3.1 Frequency of publication of this CP

New and revised approved versions of this Human Services RCA CP are published promptly at [humanservices.gov.au](http://www.humanservices.gov.au/) once approved by the Human Services PMA.

*2.3.1.1 Publication by OCAs*

All OCAs within the Healthcare Network PKI hierarchy must publish the current approved version of the Human Services RCA CPS and Human Services RCA CP on the web site(s) on which they publish their OCA CPS and any CPs that certificates are issued under.

### 2.4 Access controls on repositories

There are no access controls on the reading of this Human Services RCA CP, the Human Services RCA CPS or the CPS for the Human Services OCA or any associated OCA CPS and CPs on the web sites nominated for publication.

# 3 Identification and authentication

### 3.1 Naming

Subscribers under this CP are OCAs for the Human Services RCA.

Subscribers are termed ‘Certificate Subjects’ in the x.509 definition.

### 3.2 Initial identity validation

For the purposes of the Healthcare Network PKI, the Subscribers (Certificate Subjects) under this CP are identified and authenticated through the CA Key Signing Ceremony.

### 3.3 Identification and authentication for re-key requests

Subscribers under this CP shall be identified and authenticated and the certificates renewed using the same process as the identification and authentication process at registration.

Note: All certificate renewals under this CP involve the repeating the CA Key Signing Ceremony.

### 3.4 Identification and authentication for revocation request

Revocation of certificates under this CP shall only be requested by the Human Services PMA or Human Services IT Security Manager/Advisor or nominee with the same or higher security clearance.

# 4 Certificate life-cycle operational requirements

### 4.1 Certificate application

Upon approval from the Human Services PMA, the Human Services RCA is authorised to sign OCA certificates.

### 4.2 Certificate application processing

Human Services RCA and Human Services OCA certificate application processing are undertaken during the CA Key Signing Ceremony.

### 4.3 Certificate issuance

Certificates are issued at the CA Key Signing Ceremony and are held within the certificate creation facility and are not exposed externally to this facility.

### 4.4 Certificate acceptance

Human Services RCA and Human Services OCA certificate application processing are undertaken during the CA Key Signing Ceremony.

### 4.5 Key pair and certificate usage

The Human Services RCA key will only be used to sign Human Services OCA certificates.

4.5.1 Subscriber private key and certificate usage

Key pair generation and installation (that is, the CA Key Signing Ceremony) for the Human Services RCA and for OCAs signed by the Human Services RCA are documented with the Human Services contracted PKI Service Provider’s *SEC1* *Security Profile* (this document is not publicly available). Key usage flags are specified in technical profiles for the CA certificates in section 7. Refer to section

4.10.1 for further information regarding the operational role of the Human Services contracted PKI Service Provider

4.5.2 Relying party public key and certificate usage

Relying parties rely on public key and certificate usage only for appropriate applications outlined in this CP, and in the Subscribers’ PKI CoI policy documents.

### 4.6 Certificate renewal

Certificates issued under this CP will need to be renewed in the event of expiry of the certificates or as a result of unforeseen circumstances that may occur. They will be renewed by repeating the CA Key Signing Ceremony.

### 4.7 Certificate re-key

Certificate re-key is not supported for the Human Services RCA.

### 4.8 Certificate modification

Certificate modification is not supported for the Human Services RCA.

### 4.9 Certificate revocation and suspension

Certificates issued under this CP shall be revoked in the event of loss, destruction or theft of the RCA private key.

### 4.10 Certificate status services

4.10.1 Operational characteristics

The Human Services internet web site [(humanservices.gov.au)](http://www.humanservices.gov.au/) provides details of all current PKI policies pertaining to the Human Services RCA and OCA. This will include certificate policies for each community of interest operating under the Human Services RA.

Human Services contracted PKI Service Provider currently manages the Medicare CA and the bulk issuance of subscriber certificates. The Verizon Australia internet website ([certificatesaustralia.com.au)](http://www.certificates-australia.com.au/) provides:

1. All valid Human Services PKI certificates, and
2. The most up to date CRL.

Once a certificate is revoked, the CA will write the certificate serial number to the CRL. While the certificate is revoked immediately after the CA processes the revocation request, any end user checking the validity of the certificate will not be able to detect the revocation until the next refreshed CRL posting. End users should take into consideration the update frequency and grace period when checking CRLs.

Refer to section 7.1.2 for the CRL update frequency and grace period for the Human Services RCA.

Refer to section 7.2.2 for the CRL update frequency and grace period for the Human Services OCA. All revocation of certificates issued under Community of Interest certificate policies are published in this CRL.

4.10.2 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/)

4.10.3 Optional features

There is no optional features for certificates issued under this CP.

### 4.11 End of subscription

Certificates are terminated when they are revoked or have expired.

### 4.12 Key escrow and recovery

Key escrow is not supported by the Human Services RCA.

# 5 Facility, management and operational controls

### 5.1 Physical controls

5.1.1 Site location and construction

The Human Services RCA is housed in a CA facility accredited against the Gatekeeper Framework and operated to the level of PROTECTED as defined in the Australian Government Information Security Manual (ISM) and certified by a member of the Physical Security Evaluator as listed on the AttorneyGeneral’s website. The Gatekeeper Accredited CA is staffed on a 24 x 7 basis.

