****

**Australian Government Department of Human Services Community of Interest Certificate Policy for the digital National Authentication Service for Health Public Key Infrastructure Certificate for Healthcare Provider Organisations**

**(2 year duration)**

Policy number: 1.20.1.1

Version 1.0

June 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/

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**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Status** | **Date of Issue** | **Comments** |
| 0.1 | Draft | 10 January 2017 | Initial version reflecting changes in the Gatekeeper PKI Framework version 3.1 |
| 0.2 | Draft | 17 March 2017 | Updated following PKI Authentication Team review. |
| 0.3 | Draft | 05 April 2017 | Minor edits. |
| 0.4 | Draft | 09 June 2017 | Incorporate certificate profile feedback from the Agency |
| 0.5 | Draft | 08 August 2017 | Incorporate feedback from the Digital Health Branch |
| 0.6 | Draft | 17 August 2017 | Feedback from ADHA and Verizon |
| 0.7 | Draft | 18 October 2017 | Clean up in readiness for DTA review |
| 0.8 | Final | 11 December 2017 | Final review and clearance |
| 0.9 | Revised draft | 5 May 2018 | Incorporate access to Healthcare Identifiers Service and online delivery |
| 1.0 | Final | 30 May 2018 |  |

Contents

[1 Introduction 6](#_Toc521665426)

[1.1 Background 6](#_Toc521665427)

[1.2 Document name and identification 7](#_Toc521665428)

[1.3 PKI participants 8](#_Toc521665429)

[1.4 Certificate usage 10](#_Toc521665430)

[1.5 Policy administration 11](#_Toc521665431)

[1.6 Definitions and acronyms 11](#_Toc521665432)

[2 Publication and repository responsibilities 13](#_Toc521665433)

[3 Identification and authentication 14](#_Toc521665434)

[3.1 Naming 14](#_Toc521665435)

[3.2 Initial identity validation 14](#_Toc521665436)

[3.3 Identification and authentication for re-key requests 16](#_Toc521665437)

[3.4 Identification and authentication for revocation request 16](#_Toc521665438)

[4 Certificate life-cycle operational requirements 17](#_Toc521665439)

[4.1 Certificate application 17](#_Toc521665440)

[4.2 Certificate application processing 17](#_Toc521665441)

[4.3 Certificate issuance 18](#_Toc521665442)

[4.4 Certificate acceptance 18](#_Toc521665443)

[4.5 Key pair and certificate usage 19](#_Toc521665444)

[4.6 Certificate renewal 20](#_Toc521665445)

[4.7 Certificate re-key 20](#_Toc521665446)

[4.8 Certificate modification 21](#_Toc521665447)

[4.9 Certificate revocation and suspension 22](#_Toc521665448)

[4.10 Certificate status services 24](#_Toc521665449)

[4.11 End of subscription 24](#_Toc521665450)

[4.12 Key escrow and recovery 24](#_Toc521665451)

[5 Facility, management and operational controls 25](#_Toc521665452)

[5.1 Physical controls 25](#_Toc521665453)

[5.2 Procedural controls 25](#_Toc521665454)

[5.3 Personnel controls 25](#_Toc521665455)

[5.4 Audit logging procedures 25](#_Toc521665456)

[5.5 Records archival 25](#_Toc521665457)

[5.6 Key changeover 25](#_Toc521665458)

[5.7 Compromise and disaster recovery 26](#_Toc521665459)

[5.8 CA or RA termination 26](#_Toc521665460)

[6 Technical security controls 27](#_Toc521665461)

[6.1 Key pair generation and installation 27](#_Toc521665462)

[6.2 Private key protection and cryptographic module engineering controls 28](#_Toc521665463)

[6.3 Other aspects of key pair management 29](#_Toc521665464)

[6.4 Activation data 29](#_Toc521665465)

[6.5 Computer security controls 29](#_Toc521665466)

[6.6 Life cycle technical controls 29](#_Toc521665467)

[6.7 Network security controls 30](#_Toc521665468)

[6.8 Time-stamping 30](#_Toc521665469)

[7 Certificate, CRL and OCSP Profiles 31](#_Toc521665470)

[7.1 Certificate profile 31](#_Toc521665471)

[7.2 CRL profile 35](#_Toc521665472)

[7.3 OCSP profile 35](#_Toc521665473)

[8 Compliance audit and other assessments 36](#_Toc521665474)

[8.1 Frequency or circumstances of assessments 36](#_Toc521665475)

[8.2 Identity/qualifications of assessor 36](#_Toc521665476)

[8.3 Assessor’s relationship to assessed entity 36](#_Toc521665477)

[8.4 Topics covered by assessment 36](#_Toc521665478)

[8.5 Actions taken as a result of deficiency 36](#_Toc521665479)

[8.6 Communication of results 36](#_Toc521665480)

[9 Other business and legal matters 37](#_Toc521665481)

[9.1 Fees 37](#_Toc521665482)

