**Short Form Certificate Policy**

****

**Australian Government Department of Human Services Community of Interest Certificate Policy for the National Authentication Service for Health PKI Certificate for Individual Healthcare Providers v 2.2**

**(2 year duration)**

**January 2016**



**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 licence 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:///\\internal\Users\QLD\BRIS-140-Elizabeth\UFGBW\Desktop\Cert%20Policies\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.](http://www.dpmc.gov.au/pmc/about-pmc/core-priorities/guidelines-and-procedures-other-agencies)

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

National Manager

eClaiming Branch

Health eBusiness 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 | 14 June 2012 |  |
| 1.0 | Initial version | 28 June 2012 | Correction made to Certificate Profiles |
| 1.1 | Revised version | 05 April 2013 | Amendments to recognise use of Certificates in accessing the  NASH Directory |
| 1.2 | Revised version | 8 August 2013 | Amended to extend certificate duration and align to style and formatting of other NASH CPs |
| 2.0 | Endorsed version | 30 August 2013 | PKI Committee Endorsement |
| 2.1 | Revised version | November 2014 | Minor amendment to include automatic renewal of certificates. Updates to disclaimers regarding identity |
| 2.2 | Revised version | January 2016 | My Health Record system updates |

General Manager

Health Programs Division

Department of Human Services

Date:

**Background**

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
* enable access to eHealth infrastructure and services.

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 My Health Record system as set out in the *My Health Records Act 2012* (My Health Records Act)
* secure communications 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 individual healthcare providers, and the use of those certificates by individual healthcare providers.

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* (HI Act) and who have been issued with certificates under other certificates 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 assist 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.1

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 (OCACPS)
* National Authentication Service for Health Public Key Infrastructure Certificate for Individual Healthcare Providers Terms and Conditions of Use agreement.

In using and relying upon certificates, Subscribers are legally bound by this CP and the terms and conditions. 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, individual healthcare providers must register with the HI Service prior to, or as part of, applying for a certificate.

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

* the Department of Human Services
* the Healthcare Identifiers service operator under the HI Act
* the System Operator of the My Health Record system under the My Health Records Act, and
* the End Entity-Subscribers.

This is the CP for individual Certificates to be issued to individual healthcare providers to whom HPI-Is have been assigned under the *Healthcare Identifiers Act 2010* (Department of Human Services Individual PKI Certificate).The Department of Human Services Individual PKI Certificate enables the Individual Healthcare Providers to conduct secure transactions with the System Operator of the My Health Record system, established by the My Health Records Act.

**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.

**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 the background above.

**NASH PKI Certificate for individual healthcare providers** or **Certificate** means a certificate issued under this CP to an individual healthcare provider as described in this CP*.*

**Individual healthcare provider** means an individual to whom a HPI-I has been assigned under the

*Healthcare Identifiers Act 2010.*

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. *Health Practitioner Regulations National Law Act 2009 / 2010* (known as National Law) of each state and territory and related Commonwealth Acts and Regulations [(ahpra.gov.au](file:///C:\Users\p00240\AppData\Local\Microsoft\Windows\Temporary%20Internet%20Files\Content.Outlook\0D9H5AAX\(ahpra.gov.au)).

4. National Partnership Agreement 2009 (the COAG agreement) ([coag.gov.au](http://www.coag.gov.au)).

6. 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).

**Certificate Policy Clauses**

**CP Identification**

Certificates issued under this CP shall bear the Policy OID:

**1.2.36.174030967.1.11.1.1**

1. **Introduction**

This is the CP for certificates to be issued to individual healthcare providers (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 below.

The certificates are provided to Subscribers on a smart card or USB.

The Relationship Organisation Unit (ROU) is the program area in Human Services responsible for undertaking the Application registration.

The Relationship Organisation Unit Operators (ROUOs) are Human Services staff working in the

ROU.

* + 1. **PKI participants**
    2. **Certification authority**

All certificates issued under this CP shall be produced by the Department of 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)

* + 1. **Relationship Organisation**

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

* + 1. **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.

* + 1. **Certificate Controllers**

Certificate Controllers are ROU 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.

* + 1. **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.

**1.1.7 Subscribers**

Subscribers under this CP are individual healthcare providers to which a HPI-I has been assigned under the *Healthcare Identifiers Act 2010*.

A certificate does not verify or represent that the subscriber is 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 individual healthcare provider) is recorded as being registered with the HI Service at the time of certificate issuance and recorded as having a particular HPI-I.

A certificate does not verify or represent that:

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

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.

**1.1.8 Relying Party**

There is one Relying Party under this CP. The Relying Party is the System Operator of the My Health

Record system (see section 14 of the My Health Records Act).

