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

Version 5.0
July 2019
Notice to all parties seeking to rely

Reliance on a Certificate issued under this Certificate Policy, identified by subarcs of the object identifier 1.2.36.1.334.1.1.1.3 for the Defence Interoperability CA (DIOCA) CP 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 Board |
| Changes are authorised by: | Defence Public Key Infrastructure Policy Board |
| | Gatekeeper Competent Authority |

Change History

<table>
<thead>
<tr>
<th>Version</th>
<th>Issue Date</th>
<th>Description/ Amendment</th>
<th>Changed by</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>June 2011</td>
<td>Initial Draft</td>
<td>AKK</td>
</tr>
<tr>
<td>1.0</td>
<td>4 Aug 2011</td>
<td>Released</td>
<td>SJP</td>
</tr>
<tr>
<td>2.0</td>
<td>July 2012</td>
<td>Released</td>
<td>SJP</td>
</tr>
<tr>
<td>3.0</td>
<td>May 2014</td>
<td>Reviewed for release</td>
<td>PKI Ops Man</td>
</tr>
<tr>
<td>4.0</td>
<td>Oct 2016</td>
<td>Released</td>
<td>PKI Operations Manager</td>
</tr>
<tr>
<td>4.1</td>
<td>Nov 2016</td>
<td>Updated SHA2 certificate profile</td>
<td>Cogito Group (BB)</td>
</tr>
<tr>
<td>4.2</td>
<td>Sep 2017</td>
<td>CSO review</td>
<td>CSO</td>
</tr>
<tr>
<td>4.3</td>
<td>February 2018</td>
<td>Reviewed</td>
<td>PKI Operator (LM)</td>
</tr>
<tr>
<td>4.4</td>
<td>Dec 2018</td>
<td>Reviewed for GK</td>
<td>Ops Man</td>
</tr>
<tr>
<td>5.0</td>
<td>July 2019</td>
<td>Published</td>
<td>PKI Ops Man</td>
</tr>
</tbody>
</table>
## Signatures

<table>
<thead>
<tr>
<th>Appointment</th>
<th>Organisation</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defence PKI Policy Board (DPKIPB) Chair</td>
<td>Dept. of Defence (Defence)</td>
<td>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.</td>
</tr>
<tr>
<td>Gatekeeper Competent Authority (GCA)</td>
<td>Digital Transformation Agency (DTA)</td>
<td>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.</td>
</tr>
</tbody>
</table>
X.509 Certificate Policy

Contents

1. INTRODUCTION .......................................................................................................................... 9
   1.1 Overview ................................................................................................................................. 9
   1.2 Document name and identification ......................................................................................... 10
   1.3 PKI participants ...................................................................................................................... 11
       1.3.1 Certification authority ..................................................................................................... 11
       1.3.2 Registration authorities .................................................................................................. 11
       1.3.3 Subscribers ...................................................................................................................... 11
       1.3.4 Relying Parties ............................................................................................................... 11
       1.3.5 Other participants ........................................................................................................... 11
   1.4 Certificate usage ..................................................................................................................... 12
       1.4.1 Appropriate certificate uses ............................................................................................. 12
       1.4.2 Prohibited certificate uses ............................................................................................... 12
   1.5 Policy administration ........................................................................................................... 13
       1.5.1 Organisation administering the document ........................................................................ 13
       1.5.2 Contact person ............................................................................................................... 13
       1.5.3 Authority determining CPS suitability for the policy ....................................................... 13
       1.5.4 CPS approval procedures ............................................................................................... 13
   1.6 Definitions, acronyms and interpretation ............................................................................. 13

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES .......................................................... 13
   2.1 Repositories ............................................................................................................................ 13
   2.2 Publication of certification information ................................................................................ 13
   2.3 Time or frequency of publication ........................................................................................ 13
   2.4 Access controls on repositories ........................................................................................... 14