[9.2 Financial responsibility 37](#_Toc521665483)

[9.3 Confidentiality of business information 37](#_Toc521665484)

[9.4 Privacy of personal information 37](#_Toc521665485)

[9.5 Intellectual property rights 37](#_Toc521665486)

[9.6 Representations and warranties 37](#_Toc521665487)

[9.7 Disclaimers of warranties 37](#_Toc521665488)

[9.8 Limitations of liability 38](#_Toc521665489)

[9.9 Indemnities 38](#_Toc521665490)

[9.10 Term and termination 38](#_Toc521665491)

[9.11 Individual notices and communications with participants 38](#_Toc521665492)

[9.12 Amendments 39](#_Toc521665493)

[9.13 Dispute resolution provisions 39](#_Toc521665494)

[9.14 Governing law 39](#_Toc521665495)

[9.15 Compliance with applicable law 39](#_Toc521665496)

[9.16 Miscellaneous provisions 39](#_Toc521665497)

[9.17 Other provisions 39](#_Toc521665498)

# Introduction

## Background

The Australian Government Department of Human Services (Human Services) owns and operates the Health Network Public Key Infrastructure (Health Network PKI) to:

* facilitate the authentication of confidential communications for a number of online programmes, and
* enable access to Digital Health infrastructure and services.

As part of the Health Network PKI, Human Services provides digital National Authentication Service for Health Public Key Infrastructure (NASH PKI) certificates, which allow:

* access to the Healthcare Identifiers (HI) Service, as set out in the *Healthcare Identifiers Act 2010*
* access to the My Health Record system as set out in the *My Health Records Act 2012*
* secure communications using the Health Network PKI by healthcare providers and organisations that support healthcare providers to deliver healthcare services, and
* access to the My Health Record system and services by organisations that have a supporting role in relation to the My Health Record system and services.

This Certificate Policy (CP) applies to the issuance of certificates to healthcare provider organisations, and the use of those certificates by healthcare provider organisations.

Key pairs (that is, a private key and a public key) and certificates (that identify the subscriber, specify the public key and contain the information required by the Certificate Profile) are issued to end entity-subscribers who are:

* individual healthcare providers and healthcare provider organisations to whom healthcare identifiers (Healthcare Provider Identifier – Individual (HPI-I) and Healthcare Provider Identifier – Organisation (HPI-O)) have been assigned under the *Healthcare Identifiers Act 2010*  and who have been issued with certificates under other certificate policies within the Health Network PKI, and
* supporting organisations within the meaning of this CP.

The NASH PKI certificates issued under this policy are accredited against the Level of Assurance 2 (LOA 2) criteria as stipulated in the current published version of the Gatekeeper Public Key Infrastructure Framework (Gatekeeper PKI Framework).

The NASH PKI is a set of hardware, software, policies and procedures that let the recipient of an electronic communication know that:

* the sender of the communication was recorded as being registered with the HI Service at the time they were issued with a certificate, and information related to the sender’s registration can be reliably represented to the recipient for verification (authentication)
* the communication content has not been changed in transit between the sender and the recipient (integrity), and
* only the intended recipient is able to open the communication (confidentiality) of the relying party (assurance).

### Requirement for prior registration in the HI Service

Healthcare provider organisations must register with the HI Service prior to, or as part of, applying for a NASH PKI certificate.

For the purpose of certificates issued under this CP, the Community of Interest (CoI) comprises:

* Human Services
* the HI Service operator under the *Healthcare Identifiers Act 2010*
* the system operator of the My Health Record system under the *My Health Records Act 2012*
* the Human Services RA CoI CPs for NASH PKI for individual healthcare providers and supporting organisations, and
* end entity-subscribers.

## Document name and identification

### CP identification

Certificates issued under this CP shall bear the Policy Object Identifier (OID):

**1.2.36.174030967.1.20.1.1**

### Overview of PKI documents

This CP should be read in conjunction with the:

* *Department of Human Services Root Certification Authority Certification Practice Statement* (Human Services RCA CPS)
* *Department of Human Services Root Certification Authority Certificate Policy* (Human Services RCA CP)
* *Department of Human Services Organisation Certification Authority Certification Practice Statement* (Human Services OCA CPS)
* *National Authentication Service for Health Public Key Infrastructure Certificate for Healthcare Provider Organisations Terms and Conditions* (Terms and Conditions), and
* *National Authentication Service for Health Public Key Infrastructure Relying Party Agreement* (Relying Party Agreement).

## PKI participants

### Certification authorities

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

For information on applicable practices and procedures for certificates issued under this CP, refer to the Human Services OCA CPS, the Human Services RCA CPS and 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)](https://www.humanservices.gov.au/health-professionals/enablers/public-key-infrastructure-pki-policy-documents)

### Registration authorities

Human Services is the Registration Authority (Human Services RA) in the Health Network PKI.

