

**Australian Government Department of Human Services Root Certification Authority Certificate Practice Statement**

Version 2.7

**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)

**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**  |
| 0.1  | DRAFT  | 16 August 2006  | Robert Parker Patrick Tang  | Initial draft for internal review.  |
| 0.2  | DRAFT  | 21 August 2006  | Patrick Tang  | Accept/delete formatting to make it more readable, all fields’ macros are also removed and replaced with the actual text.  |
| 0.3  | DRAFT  | 25 August 2006  | Lynn Du Moulin  | Revision of draft, including inserting Part 9 information from OCA CPS  |
| 0.4  | DRAFT  | 29/08/2006  | Lynn Du Moulin  | Acceptance of v.03 amendments (in consultation with J Brewer); further revisions to consolidate information on Client CAs; revise information on termination and other amendments to ensure this CPS links with the OCA CPS and the RCA CP.  |
| 0.5  | Draft  | 30/08/2006  | Robert Parker  | Acceptance and review of changes  |
| 0.6  | Draft  | 01/09/2006  | Lynn Du Moulin  | Amendments re references to CoIs; deletion of settled comments; amendments to Part 9.  |
| 1.0  | FINAL  | 5/09/2006  | Lynn Du Moulin  | Acceptance of edits; deletion of comments as per meeting with John Brewer. Change of “client CA” to “OCA” as advised by S Wilson Minor edits / tidy up  |
| 1.9  | FINAL  | 8 SEPTEMBER 2006  | LYNN DU MOULIN  | NUMBER CHANGE TO 1.9 FINAL TO MATCH OID  |
| 1.9  | FINAL  | 18 Sept 2006  | Lynn Du Moulin  | Amendments to change PMA membership  |
| 1.91  | Final  | 20 November 2006  | John Brewer  | Deletion of reference to the IT Security Manager in 5.2.4  Other minor grammatical amendments  |
| 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  | November2008  | Paul Sorensen  | Amendments after review by the Gatekeeper Competent Authority and further review by Medicare Australia.  |
| 1.97  | Draft  | February 2010  | Paul Sorensen  | Updated References  |
| 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  | 27 October 2010  | Paul Sorensen  | Updates following Legal Review  |
| 2.2  | Draft  | 28 February 2011  | Paul Sorensen  | Update adjustments  |
| 2.3  | Draft  | 9 March 2011  | Lynn Du Moulin  | Update adjustments following Legal Review  |
| 2.4  | Draft  | April 2011  | Paul Sorensen  | Update adjustments following AGIMO Review  |
| 2.5  | Draft  | May 2011  | Paul Sorensen  | Update adjustments following AGIMO Review and approval  |
| 2.6  | Final  | December 2016  | John Wong  | Initial version reflecting changes in the Gatekeeper PKI Framework version 3.1  |
| 2.7  | Draft  | March 2017  | John Wong  | Relocation of the Verizon Data Centre and the CA infrastructure and DTA feedback.  |
| 2.7  | Final  | May 2017  | John Wong  | Final review & clearance  |

**Contents**

[1 Introduction 7](#_Toc60054)

[1.1 Background 7](#_Toc60055)

[1.2 Document name and identification 7](#_Toc60056)

[1.3 PKI participants 9](#_Toc60057)

[1.4 Certificate usage 15](#_Toc60058)

[1.5 Policy administration 16](#_Toc60059)

[1.6 Definitions and acronyms 17](#_Toc60060)

[2 Publication and repository responsibilities 18](#_Toc60061)

[2.1 Repositories 18](#_Toc60062)

[2.2 Publication of certification information 18](#_Toc60063)

[2.3 Time or frequency of publication 19](#_Toc60064)

[2.4 Access controls on repositories 19](#_Toc60065)

[3 Identification and authentication 20](#_Toc60066)

[3.1 Naming 20](#_Toc60067)

[3.2 Initial identity validation 20](#_Toc60068)

[3.3 Identification and authentication for re-key requests 20](#_Toc60069)

[3.4 Identification and authentication for revocation request 20](#_Toc60070)

[4 Certificate life-cycle operational requirements 21](#_Toc60071)

[5 Facility, management and operational controls 22](#_Toc60072)

[5.1 Physical controls 22](#_Toc60073)

[5.2 Procedural controls 23](#_Toc60074)

[5.3 Personnel controls 24](#_Toc60075)

[5.4 Audit logging procedures 27](#_Toc60076)

[5.5 Records archival 28](#_Toc60077)

[5.6 Key changeover 29](#_Toc60078)

[5.7 Compromise and disaster recovery 30](#_Toc60079)

[5.8 CA or RA termination 30](#_Toc60080)

[6 Technical security controls 31](#_Toc60081)

[6.1 Key pair generation and installation 31](#_Toc60082)

[6.2 Private key protection and cryptographic module engineering controls 32](#_Toc60083)

[6.3 Other aspects of key pair management 33](#_Toc60084)

[6.4 Activation data 34](#_Toc60085)

[6.5 Computer security controls 34](#_Toc60086)

[6.6 Life-cycle technical controls 35](#_Toc60087)

[6.7 Network security controls 35](#_Toc60088)

[6.8 Time-stamping 35](#_Toc60089)

[7 Certificate, CRL and OCSP profiles 36](#_Toc60090)

[7.1 Certificate profile 36](#_Toc60091)

[7.2 CRL profile 37](#_Toc60092)

[7.3 OCSP profile 37](#_Toc60093)

[8 Compliance audit and other assessments 38](#_Toc60094)

