Australian Government

Defence

X.509 Certificate Policy
for the
Australian Department of Defence

Digital Signing Certificates - Resource

Version 1.0
November 2023

Notice to all parties seeking to rely

Reliance on a Certificate issued under this Certificate Policy (CP) for the Australian Department of Defence Digital Signing Certificates - Resource , identified by subarcs of the object identifier **1.2.36.1.334.1.1.3.9**, is only permitted as set forth in this document.

Use of a certificate issued under this CP constitutes acceptance of the terms and conditions set out in this document, as such, acceptance of a Certificate by a Relying Party is at the Relying Party's risk. Refer to the CP and Defence CPS for relevant disclaimers of warranties, liabilities and indemnities.

Document Management

This document is controlled by:	Defence Public Key Infrastructure Policy Management Authority (PKI PMA)
Changes are authorised by:	Defence Public Key Infrastructure Policy Management Authority (PKI PMA) Gatekeeper Competent Authority (GCA).

Change History

Version	Issue Date	Description/ Amendment	Changed by
0.1	Dec 2021	Initial draft	CDMC (AKK)
0.2	Oct 2022	2022 updates (second draft)	CDMC (AKK)
1.0	Nov 2023	Reviewed by PKI Ops, updated	CDMC (AKK)

Signatures

Appointment	Organisation	Signature
PKI PMA Chair	Dept. of Defence	PKI Documentation published as PDF files have undergone an extensive review and endorsement process by the relevant authorities in accordance with CDMC PKI publishing processes.
Gatekeeper Competent Authority	Digital Transformation Agency (DTA)	PKI Documentation published as PDF files have undergone an extensive review and endorsement process by the relevant authorities in accordance with CDMC PKI publishing processes.

Contents

1. INTRODUCTION

Certificate Policies (CPs) are, in the X.509 version 3 digital certificate standard, the named set of rules regarding the applicability of a *Certificate* to a particular community and/or class of applications with common security requirements. A CP may be used by a *Relying Party* to help in deciding whether a certificate, and the binding therein, are sufficiently trustworthy and otherwise appropriate for a particular application.

This CP identifies the rules to manage *Australian Government Department of Defence* ("Defence") **Digital Signing – Resource certificates** that are used to sign data between systems.

This CP includes the obligations of the *Public Key Infrastructure* (PKI) entities, and how they apply to the parties, indicated in section 1.3. In general, the rules in this CP identify the minimum standards in terms of security, process and auditing for the issuance and use of keys and certificates.

The headings in this CP follow the framework set out in Internet Engineering Task Force *Request for Comment* (RFC) 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. CPs are closely related to the corresponding CPS, and the documents are frequently cross-referenced. Where this CP provides no additional information to detail provided in the CPS, sub headings of the RFC3647 framework may have been omitted.

A document hierarchy applies:

1. The provisions of any applicable contract such as a *Subscriber Agreement*, Deed of Agreement or other relevant contract override the provisions of this CP.
2. The provisions of this CP prevail over the provisions of CPS to the extent of any direct inconsistency.
3. The provisions of CPS govern any matter on which this CP is silent.

The principal documents referenced by this CP are shown in Appendix A. The contents of a referenced document may be classified.

This section identifies and introduces the set of provisions, and indicates the types of entities and applications applicable for this CP.

1.1 Overview

Digital signing certificates for Resources (AD-DS-R) certificates are used for enabling *Resources* (e.g. servers, devices, *applications*) to digitally sign data, e.g. messages, documents or files.

AD-DS-R certificates are software based, and are, primarily, generated within the resource that will be using them. Where exceptions apply, these are noted in the relevant sections.

No authority, or privilege, applies to a resource by becoming an approved Digital Signing certificate holder, other than confirming affiliation with Defence.

With respect to the nature of the data being signed, any commitments or obligations entered into by signing the data are the responsibility of the Business Owner of the system, not the Defence PKI.

1.2 Document Name and Identification

This is the Australian Department of Defence Digital Signing Certificates - Resource Certificate Policy (CP)". The *Object Identifier* (OID) for this CP is **1.2.36.1.334.1.1.3.9:**

{iso (1) iso-member (2) australia (36) government (1) department of defence (334) pki (1) public (1) resource (3) digital signing cp (9)}

1.3 PKI Participants

1.3.1 Certification Authorities

The *Certification Authorities* (CAs) that issue certificates under this CP are Defence Public CAs, which are Gatekeeper accredited. Defence Public CAs are managed by the Defence Certificate and Directory Management Centre (CDMC). Refer to [ADPRCA] for information about the Root CA and Issuing CAs.

The issuing CA can be found in the certificate "Issuer" field.

1.3.2 Registration Authorities

The *Registration Authorities* (RAs) that perform the registration function under this CP are Gatekeeper accredited Defence RAs. For further information, see CPS.

