Australian Government

Defence

X.509 Certificate Policy for the Australian Department of Defence Public Root Certificate Authority and Subordinate Certificate Authorities

Version 6.1
December 2024

Notice to all parties seeking to rely

Reliance on a Certificate issued under this Certificate Policy (CP) for the Australian Department of Defence Public Root Certificate Authority and Subordinate Certificate Authorities, identified by subarcs of the object identifier **1.2.36.1.334.1.1.1.7** *for* ADPRCA CP *and* **1.2.36.1.334.1.1.1.8** *for any* Sub CA *that is signed by the* ADPRCA, 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:	The Defence Public Key Infrastructure Policy Management Authority (PKI PMA)
Significant Changes are authorised by:	Defence Public Key Infrastructure Policy Management Authority (PKI PMA); and Gatekeeper Competent Authority (GCA)

Change History

Version	Issue Date	Description/ Amendment	Changed by
0.1	20 July 2016	Initial Release, based upon original DRCA CP.	Cogito Group (CJP)
1.0	October 2016	Approved for release	PKI Operations Manager – Acting (DK)
2.0	July 2019	Published	PKI Ops Man
2.1	Sep 2020	Minor updates incl. classification.	CDMC (AKK)
3.0	Oct 2020	Reviewed by DTA – Changes accepted - Released	CDMC (AKK)
3.1	Nov 2021	2021 update. Resource Custodian (RC) renamed to Trusted Agent (TA), harmonization with ADERCA CP, Revocation and other clarifications.	CDMC (AKK)
4.0	Dec 2021	Reviewed by DTA – Changes accepted - Released	CDMC (AKK)
4.1	Oct 2022	2022 updates, e.g. DPKIPB -> PKI PMA	CDMC (AKK)
5.0	Nov 2022	Reviewed by DTA – Changes accepted - Released	CDMC (AKK)
5.1	Nov 2023	2023 updates	CDMC (AKK)
6.0	Nov 2023	Published	CDMC (AKK)

Version	Issue Date	Description/ Amendment	Changed by
6.1	Dec 2024	2024 updates, replace “CDMC”, now “PKI Operations” (at DDIS)	DDIS (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 PKI Operations publishing processes.

Contents

Table 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) **Public Root *Certificate Authority* (ADPRCA)** certificates, as well as any ***Subordinate CAs*** **(Sub CAs)** signed by it, and any Sub CA associated *core component* certificates.

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 the 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 applies to the **Australian Defence Public Root CA (ADPRCA), its Sub CAs and their respective core component certificates**. The ADPRCA is the highest point of trust within the Defence Public PKI hierarchy and all other CA and RA entities in the hierarchy rely on this trust anchor.

The self-signed ADPRCA certificate is used to sign certificates for Sub CAs and those used for root certificate operations, including Operators, e.g. CA Operator (CAO). A Sub CA certificate is used to sign certificates for end-entities and those used for Sub CA operations (e.g. Registration Authority (RA) or Key Archive Server (KAS) etc.), including Operators. End-entity certificates are covered in other CPs.

This CP only allows the ADPRCA and any Sub CA private keys to reside on a hardware security module (HSM). Any operations certificates required for PKI core components are required to be stored in accordance with the PKI Key Management Plan (PKI KMP).

This CP only allows *Operators'*[1] keys and certificates to reside on a hardware based *token* with an embedded cryptographic engine. Before issuing Operators' keys and certificates, the applicant is required to perform a face-to-face identity verification that complies with the *Gatekeeper Evidence of*

[1] PKI Trusted Roles including ADPRCAOs, CAOs, RAAs, TAs, ROs etc.

Identity (EOI) policy for a Gatekeeper *Registration Authority Level of Assurance* (LOA) 4 (very high confidence) and be cleared to the required level in accordance with the PKI System Security Plan (SSP).

Referenced documents are listed in Appendix A.

1.2 Document name and identification

The title for this CP is the "X.509 Certificate Policy for the Department of Defence – Public Root Certificate Authority and Subordinate Certificate Authorities". The Object Identifier (OID) for the ADPRCA CP is: **1.2.36.1.334.1.1.1.7**

{iso (1) iso-member (2) australia (36) government (1) department of defence (334) pki (1) public (1) CA - certificate policy (1) public root CA (7)}

In addition, this CP is issued for any Sub CA that is signed by the ADPRCA. In these circumstances, the OID is: 1.2.36.1.334.1.1.1.8

{iso (1) iso-member (2) australia (36) government (1) department of defence (334) pki (1) public (1) CA – certificate policy (1) public sub CA (8) }

1.3 PKI participants

1.3.1 Certification authorities

The Certification Authorities (CAs) that issue certificates under this CP are Defence CAs.