[8.1 Frequency or circumstances of assessments 38](#_Toc60095)

[8.2 Identity/qualifications of assessor 38](#_Toc60096)

[8.3 Assessor’s relationship to assessed entity 38](#_Toc60097)

[8.4 Topics covered by assessment 38](#_Toc60098)

[8.5 Actions taken as a result of deficiency 38](#_Toc60099)

[8.6 Communication of results 39](#_Toc60100)

[9 Other business and legal matters 40](#_Toc60101)

[9.1 Fees 40](#_Toc60102)

[9.2 Financial responsibility 40](#_Toc60103)

[9.3 Confidentiality of business information 40](#_Toc60104)

[9.4 Privacy of personal information 40](#_Toc60105)

[9.5 Intellectual property rights 40](#_Toc60106)

[9.6 Representations and warranties 40](#_Toc60107)

[9.7 Disclaimers of warranties 40](#_Toc60108)

[9.8 Limitations of liability 41](#_Toc60109)

[9.9 Indemnities 41](#_Toc60110)

[9.10 Term and termination 41](#_Toc60111)

[9.11 Individual notices and communications with participants 42](#_Toc60112)

[9.12 Amendments 42](#_Toc60113)

[9.13 Dispute resolution provisions 42](#_Toc60114)

[9.14 Governing law 42](#_Toc60115)

[9.15 Compliance with applicable law 42](#_Toc60116)

[9.16 Miscellaneous provisions 43](#_Toc60117)

[9.17 Other provisions 43](#_Toc60118)

# Introduction

The commencement date of this Commonwealth Department of Human Services Root Certification

Authority Certification Practice Statement (Human Services RCA CPS) 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 CPS 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.

## Background

In general, a 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 and Gatekeeper criteria and policies 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.

## Document name and identification

1.2.1 Department of Human Services RCA CPS 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 Department of Human Services Policy Management Authority (Human Services PMA).

An OID is not applicable to this CPS.

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

1.2.2 Common elements

This 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 CA operations and registration operations generally being performed on a remote site managed and operated by the Human Services Registration Organisation (RO 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 security level 1
* 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 certificate 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 CPS
* the Department of Human Services Organisation Certification Authority Certificate Practice

Statement (Human Services OCA CPS) or the CPS for other OCAs within the Healthcare Network PKI Hierarchy

* the Department of Human Services Root Certification Authority Certificate Policy (Human Services RCA CP), and
* the Certificate Policy (CP) for the PKI Community of Interest (CoI) that the certificate is issued under.

1.2.4 Department of Human Services Root Certification Authority Certificate Practice Statement

This Human Services RCA CPS 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 or relevant OCA CPs, then

Page

* the Human Services OCA CPS or other Healthcare Network PKI OCA CPSs, then  the Human Services RCA CP, then  this 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 public documents:

* this Human Services RCA CPS  the Human Services RCA CP
* 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.

## PKI participants

Human Services Root Certification Authority

Human Services RCA

Human Services Organisation

Certification Authority

Human Services OCA

Human Services Registration

Authority

Human Services RA

Relying Party

Registration Organisation Unit

End User Subscriber

Page

This Human Services RCA CPS is applicable to:

* the Human Services RCA
* any subordinate Department of Human Services OCA (e.g. the Human Services OCA)
* Department of 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 CPS.

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 CPS, 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.

Generation of the Human Services RCA’s keys is performed on 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 or CRL.

### 1.3.1.2 Human Services RCA functions

The Human Services RCA performs the following functions:

* generates its own keys and issues self-signed certificates using software listed on the

Australian Signals Directorate (ASD) Evaluated Products List (EPL)

* issues to itself self-signed certificates binding itself to its own public keys
* publishes the Human Services RCA Hash on the Healthcare Public Directory
* administers the registration of OCAs in accordance with the certificate registration process described in this CPS
* generates and issue OCA certificates only on receipt of properly formatted and verified certificate requests
* ensures, at the time a OCA certificate is issued to a OCA, that:
	+ the OCA certificate information (i.e. information needed to complete an OCA certificate as required by the certificate profile) is accurate
	+ the OCA certificate contains all the elements required by the certificate profile (i.e.

the specification of the fields to be included in a OCA certificate and the contents of each), and

* + the OCA is in possession or control of the private key corresponding to the public key included in the OCA certificate
* issues certificates that are factually correct from the information known to the Human

Services RCA at the time of issue and are free from data entry errors

* receives suspension and revocation requests and take appropriate action
* make reasonable enquiries in accordance with the arrangements agreed with OCAs to determine the validity of compromises and suspected compromises of private keys at any subordinate level the Human Services RCA deems warranted in its chain of trust
* promptly notifies an OCA in the event that the Human Services RCA initiates revocation of an OCA certificate(s)
* provides relying parties access to:
	+ certificate information published in the Healthcare Public Directory, and o the public keys associated with operational certificates listed in the Healthcare Public Directory
* if appropriate, to issue a new OCA certificate to an OCA whose keys have been compromised, or are suspected to have been compromised, after receiving a properly formatted and verified request from the OCA for a new OCA certificate
* facilitates the conduct of annual audits by Human Services PMA-authorised external auditors
* when the Human Services RCA generates key pairs, ensures that each key pair can work as an operable pair of cryptographic keys
* revokes an OCA certificate as required by, and in accordance with, this Human Services RCA CPS
* registers the revocation of the OCA certificate so that this information is readily available to a relying party
* administers the registration of the subordinate Human Services OCA in accordance with the certificated registration process described in this CPS
* issues to the subordinate Human Services OCA signed certificates binding the subordinate Human Services OCA to its public keys
* publishes and certifies public keys and associated certificates of the subordinate Human

