**Short Form Certificate Policy**



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

**(2 year duration)**

Policy number: 1.12.1.1

Version 1.4

**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/](file:///C:\Users\ufgbw\AppData\Local\Microsoft\Windows\Temporary%20Internet%20Files\Content.Outlook\STIDZEHE\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 government’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 license should be sent to:

The Manager

External Communication Branch

Human Services Portfolio Communication Division

PO Box 7788

Canberra BC, ACT, 2610

**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**

|  |  |  |  |
| --- | --- | --- | --- |
| Doc  Version | Status | Date of Issue | Comments |
| 1.0 | Initial version |  |  |
| 1.1 | Revised version | 16 April 2013 | Amendments to implement a broader definition of Supporting Organisation, to allow NASH Certificates to be issued to a range of entities and persons with supporting roles within the national ehealth infrastructure and systems. |
| 1.2 | Revised version | November 2014 | Minor amendment to include automatic renewal of certificates. Updates to disclaimers regarding identity. |
| 1.3 | Revised version | January 2016 | My Health Record system updates |
| 1.4 | Revised version | May 2018 | Amendments to support NASH certificates accessing the Healthcare Identifiers Service. |

### Contents

[Contents 4](#_Toc521673629)

[1. Background 6](#_Toc521673630)

[1.1 Human Services Health Sector Public Key Infrastructure 6](#_Toc521673631)

[1.2 National Authentication Service for Health (NASH) 6](#_Toc521673632)

[1.3 Overview of PKI documents 7](#_Toc521673633)

[1.4 Requirement for prior registration in the HI Service 7](#_Toc521673634)

[1.5 Terminology 9](#_Toc521673635)

[1.6 Certificate policy clauses 10](#_Toc521673636)

[1.6.1 CP Identification 10](#_Toc521673637)

[2. Introduction 11](#_Toc521673638)

[2.1 PKI participants 11](#_Toc521673639)

[2.1.1 Certification Authority 11](#_Toc521673640)

[2.1.2 Relationship Organisation 11](#_Toc521673641)

[2.1.3 Relationship Organisation Unit 11](#_Toc521673642)

[2.1.4 Certificate controllers 11](#_Toc521673643)

[2.1.5 Relationship Organisation Unit operators 11](#_Toc521673644)

[2.1.6 Subscribers 12](#_Toc521673645)

[2.1.7 Relying party 12](#_Toc521673646)

[2.2 Certificate use 13](#_Toc521673647)

[2.2.1 Allowable certificate uses 13](#_Toc521673648)

[2.2.2 Prohibited certificate uses 13](#_Toc521673649)

[2.3 Definitions and acronyms 13](#_Toc521673650)

[3. Identification and authentication of users 14](#_Toc521673651)

[3.1 Naming of subscribers 14](#_Toc521673652)

[3.2 Identification and authentication of the subscriber at registration 14](#_Toc521673653)

[3.3 Identification and authentication of the subscriber at renewal 14](#_Toc521673654)

[3.4 Identification and authentication of revocation request 15](#_Toc521673655)

[4. Certificate life-cycle operational requirements 16](#_Toc521673656)

[4.1 Certificate creation 16](#_Toc521673657)

[4.1.1 Enrolment process and responsibilities 16](#_Toc521673658)

[4.1.2 Publication of the certificate 16](#_Toc521673659)

[4.2 Key pair and certificate usage 17](#_Toc521673660)

[4.2.1 Key pair generation and installation 17](#_Toc521673661)

[4.3 Certificate renewal 17](#_Toc521673662)

[4.4 Certificate revocation 17](#_Toc521673663)

[4.5 Certificate status services 17](#_Toc521673664)

[4.5.1 Operational characteristics 17](#_Toc521673665)

[4.5.2 Service availability 18](#_Toc521673666)

[4.5.3 Optional features 18](#_Toc521673667)

[5. Registration operational controls 19](#_Toc521673668)

[5.1 Staff controls 19](#_Toc521673669)

[5.2 Logical and technological controls 19](#_Toc521673670)