3. IDENTIFICATION AND AUTHENTICATION ............................................................................. 14
   3.1 Naming .................................................................................................................................. 14
       3.1.1 Types of names ................................................................................................................. 14
       3.1.2 Need for names to be meaningful .................................................................................... 14
       3.1.3 Anonymity or pseudonymity of Subscribers ................................................................. 14
       3.1.4 Rules for interpreting various name forms .................................................................... 14
       3.1.5 Uniqueness of names .................................................................................................... 15
       3.1.6 Recognition, authentication, and role of trademarks .................................................... 15
   3.2 Initial identity validation ......................................................................................................... 15
       3.2.1 Method to prove possession of private key ................................................................. 15
       3.2.2 Authentication of Organisation Identity ..................................................................... 15
       3.2.3 Authentication of individual identity ............................................................................ 16
       3.2.4 Non-verified Subscriber information ........................................................................ 16
       3.2.5 Validation of authority .................................................................................................. 16
       3.2.6 Criteria for interoperability .......................................................................................... 17
   3.3 Identification and authentication for re-key requests ............................................................ 17
       3.3.1 Identification and authentication for routine re-key ..................................................... 17
       3.3.2 Identification and authentication for re-key after revocation ..................................... 17
   3.4 Identification and authentication for revocation request .................................................... 17

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS ............................................ 18
   4.1 Certificate application ............................................................................................................ 18
       4.1.1 Who can submit a certificate application ................................................................. 18
       4.1.2 Enrolment process and responsibilities ................................................................. 18
   4.2 Certificate application processing ......................................................................................... 18
       4.2.1 Performing identification and authentication functions .......................................... 19
       4.2.2 Approval or rejection of certificate applications ....................................................... 20
X.509 Certificate Policy

4.2.3 Time to process certificate applications ........................................................................................................... 20

4.3 Certificate issuance .................................................................................................................................................... 20
4.3.1 CA actions during certificate issuance .................................................................................................................. 20
4.3.2 Notification to Subscriber by the CA of issuance of certificate ........................................................................... 20

4.4 Certificate acceptance ................................................................................................................................................ 20
4.4.1 Conduct constituting certificate acceptance ........................................................................................................... 20
4.4.2 Publication of the certificate by the CA .................................................................................................................. 20
4.4.3 Notification of certificate issuance by the CA to other entities ........................................................................... 20

4.5 Key pair and certificate usage .................................................................................................................................... 21
4.5.1 Subscriber private key and certificate usage .......................................................................................................... 21
4.5.2 Relying Party public key and certificate usage ....................................................................................................... 21

4.6 Certificate renewal ....................................................................................................................................................... 21
4.6.1 Circumstance for certificate renewal ....................................................................................................................... 21
4.6.2 Who may request renewal ......................................................................................................................................... 21
4.6.3 Processing certificate renewal requests .................................................................................................................... 21
4.6.4 Notification of new certificate issuance to Subscriber .......................................................................................... 21
4.6.5 Conduct constituting acceptance of a renewal certificate ....................................................................................... 21
4.6.6 Publication of the renewal certificate by the CA ...................................................................................................... 21
4.6.7 Notification of certificate issuance by the CA to other entities ........................................................................... 21

4.7 Certificate re-key .......................................................................................................................................................... 22
4.7.1 Circumstance for certificate re-key .......................................................................................................................... 22
4.7.2 Who may request certification of a new public key ................................................................................................. 22
4.7.3 Processing certificate re-keying requests .................................................................................................................. 22
4.7.4 Notification of new certificate issuance to Subscriber .......................................................................................... 22
4.7.5 Conduct constituting acceptance of a re-keyed certificate ..................................................................................... 22
4.7.6 Publication of the re-keyed certificate by the CA .................................................................................................. 22
4.7.7 Notification of certificate issuance by the CA to other entities ........................................................................... 22

4.8 Certificate modification ............................................................................................................................................. 22
4.8.1 Circumstance for certificate modification ............................................................................................................... 22
4.8.2 Who may request certificate modification ............................................................................................................ 22
4.8.3 Processing certificate modification requests ........................................................................................................... 23
4.8.4 Notification of new certificate issuance to Subscriber .......................................................................................... 23
4.8.5 Conduct constituting acceptance of modified certificate .................................................................................... 23
4.8.6 Publication of the modified certificate by the CA .................................................................................................. 23
4.8.7 Notification of certificate issuance by the CA to other entities ........................................................................... 23