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.

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](http://www.humanservices.gov.au/pki) (specifying an allowable usage), then you rely on the certificate at your own risk.

* 1. **Certificate Use**
     1. **Allowable Certificate Use**

Key Pairs (that is, a Private Key and a Public Key) and certificates issued under this CP are only to be used by individual healthcare providers for accessing digital health records in the My Health Record system as authorised by the My Health Record System Operator.

**1.2.2 Prohibited Certificate Uses**

A NASH PKI Certificate for individual healthcare providers is only permitted to be used for the purposes outlined in section 1.2.1 above.

Parties using a NASH PKI Certificate for individual healthcare providers for any other purpose, do so at their own risk.

**1.3 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
* *My Health Records Act 2012*

**2. Identification and Authentication of Users**

**2.1 Naming of Subscribers**

Subscribers (termed ‘Certificate Subjects’ in the x.509 definition) under this CP shall be named according to Human Services application and registration processes for individual healthcare providers in the CoI described in this CP.

**2.2 Identification and authentication of the Subscriber at registration**

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

For the purpose of issuing certificates to individual healthcare providers under this CP, the RO relies on the verification process provided 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 an individual healthcare provider in its application for a certificate 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 Individual Healthcare Providers for

individual healthcare providers, and

1. request information from the HI Service that verifies that an individual healthcare provider is registered with the HI Service.

**2.3 Identification and authentication of the Subscriber at renewal**

Subscribers (individual healthcare providers) under this CP may have their certificate issued under this CP renewed provided the RO is satisfied that the Subscriber’s status within the Healthcare Identifiers Service remains active.

**2.4 Identification and authentication of revocation request**

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

1. ROUOs in the event that the Subscriber becomes ineligible to remain as an Individual Healthcare Provider for the purpose of the CoI described in this CP
2. the Subscriber, or
3. Certificate Controllers.

**3. Certificate Life Cycle Operational Requirements**

**3.1 Certificate creation**

**3.1.1 Enrolment process and responsibilities**

Human Services may consider that the individual healthcare provider be enrolled for a certificate by

Certificate Controllers on the basis of:

1. receipt of an application for a NASH PKI Certificate for individual healthcare providers together with any documentations required as part of the Health Sector PKI requirements,
2. consent by the applicant to collect, disclose and use information with, from and to the service operator established under the *Healthcare Identifiers Act 2010*, and
3. verification from the HI Service that a HPI-I has been assigned to a person matching the details in the application.

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

**3.1.2 Publication of the Certificate**

The NASH Directory contains certificates issued under NASH CPs for healthcare provider organisations and supporting organisations. The directory is accessible by Subscribers under this CP. Certificates issued under this CP will not be published in the NASH directory or any other public directory unless at a later date that Human Services and the applicable End Entity-Subscriber agree to do so. 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. The HPI-I will not appear in the Certificate Revocation List.

**3.2 Key pair and Certificate Usage**

**3.2.1 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 Certificate Controllers using accredited software.

The content commitment Key and utility Key shall be stored and dispatched on a smart card.

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

**3.3 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.

**3.4 Certificate revocation**

Certificates issued under this CP may be revoked by Human Services in its absolute discretion, including but not limited to, one or more of the following:

1. in the event that a revocation is requested by the Subscriber
2. in the event that Human Services is notified of an actual or suspected loss, destruction, theft or compromise of the certificate
3. in the event that the individual healthcare provider breaches a term of this CP, the terms and conditions or the Relying Party Agreement.

Revocation must be requested in line with section 2.4.

**3.5 Certificate status services**

**3.5.1 Operational characteristics**

Refer to Section 4.10.1 of the RCA CP.

**3.5.2 Service availability**

Service availability for the Certificate Revocation List (CRL) is substantially 24 hours a day, seven days a week at [certificates-australia.com.au](http://www.certificates-australia.com.au/)

**3.5.3 Optional features**

Not applicable.

**4. Registration Operational Controls**

**4.1 Staff controls**

All Certificate Controllers under this CP shall be authorised representatives of Human Services.

**4.2 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.

**4.3 Physical controls**

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

**4.4 Business continuity of the Relationship Organisation**

Human Services (the Relationship Organisation 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 the RO in accordance with policy as determined by the government and implemented in accordance with Commonwealth machinery of government (MOG) requirements.

**4.5 Relationship Organisation termination**

Changes in Commonwealth legislation or policy may 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.