[5.3 Physical controls 19](#_Toc521673671)

[5.4 Business continuity of the Relationship Organisation 19](#_Toc521673672)

[5.5 Relationship Organisation termination 19](#_Toc521673673)

[6. Other business and legal matters 20](#_Toc521673674)

[6.1 Other business 20](#_Toc521673675)

[6.2 Legal matters 20](#_Toc521673676)

[6.2.1 Termination 20](#_Toc521673677)

[6.2.2 Disclaimer regarding identity 20](#_Toc521673678)

[6.2.3 Disclaimers of warranties 21](#_Toc521673679)

[6.2.4 Commonwealth, agencies and Human Services liability 21](#_Toc521673680)

[6.2.5 Indemnities 21](#_Toc521673681)

[7. Certificate Profiles 22](#_Toc521673682)

[7.1 NASH Supporting Organisation Certificate – Certificate Profile 22](#_Toc521673683)

# Background

## Human Services Health Sector Public Key Infrastructure

The Australian Government Department of Human Services (Human Services) owns and operates the Health Sector Public Key Infrastructure (Health Sector PKI) to facilitate the authentication of confidential communications for a number of online programs and in relation to accessing digital health infrastructure and services.

## National Authentication Service for Health (NASH)

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

* access to the Healthcare Identifiers Service (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 messaging using the Health Sector 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 issue of certificates to supporting organisations, and the use of those certificates by supporting 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 Sector PKI, and
* supporting organisations within the meaning of this CP.

The certificates issued under the Health Sector PKI for accessing the My Health Record system are Relationship Certificates, used to secure healthcare-related communications and for supporting organisations that support, or participate in, the My Health Record system and services. The Root Certification Authority (RCA) and Relationship Organisation (RO) is Human Services.

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).

## Overview of PKI documents

This CP should be read in conjunction with the:

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

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](http://www.humanservices.gov.au/pki)

## Requirement for prior registration in the HI Service

As part of Human Services Gatekeeper Accredited Relationship Organisation model for the Health Sector PKI, supporting organisations must register with the HI Service prior to, or as part of, applying for a certificate.

*Note: the Chief Executive Medicare is the service operator of the HI Service under the* Healthcare Identifiers Act 2010*. The HI Service is made up of a register of healthcare identifier numbers for individuals who receive healthcare, Individual Healthcare Providers and Healthcare Provider Organisations, as well as a Healthcare Provider Directory and access controls.*

*As an administrative extension to the HI Service, Human Services uses this service to register Supporting Organisations. Upon registration, Supporting Organisations are issued with a 16 digit registration number (that is not a Healthcare Identifier) by Human Services.*

*Supporting Organisations are issued with a 16 digit registration number under ISO/IEC 7812, commencing with the ‘800363’ Issuer Identification Number for Contracted Service Providers and the ‘800364’ Issuer Identification Number for General Supporting Organisations.*

## 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.

**Contracted service provider** means either or both of:

1. an entity that is a contracted service provider within the meaning of the *Healthcare Identifiers Act 2010*
2. a person registered as a contracted service provider under section 49 of *My Health Records Act 2012*.

**General supporting organisation** means any of the following:

1. a person that has applied to be registered as, or is registered as, a repository operator or a portal operator under sections 47 to 49 of the *My Health Records Act 2012*
2. the service operator under the *Healthcare Identifiers Act 2010*
3. the system operator under the *My Health Records Act 2012* and the operator of any component of the My Health Record system (as defined in that Act) that Human Services determines from time to time to be a general supporting organisation
4. the operator of the National Repositories Service under the *My Health Records Act 2012* and the operator of any component of that service that Human Services determines from time to time to be a general supporting organisation.

**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.

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

**NASH PKI** has the meaning provided in section 1.1.

**NASH PKI Certificate for Supporting Organisations** or **certificate** means a certificate issued under this CP to a supporting organisation described in this CP*.*

**Supporting organisation** means a contracted service provider or a general supporting organisation that is registered by the Department of Human Services in that capacity and has been issued with a 16 digit registration number in relation to that registration.