#### Certificate controllers

Certificate controllers are Human Services RA staff with responsibilities for managing certificates.

All certificate controllers operating under this CP are duly authorised representatives of Human Services.

#### Registration Organisation Unit

The Human Services Registration Organisation Units (ROUs) are business areas within Human Services that receive and process registration applications. Successful registration results in certificates issued to the subscriber for the defined CoI.

There are separately identified ROUs within the Human Services RA, usually one ROU for each CoI in the Healthcare Network PKI.

The ROU has responsibilities in the CoI for managing the subscribers in that CoI.

#### Registration Organisation Unit operators

Registration Organisation Unit operators (ROUOs) are Human Services staff working in the ROU or the HI Service operator area responsible for undertaking the application registration of the responsible officers, organisational maintenance officers and of contracted service provider officers.

ROUOs within this CoI are not certificate controllers.

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

### Subscribers

Subscribers under this CP are healthcare provider organisations to which a HPI-O has been assigned under the *Healthcare Identifiers Act 2010*.

The meaning of a NASH PKI certificate issued under this CP is nothing more and nothing less than a statement expressed in a digital format of the fact that the subscriber (i.e. the healthcare provider organisation) is recorded as being registered with the HI Service at the time of certificate issuance and recorded as having a particular HPI-O.

A certificate does not verify or represent that:

* the subscriber or any of their staff have particular qualifications or registrations other than the HI Service, and
* the subscriber is registered with the My Health Record system. This registration is a separate process that may only be taken by those healthcare provider organisations that are eligible for that registration.

There is a subscriber agreement under this CP, known as the *National Authentication Service for Health Public Key Infrastructure Certificate for Healthcare Provider Organisations Terms and Conditions of Use*.

In using and relying upon certificates, subscribers are legally bound by this CP, the Terms and Conditions and the Relying Party Agreement. A subscriber must also comply with the PKI documents mentioned in this CP that are published by Human Services on or linked to its website at [humanservices.gov.au/pki](https://www.humanservices.gov.au/health-professionals/enablers/public-key-infrastructure-pki-policy-documents)

### Relying parties

The following are relying parties:

* the system operator of the My Health Record system (see section 14 of the *My Health Records Act 2012*)
* subscribers under this CP (i.e. organisations to which a certificate has been issued)
* the Chief Executive Medicare as the service operator under the *Healthcare Identifiers Act 2010*, and
* individual healthcare providers and supporting organisations that are subscribers under another Human Services RA CoI CP for NASH PKI.

Relying parties must not use a certificate by itself, and must use means other than the NASH PKI, to determine whether they will rely on the content of an electronic communication (including any clinical statement or representation).

There are no other relying parties.

There is a relying parties agreement under this CP, known as the *National Authentication Service for Health Public Key Infrastructure Relying Party Agreement*.

Where you rely on a certificate issued under this CP and you do not have a written agreement with Human Services or authorisation or approval through a notice published at [humanservices.gov.au/pki](https://www.humanservices.gov.au/health-professionals/enablers/public-key-infrastructure-pki-policy-documents)  (specifying an allowable usage), you rely on the certificate at your own risk.

### Other participants

There are no other participants.

## Certificate usage

### Appropriate certificate use

Key pairs and certificates issued under this CP must only be used by healthcare provider organisations to:

* access digital health records in the My Health Record system as authorised by the My Health Record system operator, or
* authenticate or protect the confidentiality and integrity of electronic communications with relying parties (other than the My Health Record system operator) that are recognised under this CP in accordance with section 1.3.4.

### Prohibited certificate uses

A NASH PKI certificate for healthcare provider organisations is only permitted to be used for purposes outlined in section 1.4.1 above.

Parties using a NASH PKI certificate for healthcare provider organisations for any other purpose, do so at their own risk.

## Policy administration

For information about policy administration, 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)

## Definitions and acronyms

### Terminology

**Clinical** means anything that relates to the examination, diagnosis or treatment of individual patients by healthcare providers who are duly qualified, registered, recognised or trusted as performing those actions.

**Healthcare provider organisation** means an organisation to whom a HPI-O has been assigned under the *Healthcare Identifiers Act 2010*.

**HI Service** means, for the purposes of this CP, the healthcare identifiers service operated by the Chief Executive Medicare as the service operator under the *Healthcare Identifiers Act 2010*, and includes the administrative extensions to that service for the registration of supporting organisations by Human Services.