4.9 Certificate revocation and suspension ............................................................................................................................ 23
4.9.1 Circumstances for revocation .................................................................................................................................. 23
4.9.2 Who can request revocation ................................................................................................................................... 23
4.9.3 Procedure for revocation request ........................................................................................................................... 23
4.9.4 Revocation request grace period ............................................................................................................................ 24
4.9.5 Time within which CA must process the revocation request ............................................................................... 24
4.9.6 Revocation checking requirement for Relying Parties ............................................................................................ 24
4.9.7 CRL issuance frequency (if applicable) .................................................................................................................. 24
4.9.8 Maximum latency for CRLs (if applicable) ............................................................................................................... 24
4.9.9 On-line revocation/status checking availability .................................................................................................. 24
4.9.10 On-line revocation checking requirements ........................................................................................................ 24
4.9.11 Other forms of revocation advertisements available .......................................................................................... 24
4.9.12 Special requirements re key compromise ........................................................................................................... 24
4.9.13 Circumstances for suspension ............................................................................................................................... 24
4.9.14 Who can request suspension .................................................................................................................................. 24
4.9.15 Procedure for suspension request .......................................................................................................................... 25
4.9.16 Limits on suspension period ................................................................................................................................... 25

4.10 Certificate status services ........................................................................................................................................ 25
X.509 Certificate Policy

4.11 End of subscription ................................................................. 25
4.12 Key escrow and recovery ......................................................... 25
  4.12.1 Key escrow and recovery policy and practices ...................... 25
  4.12.2 Session key encapsulation and recovery policy and practices ...... 25

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS ............ 25
  5.1 Physical controls .................................................................. 25
  5.2 Procedural controls ............................................................... 25
  5.3 Personnel controls ................................................................. 25
  5.4 Audit logging procedures ....................................................... 25
  5.5 Records archival ................................................................. 26
  5.6 Key changeover .................................................................. 26
  5.7 Compromise and disaster recovery ......................................... 26
  5.8 CA or RA termination ........................................................... 26

6. TECHNICAL SECURITY CONTROLS ............................................ 26
  6.1 Key pair generation and installation ....................................... 26
    6.1.1 Key pair generation ......................................................... 26
    6.1.2 Private Key delivery to Subscriber .................................... 26
    6.1.3 Public key delivery to certificate issuer ............................... 26
    6.1.4 CA public key delivery to Relying Parties .......................... 26
    6.1.5 Key sizes ..................................................................... 27
    6.1.6 Public key parameters generation and quality checking ....... 27
    6.1.7 Key usage purposes (as per X.509 v3 key usage field) ......... 27
  6.2 Private key protection and cryptographic module engineering controls 27
    6.2.1 Cryptographic module standards and controls ..................... 27
    6.2.2 Private Key (n out of m) multi-person control ...................... 27
    6.2.3 Private Key escrow ........................................................ 27
    6.2.4 Private Key backup ........................................................ 27
    6.2.5 Private Key archival ....................................................... 27
    6.2.6 Private Key transfer into or from a cryptographic module ...... 27
    6.2.7 Private Key storage on cryptographic module ..................... 27
    6.2.8 Method of activating private key ........................................ 28
    6.2.9 Method of deactivating private key .................................... 28
    6.2.10 Method of destroying private key ...................................... 28
    6.2.11 Cryptographic Module Rating ........................................ 28
  6.3 Other aspects of key pair management .................................... 28
    6.3.1 Public key archival ........................................................ 28
    6.3.2 Certificate operational periods and key pair usage periods .... 28
  6.4 Activation data ..................................................................... 28
    6.4.1 Activation data generation and installation ......................... 28
    6.4.2 Activation data protection ................................................ 28
    6.4.3 Other aspects of activation data ........................................ 28
  6.5 Computer security controls ................................................... 29
  6.6 Life cycle technical controls .................................................. 29
  6.7 Network security controls ..................................................... 29
  6.8 Time-stamping ..................................................................... 29

