Australian Government

Defence

X.509 Certificate Policy for the Australian Department of Defence Secure Communications Certificates

Version 11.0
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 Secure Communications Certificates, identified by subarcs of the object identifier **1.2.36.1.334.1.1.3.1,** 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	28/4/08	Initial draft	Sarah Moylan
1.0	23 Nov 09	Released	GJF
2.0	Nov 2011	Released (minor amendments, cert profile changes)	SJP
3.0	July 2012	Released	SJP
4.0	May 2014	Reviewed for release	PKI Ops Man
5.0	Oct 2016	Released	PKI Ops Man
5.1	Dec 2016	Updated references www.defence.gov.au to crl.defence.gov.au	Cogito Group (BB)
5.2	Sep 2017	CSO Annual Review	CSO
5.3	Feb 2018	Review and updates/corrections post GK review	Operations Manager
5.4	Aug 2018	Review and updates to all variants.	CDMC (JE)
5.5	Jun 2019	Review and updates/ Remove expired SHA1 Cert Profiles	CDMC (LD)/Ops Man
6.0	July 2019	Published	PKI Ops Man
6.1	Sep 2020	Updated classification (new scheme), minor corrections and clarifications. Removed references to SSL. Removed SHA1 profiles.	CDMC (AKK)
7.0	Oct 2020	Reviewed by DTA - Changes accepted - Released	CDMC (AKK)

Version	Issue Date	Description/ Amendment	Changed by
8.0	Feb 2021	Added cert profile with max validity of 397 days, in line with CAB/Forum Baseline Requirements. Refer to [CABF-BR]	CDMC (AKK)
8.1	Oct 2021	Annual Update. Clarifications in line with Enterprise CP improvements, revocation process clarification.	CDMC (AKK)
9.0	Dec 2021	Reviewed by DTA – Changes accepted - Released	CDMC (AKK)
9.1	Jan 2022	Very minor change to wording 9.4 (legal). Published	CDMC (AKK)
9.2	Oct 2022	2022 updates – minor improvements. PKI Policy management authority now PKI PMA (prev. DPKIPB)	CDMC (AKK)
10.0	Nov 2022	Reviewed by DTA – Changes accepted - Published	CDMC (AKK)
10.1	Nov 2023	2023 updates	CDMC (AKK)
10.2	Nov 2023	Re-formulating CABF cert profile - Subject Name	CDMC (AKK)
11.0	Nov 2023	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 CP identifies the rules to manage the *Australian Government Department of Defence* (*Defence*) **Resource Certificates – Secure Communications**, that are used to establish secure communication sessions using protocols such as *Transport Layer Security* (TLS).

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

This CP only applies to certificates issued to Defence *Resources* (Non Person entities) for the establishment of secure communication sessions using TLS or a related protocol.

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

1.2 Document name and identification

The title for this CP is "X.509 Certificate Policy for the Australian Government Department of Defence Secure Communications Resource Certificates". The *Object Identifier* (OID) for this CP is 1.2.36.1.334.1.1.3.1.

{iso (1) iso-member (2) australia (36) government (1) department of defence (334) pki (1) public (1) resource (3) secure comms (1)}

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 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

Secure Communications Resource Certificates are only issued to *non-person entities* (NPE) such as servers or devices, not individuals.

The *Subscriber* of a Defence Secure Communications Resource Certificate refers to the person or legal entity that applied for that Certificate and/or administer the resource. In most cases, this will be a Resource Administrator responsible for the support of the resource using the certificate.

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 Secure Communications certificates are the resources or users that rely on the certificate presented to them, internal or external to Defence.

See also 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 to enable the Defence Resource to establish secure communications using TLS or a related protocol.

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 respective responsibilities and obligations of the Subscriber and/or Key Custodian (see 1.3.3) 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 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 certificate 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 full or partial[1] Distinguished Name (DName) must be present in the Subject field of the certificate. The Subject Common Name (CN) field must contain an identifier directly relating to an attribute or identifier of the Resource. Short names are not permitted.