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* ([comlaw.gov.au](http://www.comlaw.gov.au))
2. Healthcare Identifiers Regulations 2010 and the My Health Records Regulations 2012 ([comlaw.gov.au](http://www.comlaw.gov.au))
3. the Healthcare Identifiers Service Glossary of Terms and Conditions ([nehta.gov.au/connecting-australia/healthcare-identifiers](http://www.nehta.gov.au/connecting-australia/healthcare-identifiers))
4. PKI Gatekeeper documents, including Human Services PKI glossary ([humanservices.gov.au/health-professionals/services/public-key-infrastructure/public-key-infrastructure-policy-documents](https://www.humanservices.gov.au/organisations/health-professionals/enablers/public-key-infrastructure-pki-policy-documents/31476))

## Certificate policy clauses

### CP Identification

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

**1.2.36.174030967.1.12.1.1**

# Introduction

This is the CP for certificates to be issued to supporting organisations as described in section 1.1.6 of this policy that want to use the certificate in accordance with the acceptable uses outlined in section 1.2 of this policy.

The certificates are provided on a CD or electronically to subscribers who are responsible for uploading the certificates onto the subscribers’ client operating system.

## PKI participants

### Certification Authority

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

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

### Relationship Organisation

Human Services is the Relationship Organisation (RO) for the Community of Interest (CoI) defined in this CP.

### Relationship Organisation Unit

There is a separately identified ROU within the Health Sector PKI for the CoI defined in this CP. The ROU at Human Services has responsibilities in the CoI in managing the subscribers in the CoI.

### Certificate controllers

Certificate controllers are RO staff with responsibilities for management of certificates (see the OCA CPS for further details).

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

### Relationship Organisation Unit operators

Relationship Organisation Unit operators (ROUOs) are Human Services staff within the ROU.

ROUOs within the ROU are not certificate controllers. ROUOs operate in accordance with the processes and procedures set out in the OCA CPS and this CP.

### Subscribers

Supporting organisations are permitted subscribers under this CP.

A certificate does not verify or represent that the subscriber is a particular organisation or a particular individual. The meaning of a 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 supporting organisation) is recorded as being registered with the HI Service at the time of certificate issuance and recorded as having a particular registration number. The process used to identify and authenticate subscribers only verifies that the subscriber is recorded as having been assigned a HPI-O by the HI Service operator and does not include any independent verification.

A certificate does not verify or represent that the subscriber is registered with the My Health Record system under the *My Health Records Act 2012.* This registration is a separate process that may only be taken by those supporting organisations that are eligible for that registration.

The NASH PKI protects the confidentiality of the electronic communication, and lets the recipient of the communication know that the communication content has not been changed in transit between the sender and the recipient. A certificate does not make any other assertions about the content of an electronic communication (including any Clinical content) either prior to the communication being sent by the subscriber or after the communication is received by the relying party.

### Relying party

The following are relying parties:

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

Relying parties must not use a certificate by itself, and must use means other than reliance on 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 Party Agreement under this CP that is available at [humanservices.gov.au/pki](http://www.humanservices.gov.au/pki)

Where you rely on a certificate issued under this CP and you do not have written agreement with Human Services or authorisation or approval through a notice published at [humanservices.gov.au/pki](file:///C:\Users\p00240\AppData\Local\Microsoft\Windows\Temporary%20Internet%20Files\Content.Outlook\0D9H5AAX\www.humanservices.gov.au\pki) (specifying an allowable usage), then you rely on the certificate at your own risk.

## Certificate use

### Allowable certificate uses

Key pairs (that is, a private key and a public key) and certificates issued under this CP must only be used to authenticate the supporting organisation and protect the confidentiality and integrity of electronic communications with relying parties that are recognised under this CP in accordance with section 1.1.7.

### Prohibited certificate uses

A NASH PKI Certificate for Supporting Organisations is only permitted to be used for the purposes outlined in section 1.2.1 above.

Parties using a NASH PKI Certificate for Supporting Organisations for any other purpose, do so at their own risk.