This CP relates to:

i. the self-signed ADPRCA authentication certificates that the ADPRCA issues to itself;
ii. the authentication and confidentiality certificates signed by the ADPRCA and issued to Sub CAs;
iii. the authentication and confidentiality certificates issued by the Sub CAs for the core operational infrastructure, e.g. the Registration Authority (RA) server; the Key Archive Server (KAS); and
iv. all *Operator* certificates used for the purpose of maintenance and issuance responsibilities, such as CA Operators (CAO), RA Auditors (RAA), *Registration Officers* (ROs) and *Trusted Agents (TAs).*

1.3.2 Registration authorities

The *Registration Authority* (RA), or RAs, that perform the registration functions under this CP are authorised by the Defence PKI Policy Management Authority (PKI PMA). For those certificates issued in accordance with the Gatekeeper accreditation, a Gatekeeper accredited RA must be used. An RA is formally bound to perform the registration functions in accordance with this CP and other relevant *Approved Documents.*

1.3.3 Subscribers

As a CA issues certificates to another party in accordance with the appropriate CP, they are not considered a *Subscriber*.

Subscribers of this CP are the other PKI core components and the Operators of core components. Such certificates are only valid for use with the core components.

Operator certificates are used for the identification, authentication and non-repudiation of the individual and their actions within the PKI core components that they have been given authority and access.

All Operators are *Key Custodians* of their own private keys. Key Custodians for all other PKI core component keys are listed in the PKI KMP.

An entity issued a certificate under this CP must have access, authority or privilege to Defence assets or systems.

1.3.4 Relying Parties

Other than the chain of trust aspects there are no Relying Parties for the certificates issued under this CP. This chain of trust is created by the ADPRCA signing the Sub CA certificate that signs the certificate issued to the end-entity and the issuance of *Certificate Revocation Lists* (CRLs).

Relying Parties are bound by the relevant CP that an end-entity certificate is issued under.

1.3.5 Other participants

See CPS.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

Certificates issued under this CP, in conjunction with their associated *private keys*, allow the ADPRCA to digitally:

i. self-sign the ADPRCA certificate;
ii. sign a Sub CA certificate;
iii. sign the operational certificates required by the PKI, including OCSP responder;
iv. sign its own internal log files; and
v. sign any CRLs it generates

Certificates issued under this CP, in conjunction with their associated private keys, allow a Sub CA to digitally sign:

i. end-entity certificates (as per approved end-entity CPs);
ii. a certificate for any CA subordinate to the Sub CA;
iii. the operational certificates required by the Sub CA;
iv. its own internal log files; and
v. sign any CRLs it generates.

All other core component certificates will only be valid for use within the PKI and used for the authentication, non-repudiation and confidentiality (as appropriate) of core component activities.[2]

1.4.2 Prohibited certificate uses

The prohibited uses for certificates issued under this CP are:

i. for the ADPRCA, to sign certificates issued to end-entity Subscribers;
ii. to sign the certificate of a non PKI PMA approved CA; and

[2] NB. ROs operating the TMS use their Individual - High Assurance certificate to log in to the system.

iii. using (or configuring any resource to use) any certificate for any transaction or communication, which is any or all of the following:

- Unrelated to Defence business and/or the appropriate certificate uses;
- Illegal;
- Unauthorised;
- Unethical, or
- 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 of the CPS also applies to this CP.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

See CPS.

2.2 Publication of certification information

Defence publishes CA certificates, and the issuing CA's latest CRL in its repository. This information is available to Relying Parties both internal and external of Defence.

Defence provides for Subscribers and Relying Parties the URL of a website which Defence uses to publish:

i. this CP;
ii. the CP for any end entity certificates; and
iii. the CPS.

2.3 Time or frequency of publication

Published documentation is updated on approved changes.

Defence CAs publish new certificates and CRLs as operationally required (see 4.9.7 and relevant CP).

2.4 Access controls on repositories

See CPS.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

Every certificate issued under this CP must have:

i. a clear distinguishable and unique Distinguished Name (DN) in the certificate subjectName field;
ii. the DN in the form of an X.501 printable string and not blank; and
iii. the DN approved by the PKI PMA.

3.1.2 Need for names to be meaningful

Names used to identify the PKI core components are based on their PKI role and CA Name. Additionally, names are used to identify individual Operators to allow for system auditing.

i. The Root CA DN must be Australian Defence Public Root CA with a Generation ([Gen]) field, comprised of G<integer> being added to each new generation Root CA. and
ii. the Sub CA's DN must be one of:

   - Australian Defence Public Identity CA ([Gen]);
   - Australian Defence Public Device CA ([Gen]);
   - Australian Defence Public Identity CA AutoEnrol ([Gen]);
   - Australian Defence OSN Identity CA ([Gen]); or
   - Australian Defence OSN Device CA ([Gen]).

3.1.3 Anonymity or 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

Common names must be unique within the Defence Public 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

Private Key generation of critical PKI core components is performed using a *Hardware Security Module* (HSM) that has undergone a security evaluation though an *Australian Signals Directorate* (ASD) recognised evaluation program. These private keys are generated internally which ensures that the private key is never exposed or accidentally released. To initiate the key generation process the CA Operator must use the HSM in the presence of the required staff as dictated by the Key Management Plan (PKI KMP).

All Operators must use hard token technology to generate and securely store private keys, with passphrase access controls. The key generation process requires the Operator to enter their token's passphrase thereby proving the Operator has possession of the token with the generated private key.

PKI Operator[3] tokens must be secured in the NLZ when not in use. All operators are responsible for all activity logged using their issued token.