One or more Subject Alternative Names (SANs) must be present, containing one of the RFC5280 defined names, e.g. Fully Qualified Domain Name, and relate directly to an attribute or identifier of the Resource. Short names are not permitted.

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 DN 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.

3.1.3 Anonymity of pseudonymity of Subscribers

Not applicable.

3.1.4 Rules for interpreting various name forms

Names must be 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.

[1] N.B. For compliance with CA Browser Forum (CABForum) Baseline Requirements for Publicly Trusted certificates, **domain validated public website certificate** Subject DNames must only contain Common Name and Country fields. Refer to CABForum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, section 7.1.2.7.2.

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 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.

3.2.3 Authentication of individual identity

The TA is responsible for checking that:

i. The Resource; and
ii. 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 Secure Communications certificate holder, other than confirming affiliation with Defence. Prior to the issue of a certificate, *affiliation* with Defence is validated by the TA.

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

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 re-key after revocation 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[2] 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.

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

4. CERTIFICATE LIFE CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate application

4.1.1 Who can submit a certificate application

Any individual who has an approved affiliation with Defence, and has a valid requirement, can submit an application for a certificate.

4.1.2 Enrolment process and responsibilities

Using the resource's security functionality, the resource's administrator generates a key pair and submits a certificate request. The TA verifies the information in the request and then approves it for registration. The RA validates and signs the request, and sends it to the CA.

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.

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

1. 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.
2. 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 resource's administrator 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 is protected from access by other parties in accordance with its security classification and the KMP;

ii. the private key is only used in accordance with section 1.4 (Certificate usage) and 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

See section 1.3.4 (Relying Parties).

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.

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 not permitted under this CP, certificates must be re-keyed, see 4.7 Certificate Re-key.

4.7 Certificate re-key

Re-key of a certificates indicates renewing 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 an 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 (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

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.

Externally Defence will provide all certificates and the most up-to-date CRL.

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

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.

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 primarily generated locally within 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 establish secure communication sessions using TLS or a related protocol. See Appendix B and CPS for further information.

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

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

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 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

A Secure Communications certificate issued to a website has a maximum validity period of 397 days to limit the key lifetime. This is in line with the CAB/Forum Baseline Requirements changes that came into force in September 2020 (refer to [CABF-BR]).

Other TLS server certificates used for server to server communications may have a validity for up to 2 years. For further information, see Appendix B Certificate Profiles and CPS.

6.4 Activation data

6.4.1 Activation data generation and installation

No Stipulation.

6.4.2 Activation data protection

See CPS.

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 section 3.1, CPS and Appendix B for further information.

TLS certificates must have at least one Subject Alternative Name.

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:

T**his CPs OID** (See Appendix B for variants): **{1.2.36.1.334.1.1.3.1}**

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 – Medium (Resource): {1.2.36.1.334.1.2.2.2}

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

See also Appendix B.

7.1.7 Usage of policy constraints extension

See Appendix B.

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 the issuing CA's CP [ADPRCA].

7.3 OCSP profile

7.3.1 Version Numbers

OSCP is implemented using version 1 as specified under RFC 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

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 Subscriber/Key Custodian (see 1.3.3) 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

Terms and Abbreviations: See CPS Appendix - Glossary.

A.1 RELATED DOCUMENTS

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
[ADPRCA]	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
[CABF-BR]	Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, issued by the CA/Browser forum. https://cabforum.org/baseline-requirements-documents/
[GK2015]	Australian Government, 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
[CPS]	X.509 Certification Practice Statement for the Australian Department of Defence, available at https://defence.gov.au/pki/cps/Defence-cps.pdf
[KMP]	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
[OID Register]	Defence OID Register A register, maintained by CDMC, listing all current Defence PKI and DCD OIDs. Not available externally.
[VA CP]	X.509 Certificate Policy for the Australian Department of Defence Validation Authority Certificates, available at https://defence.gov.au/pki/_lib/doc_pdf/Defence-Validation-Authority-CP.pdf

Table 3 - References

Appendix B. CERTIFICATE PROFILES

Summary of Certificate Profiles

NB. Variations associated with this Annex will occur over time due to technical implementations. As such variations will be marginal and not materially affect the certificates issued under this CP they will not be reviewed by the Gatekeeper Competent Authority.