**4.6 My Health Record System Operator termination**

The identity of the System Operator of the My Health Record system is set out under section 14 of the My Health Records Act. A change of the identity of the System Operator can only be through amendment to the My Health Records Act or by other Acts of the Commonwealth Parliament made pursuant to changes in government policy.

**5. Other Business and Legal Matters**

**5.1 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)

**5.2 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.

**5.2.1 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.

**5.2.2 Disclaimer regarding identity**

A certificate does not verify or represent that the Subscriber is 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 individual healthcare provider) is recorded as being registered with the HI Service. A certificate does not mean that the individual healthcare provider is registered with the My Health Record system (see 1.1.6). The process used to identify and authenticate Subscribers only verifies that the Subscriber is recorded as having assigned a HPI-I by the healthcare Identifiers service operator and does not include any independent verification.

**5.2.3 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.

**5.2.4 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 shall be limited to an amount not to exceed $50,000 in aggregate for all claims, arising in connection with the Health Sector PKI.

This includes 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 PKI Documents, and
2. the carrying out or omitting to carry out, any activity related to the Gatekeeper accreditation process (see [www.finance.gov.au/agict/](http://www.finance.gov.au/agict/)).

**5.2.5 Indemnities**

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

**5.2.6 Legislation**

Section 26 of the *Healthcare Identifiers Act 2010* prohibits a person from disclosing a healthcare identifier except in specified circumstances, including where the person is authorised to disclose a healthcare identifier under that Act.

Section 24A of the *Healthcare Identifiers Act 2010* allows an entity to collect, use or disclose a healthcare provider's healthcare identifier for a purpose relating to the provision of healthcare if the healthcare provider has consented to such collection, use or disclosure.

Human Services is collecting the Individual Healthcare Provider's HPI-I to enable authentication through the Health Sector PKI of relationships in electronic transmissions (in the manner and to the extent described in this CP). This underpins the creation of a secure digital health record, which is a purpose relating to the provision of healthcare.

**6. Certificate Profiles**

**6.1 NASH Individual Healthcare Provider Certificate – Utility 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) | Human Services | M |
| 1.4.3 Common Name (CN) | Human Servcies 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) | <Healthcare Identifier of Individual> | M |
| 1.6.6. Common Name (cn) | <First Name> <Last Name> | 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 | Not present |
| 2.1.3. AuthorityCertSerialNumber | Not present |
| 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 | Not applicable |  | Non-  Critical  Non- Critical |
|  |  |  |
| 2.5. Certificate Policies |  |  |
| 2.5.1. Policy Identifier | 1.2.36.174030967.1.11.1.1 |  |
| 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 |  |

PKI Certificate for Individual Healthcare Providers v2.2

**Field Content Mandatory Critical\***

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/](file:///C:\Users\p00240\AppData\Local\Microsoft\Windows\Temporary%20Internet%20Files\Content.Outlook\0D9H5AAX\humanservices.gov.au\)

2.6. Subject Alternate Names Not present Non-

2.6.1. rfc822Name Not present

2.7. Basic Constraints

Critical

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-

2.8.1.2. Alternative Name URL[=h](http://ocsp.certificates-/)t[tp://ocsp.certificates-](http://ocsp.certificates-/) australia.com.au/maoca.pkx

Critical

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=1.2.36.73665175.1.1000

9)

< RA Number > M

**6.2 NASH Individual Healthcare Provider Certificate – Content**

**Commitment 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) | Human Services | M |  |
|  | 1.4.3 Common Name (CN) | Human Services 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) | <Healthcare Identifier of Individual> | M |  |
|  | 1.6.6. Common Name (cn) | <First Name> <Last Name> | M |  |
| 1.7. Subject Public Key Info | | RSA Public Key of 2048 bits. | M |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Field** | **Content** | **Mandatory** | **Critical\*** |
|  |  |  |  |
| 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 | Not present |
| 2.1.3.  AuthorityCertSerialNumber | Not present |
| 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 | SET |
| 2.3.3. Key Encipherment | NOT SET |
| 2.3.4. Data Encipherment | NOT 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 | Not applicable |  | Non-  Critical  Non- Critical |
|  |  |  |
| 2.5. Certificate Policies |  |  |
| 2.5.1. Policy Identifier | 1.2.36.174030967.1.11.1.1 |  |
| 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/](file:///C:\Users\p00240\AppData\Local\Microsoft\Windows\Temporary%20Internet%20Files\Content.Outlook\0D9H5AAX\humanservices.gov.au\) |  |
| 2.6. Subject Alternate Names | Not present |  | Non-  Critical |
| 2.6.1. rfc822Name | 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[=h](http://ocsp.certificates-/)t[tp://ocsp.certificates-](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 |  |