

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

Version 2.8

**May 2018**

**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** | **Comments** |
|  0.8  | Draft | 02/02/2006 | Initial re-draft.   |
|  0.9    | Final | 13/02/2006 | Incorporated feedback from 0.8.1 and submit for Medicare Australia PMA approval.   |
|  0.10   |  | 25/06/2006 | Incorporate feedback from Legal.   |
|  0.11   |  | 25/06/2006 | Incorporate further feedback from MA   |
|  0.12     |  | 27/06/2006 | Changing document title to better reflect that the OCA (Medicare Australia Human Services CA) is owned by Medicare Australia   |
|  0.13    |  | 07/07/2006 | Update the document to reflect the new ownership of the RCA and Section 9 of this document.   |
|  0.14    |  | 10/07/2006 | Update the document to reflect the new sub CA name.   |
|  0.15    | Draft | 7/8/2006 | Make consistent all terminology under new Gatekeeper Health Sector PKI Framework   |
|  0.16   | Draft | 8/8/2006 | Review and update references   |
|  0.17   | Draft | 11/8/2006 | Edit and revise to update terminology and content   |
| 0.18     | Draft | 15/8/2006 | Updated to reflect consistency between Health Sector PKI entity names, and include relationship diagram   |
| 0.19   | Draft | 16/08/2006 | Minor format editing.   |
| 0.20     | Draft | 18/08/2006 | Review of edits and acceptance of edits to Part 5.3 in v0.19; review and revision for parts 5.4 and following parts   |
| 0.21   | Draft | 23/08/2006 | Format editing.   |
| 0.22   | draft | 25/08/2006 | Final draft   |
| 0.23       | Draft | 28/08/2006 | Transfer of Part 9 substantive content to the Medicare Australia RCA CPS; insert ‘see reference’ to Part 9 the RCA CPS in this OCA CPS. Review of previous edits and acceptance / amendment as required.   |
| 0.24     | Draft | 29/08/2006 | Further amendments to link this CPS with RCA CPS; addition of clauses on OCA functions and obligations;   |
| 0.25   | Draft | 4/09/2006 | Review of changes to date   |
| 1.0     | FINAL | 4/09/2006 | Review, delete comments, amendments to Pt 9 to reflect changes in RCA CPS; minor edits, final proof read .  |
| 1.9   | FINAL | 8/09/2006 | NUMBER CHANGE TO 1.9 TO MATCH OID   |
|    | Final | 18/09/2006 | Amendment to reflect changes to PMA   |
| 1.91  | Final  | November 2006 | Deletion of reference to the IT Security Manager in 5.2.3 Amendments to grammar/phrasing/typos etc.  |
|   |   |
|  |  |
|   |   |   |  |
| 1.92    | Draft    | May 2008 | Gatekeeper Accreditation under the Relationship Organisation model.   |
| 1.93    | Draft    | June 2008 | Amendments after consultations with Legals and Technical teams.  |
| 1.94     | Draft     | June 2008 | Amendments after consultations with Legals and Technical teams. Release version to AGIMO for comments.  |
| 1.95    | Draft    | July 2008 | Amendments after review by the Gatekeeper Competent Authority.  |
| 1.96  | Draft  | November 2008   | Amendments after review by the Gatekeeper Competent Authority and further review by Medicare Australia. |
|   |   |
| 1.97  | Draft  | February 2010  | Updated References  |
| 1.98  | Draft | February 2010  | AGIMO Feedback Included  |
| 1.99    | Draft    | May 2010    | AGIMO Changes included following meeting with AGIMO. |
| 2.0   | Final   | July 2010   | Further AGIMO Changes included   |
| 2.0   | Final   | August 2010   | Final review   |
| 2.0  | Final  | 18 August 2010  | Final review & clearance for independent legalreview |
|  |  |
| 2.1  | Draft  | 29 October 2010 | Updates following legal review   |
| 2.2 | Draft | 28 Feb 2011 | Minor Updates  |
| 2.3 | Draft  | May 2011  | Updates following AGIMO review |
| 2.4  | Draft  | May 2011  | Updates approved by AGIMO  |
| 2.5  | Final  | October 2014  | Minor amendments after annual PKI Gatekeeper audit and further review by Medicare Australia.  |
| 2.6  | Final  | December 2016  | Initial version reflecting changes in the Gatekeeper PKI Framework version 3.1  |
| 2.7  | Draft  | March 2017  | Relocation of the Verizon Data Centre and the CA infrastructure and DTA feedback.  |
| 2.7  | Final  | May 2017  | Final review & clearance  |
| 2.8 | Draft | May 2017 | Replaced Healthcare Network with Health Network |
| 2.8 | Final | August | Incorporated National Authentication Service for Health Pki access to HI Service |