Services OCA on a Healthcare Public Directory when requested to do so

* operates in accordance with documented operational practice, and
* publishes this Human Services RCA CPS and the Human Services RCA CP at [humanservices.gov.au](http://www.humanservices.gov.au/)

### 1.3.1.3 Human Services RCA obligations

The Human Services RCA obligations are:

* to comply with Digital Transition Agency Gatekeeper PKI Framework
* to comply with applicable laws
* to maintain this Human Services RCA CPS and Human Services RCA CP
* to comply with, and ensure that its personnel and contractors comply with, the practice and procedures set out in this Human Services RCA CPS and the functions and obligations set out in the Human Services RCA CP, and
* to advise OCAs of their obligations under this Human Services RCA CPS and the Human Services RCA CP and make accessible a copy of these documents to each OCA.

### 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 who are subordinate to the OCA 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 a Human Services OCA keys used to sign certificates are 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 is 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 subordinate to that OCA.

The functions and obligations of an OCA when acting in the role of a Subscriber are set out at 1.3.3 of this Human Services RCA CPS.

The functions and obligations of an OCA when acting in the role of a relying party are set out at 1.3.4 of this Human Services RCA CPS.

### 1.3.1.5 Human Services OCA functions

OCAs operating under the Healthcare Network PKI hierarchy perform the following functions:

* generate their own keys
* submit their public keys together with digitally signed certification requests to the Human Services RCA, and
* publish their OCA CPS, the OCA CP or each CP for the PKI CoI under which they issue certificates on a nominated web site specified within the OCA CPS.

On the receipt of authenticated digitally signed certificate requests from authorised ROUOs, OCAs will:

* issue certificates in accordance with this Human Services RCA CPS, the Human Services RCA CP, their OCA CPS, their OCA CP (where one is required) and the CP for the PKI CoI that the certificates are issued under for: o Subscriber ROUOs, and o End User-Subscribers
* publish issued certificates in the Healthcare Public Directory where there is permission from the PKI CoI to do so
* to generate and issue certificates only on receipt of properly formatted and verified certificate requests
* to ensure, at the time a certificate is issued to a End-User Subscriber, that:
	+ the certificate information (i.e. information needed to complete a certificate as required by the certificate profile) is factually correct and accurate
	+ the certificate contains all the elements required by the certificate profile (i.e. the specification of the fields to be included in a certificate and the contents of each), and
	+ the certificate is in possession or control of the private key corresponding to the public key included in the certificate
* to receive suspension and revocation requests and take appropriate action
* revoke certificates on receipt of authenticated digitally signed revocation requests
* post Certificate Revocation Lists (CRL)s in the Healthcare Public Directory
* to make reasonable enquiries in accordance with the arrangements agreed with each PKI CoI to determine the validity of compromises and suspected compromises of private keys at any subordinate level the Human Services RCA deems warranted in its chain of trust
* to promptly notify the Registration Organisation Unit (ROU) for a PKI CoI in the event that the Human Services RCA initiates revocation of the OCAs certificate(s), and
* to revoke a certificate as required by, and in accordance with this Human Services RCA CPS.

### 1.3.1.6 Human Services OCA obligations

An OCA’s (e.g. the Human Services OCA) obligations are:

* to comply with all Gatekeeper policies and criteria and Human Services’ Gatekeeper Approved Documents
* to comply with applicable laws
* to maintain their OCA CPS and the relevant CPs for each COI
* to comply with, and ensure that its personnel and contractors comply with, the conditions and obligations set out in this Human Services RCA CPS and the practices set out in the Human Services RCA CP
* to advise End User-Subscribers of their obligations under this Human Services RCA CPS, the Human Services RCA CP, their OCA CPS and the CP relevant to that CoI and make copies accessible to each End User-Subscriber, and
* when requested by the Human Services PMA, manage the conduct of audits performed on the OCA, the certificate issuance process and ROUs.

1.3.2 Registration authorities

This Human Services RCA CPS does not include information on Registration Authorities (RAs).

Information about RAs in the Healthcare Network PKI is included in the relevant OCA CPS. The Human Services OCA CPS is available at [humanservices.com.au](http://www.humanservices.com.au/)

1.3.3 Subscribers

Subscribers of the Human Services RCA are OCAs that apply to have their certificates signed by the Human Services RCA within the Healthcare Network PKI hierarchy managed by Human Services.

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

### 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 CPS and the Human Services RCA CP, are:

* to comply with the provisions of this Human Services RCA CPS and the Human Services RCA CP
* to comply with and maintain their own Human Services Gatekeeper Approved Documents
* to comply with applicable laws
* to maintain an OCA Policy Management Authority (OCA PMA) with the authority to represent the OCA Registration Organisation (OCA RO) in matters relating to the OCA
* to ensure that all information provided to the Human Services RCA in relation to their key pairs and certificates is true and complete
* to ensure that their own key pairs are operable pairs of cryptographic keys which meet the requirements of their own and the Human Services RCA key management plan
* to keep their private keys secret
* to promptly notify the Human Services RCA in the event that the OCA’s keys have been compromised, or are suspected of having been compromised
* to cooperate with compliance audits conducted by the Human Services PMA for the Human Services RCA
* to immediately notify the Human Services RCA if the OCA:
	+ has an adverse audit finding made against it, or
	+ has any other change to their Registration Information, or any other information provided to the Human Services RCA
* to use trustworthy systems in which:
	+ only authorised personnel can make entries and changes o information can be checked for authenticity, and
	+ any technical changes compromising security are apparent to the operator
* to employ personnel who possess the expert knowledge, experience, and qualifications necessary for the provision of certification services, and who have undergone the required security clearances for the position
* to apply administrative and management procedures which are appropriate for the activities being carried out
* to enter into appropriate agreements with their own Subscribers and relying parties which clearly outline End Entity obligations, including any terms and conditions required by the Gatekeeper Competent Authority for Subscriber agreements, and
* to obtain appropriate insurance to cover the risk of liability for damages flowing from its provision of certification services.