Trusted Agents (TAs) authorised by their business area and the CDMC are able to approve a certificate request under this CP. TAs are required to undergo registration including Evidence of Identity (EOI) check and training prior to commencing their duties as TAs. PKI Operators (CDMC staff) may also act as TAs.

1.3.3 Subscribers

AD-DS-R certificates are only issued to *Non-Person Entities* (NPEs) such as servers or applications.

However, the *Subscriber* of an AD-DS-R certificate refers to the person or legal entity that applied for that Certificate, and/or administers the system that uses the Certificate. In most cases, this will be a *Resource Administrator* responsible for the support of the resource using the AD-DS-R certificate. An AD-DS-R Subscriber must be affiliated with Defence and have an entry in the Defence Corporate Directory (DCD)[1].

Certain responsibilities of the Subscriber may be delegated to one or more *Key Custodian*(s), where the Subscriber does not handle key material themselves.

In this case:

i. The Subscriber is responsible for ensuring that the correct delegation and access management is in place, and is accountable for the delegated responsibilities.
ii. A Key Custodian is responsible for private key protection and certificate management.

The responsibilities of the Subscriber are summarised in section 9.6.3 Subscriber representations and warranties).

1.3.4 Relying Parties

A Relying Party is the entity that relies on a certificate, that is, the validity of the binding of the certificate Subject's identity to a public key. The Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information, i.e. *Certificate Revocation Lists* (CRLs) or an *Online Certificate Status Protocol* (OCSP) server.

Relying Parties to AD-DS-R certificates are the resources or users that rely on the AD-DS-R certificate presented to them, internal or external to Defence.

[1] Any exceptions to this rule must be approved by PKI Operations Manager.

See also CPS.

1.3.5 Other Participants

See CPS.

1.4 Certificate Usage

1.4.1 Appropriate certificate uses

The appropriate use of an AD-DS-R certificate, in conjunction with its associated private key, is to enable a Defence resource to digitally sign data for integrity and authentication purposes.

1.4.2 Prohibited certificate uses

Prohibited use includes using (or configuring a resource to use) the certificate for any transaction or communication:

i. Unrelated to Defence business and/or the appropriate certificate uses;
ii. Illegal;
iii. Unauthorised;
iv. Unethical; or
v. Contrary to Defence policy.

Engaging in prohibited certificate use is a breach of the responsibilities and obligations of the Subscriber/Key Custodian and Defence disclaims any liability in such circumstances.

1.5 Policy Administration

1.5.1 Organisation administering the document

See CPS.

1.5.2 Contact person

See CPS.

1.5.3 Authority determining CPS suitability for the policy

See CPS.

1.5.4 CPS approval procedures

See CPS.

1.6 Definitions, Acronyms and Interpretation

Acronyms and terms used in this CP are defined in Appendix A and the CPS Glossary. Note that defined terms in this CP appear in italics the first time they are used and otherwise are not identified in this manner when appearing later throughout the CP. Defined terms may be upper or lower case.

The interpretation clause in part 3 of Appendix B of the CPS also applies to this CP.

2. PUBLICATION & REPOSITORY RESPONSIBILITIES

2.1 Repositories

See CPS.

2.2 Publication of certificate information

See CPS.

2.3 Time or frequency of publication

See CPS.

2.4 Access controls on repositories

See CPS.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

A full Distinguished Name (DName) must be present in the Subject field of the certificate.

The DName Subject Common Name field must contain a unique identifier of the Resource, System or Signing entity (e.g. Section/Unit). It must clearly indicate the entity that is signing, or on whose behalf the resource is signing, e.g. an FQDN, or the name of the entity (e.g. a section or unit) on whose behalf the Resource is signing data.

The Subject Alternative Name (SAN) field is optional. Wildcard certificates are not permitted under this CP.

Refer to Appendix B Certificate Profiles for more detail.

3.1.2 Need for names to be meaningful

The TA shall ensure that the DName in subjectName field used to identify the Subject of a certificate is:

i. Meaningful; and
ii. Relates directly to an attribute or identifier of the Resource.

The **Common Name** (CN) field of the DName must clearly indicate the entity that is signing, or on whose behalf the resource is signing, e.g. a Fully Qualified Domain Name (FQDN), or the name of the entity (e.g. a section or unit) on whose behalf the Resource is signing.

3.1.3 Anonymity or pseudonymity of Subscribers

This CP prohibits anonymity or pseudonymity of Subscribers.

3.1.4 Rules for interpreting various name forms

Name forms must be compliant with the applicable standard, e.g. X.500 for DNames.

3.1.5 Uniqueness of names

Names must be unique within the PKI name space.

3.1.6 Recognition, authentication, and role of trademarks

See CPS.

3.2 Initial Identity Validation

This section explains how the identification and authentication of the Resource and the Subscriber are carried out in order to achieve a binding between the Resource, the private key and the Subscriber.