### Contents

[1 Introduction 5](#_Toc68090)

[1.1 Background 5](#_Toc68091)

[1.2 Document name and identification 5](#_Toc68092)

[1.3 PKI participants 8](#_Toc68093)

[1.4 Certificate usage 12](#_Toc68094)

[1.5 Policy administration 13](#_Toc68095)

[1.6 Definitions and acronyms 13](#_Toc68096)

[2 Publication and repository responsibilities 14](#_Toc68097)

[2.1 Repositories 14](#_Toc68098)

[2.2 Publication of certification information 14](#_Toc68099)

[2.3 Time or frequency of publication 15](#_Toc68100)

[2.4 Access controls on repositories 15](#_Toc68101)

[3 Identification and authentication 16](#_Toc68102)

[3.1 Naming 16](#_Toc68103)

[3.2 Initial identity validation 16](#_Toc68104)

[3.3 Identification and authentication for re-key requests 16](#_Toc68105)

[3.4 Identification and authentication for revocation request 16](#_Toc68106)

[4 Certificate life-cycle operational requirements 17](#_Toc68107)

[5 Facility, management and operational controls 18](#_Toc68108)

[5.1 Physical controls 18](#_Toc68109)

[5.2 Procedural controls 19](#_Toc68110)

[5.3 Personnel controls 21](#_Toc68111)

[5.4 Audit logging procedures 23](#_Toc68112)

[5.5 Records archival 24](#_Toc68113)

[5.6 Key changeover 26](#_Toc68114)

[5.7 Compromise and disaster recovery 26](#_Toc68115)

[5.8 Human Services OCA termination 27](#_Toc68116)

[6 Technical security controls 28](#_Toc68117)

[6.1 Key pair generation and installation 28](#_Toc68118)

[6.2 Private key protection and cryptographic module engineering controls 29](#_Toc68119)

[6.3 Other aspects of key pair management 31](#_Toc68120)

[6.4 Activation data 31](#_Toc68121)

[6.5 Computer security controls 31](#_Toc68122)

[6.6 Life-cycle technical controls 32](#_Toc68123)

[6.7 Network security controls 32](#_Toc68124)

[6.8 Time-stamping 32](#_Toc68125)

[7 Certificate, CRL and OCSP profiles 33](#_Toc68126)

[7.1 Certificate profile 33](#_Toc68127)

[7.2 CRL profile 34](#_Toc68128)

[7.3 Online certificate status protocol profile 34](#_Toc68129)

[8 Compliance audit and other assessments 35](#_Toc68130)

[8.1 Frequency or circumstances of assessments 35](#_Toc68131)

[8.2 Identity/qualifications of assessor 35](#_Toc68132)

[8.3 Assessor’s relationship to assessed entity 35](#_Toc68133)

[8.4 Topics covered by assessment 35](#_Toc68134)

[8.5 Actions taken as a result of deficiency 35](#_Toc68135)

[8.6 Communication of results 36](#_Toc68136)

[9 Other business and legal matters 37](#_Toc68137)

[9.1 Fees 37](#_Toc68138)

[9.2 Financial responsibility 37](#_Toc68139)

[9.3 Confidentiality of business information 37](#_Toc68140)

[9.4 Privacy of personal information 37](#_Toc68141)

[9.5 Intellectual property rights 37](#_Toc68142)

[9.6 Representations and warranties 37](#_Toc68143)

[9.7 Disclaimers of warranties 37](#_Toc68144)

[9.8 Limitations of liability 38](#_Toc68145)

[9.9 Indemnities 38](#_Toc68146)

[9.10 Term and termination 38](#_Toc68147)

[9.11 Individual notices and communications with participants 39](#_Toc68148)

[9.12 Amendments 40](#_Toc68149)

[9.13 Dispute resolution provisions 40](#_Toc68150)

[9.14 Governing law 40](#_Toc68151)

[9.15 Compliance with applicable law 40](#_Toc68152)

[9.16 Miscellaneous provisions 40](#_Toc68153)

[9.17 Other provisions 41](#_Toc68154)

# Introduction

The Australian Government Department of Human Services (Human Services) manages the issuance of the Health Network Public Key Infrastructure (Health Network PKI) certificates as the Organisation Certificate Authority (OCA) to the healthcare sector, in accordance with the Gatekeeper PKI Framework, owned by the Digital Transformation Agency (DTA).