3.2.2 Authentication of Organization Identity

To establish the ADPRCA or a Gatekeeper compliant Sub CA, the PKI PMA and the Gatekeeper Competent Authority must grant approval prior to the key generation ceremony. The establishment of other Defence Sub CAs requires PKI PMA approval prior to key generation. As a minimum, two PKI PMA delegates must witness the CA key generation ceremony. If required by external requirements or cross-certification arrangements, external representatives or another method (e.g. videotaping) may witness the generation ceremony.

Generation of PKI core components must comply with the processes dictated in the KMP, which indicates that the key issuing process includes:

i. identification of the infrastructure element and applicable Key Custodian;
ii. witnessed generation of public and private keys;
iii. generation of certificates;
iv. verification by the Key Custodian that the key generation process was successful; and
v. entry into the PKI Trusted Element Register of the applicable information concerning the newly generated key.

3.2.3 Authentication of individual identity

This CP is for Public CAs, their respective core component certificates, and the Operator certificates to manage them. As per the CPS, section 5.2, Operators are Trusted Roles and as such must be identified and authenticated in accordance with the PKI Information and Communications Technology Security Policy (ICTSP) and System Security Plan (SSP).

In essence, before certificates are issued Operators they are required to:

i. undergo a face-to-face identity verification that complies with the Gatekeeper Evidence of Identity (EOI) policy for a Gatekeeper LOA of 4 (Very High Confidence);
ii. be cleared to a minimum level of Negative Vet (NV) 2 (except ROs and TA, who must have a minimum of NV1);
iii. be confirmed as being affiliated with Defence (via their existence in the Defence Directory); and
iv. be approved by the PKI Operations Manager to access the PKI environment.

[3] Trusted Roles (including CAOs, RAAs, etc) who manage PKI operations within the Defence Certificate and Directory Management team.

3.2.4 Non-verified Subscriber information

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

3.2.5 Validation of authority

The *PKI Operations Manager* is responsible for ensuring that all PKI core components are validated in accordance with the PKI KMP.

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 minimum identification and authentication requirements for routine re-key are as per 3.2.2 (Authentication of Organization Identity).

Verification of the Operator's identity can occur as follows:

i. as per initial registration; or
ii. use of a PKI PMA approved biometric. (Only if biometric was recorded during previous registration); or
iii. proof of possession, and ability to exercise a current private key in which the Common Name of the DN matches a Federal or State Government issued photographic ID document. This method can only be used provided no more than 6 years has passed since the Operator has been identified using the Gatekeeper EOI policy for a Gatekeeper LOA of 4 (Very High Confidence), or uses an approved biometric.

The PKI PMA may approve alternative methods to verify an Operator's identity for special circumstances. These circumstances include:

i. essential re-key in locations where sufficient EOI is unavailable (e.g. Theatre of Operation); or
ii. if such individuals do not have sufficient EOI documentation due to loss, theft or destruction of EOI documentation.

Certificates issued under special circumstances will require authorisation by the PKI PMA based on the risks associated with the circumstances. This authorisation will impose a limit on the reuse of the method by the Operator before reverting to standard method of verification (listed above). In addition, such certificates will have a defined validity period that is less than the normal certificate life of two years.

3.3.2 Identification and authentication for re-key after revocation

Re-key is not allowed after revocation for CAs.

For all other core components, and related Operators, re-key after revocation shall occur in the same manner as for initial identity validation.

3.4 Identification and authentication for revocation request

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

The PKI PMA must approve all requests for revocation of Defence CAs. Revocation of other core components, and PKI Operator certificates, are to be authenticated and approved by the PKI Operations Manager or PKI Team Lead, or the PKI Security Officer (SO).

Revocation of RO and TA certificates can be authenticated and approved by a PKI Operator.

Revocation requests should be digitally signed and sent from a valid Defence email address.

An approved[4] Operator must validate that the requestor is authorised to revoke the certificate (refer to 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 (refer to 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.

Followed by approval to revoke as described above.

Revocation of PKI core component and Operator certificates requires dual approval, e.g. if the requestor or first approver is a PKI Operator, another approved Operator must also approve the request.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate application

4.1.1 Who can submit a certificate application

People affiliated with Defence can submit a certificate application. Creation of CAs must be authorised by the PKI PMA. There is no subsequent submission of applications for the creation of PKI core components related to that CA, except those related to Operator certificates.

4.1.2 Enrolment process and responsibilities

The enrolment process and responsibilities are outlined in the PKI Operations Manual and PKI KMP.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

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

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

As a minimum, two delegates nominated by the PKI PMA are required to witness the generation of CA keys.

To initiate the CA key generation process the PKI Operator must use a HSM in a No-Lone Zone (NLZ) in the presence of competent staff.

[4] Approved means an operator with the applicable permissions for the certificate type.

Identification and authentication of all other PKI core components must be performed in accordance with the processes outlined in the PKI Operations Manual and KMP.

Note: Existing Operators or the PKI SO must perform identification and authentication of Operator applicants.

The PKI Operations Manager is not required to investigate or ascertain the authenticity of any document received by them as evidence of any matter required as part of the CA creation process unless they are aware, or should reasonably be aware, that the document is not authentic or they are otherwise required to do so by law.