5.1.2 Physical access

The Human Services PMA decides the physical security access requirements for the Healthcare Network PKI and is described in section 5.1.2 of the Human Services RCA CPS.

5.1.3 Power and air conditioning

This is described in section 5.1.3 of the Human Services RCA CPS.

5.1.4 Water exposures

This is described in section 5.1.4 of the Human Services RCA CPS.

5.1.5 Fire prevention and protection

This is described in section 5.1.5 of the Human Services RCA CPS.

5.1.6 Media storage

This is described in section 5.1.6 of the Human Services RCA CPS.

5.1.7 Waste disposal

This is described in section 5.1.7 of the Human Services RCA CPS.

5.1.8 Off-site backup

This is described in section 5.1.8 of the Human Services RCA CPS.

### 5.2 Procedural controls

5.2.1 Trusted roles

This is described in section 5.2.1 of the Human Services RCA CPS.

5.2.2 Number of persons required per task

This is described in section 5.2.2 of the Human Services RCA CPS.

5.2.3 Identification and authentication for each role

Each Healthcare Network PKI operations personnel has a separate account so all operations can be traced to an individual.

5.2.4 Roles requiring separation of duties

This is described in section 5.2.4 of the Human Services RCA CPS.

### 5.3 Personnel controls

5.3.1 Qualifications, experience and clearance requirements

All Healthcare Network PKI operations personnel related to the RCA obligations require a Negative Vetting 1 clearance prior to being granted access to Human Services RCA trusted elements.

5.3.2 Background check procedures

This is described in section 5.3.2 of the Human Services RCA CPS.

5.3.3 Training requirements

This is described in section 5.3.3 of the Human Services RCA CPS.

5.3.4 Retraining frequency and requirements

This is described in section 5.3.4 of the Human Services RCA CPS.

5.3.5 Job rotation frequency and sequence

This is described in section 5.3.5 of the Human Services RCA CPS.

5.3.6 Sanctions for unauthorised actions

This is described in section 5.3.6 of the Human Services RCA CPS.

5.3.7 Independent contractor requirements

This is described in section 5.3.7 of the Human Services RCA CPS.

5.3.8 Documentation supplied to personnel

This is described in section 5.3.8 of the Human Services RCA CPS.

### 5.4 Audit logging procedures

This is described in section 5.4 of the Human Services RCA CPS.

### 5.5 Records archival

This is described in section 5.5 of the Human Services RCA CPS.

### 5.6 Key changeover

Key changeover will be affected in such a manner as to cause minimal disruption to Subscribers and End User-Subscribers.

This is described in section 5.6 of the Human Services RCA CPS.

### 5.7 Compromise and disaster recovery

This is described in section 5.7 of the Human Services RCA CPS and in section 7 in the Human Services Certification Authority Annex Documents (this document is not publicly available).

See the Human Services RCA CPS for information about the following:

* Incident and compromise handling procedures
* Computing resources, software, and/or data are corrupted
* Entity private key compromise procedures  Business continuity capabilities after a disaster.

### 5.8 CA or RA termination

Human Services may terminate the Healthcare Network PKI at its own discretion or as directed by the Commonwealth government.

If the Healthcare Network PKI is terminated, details of transition plans and procedures will be provided to CoI participants in a timely manner.

# 6 Technical security controls

### 6.1 Key pair generation and installation

6.1.1 Key pair generation

*6.1.1.1 Human Services RCA key pair generation*

Human Services RCA key pairs are generated and installed by the Human Services RCA using software that is listed on the Defence Signals Directorate (DSD) Evaluated Products Lists (EPL).

*6.1.1.2 Human Services RCA private key pair generation*

The self-generated Human Services RCA private keys do not require delivery.

6.1.2 Private key delivery to subscriber

OCA private keys are self-generated by the OCA and do not require delivery.

6.1.3 Public key delivery to certificate issuer

This is described in section 6.1.3 of the Human Services RCA CPS.

6.1.4 CA public key delivery to relying parties

The Human Services RCA public keys are made available to End User-Subscribers and relying parties via the Healthcare Public Directory.

6.1.5 Key sizes

The Human Services RCA key length is 2048 bits.

Subscriber OCA and RA key strengths are to be minimum 2048 bits in length.

Relying parties and End User-Subscriber key strengths are to be minimum length 2048 bits in length.

6.1.6 Public key parameters generation

*6.1.6.1 Parameter generation*

The parameters used to create the Human Services RCA public keys are generated by the Human Services RCA.

The parameters used to create the OCA public keys are generated by the OCA.

In both cases, the generation of public key parameters has been certified in the course of Common Criteria EAL 4 evaluation of the CA products used for key generation.

*6.1.6.2 Parameter checking*

Parameter quality checking (including primality testing for prime numbers where appropriate) has been certified in the course of Common Criteria evaluation of the CA products used for Human Services RCA key generation.

Parameter quality checking (including primality testing for prime numbers where appropriate) shall have been certified in the course of Common Criteria evaluation of the CA products used for OCA key generation.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

The Human Services RCA generates two key pairs and associated certificates. The two key pairs differ only in key usage. One key pair will only be used to sign OCA certificates and Certificate Revocation Lists (CRL)s. The second key pair will only be used for internal transaction integrity assurance purpose. Certificate profile associated with the second key pair is not publically available.