This document outlines the rules applying to, and scope of use of, the Health Network PKI in accordance with RFC3647 ‘Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework’.

The document commences on the date that the Memorandum of Agreement (MOA) is signed by the Digital Transformation Agency and the Department of Human Services (Human Services).

## Background

In general, a Public Key Infrastructure (PKI) consists of a hierarchy of trusted elements and subscribers. In the Health 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 Health 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 Health 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 Health 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 OCA CPS identification

Specified elements under the Health 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 OCA CPS is published on [humanservices.gov.au](http://www.humanservices.gov.au/) website.

1.2.2 Common elements

This Human Services OCA CPS covers the common practices and procedures that manages the issuance of the Health Network PKI certificates.

The specific rules and uses of each individual certificate issued by Human Services OCA are included in the certificate policies relating to those certificates.

These common practices and procedures 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 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
* the institution of a continuous cycle of internal and external audits to ensure a high level of operational integrity is always maintained
* the Human Services certificate issuance process, including emergency issuance and certificate management policies and procedures, and
* the use dedicated workstation by authorised personnel who are responsible for the management of certificates.

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 Department of Human Services Organisation Certification Authority Certificate Practice Statement (Human Services OCA CPS)
* the Human Services RCA CPS
* 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 Organisation Certification Authority Certificate Practice Statement

The Human Services OCA CPS relates to the authentication and confidentiality certificates signed by the Human Services OCA and issued to end subscribers within the Health Network PKI Hierarchy.

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
* this Human Services OCA CPS, then
* the Human Services RCA CP, then
* the Human Services RCA CPS.

1.2.5 DTA Gatekeeper PKI Framework Documentation

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

* this Human Services OCA CPS
* the Human Services RCA CPS
* the Human Services RCA CP
* the relevant certificate policy the certificates are issued under
* the Human Services 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

This Human Services OCA CPS is applicable to:

* the Human Services OCA
* the Certificate Controllers who are authorised personnel with the responsible for the issuance and management of certificates
* Department of Human Services Registration Organisation Unit Operators (Human Services

ROUOs) approved to operate within the Health Network PKI hierarchy, and

* relying parties and End User-Subscribers registered for Health Network PKI keys and certificates issued under the CP for the subscribers’ PKI CoI and supported by this CPS.

Annex B details the Department of Human Services Community of Interest Registration Organisation Units.

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 Health Network PKI CoI. The Human Services OCA rely on this point of trust.

For further information, refer to Section 1.3 of the Human Services RCA CPS.

*1.3.1.2 Human Services RCA functions*

For further information, refer to Section 1.3 of the Human Services RCA CPS.

*1.3.1.3 Human Services RCA obligations*

For further information, refer to Section 1.3 of the Human Services RCA CPS.

#### 1.3.1.4 Human Services OCA overview

The Human Services OCA is immediately subordinate to the Human Services RCA in the Health Network PKI hierarchy. Its primary purpose is to provide certificates and certificate management services to relying parties and subscribers who are subordinate to the OCA in the Health Network PKI.

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.

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.

Specific functions and obligations of the Human Services OCA, as a CA within the Health Network PKI hierarchy, are dealt with in the CP under which the certificates are issued.

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

The Human Services OCA perform the following functions:

* generate its own keys
* submit its public keys together with digitally signed certification requests to the Human Services RCA, and
* publish the Human Services OCA CPS and each CP for the PKI CoI under which it issue certificates on the [humanservices.gov.au](http://www.humanservices.gov.au/) website.

On the receipt of Certificate Requests from authorised Certificate Controllers, the Human Services OCA will:

* issue certificates in accordance with this Human Services RCA CPS, the Human Services RCA CP, the Human Services OCA CPS and the CP for the PKI CoI that the certificates are issued under for:
	+ subscriber ROUOs, and
	+ 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 an 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 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*

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 this Human Services 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 OCA CPS, the Human Services RCA CP and the practices set out in the Human Services RCA CPS
* to advise End User-Subscribers of their obligations under this Human Services OCA CPS, the

Human Services RCA CP 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

Human Services is the Registration Authority (Human Services RA). The certificate issuance and management processes, and the registration processes are performed by separate business areas within Human services.