## Definitions and acronyms

Definitions and acronyms are in the:

* [Department of Human Services Public Key Infrastructure (PKI) glossary](file:///C:\Users\RWL785\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\UC0DY357\humanservices.gov.au\health-professionals\services\public-key-infrastructure\public-key-infrastructure-policy-documents)
* *Healthcare Identifiers Act 2010*
* Healthcare Identifiers Regulations 2010
* Healthcare Identifiers Glossary
* *My Health Records Act 2012.*

# Identification and authentication of users

## Naming of subscribers

Subscribers (termed ‘Certificate Subjects’ in the x.509 definition) under this CP will be named according to Human Services' application and registration processes for supporting organisations in the CoI described in this CP.

## Identification and authentication of the subscriber at registration

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

For the purpose of issuing certificates to supporting organisations under this CP, the RO relies on the verification processes undertaken by the HI Service which in turn relies on the record of information the HI Service maintains*.*

The RO does not undertake any separate action to verify or confirm the information provided by a supporting organisation in its application for a NASH PKI Certificate for Supporting Organisations, or by the HI Service.

Human Services may, in accordance with trusted practices, but will not be limited to:

1. receive an application for a NASH PKI Certificate for Supporting Organisations from supporting organisations, and
2. request information from the HI Service that verifies that a supporting organisation is registered with the HI Service.

## Identification and authentication of the subscriber at renewal

Subscribers (supporting organisations) under this CP may have their certificate issued under this CP renewed if the RO is satisfied that the subscriber’s status within the HI Service remains active.

## Identification and authentication of revocation request

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

* ROUOs in the event that the subscriber becomes ineligible to remain as a supporting organisation for the purpose of the CoI described in this CP
* the subscriber, or
* Certificate Controllers.

# Certificate life-cycle operational requirements

## Certificate creation

### Enrolment process and responsibilities

Human Services may consider that the supporting organisation be enrolled for a NASH PKI Certificate for Supporting Organisations by certificate controllers on the basis of:

a) receipt of an application for a NASH PKI Certificate for Supporting Organisations together with any documentation required as part of the Health Sector PKI requirements

b) consent by the supporting organisation applicant to the collection, disclosure and use of information between:

* itself (including its authorised officers) and Human Services,
* between the Chief Executive Medicare, Human Services and the Chief Executive Medicare as the service operator established under the

*Healthcare Identifiers Act 2010*, and

c) verification from the HI Service that a supporting organisation is registered with the HI Service.

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

### Publication of the certificate

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.

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

## Key pair and certificate usage

### Key pair generation and installation

All subscriber key pairs (that is, a private key and a public key) and certificates issued under this CP shall be generated by a certificate controller using accredited software.

The signing and encryption key will be stored in a password protected PKCS#12 file. These PKCS#12 files are securely distributed to the subscriber as instructed by the ROUO.

A personal identification code (PIC) to access the keys and certificates will also be generated and despatched separately.

## Certificate renewal

Certificates issued under this CP may be renewed automatically by the certificate controllers. This is at the discretion of Human Services. Refer to clause 2.3 for details of identification and authentication.

## Certificate revocation

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

a) after loss, destruction or theft of the certificate

b) in the event of a supporting organisation’s insolvency or if it becomes subject to any form of external administration

c) in the event that the supporting organisation breaches a term of this CP, the Terms and Conditions or the Relying Party Agreement, or

d) in the event that Human Services cancels the registration (however described) of the supporting organisation in the HI Service.

## Certificate status services

### Operational characteristics

Refer to Section 4.10.1 of the RCA CP.

### Service availability

Service availability for the Certificate Revocation List (CRL) is 24 hours per day, 7 days per week (except for designated system maintenance periods) at certificates-australia.com.au

### Optional features

Not applicable.

# Registration operational controls

## Staff controls

All certificate controllers under this CP will be authorised representatives of Human Services.

## Logical and technological controls

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

## Physical controls

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

## Business continuity of the Relationship Organisation

Human Services (the RO under this CP) is a department of state of the Commonwealth of Australia and forms part of the Commonwealth.