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

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

1.3.4 Relying parties

There are no relying parties for the RCA CPS as there are no end-user subscribers.

Relying parties for each ROU PKI CoI under an OCA are identified in the CP under which that particular ROU’s PKI CoI certificates are issued.

### 1.3.4.1 Other participants

There are no other participants in the Healthcare Network PKI Relationship 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.

End-User Subscriber certificates are issued by the Human Services OCA to subscribers of Community of Interest certificate policies.

## Certificate usage

1.4.1 Appropriate certificate use

See Section 1.4.1 of the Human Services RCA CP.

1.4.2 Prohibited certificate uses

See Section 1.4.2 of the Human Services RCA CP.

## Policy administration

1.5.1 Organisation administering the document

This Human Services RCA CPS is administered by Human Services and approved by the Human Services PMA and the Gatekeeper Competent Authority.

1.5.2 Contact person

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 CPS, the Human Services RCA CP 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 or 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.

The approved CPS will be forwarded to the Gatekeeper Competent Authority for agreement and updates the Gatekeeper Accreditation MOA.

The agreed CPS will be published electronically at the Human Services website, [humanservices.gov.au](http://www.humanservices.gov.au/) in a timely manner.

## Definitions and acronyms

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

# Publication and repository responsibilities

## Repositories

The repository for all public key certificates issued under this Human Services RCA CPS 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 ROU’s PKI CoI, OCAs or the Human Services RCA.

Note that certificate suspension is not supported in this Healthcare Network PKI.

Changes in the status of certificates issued under this Human Services RCA CPS, 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 OCA and ROU have agreed to publication.

The Healthcare Public Directory is accessible from [certificates-australia.com.au](http://www.certificates-australia.com.au/)

Technical details are at [humanservices.gov.au](http://www.humanservices.gov.au/)

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

## 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 CA 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 CPS is published electronically at the website, [humanservices.gov.au](http://www.humanservices.gov.au/)

Formal notification of changes to this Human Services RCA CPS 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 CPS. Interested parties are responsible for retrieving amendments when a revised and/or amended Human Services RCA CPS is posted to the website.

## Time or frequency of publication

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

### 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 on the web site(s) on which they publish their OCA CPS and any CPs that certificates are issued under.

## Access controls on repositories

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

# Identification and authentication

For further information, refer to Section 3 of the Human Services RCA CP.

## Naming

For further information, refer to Section 3 of the Human Services RCA CP.

## Initial identity validation

For further information, refer to Section 3 of the Human Services RCA CP.

## Identification and authentication for re-key requests

For further information, refer to Section 3 of the Human Services RCA CP.

## Identification and authentication for revocation request

Refer to Section 3.4 of the RCA CP.

# Certificate life-cycle operational requirements

For further information, refer to Section 4 of the Human Services RCA CP.

# Facility, management and operational controls

## 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 for Zone 4 by a Human Services Agency Security Advisor where Physical Security Evaluations have been undertaken. The Gatekeeper Accredited CA is operated by the Human Services contracted PKI Service Provider and 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.

The Human Services RCA is housed in a logical no-lone zone, meaning that two people must always be present for CA operations carried out at the Human Services RCA.

Physical access to servers is controlled through procedural control of keys for the server racks housing the servers.

5.1.3 Power and air conditioning

All CA Facilities are connected to a standard power supply. All critical components are connected to uninterruptible power supply (UPS) units, to prevent abnormal shutdown in the event of a power failure.

The CA Facility has an air conditioning system which controls temperature and humidity. Backup air conditioning units are provided for the no lone zones (i.e. the CA room).

5.1.4 Water exposures

The CA Facility is protected against water exposure by being located on built in raised floors of a building that is not in a flood zone.

5.1.5 Fire prevention and protection

Human Services contracted PKI Service Provider’s CA Facility is subject to normal fire prevention and protection procedures.

Early detection of smoke in the CA Facility is assured through the use of an extremely sensitive smoke detection system which continuously samples air from the CA Facility and Key Generation room itself. On detection of an unacceptably high level of smoke in the sampled air, the unit triggers a non-toxic fire suppression system.

In addition to this automatic fire suppression system, suitable fire extinguishers are maintained in the secure operating area.

The Secure Facility’s proximity swipe-card system supports emergency evacuation procedures to cater for environmental hazards such as fire, natural disasters and structural collapse.

5.1.6 Media storage

All magnetic media containing sensitive Healthcare Network PKI information, including backup media, is stored in containers, cabinets or safes with fire protection capabilities which are located either within the secure operating area or in a secure off-site storage area.

No classified Human Services Healthcare Network PKI documents may be removed from the CA Facility without approval from the Human Services PMA. All removals must be recorded in the appropriate register, for example the Classified Media Register.

