****

Australian Government Department of Human Services Community of Interest Certificate Policy for Site Certificates for website transactions

2 year duration

December 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 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** |
| 1.0 | Final | 5 December 2016 | Initial version reflecting changes in the Gatekeeper PKI Framework version 3.1 |

Contents

[1 Introduction 6](#_Toc468803293)

[1.1 Background 6](#_Toc468803294)

[1.2 Document name and identification 6](#_Toc468803295)

[1.3 PKI participants 6](#_Toc468803296)

[1.4 Certificate usage 8](#_Toc468803297)

[1.5 Policy administration 9](#_Toc468803298)

[1.6 Definitions and acronyms 9](#_Toc468803299)

[2 Publication and repository responsibilities 10](#_Toc468803300)

[3 Identification and authentication 10](#_Toc468803301)

[3.1 Naming 10](#_Toc468803302)

[3.2 Initial identity validation 11](#_Toc468803303)

[3.3 Identification and authentication for re-key requests 12](#_Toc468803304)

[3.4 Identification and authentication for revocation request 12](#_Toc468803305)

[4 Certificate life-cycle operational requirements 13](#_Toc468803306)

[4.1 Certificate application 13](#_Toc468803307)

[4.2 Certificate application processing 13](#_Toc468803308)

[4.3 Certificate issuance 14](#_Toc468803309)

[4.4 Certificate acceptance 14](#_Toc468803310)

[4.5 Key pair and certificate usage 14](#_Toc468803311)

[4.6 Certificate renewal 15](#_Toc468803312)

[4.7 Certificate re-key 16](#_Toc468803313)

[4.8 Certificate modification 16](#_Toc468803314)

[4.9 Certificate revocation and suspension 17](#_Toc468803315)

[4.10 Certificate status services 18](#_Toc468803316)

[4.11 End of subscription 19](#_Toc468803317)

[4.12 Key escrow and recovery 19](#_Toc468803318)

[5 Facility, Management and Operational Controls 20](#_Toc468803319)

[5.1 Physical controls 20](#_Toc468803320)

[5.2 Procedural controls 20](#_Toc468803321)

[5.3 Personnel controls 20](#_Toc468803322)

[5.4 Audit logging procedures 20](#_Toc468803323)

[5.5 Records archival 20](#_Toc468803324)

[5.6 Key changeover 20](#_Toc468803325)

[5.7 Compromise and disaster recovery 20](#_Toc468803326)

[5.8 CA or RA termination 21](#_Toc468803327)

[6 Technical Security Controls 22](#_Toc468803328)

[6.1 Key pair generation and installation 22](#_Toc468803329)

[6.2 Private Key Protection and Cryptographic Module Engineering Controls 23](#_Toc468803330)

[6.3 Other aspects of key pair management 24](#_Toc468803331)

[6.4 Activation data 24](#_Toc468803332)

[6.5 Computer security controls 24](#_Toc468803333)

[6.6 Life cycle technical controls 24](#_Toc468803334)

[6.7 Network security controls 24](#_Toc468803335)

[6.8 Time-stamping 24](#_Toc468803336)

[7 Certificate, CRL and OCSP Profiles 25](#_Toc468803337)

[7.1 Certificate profiles 25](#_Toc468803338)

[7.2 CRL profile 32](#_Toc468803339)

[7.3 OCSP profile 32](#_Toc468803340)

[8 Compliance audit and other assessments 33](#_Toc468803341)

[8.1 Frequency or circumstances of assessments 33](#_Toc468803342)

[8.2 Identity/qualifications of assessor 33](#_Toc468803343)

[8.3 Assessor’s relationship to assessed entity 33](#_Toc468803344)

[8.4 Topics covered by assessment 33](#_Toc468803345)

[8.5 Actions taken as a result of deficiency 33](#_Toc468803346)

[8.6 Communication of results 33](#_Toc468803347)

[9 OTHER BUSINESS AND LEGAL MATTERS 34](#_Toc468803348)