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

**NASH** is an acronym for National Authentication Service for Health.

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

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

1. *Healthcare Identifiers Act 2010* and the *My Health Records Act 2012*
2. Healthcare Identifiers Regulations 2010 and the My Health Records Regulations 2012
3. *Health Practitioner Regulations National Law Act 2009 / 2010* (known as National Law) of each state and territory and related Commonwealth Acts and Regulations
4. National Partnership Agreement 2009 (the COAG agreement)
5. PKI gatekeeper documents, including the [Department of Human Services Public Key Infrastructure (PKI) glossary](http://www.humanservices.gov.au/health-professionals/services/public-key-infrastructure/public-key-infrastructure-policy-documents)

### References

For definitions and acronyms refer to the:

* *Healthcare Identifiers Act 2010*
* Healthcare Identifiers Regulations 2010
* *My Health Records Act 2012*
* [Department of Human Services Public Key Infrastructure (PKI) glossary](https://www.humanservices.gov.au/health-professionals/enablers/public-key-infrastructure-pki-policy-documents)

# Publication and repository responsibilities

The repository for all public key certificates issued under this CP is the NASH Directory.

The NASH Directory provides information about active and revoked certificates.

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

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

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

Changes in the status of certificates issued under the 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 is accessible from [certificates-australia.com.au](http://www.certificates-australia.com.au/).

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

For information about publication and repository responsibilities, 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)

# Identification and authentication

## Naming

### Types of names

Subscribers will be assigned a distinguished name under ‘Certificate Subject’ in the X.509 definition.

### Need for names to be meaningful

Subscribers under this CP will be named according to the NASH application and HI Service registration processes for healthcare provider organisations in the CoI described in this CP.

### Anonymity or pseudonymity of subscribers

Anonymity and pseudonymity is not supported by this CP.

### Rules for interpreting various name forms

The NASH Directory supports the use of X.500 names.

### Uniqueness of names

The uniqueness of their names shall be assured by the incorporation of the healthcare identifier issued to the healthcare provider organisation into the distinguished name.

### Recognition, authentication, and role of trademarks

Not applicable.

## Initial identity validation

### Method to prove possession of private key

Subscriber private keys are generated by the Human Services OCA. The private key certificates are made available for download via a secure website to subscribers.

### Authentication of organisation identity

Subscribers under this CP will be identified and authenticated at the time of their application for a certificate by confirming that the healthcare provider organisation is registered in the HI Service.

This process may include, but is not limited to:

* receipt of an application for a NASH PKI certificate for healthcare provider organisations
* organisation identity proofing requirements under Gatekeeper PKI Framework, and/or
* requesting information from the HI Service that verifies that a HPI-O has been assigned to an entity matching the details in the application.

The Human Services ROUO does not undertake any separate action to verify or confirm the information provided by a healthcare provider organisation in its application for a NASH PKI certificate.

### Authentication of individual identity

Authorisers and certificate managers of the subscribers under this CP will be identified and authenticated at the time of their application for registration by Human Services.

If an authoriser is not the responsible officer of the organisation as set out in the *Healthcare Identifiers Act 2010*, then they will be identified and authenticated at the time of their application to request the NASH PKI certificate.

These processes may include, but are not limited to:

* individual identity proofing requirements under Gatekeeper PKI Framework
* assessment of applications and associated documents
* processing in association with the Australian Digital Health Agency (where required)
* allocation of number(s) (where required) and registration on Human Services systems (however described).

### Non-verified subscriber information

Not applicable.

### Validation of authority

The capacity of the authoriser to commit the healthcare provider organisation and to appoint a certificate manager is validated as part of the certificate application.

### Criteria for interoperation

Previous registration by the Human Services OCA for the Health Sector PKI and the associated Registration Authority number are recognised by the Human Services OCA for the Health Network PKI.

## Identification and authentication for re-key requests

### Identification and authentication for routine re-key

Subscribers under this CP shall be identified and authenticated and their certificate renewed:

* after submission of an approved application, and
* where the policy is still active and a valid address is registered with the HI Service.

### Identification and authentication for re-key after revocation

Subscribers under this CP shall be identified and authenticated and their certificate reissued, provided that:

* reissuance of a certificate is included in the revocation request, and
* the status of the healthcare provider organisation in the HI Service (Human Services as service operator of the HI Service) are active and valid for certificate issuance.

## Identification and authentication for revocation request

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

* ROUOs in the event that the subscriber becomes ineligible to remain as a healthcare provider organisation for the purpose of the CoI described in this CP
* the subscriber, or
* certificate controllers.

Subscribers under this CP shall be identified and authenticated against the details held by the Human Services.

# Certificate life-cycle operational requirements

## Certificate application

### Who can submit a certificate application

The authoriser or certificate manager of the subscriber can submit a certificate application.

Certificate applications are submitted online. If the authoriser is a different individual than the healthcare provider organisation’s responsible officer as set out in the *Healthcare Identifiers Act 2010*, then an approved alternative application must be submitted.

### Enrolment process and responsibilities

Human Services may consider that the healthcare provider organisation be enrolled for a NASH PKI certificate by certificate controllers on the basis of an approved certificate application.

Human Services may, in accordance with trusted practices, provide information to its service providers to enable a NASH PKI certificate to be issued.

## Certificate application processing

### Performing identification and authentication functions

Certificate application under this CP are processed by the Human Services ROUs.