5.1.7 Waste disposal

Paper documents and magnetic media containing any private keys or commercially sensitive or Confidential Information are securely disposed of by:

* in the case of magnetic media:

o physical damage to, or complete destruction of the asset, or o the use of an approved utility to wipe or overwrite magnetic media, or o use of an approved service to destroy the media after it has been sanitised, and

* in the case of printed material, cross-cut shredding or approved destruction services, and
* approved destruction services capable of destroying up to and including PROTECTED information.

All disposal actions will be undertaken in a manner that is compliant with the ISM.

5.1.8 Off-site backup

An approved secure site that is certified by Human Services Agency Security Advisor is used for the storage and retention of off-site backup software and data. The off-site storage:

* has appropriate levels of physical security in place, and
* may be accessed on a 24 x 7 basis by authorised personnel for the purposes of retrieving software and data.

## Procedural controls

5.2.1 Trusted roles

The Healthcare Network PKI contains a number of designated ‘positions of trust’. These positions underpin the secure and reliable operation of the Healthcare Network PKI, and as such must be filled by competent and trustworthy people (although the same person may fill several positions of trust) who have undergone the required security clearances for the position.

The general principle is that any role providing an opportunity to compromise private key material or impact on the certificate life-cycle must be a trusted role. Further details are set out in the Human Services contracted PKI Service Provider’s *SEC1* *Security Profile* (this document is not publicly available).

5.2.2 Number of persons required per task

Multi-person control is used where the requirement is to provide enhanced security and checks and balances over Healthcare Network PKI operations. In particular:

* the appropriate IT Security Administrator always remains separate from the Healthcare PKI System Operators in order to provide an independent third party when reviewing and auditing Healthcare Network PKI Operations,
* logical access controls for Healthcare Network PKI operations personnel have been implemented to ensure that no one person can manipulate the sensitive information contained on those machines,
* the CA Operators are broken into the following 2 groups:

o **Group 1** - has access to the logon passphrase for cryptographic elements, and o **Group 2** - has access to the logon database applications, and

* any task requiring the creation, backup or import into a database of a Healthcare Network PKI component private key takes place in a no-lone zone and therefore involves two trusted persons, one performing the function and the second person fulfilling a security monitoring role.

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.

Details for emergency account access to Healthcare Network PKI infrastructure are specified in the Human Services contracted PKI Service Provider’s *SEC1* *Security Profile* (this document is not a public document).

5.2.4 Roles requiring separation of duties

To enhance security of the Healthcare Network PKI the following roles are to be undertaken by different personnel:

* the Healthcare Network PKI hosting facility IT Security Administrator will normally remain separate from the Healthcare Network PKI System Operators in order to provide an independent review of audit logs unless in exceptional circumstances (i.e. personnel issues whereby integrity of the Healthcare Network PKI service being operated could be breached).

## Personnel controls

5.3.1 Qualifications, experience and clearance requirements

All Healthcare Network PKI operations personnel (excluding Registration Organisation Unit Operators (ROUOs)) require a Negative Vetting 1 clearance sponsorship by Human Services prior to being granted access to Human Services RCA trusted elements.

5.3.2 Background check procedures

The Healthcare Network PKI security clearance process will follow the guidelines of the Commonwealth Protective Security Policy Framework (PSPF).

5.3.3 Training requirements

A formal training program, founded on competency-based training principles is in place.

Human Services contracted PKI Service Provider is responsible for ensuring that new and inexperienced personnel are appropriately trained and supervised.

All of Human Services contracted PKI Service Provider’s operational personnel are trained in:

* basic Healthcare Network PKI concepts
* the use and operation of the Healthcare Network PKI software
* Human Services contracted PKI Service Provider’s PKI hosting facility procedures
* computer security awareness and procedures, and
* the meaning and effect of this Human Services RCA CPS and the Human Services RCA CP.

5.3.4 Retraining frequency and requirements

The introduction of any new security procedure or major software release will be accompanied by a corresponding education program for personnel affected by the changes to ensure that they are aware of their new responsibilities.

Remedial training is completed when recommended by audit findings and/or recommendations.

5.3.5 Job rotation frequency and sequence

This is described in the Human Services contracted PKI Service Provider’s *SEC1 Security Profile* (this document is not a public document).

5.3.6 Sanctions for unauthorised actions

Where personnel are found to have misused the resources to which they have been granted access, these actions shall be documented and passed to Human Services or Human Services contracted PKI Service Provider as appropriate for determination in accordance with the relevant legal obligations, including under relevant legislation.

Sanctions against contractors of Human Services or Human Services contracted PKI Service Provider may be applied in accordance with the terms and conditions of their relevant contract with Human Services or Human Services contracted PKI Service Provider.

In addition, legal action or prosecution may be pursued for breaches of relevant legal obligations. In some situations criminal sanctions apply for contravention of relevant legislation, for example the *Crimes Act 1914* (Commonwealth), and the *Public Services Act 1999* (Commonwealth).

Prohibited actions in the Healthcare Network PKI include (but are not limited to):

* connecting private computers, computer peripherals, or computer software to the Healthcare Network PKI network
* installing unauthorised software (including copyright infringed items). All software installations must be in accordance with the requirements of Healthcare Network PKI policies and the documented change management procedures
* using Healthcare Network PKI systems for unauthorised purposes
* having diagnostic tools (capable of testing or breaking security resident in any system) on their machines, and
* changing the configuration of any Healthcare Network PKI hardware or software without approval of the Human Services contracted PKI Service Provider PKI Security Administrator and the Human Services PMA.