[9.1 Fees 34](#_Toc468803349)

[9.2 Financial responsibility 34](#_Toc468803350)

[9.3 Confidentiality of business information 34](#_Toc468803351)

[9.4 Privacy of personal information 34](#_Toc468803352)

[9.5 Intellectual property rights 34](#_Toc468803353)

[9.6 Representations and warranties 34](#_Toc468803354)

[9.7 Disclaimers of warranties 34](#_Toc468803355)

[9.8 Limitations of liability 34](#_Toc468803356)

[9.9 Indemnities 35](#_Toc468803357)

[9.10 Term and termination 35](#_Toc468803358)

[9.11 Individual notices and communications with participants 35](#_Toc468803359)

[9.12 Amendments 35](#_Toc468803360)

[9.13 Dispute resolution provisions 35](#_Toc468803361)

[9.14 Governing law 35](#_Toc468803362)

[9.15 Compliance with applicable law 36](#_Toc468803363)

[9.16 Miscellaneous provisions 36](#_Toc468803364)

# Introduction

## Background

This is the Certificate Policy (CP) for site certificates provided by Human Services as the Registration Authority (Human Services RA) to practices and entities (however described and defined) who wish to undertake secure electronic transmissions at sites:

* with Human Services
* to access data held by Human Services
* with Human Services as service operator of the Healthcare Identifiers (HI) Service
* with relying parties within the Human Services Communities of Interest (CoIs), and/or
* within this site certificate CP CoI.

Such sites are known as Human Services RO sites and are subscribers for the purposes of this CP.

## Document name and identification

### CP Identification

Certificates issued under this CP shall bear the Policy OID:

**1.2.36.174030967.1.16.1.1**

### Overview of PKI Documents

This CP should be read in conjunction with the:

* 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), and
* Department of Human Services Root Certification Authority Certification Practice Statement (Human Services RCA CPS).

## 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)](http://www.medicareaustralia.gov.au)

### 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 issue to the subscriber for the defined Communities of Interest.

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 in managing the subscribers in that CoI.

#### Registration Organisation Unit Operators

The Relationship Organisation Unit Operators (ROUOs) are:

* Human Services staff who in the ROU,
* Human Services staff who accept and manage the registration of practices or other entities for site certificates, or
* Human Services staff acting in Human Services role as service operator of the HI Service who accept and manage registration of healthcare provider organisations or Contracted Service Providers for site certificates.

ROUOs within the Registered Human Services Site 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 include:

* practices registered with a Human Services programme and known to Human Services as such according to an application for participation in a Human Services programme
* an entity which is known to Human Services by application and/or registration and is therefore a member of a recognised Human Services Community of Interest, or
* an entity identified as a Contracted Service Provider (CSP) in accordance with the *Healthcare Identifiers Act 2010*.

#### Authoriser

An Authoriser is a member of a class of persons with a clear capacity to commit a practice or an entity, and to appoint a Certificate Manager. Persons who are members of this class may include but are not limited to a Chief Executive Officer, Company Director, Trustee, Sole Trader, Partner or Company Owner.

#### Certificate Manager

A Certificate Manager is an employee or representative of a practice or entity duly authorised by the Authoriser to perform the certificate management duties appropriate for the certificates being requested.

The Certificate Manager as described above and the person providing the Certificate Manager with the authority (the Authoriser) may be one and the same person.

### Relying parties

Relying parties under this CP are:

* Human Services, as receiver of transactions secured using the site keys and certificates,
* practices and entities known to Human Services and who are in a recognised Human Services CoI, being the other practice or entity in the CoI who conducts and receives transactions secured using the site keys and certificates, and
* individuals who are recognised Human Services RA individuals and who receive and conduct transactions secured using the site keys and certificates in conjunction with their individual keys and certificates.