### 6.2 Private key protection and cryptographic module engineering controls

6.2.1 Cryptographic module standards and controls

If approved by Human Services, cryptographic modules may be used in the Healthcare Network PKI.

6.2.2 Private key (m of n) multi-person control

Human Services RCA private keys are not under ‘m of n’ multi-person control.

Dual person control shall be present for all operations concerning OCA or Human Services RCA private keys.

6.2.3 Private key escrow

Private key escrow is not supported.

6.2.4 Private key backup

The private keys of the Human Services RCA are generated and retained in a Hardware Cryptographic Module in an encrypted format. These are further encrypted and backed up onto smartcards with backup copies under m of n format and maintained on-site and in secure off-site storage.

Private key backup is not provided for Subscribers.

6.2.5 Private key archival

Private keys of the Human Services RCA are archived in a Secure Facility operated by the Human Services contracted PKI Service Provider.

6.2.6 Private key transfer into or from a cryptographic module

The Cryptographic module that holds the private key of the OCA or RA is generated and retained in the module in an encrypted format. It will be decrypted only at the time at which it is being transferred into and from the module.

6.2.7 Private key storage on a cryptographic module

The Cryptographic module that stores the private key of the OCA or RA is generated and stored in the module in an encrypted format.

6.2.8 Method of activating private key

The private keys of the Human Services RCA and of OCAs are activated by cryptographic software following the successful completion of a login process that validates an Authorised User.

6.2.9 Method of deactivating private key

The Human Services contracted PKI Service Provider’s *SEC1 Security Profile* details which personnel are authorised to deactivate private keys and in what manner (this document is not publicly available).

6.2.10 Method of destroying private key

This is described in section 6.2.10 of the Human Services RCA CPS.

6.2.11 Cryptographic module rating

Only cryptographic modules approved by the Australian Signals Directorate (ASD) shall be use for the Human Services RCA and OCAs. There is no stipulation on the Cryptographic Module rating.

### 6.3 Other aspects of key pair management

6.3.1 Public key archival

The public keys are stored in the Healthcare Public Directory for the life of the certificate.

At the expiration of the Human Services RCA, the public key will be archived for seven years in accordance with Records Archival set out at 5.5 in the RCA CPS.

6.3.2 Certificate operational periods and key pair usage periods

Usage periods for OCA public and private keys are specified in the OCA CP or OCA CPS.

The Human Services RCA key pairs have the following usage periods:

* Authentication private and public keys – twenty (20) years
* Transaction Integrity Assurance private and public key – twenty (20) years.

### 6.4 Activation data

No activation data other than Access Control mechanisms is required to operate cryptographic modules.

6.4.1 Activation data generation and installation

No activation data other than Access Control mechanisms is required to operate cryptographic modules.

6.4.2 Activation data protection

No activation data other than Access Control mechanisms is required to operate cryptographic modules.

6.4.3 Other aspects of activation data

No activation data other than Access Control mechanisms is required to operate cryptographic modules.

### 6.5 Computer security controls

6.5.1 Specific computer security technical requirements

Human Services details its computer security technical requirements in the Human Services contracted PKI Service Provider’s *SEC1* *Security Profile* (this document is not publicly available).

6.5.2 Computer security rating

Human Services details its computer security rating in the Human Services contracted PKI Service Provider’s *SEC1* *Security Profile* (this document is not publicly available).

### 6.6 Life-cycle technical controls

6.6.1 System development controls

The Human Services RCA and OCA detail their system development controls in the Human Services contracted PKI Service Provider’s *SEC1* *Security Profile* (this document is not publicly available).

6.6.2 Security management controls

Human Services CAs detail their security management controls in the Human Services contracted PKI Service Provider’s *SEC1* *Security Profile* (this document is not publicly available).

6.6.3 Life-cycle security ratings

Healthcare Network PKI life-cycle security ratings are set out in the Human Services contracted PKI Service Provider’s *SEC1* *Security Profile* (this document is not publicly available).

### 6.7 Network security controls

Human Services has undertaken a Risk Assessment that is presented in the Human Services Certification Authority Annex Documents. It identifies and addresses all high or significant life-cycle security threats (these documents are not publicly available).

### 6.8 Time-stamping

All automatically generated logs are time-stamped using the system clock of the computer on which they were generated. Manually generated records record the date of occurrence, but generally not the time.

# 7 Certificate, CRL and OCSP profiles

### 7.1 Root CA certificate

7.1.1 Certificate profile

*7.1.1.1 Root CA certificate profile*

|  |  |
| --- | --- |
| F**i**e**l**d**/** E**x**ten**sion** | **Root CA certificate** |
| Version | **Required** |
| V3 (2) |
| Serial Number | **Required** |
| Must be unique to an Issuer |
| Issuer Signature Algorithm | **Required** |
| sha256WithRSAEncryption {1 2 840 113549 1 1 11} |
| Issuer Distinguished Name | **Required** |
| Country (C) = AU  Organisation (O) = GOV  Organisation Unit (OU) = Humanservices  Common Name (CN) = Medicare Australia Root Certification Authority |
| Validity Period | **Required** |
| 20 years |
| Subject Distinguished Name | **Required** |
| Country (C) = AU  Organisation (O) = GOV  Organisation Unit (OU) = Humanservices  Common Name (CN) = Medicare Australia Root Certification Authority |
| Subject Public Key Information | **Required** |
| Public key encoded in accordance with RFC2459 & PKCS#1  Key length 2048 bits |
| Issuer Unique Identifier | **Not Used** |