3.2.1 Method to prove possession of private key

Certificate signing requests submitted to the CA must be PKCS#10 formatted requests where proof of possession of the Private Key by the Subscriber is ensured, and that the Key Pair is generated on the Resource at the time the certificate request is created.

3.2.2 Authentication of organisation identity

The TA is responsible for checking that both the Resource requiring the certificate and the Subscriber are *affiliated* with Defence prior to approving a certificate request. Any domain name used in the certificate name must be for a domain that is controlled by Defence[2].

3.2.3 Authentication of individual identity

The TA is responsible for checking that:

i. The Resource; and
ii. the signing entity (e.g. Section/Unit) named in the certificate (Subject Common Name); and
iii. the Subscriber

are all affiliated with Defence, e.g. by confirming their entries in the Defence Corporate Directory.

3.2.4 Non-verified subscriber information

All information included in the certificate request is verified by the TA.

3.2.5 Validation of authority

No authority, or privilege, applies to a resource by becoming an approved AD-DS-R certificate holder, other than confirming affiliation with Defence. Prior to the issue of a certificate, affiliation with Defence is validated by the TA.

The PKI/TA does not validate if any authority exists in relation to commitments or obligations entered into by signing the data with an AD-DS-R certificate. This is the responsibility of the Business Owner of the system. It is also the responsibility of the Business Owner to ensure that the applicant (Subscriber) has the requisite knowledge and authority to manage and configure the use of the keys and certificate.

3.2.6 Criteria for interoperation

See CPS.

[2] Any exceptions to this rule must be approved by PKI Operations Manager.

3.3 Identification and Authentication for Re-key requests

3.3.1 Identification and authentication for routine re-key

The identification and authentication for routine re-key follows the process for an initial identity validation (section 3.2).

3.3.2 Identification and authentication for re-key after revocation

The identification and authentication for routine re-key follows the process for an initial identity validation (section 3.2).

3.4 Identification and Authentication for Revocation requests

Subscribers use the PKI web interface for requesting revocation of a certificate they manage. They then raise a job in the Defence Service Management System (DSMS). The process authenticates the requestor through the binding to their Defence network account.

In addition, any authorised requestor (see 4.9.2 Who can request revocation) may request revocation of a certificate by sending a digitally signed email from their current Defence email account to pki.ops@defence.gov.au.

An approved[3] Operator must validate that the requestor is authorised to revoke the certificate (see section 4.9.2 Who can request revocation).

In extraordinary (emergency) circumstances a revocation request can be submitted verbally or through another written channel. In this case, the approved Operator must:

i. check that the requestor is affiliated with Defence by using any reasonable means, e.g. an out-of-band source; and
ii. check that the requestor has a current entry in the Defence Corporate Directory (DCD); and
iii. check that they are authorised to request revocation of the certificate (see section 4.9.2); and
iv. ensure the requestor provides confirmation in an email with all the necessary information as soon as they are able to.

Refer to See 4.9 (Certificate revocation and suspension) for more information on revocation.

4. Certificate Lifecycle Operational Requirements

4.1 Certificate Application

4.1.1 Who can submit a certificate application

Individuals affiliated with Defence can submit a certificate application for an AD-DS-R certificate for a resource (non-person entity) that they administer. The applicant must have the requisite authorisation to act on behalf of the Section/Unit.

4.1.2 Enrolment process and responsibilities

It is the responsibility of the Business/System Owner to ensure that the certificate requester (Subscriber) has the requisite authority and understands the requirements for the digital signing certificate.

[3] An Operator with the appropriate permissions for the certificate type.

Using the resource's security functionality, the Subscriber generates a key pair and submits a certificate request. The TA verifies the information in the request and then approves it for registration.

The resource's administrator is responsible for providing accurate information in an application for the correct certificate type. The TA is responsible for checking the accuracy of that information and verifying that the application is for a Defence resource prior to approval for registration.

4.2 Certificate Application Processing

4.2.1 Performing identification and authentication functions

The following process is applied when a Certificate Signing Request (CSR) has been received by the RA and the TA is ready to assess it.

a) The TA verifies the following prior to approving the request:

   i. That the Certificate Request has a valid Subject name (see 3.1 Naming);
   ii. That the identity of the Resource and the Subscriber/Key Custodian meet the requirements (see 3.2);
   iii. That the correct certificate profile has been chosen.

b) Once the certificate request is verified by the TA, it is forwarded to the CA, which signs the certificate and returns it to the requestor. The CA only certifies certificate requests that are signed by an approved Defence RA.

4.2.2 Approval or rejection of certificate applications

A TA may reject or approve a certificate application. Reasons for rejection may include invalid application, insufficient affiliation with Defence, or the provision of incorrect or insufficient identification details.