Parties who rely on certificates issued under this CP and who:

* do not have a written agreement with Human Services or authorisation through a notice published at [humanservices.gov.au/pki](https://www.humanservices.gov.au/health-professionals/enablers/public-key-infrastructure-pki-policy-documents) (specifying authorised usage relating to a transaction type), and
* undertake transactions that are not authorised or approved by Human Services as the RA or, where relevant, by the *Healthcare Identifiers Act 2010* and the Healthcare Identifiers Regulations 2010

rely on such certificates at their own risk.

### Other participants

There are no other participants.

## Certificate usage

### Appropriate certificate use

Key pairs and certificates issued under this CP are to be used by sites conducting transactions with Human Services for programmes and services authorised or approved by Human Services and, where relevant, the *Healthcare Identifiers Act 2010* and Healthcare Identifier Regulations 2010.

### Prohibited certificate uses

There are no prohibited certificate uses.

Use of certificates outside of the Human Services CoIs is not supported.

Parties using site certificates for any transaction other than an authorised or approved transaction by Human Services or an approved transaction between parties so authorised under the *Healthcare Identifiers Act 2010*, 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

**Site Certificate** means a Certificate issued under this CP.

**Site** means:

a) the physical location of any practice registered by Human Services as a Human Services programme or service as eligible for Human Services Site Certificates under this CP. The practice may be referred to as a Registered Medicare Practice or healthcare practice and includes Pharmacies\* and aged care providers, or

b) any site of an entity, where that entity:

* is recognised by Human Services as being a member of a Human Services recognised Community of Interest. For example, that entity is a seed organisation or a Contracted Service Provider (CSP) and recognised as such under the *Healthcare Identifiers Act 2010*; and
* is known to Human Services and Human Services is the Registration Authority.

The commonly used term ‘Location Certificate’ has the same meaning as Site Certificate.

\*Pharmacies who participate in online claiming for PBS will normally be issued with a site certificate under the *Site Certificate for Pharmacy and PBS Community of Interest Certificate Policy* or . *Australian Government Department of Human Services Community of Interest Certificate Policy for Pharmacy and PBS Site Certificates for website transactions*

### References

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*
2. Healthcare Identifiers Regulations 2010
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. the Healthcare Identifiers Glossary
6. [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 Healthcare Public Directory.

The Healthcare Public Directory provides information about Active and Revoked Certificates.

The Healthcare Public Directory is accessible from [www.certificates-australia.com.au](http://www.certificates-australia.com.au/). Technical details are at [www.humanservices.gov.au](http://www.humanservices.gov.au).

The Healthcare Public Directory is substantially available 7 days a week, 24 hours

For further 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.

RFC 822 name is supported under ‘Subject Alternative Name’ by this CP.

### Need for names to be meaningful

Subscribers under this CP will be named according to Human Services’ application and registration processes for practices or entities.

This may include the name by which Human Services has recognised the entity as a member of a CoI or the name under which the entity is registered as a subscriber.

### Anonymity or pseudonymity of subscribers

Anonymity and pseudonymity is not supported by this CP.

### Rules for interpreting various name forms

The Healthcare Public Directory supports the use of X.500 and RFC 822 names.

### Uniqueness of names

The uniqueness of their names shall be assured according to Human Services’ application and registration processes for practices or entities.

### Recognition, authentication, and the 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 keys and certificates are provided to subscribers in an encrypted format in accordance to the Public Key Cryptographic Standard #12.

### Authentication of organisation identity

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

This process may include, but is not limited to:

* Trusted practices in Human Services ROUs responsible for registering practices for Human Services programmes and services,
* Organisation identity proofing requirements under Gatekeeper PKI Framework, and/or
* Trusted practices in the entity’s ROU responsible for registering that entity for a site certificate in each CoI.

### 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.

This process may include, but is 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)
* processing in association with the Department of Health (where required)
* allocation of number(s) (where required) and registration on Human Services systems (however described).

### Non-verified subscriber information

RFC 822 name under ‘Subject Alternative Name’ is not verified.