|  |  |
| --- | --- |
| F**i**e**l**d**/** E**x**ten**sion** | **Root CA certificate** |
| Subject Unique Identifier | **Not Used** |
| Issuer’s Signature | **Required** |
| ASN.1 DER encoded certificate signature value corresponding to  Issuer signature algorithm |
| Authority Key Identifier | **Optional** |
| keyID, Octet contain the 20 byte SHA–1 hash of the binary DER encoding of the subject CA’s public key information |
| **Not Used** |
| Issuer DN, Serial Number tuple |
| Subject Key Identifier | **Required** |
| Octet string contain the 20 byte SHA–1 hash of the binary DER encoding of the subject CA’s public key information |
| Key Usage | **Required**  **Critical** |
| Certificate Signing, Off-line CRL Signing, CRL Signing |
| Basic Constraints | **Required**  **Critical** |
| CA True; path length constraint absent |
| Extended Key Usage | **Not Used** |
| Private Key Usage Period | **Not Used** |
| Certificate Policies | **Required** |
| Policy identifier OID = 1.2.36.174030967.1.2.2.1  CPS Point = http://humanservices.gov.au  Policy qualifier ID = User Notice  Notice Text = ‘Certificates under this policy are issued by the Medicare  Australia Root CA to itself and to CAs subordinate to the Medicare Australia Root CA’ |
| F**i**e**l**d**/** E**x**ten**sion** | **Root CA certificate** |
| Policy Mappings | **Optional** |
| **Not Used** |
| Subject Alternative Name | **Not Used** |
| Issuer Alternative Name | **Not Used** |
| Subject Directory Attributes | **Not Used** |
| Name Constraints | **Optional** |
| **Not Used** |
| Policy Constraints | **Optional** |
| **Not Used** |
| CRL Distribution Points | **Optional** |
| **Not Used** |
| Subject Information Access | **Optional** |
| **Not Used** |
| Freshest CRL | **Not Used** |
| Inhibit Any Policy | **Optional** [[1]](#footnote-1) |
| **Not Used** |

*7.1.1.2 Version number(s)*

Certificates issued by the Human Services RCA are X.509 version 3.

*7.1.1.3 Certificate extensions*

Certificate extensions are used by the Human Services RCA certificates and are listed in the certificate profile table.

*7.1.1.4 Algorithm object identifiers*

OIDs are not allocated to algorithms in the Healthcare Network PKI.

*7.1.1.5 Name forms*

Certificates issued under the Healthcare Network PKI contain the full X.500 Distinguished Name of the certificate issuer and Certificate Subject in the issuer name (Human Services) and subject name (Human Services) fields respectively.

*7.1.1.6 Name constraints*

Anonymous names are not supported by the Human Services RCA.

*7.1.1.7 Certificate policy object identifier*

The OID of the Human Services RCA CP is carried in the standard extension field of issued X.509 certificates and is published under CP Identification in section 1.2 of this CP.

*7.1.1.8 Usage of policy constraints extension*

The Human Services RCA supports the use of the policy constraints extension.

*7.1.1.9 Policy qualifiers syntax and semantics*

The Human Services RCA supports the use of syntax and semantics policy qualifiers.

*7.1.1.10 Processing semantics for the critical certificate policy extension*

The X.509 certificate profile complies with the Australian Standard X.509 profile.

7.1.2 CRL profile

|  |  |
| --- | --- |
| F**i**e**l**d**/**E**x**ten**sion** | **Root CA Certificate Revocation List** |
| Version | **Required** |
| V2 |
| Issuer Distinguished Name | **Required** |
| Country (C) = AU  Organisation (O) = GOV  Organisation Unit (OU) = Humanservices  Common Name (CN) = Medicare Australia Root Certification Authority |
| Effective Date | **Required** |
| Effective date of CRL |
| Next Update | **Required** |
| Next time when CRL will be updated |
| Signature Algorithm | **Required** |
| sha256WithRSAEncryption {1 2 840 113549 1 1 11} |
| CRL Number | **Required** |
| Increment with each CRL update |
| Authority Key Identifier | **Required** |
| Octet string contain the 20 byte SHA–1 hash of the binary DER encoding of the subject CA’s public key information |

*7.1.2.1 Version number(s)*

The Human Services RCA supports the use of X.509 Version 2 CRLs.

*7.1.2.2 CRL and CRL entry extensions*

The Human Services RCA supports the use of X.509 Version 2 CRL entry extensions as shown in the CRL profile table.

*7.1.2.3 CRL generation frequency*

The Human Services RCA will generate a new CRL every 26 days.

*7.1.2.4 CRL Grace Period*

The Human Services RCA CRL will have a grace period of 5 days.

7.1.3 OCSP profile

Online Certificate Status Protocol (OCSP) is not currently approved by the Human Services PMA for this Human Services RCA. OCSP status for each OCA is reflected within the relevant OCA CPS.

