Australian Government

Defence

X.509 Certificate Policy for the Australian Department of Defence Validation Authority

Version 8.0
November 2022

Notice to all parties seeking to rely

Reliance on a Certificate issued under this Certificate Policy, identified by subarcs of the object identifier 1.2.36.1.334.1.1.3.5, 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 Draft	07/12/2011	Initial draft	Verizon Business
1.0	July 2012	Released	SJP
2.0	May 2014	Reviewed for Release	PKI Ops Man
3.0	June 2014	For Release	PKI TL Ops Man
4.0	Oct 2016	Released	PKI Ops Man
4.1	Dec 2016	Updated references to www.defence.gov.au to crl.defence.gov.au	Cogito Group (BB)
4.2	Feb 2018	Updated references from DTO to DTA. Reviewed Document and URLs.	CDMC (JE)
4.3	Dec 2018	Review and minor updates	NA
5.0	July 2019	Published	PKI Ops Man
5.1	Sep 2020	Removed soft certs and references to SHA-1. Other minor updates incl. classification.	CDMC (AKK)
6.0	Oct 2020	Reviewed by DTA – Changes accepted - Released	CDMC (AKK)
6.1	Oct 2021	2021 updates	CDMC (AKK)
7.0	Dec 2021	Reviewed by DTA – Changes accepted - Released	CDMC (AKK)
7.1	Oct 2022	2022 updates	CDMC (AKK)
8.0	Nov 2022	Reviewed by DTA – Changes accepted - Published	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

List of Tables

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 *Certificate Policy* (CP) identifies the rules to manage the *Australian Government Department of Defence* (Defence) *Validation Authority* (*VA*) certificates.

This CP includes the obligations of the 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.

A document hierarchy applies: the provisions of any applicable contract such as a *Subscriber Agreement*, *Deed of Agreement* or other relevant contract override the provisions of this CP. The provisions of this CP prevail over the provisions of CPS to the extent of any direct inconsistency. The provisions of CPS govern any matter on which this CP is silent. (Note: where sub titled sections of the framework provide no additional information to detail provided in the CPS they have not been further extrapolated in this document.)

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

This CP only applies to certificates issued to Defence *Validation Authorities* for the provision of certificate status responses, and does not apply to other non-individuals (organisations, resources or devices) or any individuals.

No authority, or privilege, applies to a resource by becoming an approved Validation Authority Certificate holder, other than confirming ownership by Defence.

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

OCSP will form one component of what will be referred to as a Validation Authority. From this point forward the server providing OCSP services and the additional capabilities as they are brought online will collectively comprise what is the Validation Authority.

1.2 Document name and identification

The title for this CP is "X.509 Certificate Policy for the Australian Government Department of Defence Validation Authority Certificates". The *Object Identifier* (OID) for this CP is 1.2.36.1.334.1.1.3.5.

{iso (1) member-body (2)au(36) government (1)department-of-defence (334) pki (1) public (1) resource (3) ocsp (5)}

Extensions of this OID represent the certificate variants governed by this CP. They are identified in Appendix B.

1.3 PKI participants

1.3.1 Certification authorities

The *Certification Authorities* (CAs) that issue certificates under this CP are *Gatekeeper*-accredited. For further information, see CPS.

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.

1.3.3 Subscribers

Validation Authority Certificates are only issued to *non-person entities* (NPE), not individuals.

The Subscriber of a Defence Validation Authority Certificate refers to the person or legal entity that applied for that Certificate and/or administer the resource. In most cases, this will be one or more *PKI Operators* responsible for the support of the Validation Authority using the certificate.

As *Key Custodians*, PKI Operators are responsible for private key protection and certificate management in accordance with the PKI KMP.

1.3.4 Relying parties

See CPS.

1.3.5 Other participants

See CPS.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

The appropriate use for a certificate issued under this CP, in conjunction with its associated private key, is:

i. to enable Defence to digitally sign certificate status information and permit relying parties to validate that certificate status information is authentic and issued by a trusted validation authority.
ii. to enable the digital signing of audit, transactional and operational logs produced by the validation authority.
iii. to validate certificate status information signed by the Defence Validation Authority.