### Validation of authority

The capacity of the Authoriser to commit the practice or entity and to appoint a Certificate Manager is validated as part of the certificate application.

Where a practice or entity wishes to access Human Services programmes using its certificate, Human Services reserves the right to require that the practice or entity enters into terms and conditions for participation in that programme.

Any such programme’s terms and conditions are separate from the *Site Certificate Terms and Conditions of Use*.

### Criteria for interoperation

Previous registration by the Medicare Australia 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 the certificate renewed provided that:

* the site is a registered Human Services practice and its registration status with the relevant ROU has not changed, or
* the site is an entity recognised by Human Services in a Human Services CoI and Human Services is satisfied that its registration status is valid for certificate issuance and has not changed.

### 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 site is an entity recognised by Human Services in a Human Services CoI and Human Services is satisfied that its registration status is valid for certificate issuance.

## Identification and authentication for revocation request

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 registered Human Services practice or entity recognised by Human Services as a member of a Human Services CoI
* the subscriber, or
* Certificate Controllers.

# 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.

### Enrolment process and responsibilities

Where a site is a registered Human Services practice, the site may be enrolled for certificates by Certificate Controllers on the basis of that registration.

Where a site is not a registered Human Services practice, the site, being a member of a Human Services CoI and responsible for that site, may apply to the Human Services RA Certificate Controllers to be enrolled for site certificates.

All applications are the responsibility of the site through its authorised contact person (however described). A Responsible Officer will be the authorised contact person for a seed organisation, in accordance with the *Healthcare Identifiers Act 2010*.

## Certificate application processing

### Performing identification and authentication of 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 site be approved on the basis of:

* the site is a registered Human Services practice, and in some cases, allocated an identifier,
* the entity being a member of a Human Services CoI and responsible for that site, is currently registered with Human Services for a programme or service,
* the site is a contracted servicer provider registered with and allocated a number by Human Services,
* the healthcare provider organisation is registered with and allocated a number by Human Services, in its role as the service operator of the HI Service, or
* receipt of a certificate application together with EOI commensurate with Human Services and Gatekeeper PKI Framework Level Of Assurance (LOA) 2 requirements.

### Time to process certificate applications

The time to process certificate applications are dependent on the registration criteria as set out in the application by each ROU for the subscribers in that CoI.

## Certificate issuance

### Human Services OCA actions during certificate issuance

All Subscriber key pairs under this CP shall be generated by Certificate Controllers using accredited software.

### Notification to subscriber by the Human Services OCA of issuance of certificate

The signing key and encryption key shall be stored and dispatched an encrypted format in accordance to the Public Key Cryptographic Standard #12. A Personal Identification Code (PIC) to access the keys and Certificates will also be generated and dispatched separately.

## Certificate acceptance

### Conduct constituting certificate acceptance

There is a subscriber agreement under this CP, known as the *Site Certificate* *Terms and Conditions of Use.*

The subscriber is bound by these terms and conditions when a person in the practice or entity conducts the first transaction using the site keys and certificates. This includes but not limited to, a person who is authorised by a practice or entity to bind the practice or entity (Authoriser), the Responsible Officer of a seed organisation, the Certificate Manager, the Organisation Maintenance Officer or a person who transact electronically on behalf of the practice or entity.

### Publication of the certificate by the Human Services OCA

Certificates issued under this CP will be published in the Healthcare Public Directory.

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

### Notification of certificate issuance by the Human Services OCA

The Human Services OCA may send certificates to the subscribers via the ROUs. In all circumstances the certificates will be issued in temper 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

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.

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. Parties shall not rely on a certificate that is revoked.

## Certificate renewal

### Circumstance for certificate renewal

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

### Who may request renewal

Subscribers may request their certificates be renewed from three months prior to the expiry of the certificates and no later than three months after the certificates expired.

Refer to section 3.3 for details of identification and authentication.