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

## Relationship Organisation termination

Changes in legislation or government policy will provide for termination of Human Services as the RO under this CP and for a replacement agency as the successor RO in accordance with policy as determined by the government, if required.

# Other business and legal matters

## Other business

For information on other business (for example fees, confidentiality, privacy, intellectual property, representations and warranties and disclaimers of warranties), refer to section 9 and subsections 9.1 - 9.7 of the RCA CP at [humanservices.gov.au/pki](http://www.humanservices.gov.au/health-professionals/services/public-key-infrastructure/public-key-infrastructure-policy-documents?utm_id=9)

## Legal matters

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

The following provisions apply in addition and without prejudice to those set out in section 9 (Other Business and Legal Matters) of the RCA CP.

### Termination

In addition and without prejudice to any other right to revoke a certificate, Human Services may revoke a certificate issued under this CP at any time to facilitate a transition to another NASH PKI and RO, if any.

### Disclaimer regarding identity

A certificate does not verify or represent that the supporting organisation subscriber is a particular organisation or a particular individual.

The meaning of a 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 is recorded as being registered with the HI Service. A certificate does not represent or verify that:

* the subscriber has a particular identity (i.e. is a particular organisation or individual)
* the subscriber or any of its staff have particular qualifications or registrations other than with the HI Service, or
* the subscriber is registered with the My Health Record system.

### Disclaimers of warranties

In addition and without prejudice to the disclaimers under section 9.7 of the RCA CP that apply to the Commonwealth and its agencies, the Chief Executive Medicare as the service operator under the *Healthcare Identifiers Act 2010* and Human Services disclaim all warranties, express or implied.

In addition and without prejudice to the limitation under section 9.7 of the RCA CP that applies to the Commonwealth and its agencies, if any warranties or conditions are implied by legislation, then the liability of the Chief Executive Medicare as the service operator under the *Healthcare Identifiers Act 2010* and Human Services (and of their contractors (including sub-contractors)), for any breach of the condition or warranty is limited to:

1. re-performing the services to which the warranty applied, or
2. paying the cost of re-performing those services.

### Commonwealth, agencies and Human Services liability

In addition and without prejudice to the limitation of liability under section 9.8 of the RCA CP that applies to the Commonwealth and its agencies, the aggregate liability of the Chief Executive Medicare as the service operator under the *Healthcare Identifiers Act 2010* and Human Services to any and all persons concerning all certificates will be limited to an amount not to exceed $50,000 in aggregate for all claims, arising in connection with the Health Sector PKI, including but not limited to:

1. an entity described in this CP carrying out, or omitting to carry out, any activity described in, or contemplated by, the documents, and
2. the carrying out or omitting to carry out, any activity related to the Gatekeeper accreditation process (see [finance.gov.au/agict](http://finance.gov.au/agict)).

### Indemnities

No indemnity (contractual or otherwise) arises between Human Services, the Chief Executive Medicare, subscribers and relying parties under the Health Sector PKI to which this CP applies*.*