### Approval or rejection of certificate applications

Human Services may consider that the healthcare provider organisation be enrolled for a NASH PKI certificate for healthcare provider organisations by certificate controllers on the basis of:

* receipt of an application for a NASH PKI certificate for healthcare provider organisations together with any documentation required as part of the Health Network PKI requirements
* consent by the applicant to collect, disclose and use information with, from and to the service operator established under the *Healthcare Identifiers Act 2010*
* verification from the HI Service that a HPI-O has been assigned to an entity matching the details in the application.

### Time to process certificate applications

The time to process a certificate application is dependent on the process set out in section 4.2.2. The normal online application process should be completed in 1 business day. The paper-based process should be completed in 20 business days.

Please contact the Department of Human Services using the details in the application form to enquire about status of an application.

## Certificate issuance

###  Certificate Authority actions during certificate issuance

The Certificate Authority (CA) is responsible for the issuance of the PKI certificate. Certificate controllers are duly authorised staff of the CA responsible for the management of the certificate.

All subscriber key pairs under this CP shall be generated by certificate controllers using approved software that is approved for use under the current published version of the Gatekeeper PKI Framework.

### Notification to subscriber by the Certificate Authority of issuance of certificate

The signing key and encryption key shall be made available for download via a secure website. Notification of availability will be sent separately via SMS to the certificate manager. A personal identification code (PIC) to access the key and certificate will also be generated and included in the SMS.

## Certificate acceptance

### Conduct constituting certificate acceptance

There is a subscriber agreement under this CP, known as the *National Authentication Service for Health Public Key Infrastructure Certificate for Healthcare Provider Organisations Terms and Conditions of Use.*

The subscriber agrees to be bound by these terms and conditions when the subscriber applies for the NASH PKI Certificate for Healthcare Provider Organisations.

### Publication of the certificate by the CA

The NASH Directory contains certificates issued under NASH CPs for healthcare provider organisations and supporting organisations. The NASH Directory is accessible by subscribers under this CP. Certificates issued under this CP will be published in the NASH Directory. The NASH Directory will be accessible by relying parties under this CP and under other NASH certificate policies. Human Services may choose, at its discretion, to change who can access the NASH Directory, including choosing what, if anything, is permitted to be accessed. A healthcare provider organisation’s HPI‑O that is contained in its certificate will be disclosed in the NASH Directory.

Revocation status of certificates issued under this CP will be published in the NASH Directory. The HPI-O will not appear in the Certificate Revocation List (CRL).

Changes in the status of certificates issued under the 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 is accessible from [certificates-australia.com.au](http://www.certificates-australia.com.au/).

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

### Notification of certificate issuance by the CA to other entities

The Human Services OCA may send certificates to the subscribers via the ROUs. It may issue the certificates in tamper evident packaging to ensure subscriber privacy.

## Key pair and certificate usage

### Subscriber private key and certificate usage

Subscribers shall only use their private keys and certificates only for the purposes as described in section 1.4 and consistent with ‘Key Usage’ field in the certificate profile.

Use of private keys and certificates by a subscriber are subject to the subscriber agreement under this CP.

### Relying party public key and certificate usage

Relying parties may rely on subscriber’s public keys and certificates only for the purposes as described in section 1.4 and consistent with ‘Key Usage’ field in the certificate profile.

Relying parties are responsible for checking the status of a certificate using one of the methods described in section 4.10 prior to performing any public key operations. Relying parties shall not rely on a certificate that is revoked.

## Certificate renewal

### Circumstance for certificate renewal

Subscribers under this CP may have their certificate renewed after 2 years, provided the Human Services RA is satisfied that the subscriber’s status within the HI Service remains active.

Certificates issued under this CP may be renewed in the event of expiry of the certificate.

### Who may request renewal

The certificates are automatically renewed.

### Processing certificate renewal requests

All certificate renewals under this CP involve re-keying.

Refer to section 3.3 for details of identification and authentication.

### Notification of new certificate issuance to subscriber

Refer to section 4.3 for details on notification of certificate issuance to subscribers.

### Conduct constituting acceptance of a renewal certificate

Refer to section 4.4 for details on conduct constituting acceptance of a certificate.

### Publication of the renewal certificate by the CA

Certificates and their corresponding hash values renewed under this CP are published to the NASH Directory when the certificate is generated.

Refer to section 4.4.2 for details on publication.

### Notification of certificate issuance by the CA to other entities

Formal notification of certificate issuance will not be given to any entities.

## Certificate re-key

### Circumstance for certificate re-key

All certificate renewals and reissuance under this CP involve re-keying.

### Who may request certification of a new public key

Subscribers may request their certificates be reissued after revocation.

Refer to section 3.3 for details of identification and authentication.

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

* changes to technical attributes of the certificate (e.g. Secure Hashing Algorithm)
* in response to compromise and disaster recovery detailed in section 5.7 of the Human Services OCA CPS
* as directed by the Commonwealth government.