#### 1.3.2.1 Certificate controllers

Certificate Controllers are Human Services RA personnel with responsibilities for the issuance and management of certificates.

All Certificate Controllers operating under this CPS are duly authorised representatives of the Human Services RA.

The Certificate Controllers perform the following functions:

* to prepare and submit properly formatted and verified certificate requests
* to ensure, at the time a certificate request is submitted, that:
	+ the certificate information contained in the request is factually correct and accurate, and
	+ the certificate request contains all the elements required by the certificate profile
* to receive revocation requests and take appropriate action
* to receive certificate renewal requests and take appropriate action.

#### 1.3.2.2 Registration Organisation Units

The Human Services Registration Organisation Units (ROUs) are business areas within Human Services that receive and process applications for certificates for defined Communities of Interest.

There are separately identified ROUs within the Human Services RA, usually one ROU for each CoI in the Health Network PKI. The ROU has responsibilities in the CoI in managing the subscribers in that CoI. Refer to the appropriate CoI CP for the applicable ROU.

#### 1.3.2.3 Registration Organisation Unit Operators

Registration Organisation Unit Operators (ROUOs) are Human Services staff responsible for processing registrations. ROUOs may be located within the programme area in Human Services or the relevant area within Human Services in its role as the service operator of the HI Service.

ROUOs are not Certificate Controllers.

ROUOs operate in accordance with the processes and procedures set out in this CPS and subordinate CPs.

1.3.3 Subscribers

Subscribers for certificates are members of a CoI. Each CoI is represented by an ROU

For information about subscribers, refer to the CoI CP the certificate was issued under.

1.3.4 Relying parties

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.

For information about relying parties and relevant relying party agreements, refer to the CoI CP the certificate was issued under.

Parties who rely on certificates issued under the subordinate CPs and who:

* do not have a written agreement with Human Services or authorisation through a notice published at [humanservices.gov.au/pki](https://www.humanservices.gov.au/health-professionals/enablers/public-key-infrastructure-pki-policy-documents) (specifying authorised usage relating to a transaction type), and
* undertake transactions that are not authorised or approved by Human Services rely on such certificates at their own risk.

1.3.5 Other participants

There are no other participants in Health Network PKI managed by Human Services.

## Certificate usage

1.4.1 Appropriate certificate use

The appropriate certificate use for each ROU’s CoI certificate is set out in the CP under which that particular certificate was issued.

1.4.2 Prohibited certificate uses

The appropriate certificate use for each ROU’s CoI certificate is set out in the CP under which that particular certificate was issued.

## Policy administration

1.5.1 Organisation administering the document

This Human Services OCA 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 OCA CPS and associated CPs for ROUs’ CoIs and answer questions relating to the policy, practices and procedures described in these documents.

## Definitions and acronyms

Please refer to Human Services Health Network 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](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 OCA 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.

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

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

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 ROU has 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 per week (except for designated system maintenance periods).

## Publication of certification information

2.2.1 Publication of Human Services OCA 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 OCA 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 OCA CPS is published electronically at the website, [humanservices.gov.au](http://www.humanservices.gov.au/)

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

## Time or frequency of publication

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

#### 2.3.1.1 Publication by OCAs

The Human Services OCA publish the current approved version of the Human Services RCA CPS on the website, [humanservices.gov.au](http://www.humanservices.gov.au/)

## 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.

# Identification and authentication

The process that applicants go through to authenticate themselves for each ROU’s CoI certificate is set out in the CP under which that particular certificate was issued.

## Naming

For further information, refer to Section 3 of the CP under which that particular certificate was issued.

## Initial identity validation

For further information, refer to Section 3 of the CP under which that particular certificate was issued.

## Identification and authentication for re-key requests

For further information, refer to Section 3 of the CP under which that particular certificate was issued.

## Identification and authentication for revocation request

For further information, refer to Section 3 of the CP under which that particular certificate was issued.

# Certificate life-cycle operational requirements

For further information on certificate life-cycle operational requirements, refer to Section 4 of the CP under which that particular certificate was issued.