4.2.2 Approval or rejection of certificate applications

The PKI PMA must approve or reject CA certificate applications.

The PKI Operations Manager must approve or reject other core components and PKI Operator certificate applications.RO and TA applications must be approved by the relevant Business area (owner of the resources etc.) prior to a request. The PKI SO must validate the applicant's clearance and a PKI Operator must confirm that the applicant has satisfied the application requirements.

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

Operators will be notified when a certificate has been issued and, where applicable, of any requirements necessary to update the Operator's token.

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

CA certificates will be published externally. Other certificates are published to Defence repositories as per the 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 issued to PKI core components and Operators, not end entity Subscribers. Certificates and their associated private key usage is defined above in 1.4 (Certificate Usage) and key usage parameters (see 6.1.7).

Other than the CA certificates, all other certificates and private keys are only used within the PKI environment.

Key Custodians (refer to 1.3.3) must ensure that:

i. the private key is protected from access by unauthorised 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.

If the extended key usage extension is present and implies any limitation on the use of the certificate and/or private key, the CA will operate within those limitations.

4.5.2 Relying Party public key and certificate usage

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

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

4.6.1 Circumstance for certificate renewal

CA certificates and revoked certificates cannot be renewed. See CPS for certificate renewal criteria applicable for other Core components. Where certificate renewal is permitted, it must not be used to avoid certificate re-key (i.e. generating a new key pair and a new CSR) or the associated identification and authentication processes.

4.6.2 Who may request renewal

Only the existing Key Custodian, or the PKI Operations Manager, can request renewal of a certificate.

Approval of renewal requests is as per 4.2.2 (Approval or rejection of certificate applications).

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 (Certificate Application processing), however identification and authentication complies with 3.3 (Identification and Authentication for Re-Key Requests).

4.6.4 Notification of new certificate issuance to Subscriber

Operators shall be notified when a “renewal” certificate has been issued and of any requirements necessary to update the Operator’s token.

4.6.5 Conduct constituting acceptance of a renewal certificate

Use of the certificate constitutes acceptance.

4.6.6 Publication of the renewal certificate by the CA

Renewed certificates are published to Defence repositories as per the CPS.

4.6.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.7 Certificate re-key

Re-key of a certificates indicates creating a replacement 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 CA.

4.7.1 Circumstance for certificate re-key

See CPS for relevant circumstances. Loss or compromise of a current private key requires revocation.

4.7.2 Who may request certification of a new public key

Only the current Key Custodian, the PKI Operations Manager or the PKI PMA can request re-key of a certificate.

Approval of re-key requests is as per 4.2.2 (Approval or rejection of certificate applications).

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 (Certificate Application processing), however identification and authentication complies with 3.3 (Identification and Authentication for Re-Key Requests).

4.7.4 Notification of new certificate issuance to Subscriber

The Operator receives notification when a re-keyed certificate is issued, or if a certificate request for re-key is rejected.

The PKI PMA receives notification of progress, issues and completion of PKI PMA initiated certificate re-keys.

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

Re-keyed certificates are published to Defence repositories as per the CPS.

4.7.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

The circumstances permitted for certificate modification include:

i. Details in the certificate relevant to the Operator have changed or been found to be incorrect; and

ii. Interoperation with approved "Third Party" PKI, or Defence assets and systems, require certificate attributes or contents inserted, modified or deleted.

The PKI PMA will determine other circumstances as appropriate.

A modified certificate is required to maintain the same level of trust and assurance as the original issued certificate.

4.8.2 Who may request certificate modification

Only the current Key Custodian, the PKI Operations Manager, or the PKI PMA can request a certificate modification.

Approval of certificate modification requests is as per 4.2.2 (Approval or rejection of certificate applications).

4.8.3 Processing certificate modification requests

The process for certificate modification is consistent with 4.2 (Certificate application processing). . The identification and authentication procedures must comply with 3.3 (Identification and Authentication for Re-Key Requests).

4.8.4 Notification of new certificate issuance to Subscriber

The Operator or Key Custodian receives notification when issued a modified certificate, or if rejection of a modification request occurs.

The PKI PMA receives notification of progress, issues and completion of PKI PMA initiated certificate modifications.

4.8.5 Conduct constituting acceptance of modified certificate

Use of the certificate constitutes acceptance.

4.8.6 Publication of the modified certificate by the CA

Modified certificates are published to Defence repositories as per the CPS.

4.8.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

See CPS.

4.9.2 Who can request revocation

Revocation requests may be submitted by any authorised party (see CPS).

Revocation requests for:

- **CA certificates** must be approved by the PKI PMA.
- **Core components** and associated **Operator certificates** (except RO or TA certificates) must be approved by the PKI Operations Manager.
- **RO** or **TA** certificates may be approved by Operators.

4.9.3 Procedure for revocation request

Prior to commencing the revocation request procedure all revocation requests must be approved as per 3.4 (Identification and Authentication for Revocation request).

Revocation requests may be submitted by digitally signed email to pki.ops@defence.gov.au, however a process of authenticating via other channels is outlined in section 3.4.

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.