### Processing certificate re-keying requests

All re-keying requests under this CP shall be processed by certificate controllers using approved software that is approved for use under the current published version of the Gatekeeper PKI Framework.

### Notification of new certificate issuance to subscriber

Refer to section 4.3 for details on notification of certificate issuance to subscribers.

### Conduct constituting acceptance of a re-keyed certificate

Refer to section 4.4 for details on conduct constituting acceptance of a certificate.

### Publication of the re-keyed certificate by the CA

Certificates reissued under this CP and their corresponding hash values are published to the NASH Directory when the certificate is generated.

Refer to section 4.4.2 for details on publication.

### Notification of certificate issuance by the CA to other

Formal notification of certificate issuance will not be given to any entities.

## Certificate modification

Certificate modification is not supported for this CP.

## Certificate revocation and suspension

### Circumstances for revocation

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

* receipt of a revocation request
* receipt of notification for termination of terms and conditions
* after loss, destruction or theft of the certificate
* in the event of the healthcare provider organisation’s de-registration (however described)
* in the event the Healthcare Identifiers service operator established under the *Healthcare Identifiers Act 2010* cancels the HPI-O of the healthcare provider organisation
* in the event that the healthcare provider organisation revokes any consent given under section 24A of the *Healthcare Identifiers Act 2010*  or alters any limitations regarding the consent
* in the event any healthcare provider identification number(s) (however described) are cancelled by Human Services or other organisation or body authorised to cancel such number(s)
* in the event the healthcare provider organisation ceases to exist or be recognised by Human Services or ceases to be a member of a Human Services RA CoI.

### Who can request revocation

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

* ROUOs in the event that the subscriber becomes ineligible to remain as a healthcare provider organisation recognised by Human Services or ceases to be a member of a Human Services RA CoI
* the subscriber
* certificate controllers.

### Procedure for revocation request

Revocation must be requested in line with section 3.4.

### Revocation request grace period

Subscribers may request revocation of their certificate at any time by written notice to Human Services.

### Time within which CA must process the revocation request

The Human Service OCA shall process revocation requests within 72 hours in line with the timeframe specified by the Gatekeeper PKI Framework that correspond to LOA 2. If the revocation request is made after business hours, the 72 hours begins the next day of business.

### Revocation checking requirement for relying parties

The Human Services OCA CRL is published in the NASH Directory. The NASH Directory is accessible from [certificates-australia.com.au](http://www.certificates-australia.com.au)
This notification method uses a “pull” model. Interested relying parties must exercise due care and check, on a regular basis, the NASH Directory to review and monitor any changes to certificate status. Interested relying parties are responsible for retrieving the Human Services OCA CRL when a new CRL is posted.

### CRL issuance frequency (if applicable)

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

### Maximum latency for CRLs (if applicable)

The CRL will have a grace period of 1 day.

The next refresh of a particular CRL is specified in the CRL ‘Next Update’ field.

### On-line revocation/status checking availability

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

### On-line revocation checking requirements

No stipulation.

### Other forms of revocation advertisements available

Not applicable.

### Special requirements re key compromise

Subscriber must notify the CA of a key compromise as soon as possible.

### Circumstances for suspension

Certificate suspension is not supported for this CP.

## Certificate status services

### Operational characteristics

For information about operational characteristics, 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)

### Service availability

Service availability for the CRL is 24 hours per day, 7 days per week (except for designated system maintenance periods) at [certificates-australia.com.au](http://www.certificates-australia.com.au/)

### Optional features

Not applicable.

## End of subscription

Certificates issued under this CP are terminated when they are revoked or have expired.

## Key escrow and recovery

Key escrow is not supported by the Human Services OCA.

# Facility, management and operational controls

## Physical controls

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

For more information about physical controls, refer to the Human Services OCA CPS located at humanservices.gov.au/pki

## Procedural controls

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

For more information about procedural controls, 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)

## Personnel controls

All certificate controllers under this CP shall be authorised representatives of Human Services or Human Services as the service operator for the HI Service (in relation to responsible officers and contracted service provider officers).

For more information about personnel controls, 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)

## Audit logging procedures

For information about audit logging procedures, 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)

## Records archival

For information about records archival, 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)

## Key changeover

For information about key changeover, 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)

## Compromise and disaster recovery

For information about compromise and disaster recovery, 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)

## CA or RA termination

### CA termination

For information about Human Services OCA or Human Services Health Network PKI termination, 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)

### Business Continuity of the Human Services RA

Human Services (the Registration Authority under this CP) is a statutory agency established under the *Human Services (Medicare) Act 1973* (previously the *Medicare Australia Act 1973*). Its continuation depends on continuance in force of the *Human Services (Medicare) Act 1973* or by other Acts of the Commonwealth Parliament made pursuant to government policy.

Changes in legislation or government policy will provide for business continuity of the Human Services RA in accordance with policy as determined by the government and implemented in accordance with Commonwealth Machinery of Government (MOG) requirements.