4.2.3 Time to process certificate applications

Processing for certificate applications will occur in a timely manner.

4.3 Certificate Issuance

4.3.1 CA actions during certificate issuance

See CPS.

4.3.2 Notification to subscriber by the CA of issuance of certificate

See CPS. In addition, the TA advises the Subscriber when the certificate is available to be retrieved for installation.

4.4 Certificate Acceptance

4.4.1 Conduct constituting certificate acceptance

Use of the certificate constitutes acceptance.

4.4.2 Publication of the certificate by the CA

See CPS.

4.4.3 Notification of certificate issuance by the CA to other entities

No stipulation.

4.5 Key pair and Certificate Usage

4.5.1 Subscriber private key and certificate usage

Certificates issued under this CP are only issued to non-person entities (NPE), not individuals.

The Subscriber and/or Key Custodian (see 1.3.3) must ensure that:

i. the private key and certificate are used in accordance with section 1.4 (Certificate Usage);
ii. the private key is protected from access by other parties in accordance with its security classification;
iii. the private key is only used in accordance with the key usage parameters set in the certificate; and
iv. the private key is no longer used following expiration or revocation of the certificate.

4.5.2 Relying party public key and certificate usage

1.4 (Certificate Usage) and 1.3.4 (Relying Parties) detail the Relying Party's public key and certificate usage and responsibilities.

The interpretation and compliance with extended key usage attributes, and any associated limitations on the use of the certificate and/or private key, is in accordance with [5280].

4.6 Certificate Renewal

Renewal of a certificate indicates creating a new certificate with an existing key pair, i.e. re-using a previously generated CSR. Certificate renewal is generally not permitted, certificates must be re-keyed, see 4.7 Certificate Re-key. If there is a technical requirement to retain a key pair in a new certificate, this must be approved by the PKI Operations Manager.

4.7 Certificate Re-key

Re-key of a certificate indicates creating a certificate with a new key pair, i.e. generating a new key pair on the resource, creating a new CSR which is submitted to the RA.

4.7.1 Circumstance for Certificate Re-key

The circumstances for certificate re-key include:

i. normal certificate expiration;
ii. certificate revocation;
iii. useable life of current key material has been reached; or
iv. change in algorithm, or key length, required.

See also CPS.

4.7.2 Who may request certification of a new public key

See 4.1.1 (Who can submit a certificate application).

4.7.3 Processing certificate re-keying requests

Processing of certificate re-key requests is consistent with the processing of new certificate requests, as detailed in 4.2.1 (Certificate application processing).

4.7.4 Notification of new certificate issuance to subscriber

See 4.3.2 (Notification to subscriber by the CA of issuance of certificate).

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Use of the certificate constitutes acceptance.

4.7.6 Publication of the re-keyed certificate by the CA

See 4.4.2 (Publication of the certificate by the CA).

4.7.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.8 Certificate Modification

Certificate modification is a method to re-issue a certificate with changes to certificate details. Certificate modification is not permitted under this CP. If a certificate needs to be modified, it will be re-keyed; refer to section 4.7.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

A certificate must be *revoked* when the binding between the subject and the subject's public key defined within a certificate is no longer considered valid. Circumstances that invalidate the binding include the following:

i. The private key is confirmed or suspected to be lost or compromised.
ii. Information in the certificate (e.g. identity or organisational information) is not correct due to error, or changes in circumstances.
iii. The CA obtains credible evidence any certificate it has issued has been misused.
iv. The CA is made aware that a Subscriber/Key Custodian has violated one or more of its material obligations under the terms of use agreements that apply (such as this CP).

The CPS defines further circumstances for Revocation.

4.9.2 Who can request revocation

Revocation requests may be submitted by any authorised party (see CPS), including the Subscriber/Key Custodian, a TA or a PKI Operator.

4.9.3 Procedure for Revocation request

Revocation requests are verified on receipt in accordance with 3.4 (Identification and authentication for revocation requests) and processed in priority order.

After verification, and if the revocation request is approved, the TA and/or PKI Operator processes revocation requests by using the PKI software, which captures an auditable record of the process. Dual approval is required for all requests to revoke (the 1st approver can be either a TA or a PKI Operator, the 2nd approver must be a PKI Operator).

After a certificate is revoked, the CA includes the applicable certificate (certificate serial number) in the CRL that is signed by the CA and published in the repositories.

4.9.4 Revocation request Grace Period

A grace period of one *Operational Day* is permitted from the time a Subscriber or Key Custodian becomes aware of a reason for revocation, until submitting a revocation request.

The PKI PMA, or an approved delegate, in exceptional circumstances (such as a security or law enforcement investigation, or if the revocation would cause an unacceptable outage), may approve a delay in the submission of a revocation request. An audit record of this approval is required, and must be submitted with the revocation request upon expiry of the approved delay.