Certificate Profiles that have been retired have been removed from this Appendix. To access old 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	SecureComms_- TLS Server - Standard Certificate 2 Yrs	1.2.36.1.334.1.1.3.1.**1**			
2	SecureComms - Std website - CABF BR 397 days	1.2.36.1.334.1.1.3.1.**2**			

B.1 STANDARD PROFILE: SECURECOMMS - TLS SERVER - STANDARD CERTIFICATE - 2 YRS

Standard version for server to server communications. Use B.2 Standard Profile: SecureComms - Std website - CABF BR for websites.

Multiple SANs, CP OID variant 3 (1.2.36.1.334.1.1.3.1.**3**)

Field	Critical	Value	Notes
Version		V3 (2)	
Serial		<*octet string*>	Must be unique within Defence namespace
Issuer signature algorithm		sha-2WithRSAEncryption	
Issuer distinguished name		CN=<subCAIssuer> OU= CAs OU= PKI OU= DoD O= GOV C= AU	Encoded as printable string. <subCAIssuer> represents the CA that issued the certificate. See naming convention in Section 3.1 of the Public Root CA and Sub CAs CP (http://crl.defence.gov.au/pki/documents/Defence-ADPRCA-CP.pdf)
Validity period		Not before <UTCtime> Not after <UTCtime>	Max 2 years from date of issue.
Subject distinguished name		cn=<*unique identifier*> ou=SecureComms ou=Devices ou=<subCAIssuer ou=PKI ou=DoD o=GOV c=AU	<unique identifier> as determined by device. <subCAIssuer> represents the CA that issued the certificate. See naming convention in Section 3.1 of the Public Root CA and Sub CAs CP (http://crl.defence.gov.au/pki/documents/Defence-ADPRCA-CP.pdf)
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[3]

[3] 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
Subject key identifier	No	*<octet string>*	160 bit SHA-1 hash of binary DER encoding of Subject's public key
Key usage	Yes	DigitalSignature keyEncipherment	
Extended key usage	No	ServerAuthentication ClientAuthentication	
Private key usage period	NA	-	Not Present
Certificate policies	No	[1] Policy Id: {1.2.36.1.334.1.1.3.1.3} Policy qualifier – CPS pointer: http://crl.defence.gov.au/pki	The OID of this CP (variant 3)
	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.
Policy mapping		-	Not Present
Subject Alternative Name	No	DNS Name: *<Fully Qualified Hostname>* * 25	A SAN value must be included to meet the requirements of newer internet browsers, such as Chrome 58 or newer
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: CAIssuer{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 .p7c) <subCAIssuer> represents the CA that issued the certificate. See naming convention in Section 3.1 of the Public Root CA and Sub CAs CP (http://crl.defence.gov.au/pki/documents/Defence-ADPRCA-CP.pdf)
Subject Information Access	No	-	Not Present

Field	Critical	Value	Notes
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 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). <subCAIssuer> represents the CA that issued the certificate. See naming convention in Section 3.1 of the Public Root CA and Sub CAs CP (http://crl.defence.gov.au/pki/documents/Defence-ADPRCA-CP.pdf)

B.2 STANDARD PROFILE: SECURECOMMS - STD WEBSITE - CABF BR 397 DAYS

Certificate profile for a standard website, validity (max 397 days) in line with CAB Forum Baseline Requirements [CABF-BR]

CP OID variant 12 (1.2.36.1.334.1.1.3.1.**12**)