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 a prohibited certificate use is a breach of the responsibilities and obligations agreed to by the PKI operators and Defence disclaims any and all 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 the CPS. 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 (B.3) of the CPS also applies to this CP.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

See CPS.

2.2 Publication of certification information

See CPS.

2.3 Time or frequency of publication

See 4.9.7 for CRL issuance frequency. For further information, see CPS.

2.4 Access controls on repositories

See CPS.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

A clear distinguishable and unique *Distinguished Name* (DN) must be present in the certificate Subject field.

3.1.2 Need for names to be meaningful

PKI Operators shall ensure that the DN in subject Name field used to identify the Subject of a certificate is:

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

3.1.3 Anonymity of pseudonymity of Subscribers

Not applicable.

3.1.4 Rules for interpreting various name forms

Names are compliant with the standard used (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

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 Key Custodian is ensured and that the *Key Pair* is generated at the time the certificate request is created.

3.2.2 Authentication of organisation identity

The PKI Operator authenticates the organisation identity of the resource during the approval of the certification request after checking that the information in the request is correct.

3.2.3 Authentication of individual identity

This CP covers certificates for a non-human resource, and not an individual.

The PKI Operator authenticates the identity of the resource during the approval of the certification request after checking that the information in the request is correct.

3.2.4 Non-verified subscriber information

Non-verified information shall not be included in certificates.

3.2.5 Validation of authority

PKI Operators are responsible for the resource being deployed.

The *PKI Operations Manager* is responsible for ensuring that PKI Operators are acting within the limits of their authority.

3.2.6 Criteria for interoperation

See CPS.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and authentication for routine re-key

See 3.2.2 (Authentication of organisation identity) and 3.2.3 (Authentication of individual identity).

3.3.2 Identification and authentication for re-key after revocation

See 3.2.2 (Authentication of organisation identity) and 3.2.3 (Authentication of individual identity).

3.4 Identification and Authentication for Revocation Requests

Revocation of certificates is in accordance with this section and 4.9 of this CP and the CPS.

The PKI Operations Manager, or in their absence their nominated agent, must authenticate all requests for revocation of PKI core components and the reason for revocation. Prior to revocation, the operator verifies the authority of the requestor.

The revocation process provides an auditable record of this process, which includes at a minimum:

i. the identity of the requestor;
ii. the reason for requesting revocation;
iii. the identity of the operator performing the revocation; and
iv. the issuing CA name and serial numbers of the certificates authorised for revocation, or the reason for rejecting the revocation request.

OCSP responder certificates have a very short life-span and are not expected to require revocation.

4. CERTIFICATE LIFE CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate application

4.1.1 Who can submit a certificate application

PKI Operators initiate the certificate application as part of standard operating procedures.

4.1.2 Enrolment process and responsibilities

PKI Operators will initiate the enrolment process using the CA Operator interface. The PKI Operator is responsible for conducting the enrolment in accordance with operational procedures and the KMP.

The enrolment process and responsibilities are outlined in the KMP.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

The PKI Operations Manager must ensure that each certificate application is in accordance with the PKI KMP and undergoes:

i. confirmation of approval for VA creation; and
ii. validation of all information to be included in the certificate.

4.2.2 Approval or rejection of certificate applications

A PKI Operator may reject or approve a certificate application. Reasons for rejection may include invalid application, or the provision of incorrect or insufficient identification details.

4.2.3 Time to process certificate applications

Processing of 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

Notification to the Key Custodian occurs for a certificate request either when it succeeds or fails.

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

Validation Authority certificates are only issued to *non-person entities* (NPE), not individuals.

The Key Custodian must ensure that:

i. the private key is protected from access by other parties in accordance with the KMP;
ii. the private key is only used in accordance with the key usage parameters set in the certificate; and
iii. 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 KeyUsage attributes, and any associated limitations on the use of the certificate and/or private key, is in accordance with RFC5280 and RFC6960.

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

See CPS for certificate renewal criteria.

Certificate *renewal* is only permitted in exceptional circumstances and must not be used to avoid certificate re-key or the associated identification and authentication processes. For further information, see CPS.

4.6.2 Who may request renewal

See CPS.

4.6.3 Processing certificate renewal requests

The processing of certificate renewal requests is consistent with the processing of new certificate requests, as detailed in 4.2.1 (Certificate application processing).