5.3.7 Independent contractor requirements

For all contractors employed in positions of trust within the Healthcare Network PKI in any capacity, their rights and obligations and all terms and conditions of service will be as per the contract between the contractor and Human Services or other applicable contract.

Casual Healthcare Network PKI personnel and third party users who are not already covered by an existing contract including confidentiality clauses will be required to sign a Confidentiality Deed before being granted limited access to information processing facilities. The need for the party to enter into the Confidentiality Deed is at the discretion of Human Services.

Contractors in breach of security obligations may be guilty of certain criminal offences, for example offences relating to computers, offences relating to espionage and official secrets and offences against the Government, as set out in the *Crimes Act 1914* (Commonwealth) and other Commonwealth legislation.

5.3.8 Documentation supplied to personnel

All Healthcare Network PKI operational personnel have access to the following documentation:

* all relevant hardware and software documentation
* application manuals where appropriate
* policy documents, including this CPS, and
* operational and procedure documents, including this Human Services RCA CPS, Healthcare Network PKI operating procedures and OCA and certificate issuance operating procedures, as appropriate.

Note: the Healthcare Network PKI is largely composed of commercial-off-the-shelf products. Software documentation is therefore widely available to Healthcare Network PKI personnel.

General documents relating to the operation of the Healthcare Network PKI such as this Human Services RCA CPS and Human Services RCA CP are available to Human Services personnel, for example through publication on the Human Services intranet or to the public through the Human Services website [humanservices.gov.au](http://www.humanservices.gov.au/)

## Audit logging procedures

Human Services will maintain Records and Archives of information for the activities of the Human Services RCA and the Medicare OCA as required by the *Archives Act 1983* (Commonwealth).

Contracted service providers for the CAs and/or certificate issuance process will be contractually bound to comply with the *Archives Act 1983.*

5.4.1 Types of events recorded

The minimum audit records to be kept include all:

* registration records
* key generation records
* certificate generation requests
* certificate issuance records, including Certificate Revocation Lists (CRLs)  audit records including security related events, and  revocation records.

5.4.2 Frequency of processing log

Audit logs are processed on a daily, weekly, monthly and annual basis.

5.4.3 Retention period for audit log

Audit logs are maintained on site prior to archiving for a maximum period of three months and then transferred to the off-site archive facility. Archived logs are retained for a period of seven years (from the date of archival).

5.4.4 Protection of audit log

Human Services RCA audit logs are stored in a Zone 4 location within the Human Services contracted PKI Service Providers PKI premises. Audit logs are digitally signed prior to archive.

Archived Healthcare Network PKI audit logs are stored in a secure off-site facility from the data centre that is certified by Human Services Agency Security Advisor.

5.4.5 Audit log backup procedures

A detailed backup procedure for audit logs has been established and maintained and is documented in the Human Services contracted PKI Service Provider’s *SEC1 Security Profile* (this document is not publicly available).

5.4.6 Audit collection system (internal vs. external)

The Human Services RCA audit collection system for the Human Services RCA is a combination of automated and manual processes performed by the operating system running the UniCERT software, the UniCERT software itself, and by operational personnel. The audit mechanisms and procedures used are documented in the Human Services contracted PKI Service Provider’s *SEC1 Security Profile* (this document is not publicly available).

5.4.7 Notification to event-causing subject

Operations personnel notify the Human Services Certificate Manager when a process or action causes a critical security event or discrepancy. The Human Services Certificate Manager shall inform Human Services PMA who are responsible for notifying the Gatekeeper Competent Authority. The event handling procedure is documented in the Human Services contracted PKI Service Provider’s *SEC1 Security Profile* (this document is not publicly available).

5.4.8 Vulnerability assessments

The Human Services RCA audit logging procedures are regularly reviewed through the Gatekeeper PKI Framework Information Security Registered Assessors Program (IRAP) and Compliance Audit Program.

## Records archival

5.5.1 Types of record archived

The following information is archived by the Human Services RCA:

 Audit logs (refer to 5.4 of this document)  Certificate request information, and  Complete back up registers.

Each CA or RA or certificate issuance entity in the Healthcare Network PKI Hierarchy is required to maintain an archive of relevant records. 5.5.2 Retention period for archive

### 5.5.2.1 Secure maintenance of keys

Human Services Service Provider retains copies of the public and private keys of the Human Services RCA and subordinate OCAs in a Secure Facility.

### 5.5.2.2 Secure maintenance of certificates

Human Services Service Provider retains copies of the public and private certificates of the Human Services RCA and subordinate OCAs in a Secure Facility.

### 5.5.2.3 Term of archive maintenance

Archives are retained for a period of seven years from date of generation in accordance with the requirements of the *Archives Act 1983* (Commonwealth).

5.5.3 Protection of archive

Archive media is protected by physical security and cryptographic protection commensurate with the security classification of the contents and in accordance with relevant provisions of the PSPF.

5.5.4 Archive backup procedures

Archive backup procedures have been established to ensure complete restoration of current service or verification. Details are specified in the Human Services contracted PKI Service Provider’s SEC1 Security Profile (this document is not publicly available).

5.5.5 Requirements for time-stamping of records

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

5.5.6 Archive collection system (internal or external)

Archiving is performed by operations personnel delegated with the responsibility for doing so. Detailed procedures for backups, archiving and storage are set out in the Human Services contracted PKI Service Provider’s SEC1 Security Profile (this document is not publicly available).