4.9.3.1 PKI core component certificates

Revocation requests for PKI core components are processed by a PKI Operator with CA Operator (CAO) permissions. The request must be validated by the PKI Operations Manager prior to initiation. The Disaster Recovery and Business Continuity Plan (DRBCP) details the revocation process for any Defence CA in the event of an emergency.

After verification, and if the revocation request is approved, the PKI Operator processes revocation requests by using the PKI software, which captures an auditable record of the process.

After a certificate is revoked, the issuing CA includes the revoked certificate's details (certificate serial number) and a reason code (if entered) in the CRL that is signed by the CA and published in the repositories.

4.9.3.2 Operator certificates

Revocation requests for Operator certificates are verified on receipt in accordance with 3.4 (Identification and authentication for revocation requests) and processed in priority order. Prior to revocation, the requestor and reasons are documented.

The PKI Operations Manager must approve the revocation request entry for a PKI Operator certificate prior to processing. Dual approval by Operators is required for all other Operator revocation requests, other than where an Operator has self-requested revocation.

After verification, and if the revocation request is approved, the relevant Operator processes revocation requests by using the PKI software, which captures an auditable record of the process.

After a certificate is revoked, where applicable, the CA includes the revoked certificate's details (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 an authorised party 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), 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, once all approvals and validations have been completed.

4.9.6 Revocation checking requirement for Relying Parties

Before using a certificate, the Relying Party must validate it against the CRL or OCSP. It is the Relying Party's responsibility to determine their requirement for revocation checking.

4.9.7 CRL issuance frequency (if applicable)

CRLs for the ADPRCA are published when a Sub CA is revoked or monthly.

CRLs for Sub CAs 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

See 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

This CP does not support certificate suspension.

4.9.14 Who can request suspension

This CP does not support certificate suspension.

4.9.15 Procedure for suspension request

This CP does not support certificate suspension.

4.9.16 Limits on suspension period

This CP does not support certificate suspension.

4.10 Certificate status services

See CPS.

4.11 End of subscription

See CPS.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

Escrow, backup and archiving of private keys issued under this CP is permitted to enable the retrieval of keys in a disaster recovery situation, including the backup of PKI Operator tokens. However, RO or TA hard tokens shall not be backed up or cloned.

Escrow, backup and archiving is to be undertaken in accordance with the PKI KMP.

Retrieval will be undertaken in accordance with the PKI DRBCP recovery policy and practices.

4.12.2 Session key encapsulation and recovery policy and practices

Symmetric keys are not required to be escrowed.

5. Facility, Management, and Operational Controls

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

6.1 Key pair generation and installation

6.1.1 Key pair generation

Key pair generation is via a combination of product and processes approved by the National Cryptographic Authority (NCA). Key pair generation is in accordance with the PKI KMP and as such:

i. critical core components (e.g. CA, RA and KAS) generate keys within a HSM;
ii. Operators generate keys within a hard token; and
iii. non-critical core components (e.g. Certificate Status Server, Registration Authority Exchange) generate keys using ASD recognised security evaluated software (and protect them within Personal Security Environment (PSE) files).

6.1.2 Private Key delivery to Subscriber

Private key delivery is in accordance with the PKI KMP.

Private keys generated within hardware elements (tokens, HSMs) are not delivered. Soft tokens for core components are delivered direct to the PKI core component protected by a PSE file.

6.1.3 Public key delivery to certificate issuer

ADPRCA public keys are self generated and do not require delivery.

SubCA public key delivery to the ADPRCA is a witnessed event, with the key being delivered via airgap in a PKCS#10 file, signed with the corresponding private key.

Other PKI core components' public keys are either delivered protected within the PKI software, or delivered to the issuer in a PKCS#10 file, signed with the corresponding private key.

6.1.4 CA public key delivery to Relying Parties

See CPS.

6.1.5 Key sizes

Keys used for this CP are in accordance with the PKI KMP and support SHA2 for signing and RSA public key algorithm. The key sizes for:

i. ADPRCA is a minimum of 2048 bits;
ii. Sub CAs and components, other than operators, are a minimum 2048 bits; and
iii. Operators are a minimum 2048 bits.

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)

Certificates include key usage extension fields to specify the purposes for which the Certificate may be used (see section 1.4) and also to technically limit the functionality of the certificate when used with the PKI software.

Note that the CAs have key usages "Digital Signature" and "Non-Repudiation" for the purpose of signing their own log entries.

Key usages for CA certificates are specified in the Certificate Profiles set forth in Appendix B.

6.2 Private key protection and cryptographic module engineering controls

6.2.1 Cryptographic module standards and controls

All cryptographic modules used with PKI core components must have undergone a security evaluation though an NCA or Defence recognised evaluation program and be approved for the uses intended in this CP by the PKI PMA.

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

See CPS.

6.2.3 Private Key escrow

Escrow of private keys, other than Operator tokens, is permitted and occurs in accordance with the PKI KMP and the PKI DRBCP. Refer to CPS for escrow controls.

6.2.4 Private Key backup

See CPS.

6.2.5 Private Key archival

Private Key archival occurs in accordance with the PKI KMP and the PKI DRBCP.