4.9.5 Time within which CA must Process the Revocation request

A CA shall process revocation requests for certificates issued under this CP promptly after receipt.

4.9.6 Revocation Checking Requirement for Relying Parties

It is the Relying Party's responsibility to determine their requirement for revocation checking.

4.9.7 CRL issuance frequency

CRL issuance frequency for certificates issued under this CP is upon each certificate revocation, or at intervals no longer than 24 hours if there are no updates.

4.9.8 Maximum latency for CRLs (if applicable)

The maximum latency between the generation and publication of CRLs is 3 days.

4.9.9 On-line revocation/status checking availability

Online Certificate Status Protocol service (OCSP) is available at:

http://ocsp.defence.gov.au

Refer to the relevant Certificate Profile in Appendix B - if the certificate is issued with an OCSP access location reference (Authority Information Access extension), OCSP is available to the Relying Party as a certificate status checking method.

The latest CRL is available from the published repositories; refer to 2.1 (Repositories) and the certificates CRL Distribution Point for further information.

4.9.10 On-line revocation checking requirements

Refer to 4.9.6 (Revocation checking requirement for relying parties)

4.9.11 Other forms of revocation advertisements available

See CPS.

4.9.12 Special requirements re key compromise

See CPS section 5.7 (Compromise and disaster recovery).

4.9.13 Circumstances for suspension

Certificate suspension is not supported under this CP.

4.9.14 Who can request suspension

Certificate suspension is not supported under this CP.

4.9.15 Procedure for suspension request

Certificate suspension is not supported under this CP.

4.9.16 Limits on suspension period

Certificate suspension is not supported under this CP.

4.10 Certificate status services

The Defence PKI provides certificate status services via CRLs and OCSP.

4.10.1 Operational characteristics

See CPS.

4.10.2 Service availability

See CPS.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

See CPS.

4.12 Key escrow and recovery

Keys are not escrowed by the CA.

5. Facility, Management, and Operational Controls

The CPS describes the Facility, Management and Operational Controls of the Defence CA and RA environments.

5.1 Physical controls

See CPS.

5.2 Procedural controls

See CPS.

5.3 Personnel controls

See CPS.

5.4 Audit logging procedures

See CPS.

5.5 Records archival

See CPS.

5.6 Key changeover

See CPS.

5.7 Compromise and disaster recovery

See CPS.

5.8 CA or RA termination

See CPS.

6. Technical Security Controls

The CPS describes any Technical Security Controls for the CA and RA environments.

This section describes the Technical Security Controls for the End Entity environment.

6.1 Key pair Generation and Installation

6.1.1 Key Pair generation

Keys are generated locally within a cryptographic module on the resource during the requesting process. If this is not possible, private keys must only be transported encrypted to where they are installed, and any copies destroyed (see 6.2).

6.1.2 Private key delivery to subscriber

Generally the key generation is performed within the resource so no delivery is required.

Where resources are working in a failover or high availability configuration, cloning of the key pair and certificate is permitted. See section 6.2.6.

6.1.3 Public key delivery to certificate issuer

The public key is provided to the CA in a PKCS#10 certificate request file signed with the corresponding private key.

6.1.4 CA public key delivery to relying parties

See CPS.

6.1.5 Key sizes

See Appendix B. The minimum key size for RSA keys is 2048 bits.

For minimum key size for Elliptic Curve (ECC) algorithms, refer to the current version of the Australian Government Information Security Manual [ISM].

6.1.6 Public key parameters generation and quality checking

See CPS.

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

Keys issued under this CP allow a resource to digitally sign data. See Appendix B and CPS for further information.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

This section refers to the protection of AD-DS-R private keys. Private key protection for CAs and RAs is covered in the CPS.

6.2.1 Cryptographic module standards and controls

Cryptographic module standards and controls must comply with the Defence requirements.

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

Not applicable.

6.2.3 Private key escrow

The CA does not escrow AD-DS-R private keys.

6.2.4 Private key backup

Private authentication keys are not backed up by the CA.

6.2.5 Private key archival

Private authentication keys are not archived by the CA.

6.2.6 Private key transfer into or from a cryptographic module

Where resources are working in a failover or high availability configuration, cloning of the key pair and certificate is permitted. It is the Subscriber/Key Custodian’s responsibility to ensure that:

i. Private keys are protected during transit (e.g. by using a token with a PKCS#12 password protected software vault);
ii. Keys are installed in the correct location(s); and
iii. Copies of the transport file are destroyed.

The Subscriber/Key Custodian must protect Private keys during transit by using an approved cryptographic algorithm of at least the same strength as the key being transferred.

6.2.7 Private key storage on cryptographic module

The private keys are stored in a protected area within the applicable cryptographic module.

6.2.8 Method of activating private key

Activating private keys occurs by the Key Custodian authenticating to the cryptographic module. The session stays live until deactivated (see 6.2.9).