### 7.2 Organisation CA certificate

7.2.1 Certificate profile

*7.2.1.1 Organisation CA certificate profile*

|  |  |
| --- | --- |
| F**i**e**l**d**/** E**x**ten**sion** | **Organisation CA certificate** |
| Version | **Required** |
| V3 |
| Serial Number | **Required** |
| Must be unique to an Issuer |
| Issuer Signature Algorithm | **Required** |
| sha256WithRSAEncryption {1 2 840 113549 1 1 11} |
| Issuer Distinguished Name | **Required** |
| Country (C) = AU  Organisation (O) = GOV  Organisation Unit (OU) = Humanservices  Common Name (CN) = Medicare Australia Root Certification Authority |
| Validity Period | **Required** |
| 10 years |
| Subject Distinguished Name | **Required** |

|  |  |
| --- | --- |
| F**i**e**l**d**/** E**x**ten**sion** | **Organisation CA certificate** |
|  | Country (C) = AU  Organisation (O) = GOV  Organisation Unit (OU) = Humanservices  Common Name (CN) = Medicare Australia Organisation Certification Authority |
| Subject Public Key Information | **Required** |
| Public key encoded in accordance with RFC2459 & PKCS#1  Key length 2048 bits |
| Issuer Unique Identifier | Not Used |
| Subject Unique Identifier | Not Used |
| Issuer’s Signature | **Required** |
| ASN.1 DER encoded certificate signature value corresponding to  Issuer signature algorithm |
| Authority Key Identifier | **Optional** |
| keyID, Octet contain the 20 byte SHA–1 hash of the binary DER encoding of the subject CA’s public key information |
| **Not Used** |
| Issuer DN, Serial Number tuple |
| Subject Key Identifier | **Required** |
| Octet string contain the 20 byte SHA–1 hash of the binary DER encoding of the subject CA’s public key information |
| Key Usage | **Required**  **Critical** |
| Certificate Signing, Off-line CRL Signing, CRL Signing |
| Basic Constraints | **Required**  **Critical** |
| CA True; path length constraint absent |

|  |  |
| --- | --- |
| F**i**e**l**d**/** E**x**ten**sion** | **Organisation CA certificate** |
| Extended Key Usage | **Not Used** |
| Private Key Usage Period | **Not Used** |
| Certificate Policies | **Required** |
| Policy identifier OID = 1.2.36.174030967.1.2.2.1  CPS Point = http://humanservices.gov.au  Policy qualifier ID = User Notice  Notice Text = ‘Certificates under this policy are issued by the Medicare  Australia Root CA to CAs subordinate to the Medicare Australia Root CA’ |
| Policy Mappings | **Optional** |
| **Not Used** |
| Subject Alternative Name | **Not Used** |
| Issuer Alternative Name | **Not Used** |
| Subject Directory Attributes | **Not Used** |
| Name Constraints | **Optional** |
| **Not Used** |
| Policy Constraints | **Optional** |
| **Not Used** |
| CRL Distribution Points | **Optional** |
| **Not Used** |
| Subject Information Access | **Optional** |
| **Not Used** |
| Freshest CRL | Not Used |
| Inhibit Any Policy | **Optional** [[2]](#footnote-2) |
| Not Used |

*7.2.1.2 Version number(s)*

Certificates issued by the Human Services RCA are X.509 version 3.

*7.2.1.3 Certificate extensions*

Certificate extensions are used by the Human Services OCA certificates and are listed in the certificate profile table.

*7.2.1.4 Algorithm object identifiers*

OIDs are not allocated to algorithms in the Healthcare Network PKI.

*7.2.1.5 Name forms*

Certificates issued under the Healthcare Network PKI contain the full X.500 Distinguished Name of the certificate issuer and Certificate Subject in the issuer name (Human Services) and subject name (Human Services) fields respectively.

*7.2.1.6 Name constraints*

Anonymous names are not supported by the Human Services OCA.

*7.2.1.7 Certificate policy object identifier*

The OID of the Human Services RCA CP is carried in the standard extension field of issued X.509 certificates and is published under CP Identification in section 1.2 of this CP.

*7.2.1.8 Usage of policy constraints extension*

The Human Services OCA supports the use of the policy constraints extension.

*7.2.1.9 Policy qualifiers syntax and semantics*

The Human Services OCA supports the use of syntax and semantics policy qualifiers.

*7.2.1.10 Processing semantics for the critical certificate policy extension*

The X.509 certificate profile complies with the Australian Standard X.509 profile.

7.2.2 CRL profile

|  |  |
| --- | --- |
| F**i**e**l**d**/**E**x**ten**sion** | **Organisation CA Certificate Revocation List** |
| Version | **Required** |
| V2 |
| Issuer Distinguished Name | **Required** |
| Country (C) = AU  Organisation (O) = GOV  Organisation Unit (OU) = Humanservices  Common Name (CN) = Medicare Australia Organisation Certification Authority |
| Effective Date | **Required** |
| Effective date of CRL |
| Next Update | **Required** |
| Next time when CRL will be updated |
| Signature Algorithm | **Required** |
| sha256WithRSAEncryption {1 2 840 113549 1 1 11} |
| CRL Number | **Required** |
| Increment with each CRL update |
| Authority Key Identifier | **Required** |
| Octet string contain the 20 byte SHA–1 hash of the binary DER encoding of the subject CA’s public key information |

*7.2.2.1 Version number(s)*

The Human Services OCA supports the use of X.509 Version 2 CRLs.

*7.2.2.2 CRL and CRL entry extensions*

The Human Services OCA supports the use of X.509 Version 2 CRL entry extensions as shown in the CRL profile table.

*7.2.2.3 CRL generation frequency*

The Human Services OCA will generate a new CRL every 30 minutes.