6.2.6 Private Key transfer into or from a cryptographic module

Transfer of private keys into or from a cryptographic module is permitted where authorised in the KMP (to enable duplication of critical core components) or where they are clustered for high availability or redundancy purposes. The Key Custodian must protect private keys during the transfer by an approved cryptographic algorithm of at least the same strength as the key being transferred.

6.2.7 Private Key storage on cryptographic module

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

6.2.8 Method of activating private key

Activating private keys occurs by the CAO or RAO or Key Custodian authenticating to the cryptographic module. For HSMs it is activated with the applicable physical key in the *PIN Entry Device* (PED). The session stays live until deactivated (see 6.2.9 - Method of deactivating private key).

6.2.9 Method of deactivating private key

Deactivation can be achieved via:

i. shut down or restart of the system;
ii. removal of the token; or
iii. shut down of the service that operates the token.

6.2.10 Method of destroying private key

See CPS.

6.2.11 Cryptographic Module Rating

See 6.2.1 (Cryptographic 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

The ADPRCA certificate validity has a maximum period of twenty (20) years to limit the key lifetime.

A Sub CA certificate may have a validity period of up to ten (10) years.

Certificate lives and key pair usage for all other core components, other than Operators, complements the relevant CA they are associated with.

Operator certificates have a maximum validity period of two years.

For further information, refer to Appendix B Certificate Profiles and CPS.

6.4 Activation data

6.4.1 Activation data generation and installation

To protect private keys, a passphrase is entered by the Key Custodian at the time of key generation. This passphrase is used to activate the key pair for usage.

Other passphrases and PINs used within the PKI system are created by Operators at the time of installation. All passwords must comply with Defence Password Policy.

Lifecycle management of passphrases, passwords and PINs used in the system is in accordance with the PKI KMP and Defence Policy.

6.4.2 Activation data protection

Lifecycle management of passphrases, passwords and PINs used in the system is in accordance with Defence policy and 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 for the ADPRCA, its Sub CAs, and their associated CRLs.

Certificate profiles for other Core components and operator certificates are documented in internal documentation.

OCSP certificate profiles are documented in the Validation Authority (VA) CP.

7.1 Certificate profile

7.1.1 Version Numbers

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.

rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
Id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-x9-62(10045) public-key-type (2) 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

CAs shall certify only public keys associated with the crypto-algorithms identified above, and shall only use the signature crypto-algorithms described above to sign certificates, CRLs and any other PKI product, including other forms of revocation such as OCSP responses.

7.1.4 Name Forms

Name forms are to be presented as a printable string. Refer to 3.1.2 (Need for names to be meaningful) in regards to the naming convention. Also, refer to Appendix B and the CPS for further information.

7.1.5 Name Constraints

Name constraints are not present.

7.1.6 Certificate Policy Object Identifier

CA Certificates issued under this policy shall assert the OID **{1.2.36.1.334.1.1.1.7}** for ADPRCA certificates or **{1.2.36.1.334.1.1.1.8}** for Sub CA certificates.

The ADPRCA and Sub CA certificates shall also assert the "any Policy" OID of {**2.5.29.32.0**}.

The Sub CA certificates shall also assert the following OIDs representing *Levels of Assurance* of certificates issued:

Individual:	Low	1.2.36.1.334.1.2.1.1
	Medium	1.2.36.1.334.1.2.1.2
	High	1.2.36.1.334.1.2.1.3
	Very High	1.2.36.1.334.1.2.1.4
Resources:	Low	1.2.36.1.334.1.2.2.1
	Medium	1.2.36.1.334.1.2.2.2
	High	1.2.36.1.334.1.2.2.3

Table 3 – Level of Assurance OIDs

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 policy 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 Numbers

CRLs issued under this CP shall assert a version number as described in the X.509 standard [ISO9594-8]. CRLs shall assert Version 2.

7.2.2 CRL and CRL Entry Extensions

Detailed CRL profiles covering the use of each extension are available in Appendix B.

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

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 a 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

See CPS.

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

9.2.1 Insurance coverage

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.

9.4 Privacy of personal information

9.4.1 Privacy plan

No Personal Information (as defined in the *Privacy Act 1988*) will be collected during the creation of the ADPRCA or a Sub CA but it will be collected for the issuance of Operator certificates. If personal information is gathered, the collection, use and disclosure of such information is governed by the Privacy Act 1988 (Cth) (Privacy Act) and the Information Privacy Act 2014 (Cth).

The Defence PKI Privacy Notice is available from https://crl.defence.gov.au/pki

9.4.2 Information treated as private

Not applicable for core components other than Operators. The PKI only retains details of EOI documentation presented and the unique document identifiers. This information is to be stored in accordance with Defence requirements, and protected in accordance with the requirements of the PKI Privacy Notice. Personal Information of Operators is not to be published outside of the PKI.

9.4.3 Information not deemed private

Not applicable for core components other than Operators. By accepting their role as an Operator, an Operator acknowledges that their email address and name may be contained in their Operator certificate and may be disclosed.

Revocation of a Certificate requires publishing in the CRL in accordance with this CP. Revocation information is not treated as private.

9.4.4 Responsibility to protect private information

See CPS.

9.4.5 Notice and consent to use private information

Not applicable for core components other than Operators. Acknowledgement by the Operator to the use of Personal Information is provided during induction into the PKI.