4.6.4 Notification of new certificate issuance to subscriber

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

4.6.5 Conduct constituting acceptance of a renewal certificate

See 4.4.1 (Conduct constituting certificate acceptance).

4.6.6 Publication of the renewal certificate by the CA

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

4.6.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

See 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 (Performing identification and authentication functions).

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

See 4.4.1 (Conduct constituting certificate 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

This CP does not support certificate modification. 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

See CPS.

4.9.2 Who can request revocation

See CPS.

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 PKI Operator processes revocation requests by completing the revocation request form provided by the RA, which captures an auditable record of the process.

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 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 Parties responsibility to determine their requirement for revocation checking.

4.9.7 CRL issuance frequency (if applicable)

CRL issuance frequency for certificates issued under this CP are published on 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

No on-line revocation/status checking server is available to get the revocation status of the Validation Authority certificate.

4.9.10 On-line revocation checking requirements

See section 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

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 will not be escrowed.

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

5.5.1 Types of records archived

See CPS.

5.5.2 Retention period for archive

See CPS.

5.5.3 Protection of archive

See CPS.

5.5.4 Archive backup procedures

See CPS.

5.5.5 Requirements for time-stamping of records

See CPS.

5.5.6 Archive collection system (internal or external)

No Stipulation.

5.5.7 Procedures to obtain and verify archive information

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 Technical Security Controls for the CA and RA environments.

6.1 Key pair generation and installation

6.1.1 Key pair generation

Keys are generated by the accredited Validation Authority application.

6.1.2 Private key delivery to subscriber

The private key will be generated using the Validation Authority software on the *hardware security module* (HSM). To increase the level of security the private key will be created on and stored securely within the HSM and will never leave the device.

6.1.3 Public key delivery to certificate issuer

A *certificate signing request* (CSR) file is created at the same time as the creation of the private key. The certificate request file is transported via physical media from the OCSP Server to the appropriate CA. On validating the OCSP CSR, the public key will be sign by the appropriate CA. The public key and certificate will be transported via physical media to the OCSP Server and imported into the HSM.

The Key Custodian is responsible for the transport of the request and the issued public certificate.

6.1.4 CA public key delivery to relying parties

See CPS.

6.1.5 Key sizes

See Appendix B.

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 Defence Validation Authority to provide signed certificate status information.

Key usages are specified in the Certificate Profile set forth in Appendix B.

6.2 Private key protection and cryptographic module engineering controls

6.2.1 Cryptographic module standards and controls

See CPS.

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

See CPS.

6.2.3 Private key escrow

Escrow of keys does not occur.

6.2.4 Private key backup

See CPS.

6.2.5 Private key archival

See CPS.

6.2.6 Private key transfer into or from a cryptographic module

See CPS.

6.2.7 Private key storage on cryptographic module

See CPS.

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

See CPS.

6.2.11 Cryptographic Module Rating

See CPS.

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

As the key pair is generated and stored in an accredited hardware security module (HSM), the Validation Authority certificate and key pair has a maximum validity period of 2 years. Replacement keys and certificates are created annually.

For further information, see CPS.

6.4 Activation data

6.4.1 Activation data generation and installation

No Stipulation.

6.4.2 Activation data protection

All passphrases used to activate core components are kept in accordance with Defence policy. See PKI KMP.

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

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 the following OID for signatures.

sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

Table 1 - Signature OIDs

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}

Table 2 - Algorithm OIDs

7.1.4 Name forms

See CPS and Appendix B for further information.

7.1.5 Name constraints

Name constraints are not present in the CA's certificate, however names must be must be for a domain that is controlled by Defence.

7.1.6 Certificate policy object identifier

Certificates issued under this CP shall assert this CP's OID:

(1.2.36.1.334.1.1.3.5)

Certificates issued under this policy shall also assert the following LoA OID:

{1.2.36.1.334.1.2.2.2} Level of Assurance – Medium (Resource)

In addition; to enable the use of the certificate at lower Levels of Assurance, this policy also asserts the following OID:

{1.2.36.1.334.1.2.2.1} Level of Assurance – Low (Resource).

See also Appendix B.

7.1.7 Usage of policy constraints extension

Policy constraints are not present.