# Facility, management and operational controls

## Physical controls

5.1.1 Site location and construction

The Human Services OCA 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 Secure Facility is operated by 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 Health Network PKI.

The Human Services OCA 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 OCA.

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 Secure 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 Secure 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 Secure 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

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

Early detection of smoke in the Secure 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 Health 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 Health Network PKI documents may be removed from the Secure 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

* 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 a Human Services Agency 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 Health Network PKI contains a number of designated ‘positions of trust’. These positions underpin the secure and reliable operation of the Health 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 Health Network PKI operations. In particular:

* the appropriate IT Security Administrator always remains separate from the Health Network PKI System Operators in order to provide an independent third party when reviewing and auditing Health Network PKI Operations
* logical access controls for Health 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:
	+ **Group 1** - has access to the logon passphrase for cryptographic elements, and
	+ **Group 2** - has access to the logon database applications, and
* any task requiring the creation, backup or import into a database of a Health 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 Health Network PKI operations personnel has a separate account so all operations can be traced to an individual.

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

5.2.4 Roles requiring separation of duties

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

* the Health Network PKI hosting facility Security Administrator will normally remain separate from the Health 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 Health Network PKI service being operated could be breached).

## Personnel controls

5.3.1 Qualifications, experience and clearance requirements

All Health 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 OCA trusted elements.

5.3.2 Background check procedures

The Health 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.

The Health Network PKI operation centre Team Leader is responsible for ensuring that new and inexperienced personnel are appropriately trained and supervised.

All Health Network PKI operational personnel are trained in:

* basic Health Network PKI concepts
* the use and operation of the Health Network PKI software
* the Human Services contracted PKI Service Provider’sPKI hosting facility procedures
* computer security awareness and procedures, and
* the meaning and effect of this Human Services OCA CPS, the 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 publicly available).

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 applicable in accordance with the terms and conditions of their relevant contract with the 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 Health Network PKI include (but are not limited to):

* connecting private computers, computer peripherals, or computer software to the Health Network PKI network
* installing unauthorised software (including copyright infringed items). All software installations must be in accordance with the requirements of Health Network PKI policies and the documented change management procedures
* using Health 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 Health 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 Health 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 Health 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 Health 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, Health Network PKI operating procedures and OCA and certificate issuance operating procedures, as appropriate.

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

General documents relating to the operation of the Health Network PKI such as this Human

Services RCA CPS ,Human Services RCA CP and Human Services OCA CPS are available to the 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 OCA audit logs are stored in a Zone 4 rated location within the Human Services contracted PKI Service Provider’s PKI premises. Audit logs are digitally signed

Archived Health Network PKI audit logs are stored in a secure off-site facility from the data centre that is certified by a 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 OCA 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 the 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 OCA 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 OCA:

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

5.5.2 Retention period for archive

*5.5.2.1 Secure maintenance of keys*

The Human Services OCA does not make or retain copies of public and private keys.

*5.5.2.2 Secure maintenance of certificates*

The Human Services OCA does not make or retain copies of certificates.

#### 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* and the *OP1 Operations Manual* (these documents are 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) as follows:

* annually at the time of the programmed security audit
* at any time when a full security audit is required, and
* at the time the Archive is prepared.

## Key changeover

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

The Human Services OCA shall 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

Health 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 Health 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 OCA. 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 OCA.

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, 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 a private key is compromised, for whatever reason, the procedures outlined for CA termination will be followed. Details are provided in Human Services contracted PKI Service Provider’s *SEC1 Security Profile* (this document is 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.

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 *Disaster Recovery and Business Continuity Plan* (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.

## Human Services OCA termination

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

If the Health Network PKI is terminated, details of transition plans and procedures will be provided to Health Network PKI participants.

# Technical security controls

## Key pair generation and installation

6.1.1 Key pair generation

#### 6.1.1.1 Human Services OCA key pair generation

Human Services OCA key pairs are generated using software that is listed on the Australian Signals Directorate (ASD) Evaluated Products Lists (EPL).

#### 6.1.1.2 Human Services OCA private key pair generation

The self-generated Human Services OCA private keys do not require delivery. Following this, a properly formatted and verified certificate request is forwarded to the RCA.

#### 6.1.1.3 Subscriber key pair generation

For more information about subscriber key pair generation, refer to the CoI CP the certificate was issued under.