6.2.9 Method of deactivating private key

Deactivation can be achieved via:

i. shut down or restart of the system; or
ii. shut down of the service that exercises the private key.

6.2.10 Method of destroying private key

Key Custodians must destroy private keys when no longer needed either by securely erasing, overwriting or destroying the soft token in accordance with Defence requirements.

6.2.11 Cryptographic Module Rating

See 6.2.1 (Cryptographic module standards and controls)

6.3 Other aspects of key pair management

6.3.1 Public key archival

See CPS.

6.3.2 Certificate operational periods and key pair usage periods

See Appendix B Certificate Profiles and CPS.

6.4 Activation data

6.4.1 Activation data generation and installation

All passphrases or passwords used to activate the private key must be accordance with [ISM].

6.4.2 Activation data protection

All passphrases or passwords used to activate the private key shall be kept in accordance with the [ISM].

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

See CPS.

6.6 Life cycle technical controls

See CPS.

6.7 Network security controls

See CPS.

6.8 Time-stamping

See CPS.

7. CERTIFICATE, CRL, AND OCSP PROFILES

Refer to Appendix B for full certificate profiles.

7.1 Certificate Profile

Refer to Appendix B for full certificate profiles.

7.1.1 Version number(s)

All certificates are X.509 Version 3 certificates.

7.1.2 Certificate extensions

See Appendix B.

7.1.3 Algorithm object identifiers

Certificates under this CP will use one of the following OIDs for signatures:

Sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

Certificates under this CP will use one of the following OIDs for identifying the algorithm for which the subject key was generated:

Id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-x9-62(10045) public-key-type (2) 1}
rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
Dhpublicnumber	{iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}
id-keyExchangeAlgorithm	{joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) algorithms(1) 22}

7.1.4 Name forms

See section 3.1, CPS and Appendix B for further information.

7.1.5 Name constraints

Refer to the Issuing CA's CP.

7.1.6 Certificate policy object identifier

Certificates issued under this CP shall include the following Certificate Policy Identifiers:

This **CPs OID** (See Appendix B for variants): **{1.2.36.1.334.1.1.3.9}**

Certificates issued under this policy shall also assert the appropriate *Level of Assurance* (LoA) OID and, to enable the use of the certificate at lower LoA, this policy enables the additional assertion of the lower (or 'stacked') LoA OIDs. LoA OIDs able to be asserted under this policy include:

Level of Assurance (LoA) OID (Medium – Resource): **{1.2.36.1.334.1.2.2.2}**

Level of Assurance (LoA) OID (Low – Resource): **{1.2.36.1.334.1.2.2.1}**

7.1.7 Usage of policy constraints extension

Refer to the Issuing CA's CP.

7.1.8 Policy qualifiers syntax and semantics

See Appendix B.

7.1.9 Processing semantics for the critical certificate policies extension

This CP does not require the certificate policies extension to be critical. Relying Parties whose client software does not process this extension do so at their own risk.

7.2 CRL Profile

7.2.1 Version number(s)

CRLs issued shall be X.509 version 2.

7.2.2 CRL and CRL entry extensions

Refer to Issuing CA's CP [ADPRCA].

7.3 OCSP Profile

7.3.1 Version Numbers

OCSP is implemented using version 1 as specified under [6960].

7.3.2 OCSP Extensions

Refer to CPS and Validation Authority (VA) CP for full OCSP profile.

8. Compliance Audit and Other Assessments

8.1 Frequency or circumstances of assessment

See CPS.

8.2 Identity/qualifications of assessor

See CPS.

8.3 Assessor's relationship to assessed entity

See CPS.

8.4 Topics covered by assessment

See CPS.

8.5 Actions Taken as a Result of Deficiency

See CPS.

8.6 Communication of Results

See CPS.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

No stipulation.

9.1.2 Certificate access fees

There is no fee for accessing Certificates from approved repositories.

9.1.3 Revocation or status information access fees

There is no fee for accessing the CRL from approved repositories.

9.1.4 Fees for other services

No stipulation.

9.1.5 Refund policy

See CPS.

9.2 Financial Responsibility

9.2.1 Insurance

No stipulation.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

No stipulation.

9.3 Confidentiality of Business Information

See CPS.

9.3.1 Scope of confidential information

No stipulation.

9.3.2 Information not within the scope of confidential information

No stipulation.

9.3.3 Responsibility to protect confidential information

See CPS.

9.4 Privacy of Personal Information

Resource Certificates pertain to non-person entities, not individuals, and do not contain any personal information (as defined in the Privacy Act 1988 (Cth)).

For any personal information that may be collected at registration, refer to CPS.

9.5 Intellectual Property Rights

See CPS.

9.6 Representations and Warranties

See CPS.

9.6.1 CA representations and warranties

See CPS.