Field	Critical	Value	Notes
Version		V3 (2)	
Serial		<*octet string*>	Must be unique within Defence namespace
Issuer signature algorithm		sha-2WithRSAEncryption	
Issuer distinguished name		CN=<subCAIssuer> OU= CAs OU= PKI OU= DoD O= GOV C= AU	Encoded as printable string. <subCAIssuer> represents the CA that issued the certificate. See naming convention in Section 3.1 of the Public Root CA and Sub CAs CP (http://crl.defence.gov.au/pki/documents/Defence-ADPRCA-CP.pdf)
Validity period		Not before <UTCtime> Not after <UTCtime>	Max 397 days from date of issue. (In line with CAB Forum Baseline Requirements)
Subject distinguished name		cn=<*unique identifier*> ou=SecureComms (see Notes) ou=Devices (see Notes) ou=<subCAIssuer> (see Notes) ou=PKI (see Notes) ou=DoD (see Notes) o=GOV (see Notes) c=AU	N.B. CABForum Baseline Requirements for Domain Validated certificates do not allow other elements of the DName than CN= and C=. Older certificates issued under this registration profile may still contain OU= and O= elements. See 3.1.1 <unique identifier> as determined by device. <subCAIssuer> represents the CA that issued the certificate. See naming convention in Section 3.1 of the Public Root CA and Sub CAs CP (http://crl.defence.gov.au/pki/documents/Defence-ADPRCA-CP.pdf)
Subject public key information		2048 bit RSA key modulus	
Issuer unique identifier		-	Not Present
Subject unique identifier		-	Not Present

Field	Critical	Value	Notes
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[4]
Subject key identifier	No	<*octet string*>	160 bit SHA-1 hash of binary DER encoding of Subject's public key
Key usage	Yes	DigitalSignature keyEncipherment	
Extended key usage	No	ServerAuthentication ClientAuthentication	
Private key usage period	NA	-	Not Present
Certificate policies	No	[1] Policy Id: {1.2.36.1.334.1.1.3.1.12} Policy qualifier – CPS pointer: http://crl.defence.gov.au/pki	The OID of this CP (variant 12)
	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.
Policy mapping		-	Not Present
Subject Alternative Name	No	DNS Name: <*Fully Qualified Hostname*> * 25	A SAN value should be included to meet the requirements of newer internet browsers, such as Chrome 58 or newer
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: CAIssuer{1.3.6.1.5.5.7.48.2} Access location: http://crl.defence.gov.au/pki/Certificates/<subCAIssuer>	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 .p7c) <subCAIssuer> represents the CA that issued the certificate. See naming convention in Section 3.1 of the Public Root CA and

[4] 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
		[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	Sub CAs CP (http://crl.defence.gov.au/pki/documents/Defence-ADPRCA-CP.pdf)
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 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). <subCAIssuer> represents the CA that issued the certificate. See naming convention in Section 3.1 of the Public Root CA and Sub CAs CP https://crl.defence.gov.au/pki/documents/Defence-ADPRCA-CP.pdf

Appendix C. CRL FORMAT

Please refer to the issuing CA's Certificate Policy [RCA CP].

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 Trusted Agent 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 TA is a trusted role, and the TA 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 resource using a cryptographic software module which also provides protection for the soft token during its lifecycle. See 6.2 (Private key protection and cryptographic module engineering controls).
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] (2021) 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.

REQUIREMENT	CP'S MAPPING TO REQUIREMENT
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 resource itself. While the issuance process is not necessarily contiguous, the certificate signing request binds the certificate to the private key generated on the resource. The certificate also has a subject name which contains an identifier determined by the resource (see Appendix B. Certificate Profiles).
Revocation (Publication)	As covered in section 4.9.7, the CRL is published weekly, or on a certificate revocation, which exceeds the requirements. This is as a result of issuing from the High Assurance CA.
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 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 particular risks were identified in the alignment of this Certificate Policy with the requirements for Medium Assurance.

LOA REQUIREMENT	IDENTIFIED RISK	MITIGATION / CONTROLS