*7.2.2.4 CRL Grace Period*

The Human Services OCA CRL will have a grace period of 1 day.

7.2.3 OCSP profile

Online Certificate Status Protocol (OCSP) is not currently approved by the Human Services PMA for this Human Services OCA. OCSP status for each OCA is reflected within the relevant OCA CPS.

# 8 Compliance audit and other assessments

The Human Services PMA will authorise audits and assessments for compliance where necessary.

### 8.1 Frequency or circumstances of assessments

The Human Services PMA may conduct regular internal assessments of Human Services RCA processes in addition to the annual Gatekeeper audit conducted by a member of the Audit Panel listed on the Gatekeeper website.

### 8.2 Identity/qualifications of assessor

External assessments will be conducted by a Human Services-approved Authorised Assessor.

Internal assessments will be conducted by a qualified physical and logical security assessor.

### 8.3 Assessor’s relationship to assessed entity

This is described in section 8.3 of the Human Services RCA CPS and in the Human Services contracted PKI Service Provider’s *SEC1* *Security Profile* (this document is not publicly available).

### 8.4 Topics covered by assessment

This is described in section 8.4 of the Human Services RCA CPS and in the Human Services contracted PKI Service Provider’s *SEC1* *Security Profile* (this document is not publicly available).

### 8.5 Actions taken as a result of deficiency

This is described in section 8.5 of the Human Services RCA CPS and in the Human Services contracted PKI Service Provider’s *SEC1* *Security Profile* (this document is not public available).

### 8.6 Communication of results

External audit results will be communicated to the Human Services PMA and also to the Gatekeeper Competent Authority.

# 9 Other business and legal matters

### 9.1 Fees

Not applicable.

### 9.2 Financial responsibility

9.2.1 Insurance coverage

All insurances are the responsibility of each Subscriber.

9.2.2 Other assets

Other assets are not considered under this Human Services RCA CP.

9.2.3 Warranty coverage

There is no warranty coverage available for Subscribers or relying parties under this Human Services RCA CP.

### 9.3 Confidentiality of business information

9.3.1 Scope of confidential information

For information about scope of confidential information, refer to the Human Services privacy policy located at [humanservices.gov.au](http://www.humanservices.gov.au/)

9.3.2 Information not within the scope of confidential information

For information about information not within the scope of confidential information, refer to the Human Services privacy policy located at [humanservices.gov.au](http://www.humanservices.gov.au/)

9.3.3 Responsibility to protect confidential information

For information about responsibility to protect confidential information, refer to the Human Services privacy policy located at [humanservices.gov.au](http://www.humanservices.gov.au/)

### 9.4 Privacy of personal information

For information about privacy of personal information, refer to the Human Services privacy policy located at [humanservices.gov.au](http://www.humanservices.gov.au/)

9.4.1 Privacy plan

For information about privacy plan, refer to the Human Services privacy policy located at [humanservices.gov.au](http://www.humanservices.gov.au/)

9.4.2 Information treated as private

For information about information treated as private, refer to the Human Services privacy policy located at [humanservices.gov.au](http://www.humanservices.gov.au/)

9.4.3 Information not deemed private

For information about information not deemed private, refer to the Human Services privacy policy located at [humanservices.gov.au](http://www.humanservices.gov.au/)

9.4.4 Responsibility to protect private information

For information about responsibility to protect private information, refer to the Human Services privacy policy located at [humanservices.gov.au](http://www.humanservices.gov.au/)

9.4.5 Notice and consent to use private information

For information about notice and consent to use private information, refer to the Human Services privacy policy located at [humanservices.gov.au](http://www.humanservices.gov.au/)

9.4.6 Disclosure pursuant to judicial or administrative process

Human Services and/or Human Services contracted PKI Service Provider will comply, where required by a court of law or a tribunal, in accordance with the Rules of that Court or the procedures of that Tribunal and with the Legal Services Directions (Commonwealth).

9.4.7 Other information disclosure circumstances

For information about other information disclosure circumstances, refer to the Human Services privacy policy located at [humanservices.gov.au](http://www.humanservices.gov.au/)

### 9.5 Intellectual property rights

Human Services materials include, but are not limited to:

* the Human Services RCA certificate and keys
* this Human Services RCA CP
* the Human Services RCA CPS
* the Human Services OCA certificate and keys
* the Human Services OCA CPS
* the contents of the Healthcare Public Directory
* any other data or database created by Human Services, the Human Services RCA, the Human Services OCA, the Card Management System or Human Services contractors and subcontractors for the purposes of the Healthcare Network PKI
* all certificate policies for all ROU CoIs
* all applications and Terms and Conditions between Human Services and the Subscribers in Human Services ROUs’ CoI, and
* all other documents owned by Human Services and published on the Human Services website [(humanservices.gov.au)](http://www.humanservices.gov.au/) for the purposes of the Healthcare Network PKI.

Intellectual Property Rights in Human Services materials and in any modifications or enhancements made to Human Services materials remain, or are from the date of creation, the property of the Human Services.

The Human Services RCA, Human Services OCA, Human Services Subscribers and relying parties must ensure that Human Services materials are, to the extent practicable, identified as the property of Human Services (for the Commonwealth) and that Human Services materials remain at all times free of any lien, charge or other encumbrance of a third party.