9.4.6 Disclosure pursuant to judicial or administrative process

See CPS.

9.4.7 Other information disclosure circumstances

No stipulation

9.5 Intellectual property rights

See CPS.

9.6 Representations and warranties

See CPS.

However, any representations and warranties given by a Subscriber pursuant to the CPS do not apply.

9.7 Disclaimers 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

No Stipulation.

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
[EOI]	Gatekeeper Evidence of Identity (EOI) policy available at https://www.dta.gov.au/standard/design-guides/authentication-frameworks/national-e-authentication-framework
[GK2015]	Digital Transformation Office, Gatekeeper PKI Framework v3.1 Dec 2015, available at https://www.dta.gov.au/standard/design-guides/authentication-frameworks/gatekeeper-public-key-infrastructure-framework/
[PKI 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
[OID Register]	Defence OID Register; a register maintained by PKI Operations, which lists all current Defence PKI and DCD OIDs.
[SSP]	Australian Department of Defence System Security Plan Defence Public Key Infrastructure (classified)
[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 4 - References

APPENDIX B. CERTIFICATE AND CRL PROFILES AND FORMATS

B.1 ADPRCA Signature/Authentication Certificate

Field	Critical	Defence Root Certificate Value	Notes
Version		V3 (2)	Version 3 of X.509
Serial		<octet string>	Must be unique within Defence namespace
Issuer Signature Algorithm		SHA-2WithRSAEncryption	

Issuer Distinguished Name		CN= Australian Defence Public Root CA [G<integer>]
		OU= CAs
		OU= PKI
		OU= DoD
		O= GOV
		C= AU
			Encoded as printable string.
			[G<integer>] is an optional extension for future generations of the public root CA.

Validity Period		Not before <UTCtime> Not after <UTCtime>	Maximum 20 years from date of issue

Subject Distinguished Name		CN= Australian Defence Public Root CA [G<integer>]
		OU= CAs
		OU= PKI
		OU= DoD
		O= GOV
		C= AU
			Encoded as printable string.
			[G<integer>] is an optional extension for future generations of the public root CA.

Subject Public Key Information		Minimum 2048 bit RSA key modulus, rsaEncryption	
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 the issuing CA's public key[5]
Subject Key Identifier	No	<octet string>	160 bit SHA-1 hash of binary DER encoding of subject's public key
Key usage	Yes	digitalSignature, nonRepudiation, Certificate signing, CRLsigning, Off-line CRL signing	Digital signature and non-repudiation key usages are present to allow for the signing of the CA's own log entries.
Extended key usage		Not Present	

[5] 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	Defence Root Certificate Value	Notes
Private key usage period		Not Present	
Certificate policies	No	[1] Policy OID: {1.2.36.1.334.1.1.1.7} Policy Qualifier - CPS pointer: http://crl.defence.gov.au/pki	The OID of this CP (RCA)
		[2] Policy OID: {2.5.29.32.0}	anyPolicy OID
Policy Mapping		Not Present	
Subject Alternative Name		Not Present	
Issuer Alternative Name		Not Present	
Subject Directory Attributes		Not Present	
Basic Constraints	Yes	CA=True, path length constraint=none	
Name Constraints		Not Present	
Policy Constraints		Not Present	
Authority Information Access		Not Present	
CRL Distribution Points		Not Present	

Table 5 – Defence Root Certification Authority Signature/Authentication Certificate Profile

B.2 ADPRCA CRL

See RFC5280 for detailed syntax. The following table lists which fields are expected.

Field	Critical	Defence Root CA CRL Value	Notes
Version		V2 (1)	X.509 Version 2 CRL profile
Issuer Signature Algorithm		SHA-2WithRSAEncryption	

Issuer Distinguished Name		CN= Australian Defence Public Root CA [G<integer>]
		OU= CAs
		OU= PKI
		OU= DoD
		O= GOV
		C= AU
			[G<integer>] is an optional extension for future generations of the public root CA.

thisUpdate		<UTCTime>	
nextUpdate		<UTCTime>	Date by which the next CRL will be issued (at the latest – if a certificate is revoked, a CRL will be issued at that time) thisUpdate + 365 days. The CRL will be issued as per Policy defined in 4.9.7 the nextUpdate value is used to determine when the CRLs validity expires.
Revoked certificates list		0 or more 2-tuple of certificate serial number and revocation date (in UTCTime)	
CRL extensions			
CRL Number	No	<Integer>	
Authority Key Identifier	No	<Octet String>	The value of this field is the 160 bit SHA-1 hash of the binary DER encoding of the CA public key information[6]
CRL entry extensions			
Invalidity Date	No	Optional	Date on which it is known or suspected that the private key was compromised or that the certificate otherwise became invalid.
Reason Code	No	Optional	A meaningful reason code must be included in the entry for a revoked CA. (CABForum)

Table 6 – Defence Root CA CRL Profile

[6] 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.