#### ROU termination or transfer

Human Services is a statutory agency established under the *Human Services (Medicare) Act 1973.* Its termination or change of entity status can only be through amendments to the *Human Services (Medicare) Act 1973* or by other Acts of the Commonwealth Parliament made pursuant to government policy.

Changes in legislation or government policy will provide for termination of Human Services as the ROU under this CP and provide for a replacement agency as the successor RA in accordance with policy as determined by the government and implemented in accordance with legislation passed by the Commonwealth Parliament.

The system operator of the My Health Record system is established under section 14 of the *My Health Records Act 2012*. A change of status of the system operator can only be through amendment to the *My Health Records Act 2012* or by other Acts of the Commonwealth Parliament made pursuant to changes in government policy.

# Technical security controls

Certificate requests will be processed by the authorised certificate controllers of Human Services in accordance with the security provisions of 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)

## Key pair generation and installation

### Key pair generation

All subscriber key pairs[[1]](#footnote-1) and certificates issued under this CP shall be generated by certificate controllers using approved software that is approved for use under the current published version of the Gatekeeper PKI Framework.

### Private key delivery to subscriber

The content commitment key and utility key shall be made available for download via a secure website. Notification of availability will be sent separately via SMS to the certificate manager. A Personal Identification Code (PIC) to access the key and certificate will be generated and included in the SMS.

### Public key delivery to certificate issuer

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.

### CA public key delivery to relying parties

The Human Services OCA public keys are made available to subscribers and relying parties via the NASH Directory located at [certificates-australia.com.au](http://www.certificates-australia.com.au/)

### Key sizes

Subscriber keys have a minimum length of 2048 bits.

### Public key parameters generation

The parameters used to create public keys for subscribers are generated using a product listed on the Australian Signals Directorate (ASD) Evaluated Products List (EPL).

### Key usage purposes (as per X.509 v3 ‘Key Usage’ field)

Subscriber keys will be used for the purposes listed under the ‘Key Usage’ field contained in the certificate profiles in section 7.

## Private key protection and cryptographic module engineering controls

### Cryptographic module standards and controls

Public Key Cryptography Standards (PKCS) #12 standard are used for digital files.

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

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

### Private key escrow

Private key escrow is not supported.

### Private key backup

Private key backup is not provided for subscribers.

### Private key archival

Private key archival is not provided for subscribers.

### Private key transfer into or from a cryptographic module

The subscriber private keys are generated using approved software that is approved for use under the current published version of the Gatekeeper PKI Framework and remains in the PKCS #12 format.

### Private key storage on a cryptographic module

The subscriber private keys are stored in a password protected PKCS#12 digital file.

### Method of activating private key

The subscriber private keys are activated by the entering of the PIC.

### Method of deactivating private key

The subscriber private keys are deactivated when the certificate is revoked.

### Method of destroying private key

No stipulation.

### Cryptographic module rating

Only cryptographic modules evaluated and approved by the ASD shall be used.

## Other aspects of key pair management

### Public key archival

The public keys are not archived.

### Certificate operational periods and key pair usage periods

The subscriber certificates and key pairs are valid for two years from the date of issuance.

## Activation data

### Activation data generation and installation

No activation data other than access control mechanisms via the PIC is required to download and install the digital certificate.

### Activation data protection

Not applicable.

### Other aspects of activation data

Not applicable.

## Computer security controls

For information about computer security controls, 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)

## Life cycle technical controls

For information about life cycle technical controls, 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)

## Network security controls

For information about network security controls, 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)

## Time-stamping

For information about time-stamping, 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)