5.5.7 Procedures to obtain and verify archive information

The integrity of the Archives is verified in accordance with the criteria set out in the Human Services contracted PKI Service Provider’s SEC1 Security Profile (this document is not publicly available).

## Key changeover

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

OCAs shall each obtain a new authentication key pair a minimum of two years prior to the expiry of the certificate associated with their respective current private authentication key, and then commence signing new certificates with the new private authentication key.

During this changeover period until the expiry of the certificate associated with the current

Healthcare Network PKI private authentication key, both authentication public keys in the associated certificate will be in use and published in the Healthcare Public Directory.

The Healthcare Network PKI is committed to:

 ensuring that key changeover causes minimal disruption to Subscribers, and  providing Subscribers with reasonable notice of planned key changeover.

## Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

Human Services will maintain a *Disaster Recovery and Business Continuity Plan* for the Human Services RCA. This plan, although not publicly available, will be made available to those persons responsible for and authorised to, conduct security audits as well as those persons who provide ongoing support for the RCA.

5.7.2 Computing resources, software and/or data are corrupted

Directions for managing service restoration in the event of a corruption of computing resources, software and/or data are provided in the Human Services contracted PKI Service Provider’s *SEC1* *Security Profile and Standard Operating Procedures, and the Disaster Recovery and Business Continuity Plan* (these documents are not publicly available).

5.7.3 Entity private key compromise procedures

In the situation that the Human Services RCA or the Human Services OCA or any other OCA private key is compromised, for whatever reason, the procedures outlined for a termination of the entity whose private key was compromised, would be followed. Details for the termination of the entity are provided in the Human Services contracted PKI Service Provider’s *SEC1* *Security Profile* (these documents are not publicly available).

The Human Services PMA shall promptly advise the Gatekeeper Competent Authority of any compromise or suspected compromise of any of the private keys belonging to any Gatekeeper Accredited CA in the Healthcare Network PKI hierarchy.

5.7.4 Business continuity capabilities after a disaster

Actions will be taken in order to restore core business operation as quickly as practicable following fire, strikes or similar events. Details are provided in the Human Services contracted PKI Service Provider’s *SEC1* *Security Profile* (this document is not publicly available). Human Services will provide notification of any business outages through a number of channels such as the Human Services’ website, [humanservices.gov.au](http://www.humanservices.gov.au/) or through its client relations helpdesk framework.

## 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 Healthcare Network PKI participants.

# Technical security controls

## 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 Australian Signals Directorate (ASD) 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 generated by the OCA and do not require delivery.

6.1.3 Public key delivery to certificate issuer

OCA public keys are delivered to the Human Services RCA, personally escorted by trusted OCA personnel.

The OCAs PKCS#10 certificate request must be transferred to the Human Services RCA in a way that ensures that:

* it has not been changed during transit
* the sender possesses the private key that corresponds to the transferred public key, and  the sender of the public key is the legitimate user claimed in the certificate application.

6.1.4 CA public key delivery to relying parties

The CA 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 keys 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 EAL 4 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 EAL 4 evaluation of the CA products used for OCA key generation.

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

Human Services RCA keys will be used for the purposes set out in the Human Services RCA CP.

Subscriber keys will be used for the purposes and in the manner described in the CP under which the certificates are issued.

## 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 ‘n out of m’ 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 cryptographic module in an encrypted format. These are further encrypted and backed up onto smartcards with backup copies 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.

Private key archival is not provided for Subscribers, relying parties and End User-Subscribers.

6.2.6 Private key transfer into or from a cryptographic module

If a cryptographic module is used, 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 used.

6.2.7 Private key storage on a cryptographic module

If a cryptographic module is used, 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 used.

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 Verizon Australia Pty Ltd *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

Media containing Subscriber private keys are securely destroyed by, in the case of:

* compact disks – destruction by disintegration or burning, or
* hard disks – sanitisation by overwriting in accordance with the ISM, or  other media – in accordance with recommendations in the ISM.

Media containing a private key of the Human Services RCA will be securely disposed of by sanitisation by overwriting (where feasible), then supervised physical destruction in accordance with the ISM.

Further detail on private key destruction is contained in the Human Services contracted PKI Service Provider’s *SEC1* Security Profile (this document is not publicly available).

6.2.11 Cryptographic module rating

Only cryptographic modules evaluated and approved by the ASD shall be use for the Human Services RCA and OCAs. There is no stipulation on the cryptographic module rating.

## 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 the *Archives Act 1983* (Commonwealth).

6.3.2 Certificate operational periods and key pair usage periods

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.

Refer to Human Services OCA CPS section 6.3.2 for usage periods for OCA public and private keys.

## 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.

## Computer security controls

6.5.1 Specific computer security technical requirements

The Human Services RCA 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

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

## Life-cycle technical controls

6.6.1 System development controls

The Human Services RCA and OCA system development controls are detailed 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 security management controls are detailed 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).

## Network security controls

Human Services RCA and OCAs have 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).

## 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.

# Certificate, CRL and OCSP profiles

## Certificate profile

For this information, please refer to the RCA CP under which the certificate was issued.

7.1.1 Version number(s)

For this information, please refer to the RCA CP under which the certificate was issued.

7.1.2 Certificate extensions

For this information, please refer to the RCA CP under which the certificate was issued.

7.1.3 Algorithm object identifiers

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

7.1.4 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 and subject name fields respectively. 7.1.5 Name constraints

For this information, please refer to the RCA CP under which the certificate was issued.

7.1.6 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 the Human Services RCA CP.

7.1.7 Usage of policy constraints extension

For this information, please refer to the RCA CP under which the certificate was issued.