# Certificate Profiles

## NASH Supporting Organisation Certificate – Certificate Profile

| **Field** | **Content** | **Mandatory** | **Critical\*** |
| --- | --- | --- | --- |
| 1.        X.509v1 Field |  |  | N/A |
| 1.1.      Version | V3 | M |
| 1.2.      Serial Number | A positive integer that uniquely identifies the Certificate. | M |
| 1.3.      Signature Algorithm | SHA-1 RSA,  SHA-1 hashing algorithm using the RSA signing algorithm. | M |
| 1.4.      Issuer Distinguished Name |  | M |
| 1.4.1.           Country (C) | AU | M |
| 1.4.2.           Organization (O) | GOV | M |
| 1.4.3. Organization Unit (OU) | Medicare Australia | M |
| 1.4.3           Common Name (CN) | Medicare Australia Organisation Certification Authority | M |
| 1.5.      Validity |  |  |
| 1.5.1.           Not Before | The date that the Certificate is valid from (system time at certificate issuance).  YYMMDDHHMMSSZ encoded as UTCTime for dates up to 2049 and encoded as GeneralizedTime for dates in 2050 or later. | M |
| 1.5.2.           Not After | The date that the Certificate is valid until. 2 years from Start Validity, i.e. certificate issuance.  YYMMDDHHMMSSZ encoded as UTCTime for dates up to 2049 and encoded as GeneralizedTime for dates in 2050 or later | M |
| 1.6.      Subject |  |  |
| 1.6.1. Domain Component (dc) | au | M |
| 1.6.2. Domain Component (dc) | net | M |
| 1.6.3. Domain Component (dc) | electronichealth | M |
| 1.6.4. Domain Component (dc) | id | M |
| 1.6.5. Domain Component (dc) | <Identifier of Supporting Organisation> | M |
| 1.6.6. Organisation (o) | <Organisation Name> | M |
| 1.6.7 Organisation Unit (ou) | <Organisation Unit Name> | M |
| 1.6.8. Common Name (cn) | <usage>.< Identifier of Supporting Organisation>.id.electronichealth.net.au | M |
| 1.7.      Subject Public Key Info | RSA Public Key of 2048 bits. | M |
| 2.        X.509v3 Extensions |  |  |  |
| 2.1.      Authority Key Identifier |  | M | Non-Critical |
| 2.1.1.           Key Identifier | SHA-1 hash (60 bits) of the Issuer's public key. |
| 2.1.2.           AuthorityCertIssuer | Human Services Root Certification Authority |
| 2.1.3.           AuthorityCertSerialNumber | A positive integer that uniquely identifies the Certificate. |
| 2.2.      Subject Key Identifier | SHA-1 hash (60 bits) of the Subject's public key. | M | Non-Critical |
| 2.3.      Key Usage |  | M | Critical |
| 2.3.1.           Digital Signature | SET |
| 2.3.2.           Non Repudiation | NOT SET |
| 2.3.3.           Key Encipherment | SET |
| 2.3.4.           Data Encipherment | SET |
| 2.3.5.           Key Agreement | NOT SET |
| 2.3.6.           Key Certificate Signature | Not Selected |
| 2.3.7.           CRL Signature | Not Selected |
| 2.4.      Extended Key Usage |  | M | Non-Critical |
| 2.4.1.            id-kp-clientAuth | Set |
| 2.5.      Certificate Policies |  |  | Non-Critical |
| 2.5.1.           Policy Identifier | 1.2.36.174030967.1.12.1.1 |  |
| 2.5.1.1.                 Policy Qualifier ID | User Notice |  |
| 2.5.1.2.                  User Notice | Certificates issued under this CP must only be relied on by entities within the Community of Interest, unless otherwise agreed, and not for purposes other than those permitted by this CP. |  |
| 2.5.1.3.                 Policy Qualifier ID | CPS URI |  |
| 2.5.1.4.                  CPS URI | humanservices.gov.au/ |  |
| 2.6.      Subject Alternate Names | Not present |  | Non-Critical |
| 2.6.1.           rfc822Name | Not present |  |
| 2.6.2. Uniform Resource Identifier | Not present |  |
| 2.7.      Basic Constraints |  |  |  |
| 2.7.1.           Subject Type | Not CA |  | Critical |
| 2.7.2.           Path Length Constraint | Not present |  |
| 2.8.      Authority Information Access |  |  |  |
| 2.8.1.           Access Description | Not present |  |  |
| 2.8.1.1.                  Access Method | On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) |  | Non-Critical |
| 2.8.1.2.                  Alternative Name | URL=http://ocsp.certificates-australia.com.au/maoca.pkx |  |
| 2.9 CRL Distribution Point |  |  |  |
| 2.9.1 URL | http://www.certificates-  australia.com.au/general/cert\_search\_health.shtml |  | Non-Critical |
| 3.0 Other Fields - Generic |  |  |  |
| 3.0.1 Generic IA5 String:  RA Number (OID=1.2.36.73665175.1.10009) | < RA Number > | M |  |