# Certificate, CRL and OCSP Profiles

## Certificate profile

| **F**i**e**l**d**/ **E**x**ten**sion | Utility Certificate |
| --- | --- |
| Version | **Required** |
| V3 |
| Serial Number | **Required** |
| A positive integer that uniquely identifies the certificate |
| Issuer Signature Algorithm | **Required** |
| **sha256WithRSAEncryption {1 2 840 113549 1 1 11}** |
| Issuer Distinguished Name | **Required** |
| Country (C) = AUOrganisation (O) = GOVOrganisation Unit (OU) = HumanservicesCommon Name (CN) = Medicare Australia Organisation Certification Authority |
| Validity Period | **Required** |
| 2 years  |
| Subject Distinguished Name | **Required** |
| Domain Component (dc) = auDomain Component (dc) = netDomain Component (dc) = electronichealthDomain Component (dc) = idDomain Component (dc) = <Healthcare Identifier of Organisation>Organisation (O) = <Name of Organisation>Common Name (CN) = general.<Healthcare Identifier of Organisation>.id.electronichealth.net.au |
| Subject Public Key Information | **Required** |
| Public Key encoded in accordance with RFC2459 & PKCS#1Key length 2048 bits |
| Issuer Unique Identifier | **Not Used** |
| Subject Unique Identifier | **Not Used** |
| Issuer’s Signature | **Required** |
| ASN.1 DER encoded certificate signature value corresponding to Issuer signature algorithm |
| Authority Key Identifier | **Required** |
| Octet string contain the 20 byte SHA–1 hash of the binary DER encoding of the subject CA’s public key information |
| Subject Key Identifier | **Required** |
| Octet string contain the 20 byte SHA–1 hash of the binary DER encoding of the subject CA’s public key information |
| Key Usage | **Required critical** |
| Digital Signature, Key Encipherment, Data Encipherment |
| Basic Constraints | **Required critical** |
| Not CA; path length constraint absent |
| Extended Key Usage | **Not Used** |
| Private Key Usage Period | **Not Used** |
| Certificate Policies | **Required** |
| Policy Identifier OID = 1.2.36.174030967.1.20.1.1CPS Point = http://humanservices.gov.auPolicy Qualifier ID = User NoticeNotice Text = ‘Certificates issued under this CP must only be relied on by entities within the Community of Interest, unless otherwise agreed, and not for purposes other than those permitted by this CP.’ |
| Policy Mappings | **Not Used** |
| Subject Alternative NameRFC822 Name | **Not Used** |
| Subject Alternative NameURI | **Not Used** |
| Issuer Alternative Name | **Not Used** |
| Subject Directory Attributes | **Not Used** |
| Name Constraints | **Not Used** |
| Policy Constraints | **Not Used** |
| Authority Information Access | **Required** |
| **Access Method = On-line Certificate Status Protocol {1.3.6.1.5.5.7.4.1)****URL = http://ocsp.certificates-australia.com.au/maoca2.pkx** |
| CRL Distribution Points | **Required** |
| **URL = http://www.certificates-australia.com.au/cgi-bin/download.pl?DN=cn=Medicare Australia Organisation Certification Authority, ou=Humanservices, o=GOV, c=AU & downloadType=CRL & filename=Medicare Australia Organisation CA.crl & healthDir=true****(**<http://www.certificates-australia.com.au/cgi-bin/download.pl?DN=cn%3DMedicare%20Australia%20Organisation%20Certification%20Authority%2Cou%3DHumanservices%2Co%3DGOV%2Cc%3DAU&downloadType=CRL&filename=Medicare%20Australia%20Organisation%20CA.crl&healthDir=true>**)** |
| Subject Information Access | **Not Used** |
| Freshest CRL | **Not Used** |
| Inhibit Any Policy | **Not Used** |
| RA Number{1.2.36.73665175.1.10009}  | **Required** |
| **<RA Number>**  |
| Friendly Name | **Required** |
| **<CN of Subject>** |

### Version number(s)

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

### Certificate extensions

Certificate extensions are used by the Human Services OCA Certificates and are listed in the certificate profile tables.

### Algorithm object identifiers

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

### 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.

### Name constraints

Anonymous names are not supported.

### Certificate policy object identifier

The OID of this CP is carried in the standard extension field of issued X.509 Certificates and is defined in section 1.2.

### Usage of policy constraints extension

Policy constraints extension is not used.

### Policy qualifiers syntax and semantics

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

### Processing semantics for the critical certificate policy extension

The X.509 Certificate Profile complies with the Australian Standard X.509 profile.

## CRL profile

For information about CRL profile, 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)

## OCSP profile

For information about OCSP profile, 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)

# Compliance audit and other assessments

## Frequency or circumstances of assessments

For information about frequency or circumstances of assessments, 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)

## Identity/qualifications of assessor

For information about identity/qualifications of assessor, 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)

## Assessor’s relationship to assessed entity

For information about assessor’s relationship to assessed entity, 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)

## Topics covered by assessment

For information about topics covered by assessment, 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)

## Actions taken as a result of deficiency

For information about actions taken as a result of deficiency, 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)

## Communication of results

For information about communication of results, 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)

# Other business and legal matters

## Fees

Not applicable

## Financial responsibility

### Insurance coverage

All insurances are the responsibility of each subscriber.

### Other assets

Other assets are not considered under this CP.

### Warranty coverage

There is no warranty coverage available for subscribers or relying parties under this CP.

## 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

For information about disclaimers of 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)

## 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 CP applies.

## Term and termination

### Term

This CP will be ongoing.

### Termination

Human services may terminate this CP at its own discretion or otherwise as may be required by the Commonwealth government.

Human Services will promptly notify, in accordance with section 9.11, all OCAs, RAs, subscribers, relying parties, the Gatekeeper Competent Authority and other participants of the intended termination of this CP.

### Effect of termination and survival

The Human Services OCA will, on notification of termination, cease to generate and issue certificates under this CP.

On termination, all certificates issued under this CP remain in force for any period left of the two-year operative time of the certificate.

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

## 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

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

1. A pair of asymmetric cryptographic keys (e.g. one decrypts messages which have been encrypted using the other) consisting of a public key and a private key. [↑](#footnote-ref-1)