7. CERTIFICATE, CRL AND OCSP PROFILES ................................. 29
  7.1 Certificate profile ................................................................. 29
    7.1.1 Version Numbers ............................................................. 29
    7.1.2 Certificate Extensions ...................................................... 29
    7.1.3 Algorithm Object Identifiers ............................................. 29
    7.1.4 Name Forms .................................................................. 30
    7.1.5 Name Constraints .......................................................... 30
X.509 Certificate Policy

7.1.6 Certificate Policy Object Identifier ................................................................. 30
7.1.7 Usage of Policy Constraints Extension ............................................................... 30
7.1.8 Policy Qualifiers Syntax and Semantics ........................................................... 31
7.1.9 Processing Semantics for the Critical Certificate Policies Extension ................... 31

7.2 CRL profile ............................................................................................................. 31
7.2.1 Version Numbers ............................................................................................... 31
7.2.2 CRL and CRL Entry Extensions ....................................................................... 31

7.3 OCSP profile ......................................................................................................... 31
7.3.1 Version Numbers ............................................................................................... 31
7.3.2 OCSP Extensions .............................................................................................. 31

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS ............................................ 31

8.1 Frequency or circumstances of assessment ............................................................ 31
8.2 Identity/qualifications of assessor ........................................................................ 31
8.3 Assessor’s relationship to assessed entity .............................................................. 31
8.4 Topics covered by assessment ............................................................................. 32
8.5 Actions taken as a result of deficiency .................................................................. 32
8.6 Communication of results .................................................................................... 32

9. OTHER BUSINESS AND LEGAL MATTERS ......................................................... 32

9.1 Fees ........................................................................................................................ 32
  9.1.1 Certificate issuance or renewal fees ................................................................. 32
  9.1.2 Certificate access fees ..................................................................................... 32
  9.1.3 Revocation or status information access fees .................................................... 32
  9.1.4 Fees for other services ..................................................................................... 32
  9.1.5 Refund policy ................................................................................................ 32

9.2 Financial responsibility .......................................................................................... 32
  9.2.1 Insurance coverage ......................................................................................... 32
  9.2.2 Other assets .................................................................................................... 32
  9.2.3 Insurance or warranty coverage for end-entities .............................................. 32

9.3 Confidentiality of business information ................................................................. 33

9.4 Privacy of personal information ........................................................................... 33
  9.4.1 Privacy plan ..................................................................................................... 33
  9.4.2 Information treated as private ....................................................................... 33
  9.4.3 Information not deemed private ..................................................................... 33
  9.4.4 Responsibility to protect private information ................................................... 33
  9.4.5 Notice and consent to use private information ............................................... 33
  9.4.6 Disclosure pursuant to judicial or administrative process ............................... 33
  9.4.7 Other information disclosure circumstances ............................................... 33

9.5 Intellectual property rights .................................................................................... 33

9.6 Representations and warranties ............................................................................ 33

9.7 Disclaimers of warranties ..................................................................................... 34

9.8 Limitations of liability ........................................................................................... 34

9.9 Indemnities ............................................................................................................ 34

9.10 Term and termination .......................................................................................... 34
  9.10.1 Term ................................................................................................................ 34
  9.10.2 Termination .................................................................................................... 34
  9.10.3 Effect of termination and survival ................................................................. 34

9.11 Individual notices and communications with participants .................................... 34

9.12 Amendments ......................................................................................................... 35
  9.12.1 Procedure for amendment .......................................................................... 35
  9.12.2 Notification mechanism and period ............................................................... 35
  9.12.3 Circumstances under which OID must be changed ..................................... 35

9.13 Dispute resolution provisions .............................................................................. 35
X.509 Certificate Policy

9.14 Governing law ................................................................................................................. 35
9.15 Compliance with applicable law ......................................................................................... 35
9.16 Miscellaneous provisions ................................................................................................. 35
9.17 Other provisions ................................................................................................................. 35

APPENDIX A. REFERENCES ........................................................................................................ 36