Human Services grants to Subscribers and relying parties a revocable, royalty-free, nonexclusive, non-transferable license for the terms of a Subscriber’s certificate, to view, display and use

(including downloading, reproducing and printing) Human Services materials for the purpose of:  participating in the Healthcare Network PKI, and

 understanding their rights and obligations under the Healthcare Network PKI, including obtaining legal or other advice as necessary.

### 9.6 Representations and warranties

9.6.1 CA representations and warranties

To the extent permitted by law and notwithstanding any other provision of any Healthcare Network PKI documents or whether keys or certificates are used in a transaction or not, the Commonwealth, its Agencies and Human Services make no representations or warranties to any:

* Agency
* CA service provider  RA service provider
* Subscriber
* relying party, or
* other participant

in relation to their activities or performance of the Healthcare Network PKI and any services or products associated with, or part of, or used in delivery of the Healthcare Network PKI.

9.6.2 RA representations and warranties

To the extent permitted by law and notwithstanding any other provision of any Healthcare Network PKI documents or whether keys or certificates are used in a transaction or not, Agencies, RA service providers, Subscribers, relying parties and other participants (collectively, other parties) make no representations or warranties to the:

* Commonwealth
* any Commonwealth Agencies
* Human Services, or
* each other

in relation to their activities or performance of the Healthcare Network PKI and any services or products associated with, or part of, or used in delivery of the Healthcare Network PKI.

### 9.7 Disclaimers of warranties

9.7.1 CA Disclaimer of warranties

The Commonwealth, it’s Agencies and Human Services disclaims all warranties, express or implied.

If any warranties or conditions are implied by legislation, then the liability of the Commonwealth, its Agencies and Human Services (and of any of their officers, staff and contractors (including subcontractors)), for any breach of the condition or warranty is limited to:  re-performing the services to which the warranty applied, or  paying the cost of re-performing those services.

9.7.2 Gatekeeper accreditation disclaimer

The Gatekeeper Competent Authority is responsible for ensuring that the accreditation process is conducted with due care and in accordance with published Gatekeeper criteria and policies. The Gatekeeper Competent Authority is not liable for any errors and/or omissions in the final approved documents, which remain the responsibility of the accredited service provider.

The Digital Transformation Agency is not responsible and cannot be held liable for any loss of any kind in relation to the use of digital keys and certificates issued by a Gatekeeper accredited service provider. By granting a service provider Gatekeeper Accreditation the Digital Transformation Agency makes no representation and gives no warranty as to the:

* accuracy of any statements or representations made in, or suitability of, the approved documents of a Gatekeeper accredited service provider
* accuracy of any statement or representation made in, or suitability of, the documentation of a service provider in a Gatekeeper recognised PKI domain, or
* standard or suitability of any services thereby provided by any Subscriber or relying party or application.

### 9.8 Limitations of liability

9.8.1 Limitation of liability

The aggregate liability of the Commonwealth and its Agencies and Human Services (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 Healthcare Network PKI, including but not limited to:

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

9.8.2 Gatekeeper core obligations

The parties acknowledge that the limitation of liability in clause 9.8.1 does not exclude Human Services’ obligation to comply with its Gatekeeper core obligations.

### 9.9 Indemnities

Indemnities are not provided between parties in the Healthcare Network PKI to which this Human Services RCA CP applies.

### 9.10 Term and termination

9.10.1 Term

The RCA CP will be ongoing. Refer to 9.10.2 for details as to when it may be terminated.

9.10.2 Termination

Human Services may terminate this Healthcare Network PKI at its own discretion or otherwise as may be required by the Commonwealth government.

Human Services will promptly notify, in accordance with clause 9.11, all OCAs, RAs, Subscribers, relying parties, the Gatekeeper Competent Authority and other participants of the intended termination of the Healthcare Network PKI.

9.10.3 Effect of termination and survival

The Human Services RCA and the Human Services OCA will, on notification of termination, cease to generate and issue certificates.

On termination, all certificates issued under this Human Services RCA CP and under any CP remain in force for any period left of the two-year or five year operative time of the certificate in accordance with that relevant CP.

The Healthcare Public Directory will be maintained for the period left of all certificates current at the date of termination.

### 9.11 Individual notices and communications with participants

For the purpose of this clause, a Notice includes a consent, information, application, request or any other communication provided under or in connection with this Human Services RCA CP.

A Notice to a party under this Human Services RCA CP is only given or made if it is in writing and distributed in one of the following ways:

* delivered or posted to that party at its postal address
* emailed to that party at its email address
* faxed to that party at its fax number, or
* posted on the Human Services website ([humanservices.gov.au)](http://www.humanservices.gov.au/) in accordance with this clause.

A Notice can only be provided by email where:

* the sender and recipient are holders of current certificates which have not been revoked, and
* the sender digitally signs the message using the sender’s private authentication key.

A Notice will be issued and posted to the relevant websites when any of the following events occurs:

* a new Human Services RCA CP or Human Services CPS is approved
* there is a change or alteration to an existing Human Services CP or Human Services RCA CPS, and/or
* any other event which the Human Services PMA deem appropriate.

If a party gives the other parties three Business Days’ notice of a change of its postal address, fax number or email address, a Notice is only given or made by that other party if it is delivered, posted, faxed or emailed to the latest postal or email address or fax number.