6.1.2 Private key delivery to subscriber

For more information about private key delivery to subscribers, refer to the CoI CP the certificate was issued under.

6.1.3 Public key delivery to certificate issuer

#### 6.1.3.1 Human Services OCA public keys

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

#### 6.1.3.2 Subscriber public keys

The Human Services OCA is the issuer for subscriber certificates. Public keys for subscriber certificates are secured delivered internally between the Human Services OCA trusted elements.

6.1.4 CA public key delivery to relying parties

The Human Services OCA public keys are made available to subscribers and relying parties via the

Healthcare Public Directory located at [certificates-australia.com.au](http://www.certificates-australia.com.au/)

6.1.5 Key sizes

The Human Services OCA key length is 2048 bits.

Subscriber keys 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 public keys for subscribers are generated using a product listed on the Defence Signals Directorate (DSD) Evaluated Products List (EPL).

#### 6.1.6.2 Parameter checking

Parameter quality checking is ensured through the use of a product listed on the EPL.

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

Human Services OCA 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 CoI 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 Health Network PKI.

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

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

Dual person control shall be present for all operations concerning OCA 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 OCA 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 OCA are archived in a Secure Facility.

Private key archival is not provided for subscribers.

6.2.6 Private key transfer into or from a cryptographic module

The private key of the Human Services OCA 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

The private key of the Human Services OCA 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 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

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 OCA 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 OCA. 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 OCA, 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 OCA key pairs have the following usage periods:

* Authentication private and public keys – ten (10) years
* Confidentiality public key – ten (10) years
* Confidentiality private key – no expiry.

The usage period for subscriber public and private keys is documented in the applicable CoI CP.

## Activation data

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 OCA 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 OCA 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 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

The Human Services OCA 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

Health Network PKI life-cycle security ratings are set out in the Verizon Australia Pty Ltd *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 Department of 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 CoI CP under which the certificate was issued.

7.1.1 Version number(s)

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

7.1.2 Certificate extensions

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

7.1.3 Algorithm object identifiers

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

7.1.4 Name forms

Certificates issued under the Health 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 CoI CP under which the certificate was issued.

7.1.6 Certificate policy object identifier

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

7.1.7 Usage of policy constraints extension

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

7.1.8 Policy qualifiers syntax and semantics

For this information, please refer to the CoI 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 OCA supports the use of X.509 Version 2 CRLs.

7.2.2 CRL and CRL entry extensions

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

## Online certificate status protocol profile

The Human Services OCA supports the use of the Online Certificate Status Protocol (OCSP) requests in a limited manner, in so far as OCSP requests need not be digitally singed by the sender.

7.3.1 OCSP extensions

Dependant on the responder deployed and its configuration, OCSP extensions will be supported by the Medicare Australia OCA.

# 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 OCA 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 OCA 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 OCA’s operations.

## Topics covered by assessment

The areas of the Human Services OCA 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 Health 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 OCA 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 OCA, 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 OCA CPS.

9.2.3 Warranty coverage

There is no warranty coverage available for subscribers or relying parties under this Human Services OCA CPS or the Human Services RCA 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 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 Health Network PKI to which this Human Services OCA CPS applies.

## Term and termination

9.10.1 Term

The OCA 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 the purpose of this clause, a Notice includes a consent, information, application, request or any other communication provided under or in connection with the Community of Interests certificate policy that certificates are issued under.

A Notice to a party under a CoI 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.medicareaustralia.gov.au/) in accordance with this clause.

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

* a new Human Services CoI CP, Subscriber Agreement or Relying Party Agreement is approved
* there is a change or alteration to an existing Human Services CoI CP, Subscriber Agreement, Relying Party Agreement or this 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.

For more information about individual notices and communications in connection with the Human

Services OCA, 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 OCA CPS, the Human Services RCA 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

There is no other provision.

### Annex A Department of Human Services PKI website

The Health 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.

### Annex B Human Services Communities of Interest

* Human Services Online Claiming for Pharmacy and Pharmaceutical Benefits Scheme (PBS)
* Human Services site certificates
* Human Services healthcare individual certificates
* Human Services individual certificates for healthcare provider individuals under the Healthcare Identifiers Service
* Human Services individual certificates for an authorised organisation maintenance officer under the Healthcare Identifiers Service
* Human Services site certificates for network organisations under the Healthcare Identifiers Service