B.3 SUB CA SIGNATURE/AUTHENTICATION CERTIFICATE

Field	Critical	Sub-Certification Authority Certificate Value	Notes
Version		V3 (2)	Version 3 of X.509
Serial		<octet string>	Must be unique within Defence namespace
Issuer Signature Algorithm		SHA-2WithRSAEncryption	

Issuer Distinguished Name		CN= Australian Defence Public Root CA [G<integer>]
		OU= CAs
		OU= PKI
		OU= DoD
		O= GOV
		C= AU
			Encoded as printable string.
			[G<integer>] is an optional extension for future generations of the public root CA.

Validity Period		Not before <UTCtime> Not after <UTCtime>	Maximum 10 years from date of issue

Subject Distinguished Name		CN= Australian Defence <network> <type> <optional type variant> CA [G<integer>]
		OU= CAs
		OU= PKI
		OU= DoD
		O= GOV
		C= AU
			Encoded as printable string.
			<network> = Public or OSN
			<type> = Identity or Device
			<optional type variant> - e.g. "Autoenrol"
			[G<integer>] is an optional extension for future generations of the public root CA.
			e.g: Australian Defence Public Identity CA or Australian Defence OSN Device CA.

Subject Public Key Information		Minimum 2048bit RSA key modulus, rsaEncryption	
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 the issuing CA's public key[7]
Subject Key Identifier	No	<octet string>	160 bit SHA-1 hash of binary DER encoding of subject's public key
Key usage	Yes	digitalSignature, nonRepudiation, Certificate Signing, Off-line CRL Signing, CRL Signing	Digital signature and Non repudiation key usages are present to allow for signing the CA's own log entries.
Extended key usage		Not Present	

[7] 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	Sub-Certification Authority Certificate Value	Notes
Private key usage period		Not Present	
Certificate policies	No	[1] Policy OID: {1.2.36.1.334.1.1.1.8} (this CP/SubCAs) Policy Qualifier - CPS pointer: http://crl.defence.gov.au/pki	The OID of this CP (SubCA)
		[2] Policy OID: {2.5.29.32.0}	OID for "anyPolicy"
		[3] Policy OID: {1.2.36.1.334.1.2.1.1} (Individual – Low Assurance)	
		[4] Policy OID: {1.2.36.1.334.1.2.1.2} (Individual – Medium Assurance)	
		[5] Policy OID: {1.2.36.1.334.1.2.1.3} (Individual - High Assurance)	
		[6] Policy OID: {1.2.36.1.334.1.2.1.4} (Individual – Very high Assurance)	
		[7] Policy OID: {1.2.36.1.334.1.2.2.1} (Resource – Low Assurance)	
		[8] Policy OID: {1.2.36.1.334.1.2.2.2} (Resource – Medium Assurance)	
		[9] Policy OID: {1.2.36.1.334.1.2.2.3} (Resource – High Assurance)	
Policy Mapping		Not Present	
Subject Alternative Name		Not Present	
Issuer Alternative Name		Not Present	
Subject Directory Attributes		Not Present	
Basic Constraints	Yes	CA=True, Path length constraint=0	
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/ADPRCA[G<integer>]
		[3]Access method: CA Issuer {1.3.6.1.5.5.7.48.2}
		Access location: ldap://dir.defence.gov.au/cn=Australian Defence Public Root CA [G<integer>],ou=CAs,ou=PKI, ou=DoD,o=GOV,c=AU?cACertificate;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).
			The AIA must reference the Issuing Authority.

CRL Distribution Points	No	[1] Distribution Point: http://crl.defence.gov.au/pki/crl/ADPRCA.crl [2] Distribution Point Name (ldap): ldap://dir.defence.gov.au/cn=Australian Defence Public Root CA [G<integer>],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 URL name form. The reason field may 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). The missing ";binary" at the end of the LDAP URI is a Unicert limitation.

Table 7 – Sub CA Signature/Authentication Certificate Profile

B.4 SUB CA CRL

See RFC5280 for detailed syntax. The following table lists which fields are expected.

Field	Critical	Defence Root CA CRL Value	Notes
Version		V2 (1)	X.509 Version 2 CRL profile
Issuer Signature Algorithm		SHA-2WithRSAEncryption	

Issuer Distinguished Name		CN= Australian Defence <network> <type> <optional type variant> CA[<G<integer>]
		OU= CAs
		OU= PKI
		OU= DoD
		O= GOV
		C= AU
			Encoded as printable string.
			<network> = Public or OSN
			<type> = Identity or Device
			<optional type variant> - e.g. "Autoenrol"
			[G<integer>] is an optional extension for future generations of the public root CA.

thisUpdate		<UTCTime>	
nextUpdate		<UTCTime>	Date by which the next CRL will be issued (at the latest – if a certificate is revoked, a CRL will be issued at that time) thisUpdate + 10 days
Revoked certificates list		0 or more 2-tuple of certificate serial number and revocation date (in UTCTime)	
CRL extensions			
CRL Number	No	<Integer>	
Authority Key Identifier	No	<Octet String>	The value of this field is the 160 bit SHA-1 hash of the binary DER encoding of the CA public key information[8]
CRL entry extensions			
Invalidity Date	No	Optional	Date on which it is known or suspected that the private key was compromised or that the certificate otherwise became invalid.
Reason Code	No	Optional	

Table 8 – Sub CA CRL Profile

[8] 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.