A Notice is given or made as follows:

* if it is delivered, when it is left at the relevant address
* if it is sent by post, three Business Days after it is posted (seven days if posted to or from a place outside Australia)
* if it is sent by facsimile, as soon as the sender receives from the sender’s facsimile machine a report of an error free transmission to the correct facsimile number
* if it is sent by email, as soon as the recipient’s host machine receives the Notice and the

Digital Signature has been verified and authenticated, and/or

* if it is posted on the Human Services website ([humanservices.gov.au)](http://www.humanservices.gov.au/), five Business Days after it is posted.

If a Notice is delivered, or an error free transmission report in relation to it is received, on a day that is not a Business Day, or if on a Business Day, after 5pm on that day in the place of the party to whom it is sent, it is to be treated as having been given or made at the beginning of the next Business Day.

## 9.12 Amendments

The policy approval authority for this Human Services RCA CP, the Human Services RCA CPS, the Human Services OCA CPS and related CP documents is the Human Services PMA.

9.12.1 Procedure for amendment

Human Services operates the Human Services PMA which is responsible for setting certificate policies for the Healthcare Network PKI operated by Human Services.

The Human Services PMA also gives internal approval to CPs within the Healthcare Network PKI operated by Human Services.

The Human Services PMA is the General Manager or nominee, Health Service Delivery Division, Human Services.

All proposed amendments must be approved by the Human Services PMA.

9.12.2 Notification mechanism and period

Amended or varied CPS and CPs will be posted at [humanservices.gov.au/pki](https://www.humanservices.gov.au/health-professionals/enablers/public-key-infrastructure-pki-policy-documents) as soon as practicable after approval by the Human Services PMA.

9.12.3 Circumstances under which OID must be changed

Where a change to a CPS or CP is required, the OID of the policy will stay the same. However, a new version number will be allocated by the Human Services PMA on its endorsement of the amended CPS or CP.

A new OID must be given when a new CP is created for a different CoI of Interest.

## 9.13 Dispute resolution provisions

Disputes arising out of the CP the certificates is issued under shall be resolved using the following processes:

* The parties shall use their best endeavours to resolve any problem that arises by negotiating with each other.
* No party shall resort to court proceedings (except for proceedings necessary to seek an urgent interim relief) in respect of a dispute arising out of or in connection with the CP the certificates is issued under until the process outlined in this section has been exhausted.
* If a problem arises (including a breach or an alleged breach) which is not resolved at the operational level, or is sufficiently serious that it cannot be resolved at the operational level, the party with the problem shall notify the other party, and the management representatives of each of the parties shall endeavour to agree on a resolution.
* If the management representatives of each of the parties fail to reach a solution to the dispute within five Business Days from the date notice of the problem was first given, the parties may seek to settle the matter by referring the issue for mediation, administered by the Australian Commercial Disputes Centre (ACDC).
* The mediation is to be conducted in accordance with the latest version of the ACDC Mediation Guidelines to the extent that such guidelines are not inconsistent with any other provisions of this CP unless the mediation is administered by an organisation other than the ACDC, in which case the mediation is to be conducted in accordance with the current guidelines of that organisation, to the extent that such guidelines are not inconsistent with any other provision of the CP the certificates is issued under.
* In the event that the dispute has not been settled within twenty eight (28) Business Days or other such period as agreed to in writing between the parties after the appointment of the mediator, the dispute may be submitted to arbitration administered by ACDC and in accordance with their current arbitration guidelines.
* The arbitrator shall not be the same person as the mediator.
* The parties will promptly furnish to the arbitrator (imposing appropriate obligations of confidence) all information reasonably requested by the arbitrator relating to the dispute.
* If either party breaches any provision of this section in relation to a dispute, the other party need not comply with that provision in relation to that same dispute.
* Unless prevented by the nature of the dispute, the parties shall continue to perform in accordance with the CP the certificate is issued under while attempts are made to resolve the dispute.
* The parties will share equally the fees and expenses of the mediator or the arbitrator, as the case may be.

Disputes relating to any contractual relationship referred to in, or related to the CP the certificates is issued under, other than disputes relating to a CP, must be resolved in accordance with the contract governing that relationship.

## 9.14 Governing law

All CPSs and each CP are governed by, and are to be construed in accordance with, the laws from time to time in force in the Australian Capital Territory.

The parties agree to submit to the courts having jurisdiction in the Australian Capital Territory.

## 9.15 Compliance with applicable law

In conducting the activities under the CP the certificates are issued under, all parties agree to abide by the provisions of all relevant legislation, and the requirements of any Commonwealth, State, Territory or local body.

## 9.16 Miscellaneous provisions

Clauses that relate to Intellectual Property Rights, safety, integrity, accuracy of information, confidentiality, privacy, liability and indemnity will survive the expiration or termination (for whatever reason) of this Human Services RCA CP, the Human Services RCA CPS, the Human Services OCA CPS and the CP the certificate is issued.

## 9.17 Other provisions

For information about other provisions, refer to the Human Services OCA CPS located at [humanservices.gov.au/pki](https://www.humanservices.gov.au/health-professionals/enablers/public-key-infrastructure-pki-policy-documents)

1. This is not conformant to RFC 5280 however is required do overcome potential application compatibility issues [↑](#footnote-ref-1)
2. This is not conformant to RFC 5280 however is required do overcome potential application compatibility issues [↑](#footnote-ref-2)