9.6.2 RA representations and warranties

See CPS.

9.6.3 Subscriber representations and warranties

As the trusted role responsible for the private keys, the relevant Subscriber/Key Custodian (see 1.3.3) warrants to:

i. only use Keys and digital certificates within the limits specified in this CP;
ii. take all reasonable measures to protect the Private Key(s) in their custody from compromise and take all necessary precautions to prevent loss, disclosure, modification, or unauthorised use of the Private Key(s); and
iii. promptly notify a TA or CDMC in the event that they consider or suspect there has been a compromise of the Private Key(s).

9.6.4 Relying party representations and warranties

See CPS. In addition, certificates issued under this CP do not contain, or imply, any authority, access or privilege. Relying Parties assume responsibility for any financial limit they may wish to apply for transactions authenticated using certificates issued under this CP.

9.6.5 Representations and warranties of other participants

No Stipulation.

9.7 Disclaimer of Warranties

See CPS.

9.8 Limitations of Liability

See CPS.

In Addition: GATEKEEPER ACCREDITATION DISCLAIMER

The Gatekeeper Competent Authority is responsible for ensuring that the accreditation process is conducted with due care and in accordance with published Gatekeeper Criteria and Policies. The Gatekeeper Competent Authority is not liable for any errors and/or omissions in the final Approved Documents, which remain the responsibility of the accredited Service Provider. The Digital Transformation Agency is not responsible and cannot be held liable for any loss of any kind in relation to the use of digital keys and certificates issued by a Gatekeeper accredited

Service Provider. By granting a Service Provider Gatekeeper Accreditation the Digital Transformation Agency makes no representation and gives no warranty as to the:

- Accuracy of any statements or representations made in, or suitability of, the Approved Documents of a Gatekeeper accredited Service Provider;
- Accuracy of any statement or representation made in, or suitability of, the documentation of a Service Provider in a Gatekeeper recognised PKI domain; or
- Standard or suitability of any services thereby provided by any Subscriber or Relying Party or application.

9.9 Indemnities

See CPS.

9.10 Term and Termination

9.10.1 Term

This CP and any amendments shall become effective upon publication in the Repository and will remain in effect until the notice of its termination is communicated by the Defence PKI on its web site or Repository.

9.10.2 Termination

See CPS.

9.10.3 Effect of termination and survival

See CPS.

9.11 Individual notices and communications with participants

See CPS.

9.12 Amendments

See CPS.

9.13 Dispute resolution provisions

See CPS.

9.14 Governing Law

See CPS.

9.15 Compliance with Applicable Law

See CPS.

9.16 Miscellaneous provisions

See CPS.

9.17 Other provisions

See CPS.

Appendix A REFERENCES

Terms and Abbreviations: See CPS Appendix - Glossary

Appendix A.1. RELATED DOCUMENTS

Reference	Document
[6960]	RFC6960 Internet X.509 Public Key Infrastructure On-line Certificate Status Protocol (ocsp), Internet Engineering Task Force, available at https://www.ietf.org/rfc/rfc6960.txt
[3647]	RFC3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Internet Engineering Task Force, available at https://www.ietf.org/rfc/rfc3647.txt
[5280]	RFC5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Internet Engineering Task Force, available at https://www.ietf.org/rfc/rfc5280.txt
[ADPRCA]	Australian Defence Public Root CA and Sub CA Certificate Policy http://crl.defence.gov.au/pki/Policy.html
[CPS]	Australian Defence PKI Certification Practice Statement http://defence.gov.au/pki/cps/Defence-CPS.pdf
[DSPF]	Defence Security Principles Framework http://drnet/AssociateSecretary/security/policy/Pages/dspf.aspx
[GK2015]	Digital Transformation Office, Gatekeeper PKI Framework v3.1 Dec 2015, available at https://www.dta.gov.au/standard/design-guides/authentication-frameworks/gatekeeper-public-key-infrastructure-framework/
[ISM]	Australian Government Information Security Manual. Current version can be found at https://www.cyber.gov.au/acsc/view-all-content/ism
[LoA]	Defence Public Key Infrastructure Levels of Assurance Requirements Certificate Policy Object Identifiers (OIDs) http://crl.defence.gov.au/pki/documents/Public/Defence-Levels-of-Assurance.pdf
[OID Register]	Defence OID Register A register, maintained by CDMC, listing all current Defence PKI and DCD OIDs. Not available externally.

Appendix A.2. USEFUL LINKS

i. Defence PKI Services – https://pki.defence.gov.au/
ii. Digital Signatures: RFC 5652 Cryptographic Message Syntax (PKCS#7) - https://datatracker.ietf.org/doc/html/rfc5652
iii. Digital Signatures: RFC 3275 XML Signatures Syntax and Processing Digital Signatures – https://datatracker.ietf.ort/doc/html/rfc3275

Appendix B CERTIFICATE PROFILES

Summary of Certificate profiles

N.B. Variants no longer in use will be removed from this Appendix. For information of older certificate profiles, refer to [OID register] and older versions of this CP.