### Processing certificate renewal requests

Certificates issued under this CP may be renewed automatically by the Certificate Controllers. This is at the discretion of Human Services.

All certificate renewals under this CP involve re-keying.

### 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 Human Services OCA

Certificates and their corresponding hash values renewed under this CP are published to the Healthcare Public Directory when the Certificate is generated.

Refer to section 2 for details on publication.

### Notification of certificate issuance by the Human Services OCA

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

## Certificate re-key

### Circumstance for certificate re-key

All certificate 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 accredited software.

### 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 Human Services OCA

Certificates reissued under this CP and their corresponding hash values are published to the Healthcare Public Directory when the Certificate is generated.

Refer to section 2 for details on publication.

### Notification of certificate issuance by the Human Services OCA

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 site certificate
* in the event the site (however described) is de-registered, whether in relation to participation in any Human Services programme or not
* in the event any approvals (however described) relating to the site are cancelled by Human Services
* in the event any site 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 site 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 site recognised by Human Services or ceases to be a member of a Human Services RA CoI,
* the subscriber, or
* Certificate Controllers.

### Procedure for revocation request

Revocation must be requested in line with section 3.4.

### Time to request certificate revocation

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

### Processing certificate revocation requests

Certificates requests are processed by Certificate Controllers and actioned by the Human Services OCA.

Refer to section 1.3 of the Human Services OCA CPS for functions and obligations relating the revocation requests.

### Time to process revocation requests

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.

### Notification of certificate revocation

Once a Certificate is revoked, the Human Services OCA will write the Certificate serial number to the Human Services OCA CRL. While the Certificate is revoked immediately after the Human Services OCA processes the revocation request, any end user checking the validity of the Certificate will not be able to detect the revocation until the next refreshed CRL posting.

### Revocation checking requirement for relying parties

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

### CRL issuance frequency

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

### Maximum latency for CRLs

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.

### Online Certificate Status Protocol support

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

### Online revocation/status checking availability

The Healthcare Public Directory is substantially available 7 days a week, 24 hours

### On-line revocation checking requirements

No stipulation.

### Notification of certificate revocation by the Human Services OCA

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

### Certificate 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 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/)

### 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](https://www.humanservices.gov.au/health-professionals/enablers/public-key-infrastructure-pki-policy-documents)

## 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 ROUOs 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, Organisation Maintenance Officers and CSP officers).

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

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 Service 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 through the relevant business areas and provide a replacement agency as the successor ROU in accordance with policy as determined by the government and implemented in accordance with legislation passed by the Commonwealth Parliament.

# 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 a Certificate Controller using accredited software.

### Private key delivery to subscriber

The signing key and encryption key shall be stored in separate password protected PKCS#12 files. The first file contains the signing key and certificate. The second file contain the encypherment key and certificate. These PKCS#12 files are securely distributed as instructed by the ROUO. A Personal Identification Code (PIC) to access the keys and certificates will be generated and dispatched separately.

Subscribers are responsible for uploading the certificates onto the subscribers’ client operating system.

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

### Key sizes

Subscriber Keys are to be minimum length 2048 bits in length.

### Public key parameters generation

The parameters used to create Public Keys for Subscribers are generated using a product listed on the Defence Signals Directorate (DSD) Evaluated Products List (EPL).

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

Subscriber Keys will be used for the purposes and in the manner described in the CoI CP under which the Certificates are issued.

## Private Key Protection and Cryptographic Module Engineering Controls

### Cryptographic module standards and controls

Public Key Cryptography Standards (PKCS) #11 standard are used for secure token.

### 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 transferred into the secure token using accredited software and remains in the token.

### Private key storage on a cryptographic module

The Subscriber Private Keys are stored in the secure token.

### 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 secure token is removed from the computer.

### Method of destroying private key

No stipulation.

### Cryptographic module rating

Only Cryptographic modules evaluated and approved by the ASD shall be use.