APPENDIX B. CERTIFICATE, CRL AND OCSP PROFILES AND FORMATS ......................... 37

B.1 DIOCA SHA1 certificate [DIOCA-C] .................................................................................... 37
B.2 Principal SHA1 Cross Certificate [DIOCA-PXC] ..................................................................... 39
B.3 DIOCA SHA1 Secondary Cross Certificate [DIOCA-SXC] .................................................... 42
B.4 DIOCA SHA2 certificate [DIOCA-C] .................................................................................... 45
B.5 Principal SHA2 Cross Certificate [DIOCA-PXC] ..................................................................... 47
B.6 DIOCA SHA2 Secondary Cross Certificate [DIOCA-SXC] .................................................... 49
B.7 DIOCA SHA1 CRL ............................................................................................................... 52
B.8 DIOCA SHA2 CRL ............................................................................................................... 53

Table of Tables

Table 1 – Signature OIDs ............................................................................................................. 29
Table 2 – Algorithm OIDs .......................................................................................................... 29
Table 3 – Levels of Assurance ................................................................................................... 30
Table 4 - References .................................................................................................................. 36
Table 5 – DIOCA SHA1 Certificate [DIOCA-C] Profile ............................................................... 38
Table 6 - DIOCA SHA1 Principal Cross-Certificate [DIOCA-PXC] Profile ................................. 41
Table 7 - DIOCA SHA1 Secondary Cross-Certificate [DIOCA-SXC] Profile .............................. 44
Table 8 – DIOCA SHA2 Certificate [DIOCA-C] Profile ............................................................... 46
Table 9 - DIOCA SHA2 Principal Cross-Certificate [DIOCA-PXC] Profile ................................. 48
Table 10 – DIOCA SHA2 Secondary Cross-Certificate [DIOCA-SXC] Profile ......................... 51
Table 11 – DIOCA SHA1 CRL Profile ........................................................................................ 52
Table 12 – DIOCA SHA2 CRL Profile ........................................................................................ 53

Table of Figures

Figure 1 – Extended Bilateral Cross-certification model - example ........................................... 10
1. INTRODUCTION

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

This Certificate Policy (CP) identifies the rules to manage the Australian Government Department of Defence (Defence) Interoperability Certificate Authority (DIOCA) certificates. It is specifically written to describe the obligations of the Public Key Infrastructure (PKI) entities in relation to the issuing and use of certificates under a cross-certification trust model such as the one described in PKI Cross-certification between CCEB nations (ACP185).\(^1\) It does not describe how to implement these rules as that information is in the Defence PKI Certification Practice Statement (CPS), or documents referenced by the CPS. In general, the rules identify the minimum standards in terms of performance, security and/or quality.


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

This section identifies and introduces the set of provisions, and indicates the types of entities and applications applicable for this Defence Interoperability Certification Authority (DIOCA) Certificate Policy (CP).

1.1 Overview

The DIOCA is a Defence Root CA dedicated to issuing cross-certificates in order to execute CCAs entered into between the Defence PKI and other ("Peer") PKIs.

In the "extended bilateral cross-certification" model favoured by the Defence PKI (as described in ACP185), the Interoperability CA acts as a trusted root CA which creates the certificate paths required for end entities of a Defence Operational CA to trust end entities of a Peer PKI’s Operational CA.

The DIOCA issues two types of cross-certificates to assist the cross-certification of two PKIs:

i. Principal cross-certificate, which is the certificate in which the DIOCA signs a Peer PKI’s chosen Interoperability CA’s public key; and

ii. Secondary cross-certificate, in which the DIOCA signs the public key of a Defence Operational CA.

In order to fully establish the mutual trust intended by a CCA (i.e. so that end entities of the Peer PKI can trust end entities of the Defence PKI) the Peer PKI needs to issue the corresponding cross-certificates in which their chosen Interoperability CA has signed the DIOCA’s public key (Principal) and

\(^1\) Note that cross-certification is not limited to CCEB (Combined Communications Electronics Board) nations, however the model would stay the same, i.e. the “extended bilateral” trust model.
UNCLASSIFIED (PUBLIC DOMAIN)

X.509 Certificate Policy

Introduction

their own operational CA’s public key (Secondary). Those cross-certificates, issued by the Peer PKI, are not covered by this CP.