7.1.8 Policy qualifiers syntax and semantics

For this information, please refer to the RCA CP under which the certificate was issued.

7.1.9 Processing semantics for the critical certificate policy extension

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

## CRL profile

7.2.1 Version number(s)

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

7.2.2 CRL and CRL entry extensions

The Human Services RCA supports the use of X.509 Version 2 CRL entry extensions.

OCAs support the use of X.509 Version 2 CRL entry extensions.

## 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.

# Compliance audit and other assessments

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

## 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.

## Identity/qualifications of assessor

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

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

## Assessor’s relationship to assessed entity

External assessors will be organisationally independent of the Human Services RCA and shall not have any current or planned financial, legal, or other relationship that could result in a conflict of interest during the period of the audit.

Internal assessors will be organisationally independent of the Human Services RCA’s operations.

## Topics covered by assessment

The areas of the Human Services RCA to be assessed include, but are not limited to:

* compliance with Gatekeeper approved documents, policies, criteria and processes
* plans, including but not limited to security, business continuity and disaster recovery plans
* physical and logical security
* vetting of operational personnel and personnel management
* technology
* data and information management
* management of Healthcare Network PKI services, and  privacy.

## Actions taken as a result of deficiency

The results of the audit will be provided to the Human Services PMA and recorded in the Human Services RCA audit log. The Human Services PMA Chair is responsible for addressing any serious deficiencies in a timely manner.

When irregularities are found after an internal audit of the Human Services RCA, the Human Services PMA shall promptly oversee or implement appropriate corrective action.

## Communication of results

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

# Other business and legal matters

## Fees

Not applicable.

## 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 CPS.

9.2.3 Warranty coverage

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

## Confidentiality of business information

For information about confidentiality of business information, refer to the Human Services RCA CP located at [humanservices.gov.au/pki](https://www.humanservices.gov.au/health-professionals/enablers/public-key-infrastructure-pki-policy-documents)

## Privacy of personal information

For information about privacy of personal information, refer to the Human Services RCA CP located at [humanservices.gov.au/pki](https://www.humanservices.gov.au/health-professionals/enablers/public-key-infrastructure-pki-policy-documents)

## Intellectual property rights

For information about intellectual property rights, refer to the Human Services RCA CP located at [humanservices.gov.au/pki](https://www.humanservices.gov.au/health-professionals/enablers/public-key-infrastructure-pki-policy-documents)

## Representations and warranties

For information about representations and warranties, refer to the Human Services RCA CP located at [humanservices.gov.au/pki](https://www.humanservices.gov.au/health-professionals/enablers/public-key-infrastructure-pki-policy-documents)

## 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.

## Limitations of liability

For information about limitations of liability, refer to the Human Services RCA CP located at [humanservices.gov.au/pki](https://www.humanservices.gov.au/health-professionals/enablers/public-key-infrastructure-pki-policy-documents)

## Indemnities

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

## Term and termination

9.10.1 Term

The RCA CPS will be ongoing. For more information, refer to the Human Services RCA CP located at [humanservices.gov.au/pki](https://www.humanservices.gov.au/health-professionals/enablers/public-key-infrastructure-pki-policy-documents)

9.10.2 Termination

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

9.10.3 Effect of termination and survival

For information about effect of termination and survival, refer to the Human Services RCA CP located at [humanservices.gov.au/pki](https://www.humanservices.gov.au/health-professionals/enablers/public-key-infrastructure-pki-policy-documents)

## Individual notices and communications with participants

For information about individual notices and communications with participants, refer to the Human

Services RCA CP located at [humanservices.gov.au/pki](https://www.humanservices.gov.au/health-professionals/enablers/public-key-infrastructure-pki-policy-documents)

## Amendments

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

9.12.1 Procedure for amendment

For information about procedure for amendment, refer to the Human Services RCA CP located at [humanservices.gov.au/pki](https://www.humanservices.gov.au/health-professionals/enablers/public-key-infrastructure-pki-policy-documents)

9.12.2 Notification mechanism and period

For information about notification mechanism and period, refer to the Human Services RCA CP located at [humanservices.gov.au/pki](https://www.humanservices.gov.au/health-professionals/enablers/public-key-infrastructure-pki-policy-documents)

9.12.3 Circumstances under which OID must be changed

For information about circumstances under which OID must be changed, refer to the Human Services RCA CP located at [humanservices.gov.au/pki](https://www.humanservices.gov.au/health-professionals/enablers/public-key-infrastructure-pki-policy-documents)

## Dispute resolution provisions

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

## Governing law

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

## Compliance with applicable law

For information about compliance with applicable law, refer to the Human Services RCA CP located at [humanservices.gov.au/pki](https://www.humanservices.gov.au/health-professionals/enablers/public-key-infrastructure-pki-policy-documents)

## Miscellaneous provisions

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

## 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)

**Annex A Department of Human Services PKI website**

The Healthcare Network PKI uses the following documents and websites for the provision of information to relying parties and Subscribers:

* Human Services RCA CPS
* Human Services RCA CP
* Human Services OCA CPS
* Certificate policies for PKI CoIs
* Subscriber Application and Terms and Conditions documents
* Relying Party Agreements  Human Services privacy policy, and  Human Services PKI Glossary.

All documents are located at [humanservices.gov.au](http://www.humanservices.gov.au/)

The [certificates-australia.com.au](http://www.certificates-australia.com.au/) website also provides the Healthcare Public PKI Directory, CA Certificates and their hash values.