7.1.8 Policy qualifiers syntax and semantics

The only policy qualifiers that are permitted are the CPS Pointer qualifier and the User notice qualifier.

The CPS Pointer, if used, shall contain a HTTP URI link to the Certification Practice Statement (CPS) published by the CA, or to a webpage from which the CPS can then be downloaded.

The User notice, if used, shall only contain the explicitText field.

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 CRLs.

7.2.2 CRL and CRL entry extensions

Refer to the issuing CA's CP..

7.3 OCSP profile

7.3.1 Version Numbers

OCSP is implemented using version 1 as specified under RFC 6960.

7.3.2 OCSP Extensions

All OCSP extensions are to comply with RFC 6960.

OCSP responder certificates are issued with the no-check extension enabled, negating the need of the relying party to validate the OCSP responder's certificate through another sources such as the CRL.

This extension will not be marked critical.

See Appendix B for full details.

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

See CPS regarding fees for access to this CP. No fee has been stipulated for other services.

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 Key Custodian warrants to:

i. only use Keys and digital certificates within the limits specified in the 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 the RA 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

The following documents are referenced in this CP:

[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
[CPS]	X.509 Certification Practice Statement for the Australian Department of Defence, available at https://defence.gov.au/pki/cps/Defence-cps.pdf
[GK2015]	Digital Transformation Agency, 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 Signals Directorate, Australian Government Information Security Manual Controls, available at https://www.asd.gov.au/infosec/ism/index.htm
[KMP]	Australian Department of Defence Public Key Infrastructure Key Management Plan (classified)
[LOA]	Department of Defence Public Key Infrastructure Assurance Level Requirements document, available at https://defence.gov.au/pki/_lib/doc_pdf/LOA.pdf
[RCA CP]	X.509 Certificate Policy for the Australian Department of Defence Root Certification Authority and Subordinate Certificate Authorities, available at https://defence.gov.au/pki/_lib/doc_pdf/Defence-ADPRCA-CP.pdf
[VA CP]	X.509 Certificate Policy for the Australian Department of Defence Validation Authority Certificates (this document), available at https://defence.gov.au/pki/_lib/doc_pdf/Defence-Validation-Authority-CP.pdf

Table 3 - References

APPENDIX B. CERTIFICATE PROFILES

B.1 OCSP Responder SHA2 Certificate format Hardware

Field	Critical	Value	Notes
Version		V3 (2)	X.509 version v3 PKI Certificate and CRL profile
Serial		<*octet string*>	Must be unique within Defence namespace
Issuer signature algorithm		sha-2WithRSAEncryption	
Issuer distinguished name		CN= <CAIssuer> OU= CAs OU= PKI OU= DoD O= GOV C= AU	See Defence-ADPRCA-CP for the <CAIssuer> naming convention.
Validity period		Not before <UTCtime> Not after <UTCtime>	Maximum 2 years from date of issue
Subject distinguished name		cn=<OCSP Responder name > ou=PKI Services ou=PKI ou=DoD o=GOV c=AU	OCS Responder Name; e.g. <CAName_(location)_OCSP>
Subject public key information		Minimum 2048 bit RSA key modulus	
Issuer unique identifier		-	Not Present
Subject unique identifier		-	Not Present
Issuer's signature		sha-2WithRSAEncryption	
Authority key identifier	No	<*octet string*>	160 bit SHA-1 hash of binary DER encoding of signing CA's public key[1]
Subject key identifier	No	<*octet string*>	160 bit SHA-1 hash of binary DER encoding of subject's public key
Key usage	Yes	digitalSignature	
Extended key usage	Yes	id-kp-OCSPSigning	
Private key usage period		-	Not Present
Certificate policies	No	[1] Policy ID:{ 1.2.36.1.334.1.1.3.5} Policy Qualifier: CPS Pointer: http://crl.defence.gov.au/pki	This CP

[1] The AKI field is used as a method of uniquely identifying the certificate or key pair that was used to sign the current certificate. The currently specified method of generating the AKI is one of the recommended methods as specified in RFC 5280. Using SHA-1 poses no risks as the field is not used for verification.