## Other aspects of key pair management

### Public key archival

The Public Keys are stored in the Healthcare Public Directory for the life of the Certificate.

### 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 protection

No activation data other than Access Control mechanisms via the PIC is required to operate the secure token.

### 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 profiles

### Encipherment Certificate profile

| **F**i**e**l**d**/ **E**x**ten**sion | Site Encipherment 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) = AU  Organisation (O) = GOV  Organisation Unit (OU) = Humanservices  Common Name (CN) = Medicare Australia Organisation Certification Authority |
| Validity Period | **Required** |
| 2 years |
| Subject Distinguished Name | **Required** |
| Country (C) = AU  State (S) = <STATE>  Locality (L) = <Suburb Name>  Organisation (O) = <Trading Name <Locality>>  Organisation Unit (OU) = <Organisation Unit <Locality>>  Common Name (CN) = <Trading Name <Locality>> :RA Number |
| Subject Public Key Information | **Required** |
| Public Key encoded in accordance with RFC2459 & PKCS#1  Key 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** |
| Key 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 = 1.2.36.174030967.1.16.1.1  CPS Point = http://humanservices.gov.au  Policy Qualifier ID = User Notice  Notice 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 Name  RFC822 Name | **Optional critical** |
| **<Email address>** |
| Subject Alternative Name  URI | **Optional** |
| <Uniform Resource Identifier> |
| 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/general/cert\_search\_health.shtml** |
| 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>** |
| Healthcare Provider Identifier  {1.2.36.174030967.0.4} | **Optional** |
| **<Healthcare Provider Identifier>** |
| Medicare Identifier  {1.2.36.174030967.0.5} | **Optional** |
| **<Medicare Identifier>** |
| Pharmacy Approval Number  {1.2.36.174030967.0.6} | **Optional** |
| **<Pharmacy Approval>** |
| Location ID  {1.2.36.174030967.1.6.2.1} | **Optional** |
| **<Location ID>** |

### Signing Certificate profile

| ****F****i****e****l****d****/ ****E****x****ten****sion | Site Signing 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) = AU  Organisation (O) = GOV  Organisation Unit (OU) = Humanservices  Common Name (CN) = Medicare Australia Organisation Certification Authority |
| Validity Period | **Required** |
| 2 years |
| Subject Distinguished Name | **Required** |
| Country (C) = AU  State (S) = <STATE>  Locality (L) = <Suburb Name>  Organisation (O) = <Trading Name <Locality>>  Organisation Unit (OU) = <Organisation Unit <Locality>>  Common Name (CN) = <Trading Name <Locality>> :RA Number |
| Subject Public Key Information | **Required** |
| Public Key encoded in accordance with RFC2459 & PKCS#1  Key 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 |
| 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 = 1.2.36.174030967.1.16.1.1  CPS Point = http://humanservices.gov.au  Policy Qualifier ID = User Notice  Notice 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 Name  RFC822 Name | **Optional critical** |
| **<Email address>** |
| Subject Alternative Name  URI | **Optional** |
| <Uniform Resource Identifier> |
| 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/general/cert\_search\_health.shtml** |
| 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>** |
| Healthcare Provider Identifier  {1.2.36.174030967.0.4} | **Optional** |
| **<Healthcare Provider Identifier>** |
| Medicare Identifier  {1.2.36.174030967.0.5} | **Optional** |
| **<Medicare Identifier>** |
| Pharmacy Approval Number  {1.2.36.174030967.0.6} | **Optional** |
| **<Pharmacy Approval>** |
| Location ID  {1.2.36.174030967.1.6.2.1} | **Optional** |
| **<Location ID>** |

### 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 further information, refer to the Human Services Privacy Policy on its website [www.humanservices.gov.au](http://www.humanservices.gov.au).

## Privacy of personal information

For further information, refer to the Human Services Privacy Policy on its website [www.humanservices.gov.au](http://www.humanservices.gov.au).

## 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 Healthcare Public 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 OCA CPS 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)

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)