Variant No. (OID extension)	Name/description	Variant OID	RP Name/ID	Customer	Month/year implemented
1	Digital Signature – Resource - Standard	1.2.36.1.334.1.1.3.9.1			Dec 2021

Appendix B.1. Digital Signature – Resource – Standard

Field	Critical	Value	Notes
Version		V3 (2)	
Serial		Randomly Generated Number	Unique value generated by the issuing CA
Issuer signature algorithm		SHA-2WithRSAEncryption	Minimum cryptographic level

Issuer distinguished name		CN = <SubCAIssuer>
		OU = CAs
		OU = PKI
		OU= DoD
		O = GOV
		C = AU
			Encoded as printable string.
			<SubCAIssuer> denotes the issuing Sub CA; one of the Defence Public CAs.

Validity period		2 years	2 years from date of issue

Subject distinguished name		cn=<*unique identifier*>
		ou=Digital Signature
		ou=Devices
		ou=<subCAIssuer>
		ou=PKI
		ou=DoD
		o=GOV
		c=AU
			<unique identifier> is an identifier of the Resource, System or Signing entity (e.g. Section/Unit). Must clearly indicate the entity that is signing, or on whose behalf the resource is signing, e.g. an FQDN, or the name of the entity (e.g. a section or unit) on whose behalf the Resource is signing data.

Subject public key information		2048 bit RSA key modulus	
Issuer unique identifier			Not Present
Subject unique identifier			Not Present
X.509 v3 extensions			
Authority key identifier	No	<octet string>	160 bit SHA-1 hash of binary DER encoding of signing CA's public key

Field	Critical	Value	Notes
Subject key identifier	No	<octet string>	160 bit SHA-1 hash of binary DER encoding of subject's public key
Key usage	Yes	Digital Signature	
Extended key usage	No	See Notes	An EKU should be used where possible, either[4]: • X.509 Email Protection, or • MS Enhanced Key Usage Document Signing (XCN_OID_KP_DOCUMENT_SIGNING (1.3.6.1.4.1.311.10.3.12)
Private key usage period	NA		Not Present
Certificate policies	No	[1] CP Id: {1.2.36.1.334.1.1.3.9.1} Policy qualifier – CPS pointer: http://crl.defence.gov.au/pki Policy qualifier - User Notice: "Other than confirming affiliation with the DoD, the PKI infers no authority or privilege to the Subscriber of this certificate. Certificates must not be used for any purpose not permitted by the CP."	The OID of the CP, variation <1>
	No	[2] Policy OID: {1.2.36.1.334.1.2.2.2}	Level of Assurance – Medium (Resource) The Level of Assurance of this certificate
	No	[3] Policy OID: {1.2.36.1.334.1.2.2.1}	Level of Assurance – Low (Resource) Included to allow the certificate to be used in lower assurance context.
Subject Alternative Name	No		Optional
Policy mapping		-	Not Present

[4] Or, when implemented: https://datatracker.ietf.org/doc/draft-ito-documentsigning-eku/

Field	Critical	Value	Notes
Issuer alternative name		-	Not Present
Subject directory attributes		-	Not Present
Basic constraints			Not Present
Name constraints		-	Not Present
Policy constraints		-	Not Present
Subject Information Access		-	Not Present

Authority information access	No	[1] Access method: OCSP {1.3.6.1.5.5.7.48.1}
		Access location: http://ocsp.defence.gov.au
		[2] Access method: CA Issuer {1.3.6.1.5.5.7.48.2}
		Access location: http://crl.defence.gov.au/pki/Certificates/<SubCAIssuer>
		[3] Access method: CA Issuer {1.3.6.1.5.5.7.48.2}
		Access location: ldap://dir.defence.gov.au/cn=<SubCAIssuer>,ou=CAs, ou=PKI,ou=DoD,o=GOV,c=AU?cACertificate;binary, crossCertificatePair;binary
			Defence uses a URL rewrite (redirection) rule in the Web Server to ensure that AIA urls without a file extension are assigned the correct filetype (.crt or .p7b)
			<SubCAIssuer> denotes the issuing Sub CA; one of the Defence CAs

CRL Distribution Point	No	[1] Distribution Point Name (http):
		http://crl.defence.gov.au/pki/crl/<SubCAIssuer>.crl
		[2] Distribution Point Name (ldap):
		ldap://dir.defence.gov.au/cn=<SubCAIssuer>,ou=CAs, ou=PKI,ou=DoD,o=GOV,c=AU?certificateRevocationList
			The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and CRL Issuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).
			<SubCAIssuer> denotes the issuing Sub CA; one of the Defence Public CAs.