Field	Critical	Value	Notes
		[2] Policy OID: {1.2.36.1.334.1.2.2.2}	Level of Assurance – Medium (Resource) The Level of Assurance of this certificate
		[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.
Policy mapping		-	Not Present
Subject Alternative Name		-	Not Present
Issuer alternative name		-	Not Present
Subject directory attributes		-	Not Present
Basic constraints	No	Subject type=End Entity	
Name constraints		-	Not Present
Policy constraints		-	Not Present
Authority information access	No	[1] Access method=CAIssuer {1.3.6.1.5.5.7.48.2}: Access location: http://crl.defence.gov.au/pki/certificates/<CAIssuer> [2] Access method=CAIssuer {1.3.6.1.5.5.7.48.2}: Access location: ldap://dir.defence.gov.au/cn=<CAIssuer>,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)
CRL Distribution Point	No	http://crl.defence.gov.au/pki/crl/<CAIssuer>.crl ldap://dir.defence.gov.au/cn=<CAIssuer>,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 cRLIssuer 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).
OCSP No Check	No	id-pkix-ocsp-nocheck: NULL {1.3.6.1.5.5.7.48.1.5}	This extension tells a client that it is not necessary to check the certificate status of this certificate.

Table 4 - OCSP Responder Hardware SHA2 Certificate profile

APPENDIX C. CRL PROFILE

Please refer to the issuing CA's Certificate Policy.

APPENDIX D. LEVEL OF ASSURANCE MAPPING

D.1 Assurance Level

The following table documents the mapping of this CP to the requirements of an associated assurance level as documented in the Defence PKI Assurance Level Requirements paper [LOA]:

CP's Level of Assurance:	**Medium Assurance -Resource {1.2.36.1.334.1.2.2.2}.** As documented in section 7.1.6 above.

REQUIREMENT	CP'S MAPPING TO REQUIREMENT
IDENTITY PROOFING	
EOI	A PKI Operator is responsible for the identification of a resource and the verification of a certificate request during the enrolment of a resource, as described in 4.1.2 (Enrolment process and responsibilities). The PKI Operator is a trusted role, and the PKI Operator has proven their affiliation with Defence and identity as part of their enrolment.
Evidence of Relationship	By being configured for use on the Defence SIE by a trusted administrator with the required access permissions, the resource is authorised for registration to the Defence PKI.
Location	The identification of a resource maybe local or remote.
CREDENTIAL STRENGTH	
Token Protection	Private and public key pairs are generated on the accredited HSM and the private key does not leave the HSM.
Token Activation	Access to the private key is protected by passphrase in accordance with Defence security requirements.
Life (Time) of Key Strength	Certificates that make use of SHA-2, with at least 128 security bits (SHA-256) and a RSA key size of at least 2048 bits are recommended in [ISM] 2020 for OFFICIAL and PROTECTED,
CERTIFICATE MANAGEMENT	
CA Protection	The CA is both physically and logically secure from the unauthorised access. The CA protection requirements are documented in the CPS and sections 5 and 6 of this CP.
Binding	As documented in section 4 (Certificate Lifecycle Operational Requirements), the key generation and issuance of a certificate to a resource is carried out by trusted roles, using the cryptographic capability on the PKI software. While the issuance process is not necessarily contiguous, the certificate signing request binds the certificate to the private key generated in the cryptographic module.
Revocation (Publication)	The CRL is published in accordance with the issuing CA's CP. The issuing CA is a High Assurance CA, so exceeds the requirement.

REQUIREMENT	CP'S MAPPING TO REQUIREMENT
Compliance	The Compliance requirements are covered in the CPS and section 8 (Compliance audit and other assessments). The Defence PKI environment is certified under the Australian Government Gatekeeper program, to support the issuance of up to a Gatekeeper LOA 4 (Very High Assurance) level.

D.2 Risk Assessment

The issuances of certificates using this Certificate Policy has been aligned with an Australian Defence Medium Assurance, which as documented in the [LOA] paper should provide a relying party some assurance in the asserted identity.

As discussed in the section 1.3 of the [LOA] paper, any deviations within the CP from those requirements documented for the associated assurance level should be appropriately risk managed.

No risks were identified and managed in the alignment of this Certificate Policy with the requirements for Medium Assurance.

LOA REQUIREMENT	IDENTIFIED RISK	MITIGATION / CONTROLS