See example in Figure 1 – Extended Bilateral Cross-certification model.

![Diagram of ADO PKI Environment and Peer PKI Environment with cross-certification]

**Figure 1 – Extended Bilateral Cross-certification model - example**

Thus, this certificate policy covers four types of certificates:

i. The self-signed certificate of the DIOCA (“DIOCA-C”)

ii. Principal cross-certificates (to a Peer PKI) signed by DIOCA (“DIOCA-PXC”)

iii. Secondary cross-certificates (to a Defence Operational CA) signed by DIOCA (“DIOCA-SXC”)

iv. Certificates issued to the operators of the DIOCA to ensure their abilities to undertake administrative activities.

Note that cross-certification of a Peer PKI does not involve key generation: i.e. the DIOCA does not generate keys for DIOCA-PXC and DIOCA-SXC, it merely signs a certificate signing request associated with an already existing private key. Hence, sections of this document that refer to private key generation and management only apply to the DIOCA (and related operator) private keys.

1.2 Document name and identification

The title for this CP is the “X.509 Certificate Policy for the Department of Defence – Interoperability Certificate Authority”. The Object Identifier (OID) for the DIOCA CP is: 1.2.36.1.334.1.1.1.3.

{iso (1) iso-member (2) australia (36) government (1) department of defence (334) pki (1) certificate policy (1) certificate authority (1) interoperability (3)}
1.3 PKI participants

1.3.1 Certification authority
The Certification Authority (CA), or CAs, that issue certificates under this CP are Defence CAs.

This CP relates to:

i. the self-signed DIOCA authentication certificate that the DIOCA issues to itself (DIOCA-C);
ii. Principal Cross-certificate (DIOCA-PXC) - authentication certificates signed by the DIOCA and issued to Peer CAs;
iii. Secondary Cross-certificate (DIOCA-SXC) - authentication certificates signed by the DIOCA and issued to Defence Operational CAs; and
iv. All operator certificates used for the purpose of DIOCA maintenance and issuance responsibilities.

1.3.2 Registration authorities
The DIOCA does not use the services of an RA. Cross-certification requests are submitted directly to the CA. Processes that would normally be carried out by an RA such as identification and authentication of a certificate applicant and their affiliation with the organisation, are carried out as part of the Cross-certification Arrangement negotiations and during the cross-certification ceremony.

1.3.3 Subscribers
A Subscriber is defined in Appendix B of the CPS to be, as the context allows:

i. the entity (e.g. an individual, device, web site, application or resource) whose Distinguished Name (DN) appears as the "Subject Distinguished Name" on the relevant Certificate, and / or
ii. the person or legal entity that applied for that Certificate, and / or entered into the Subscriber Agreement in respect of that Certificate.

No end-entities are issued certificates under this CP. Where the term “Subscriber” is used in this document, it refers to the person or legal entity that applied for that certificate, as identified in the relevant CCA.

1.3.4 Relying Parties
A new chain of trust is created by the DIOCA signing other CAs' certificates to create a certification path between PKIs that have entered into a Cross-certification Arrangement. Other than the chain of trust aspects there are no Relying Parties for the certificates issued under this CP.

Relying Parties are bound by the relevant CP that an end-entity certificate is issued under. PKIs may use policy mapping and/or policy constraints to limit the types of certificates that they choose to trust.

1.3.5 Other participants
Other participants include:

i. The Peer PKI with which Defence PKI is cross-certifying. The Peer PKI enters into a CCA with Defence and provides a cross-certification request for a Principal Cross-certificate (DIOCA-PXC). Full responsibilities of the parties are described in the CCA.
ii. the DPKIPB – refer to the Certification Practice Statement (CPS) for their responsibilities which specifically include:
   a) review and approval of this CP;
   b) presiding over the PKI audit process;
   c) approving mechanisms and controls for the management of the accredited infrastructure (CA);
X.509 Certificate Policy

INTRODUCTION

d) approval of operational standards and guidelines to be followed.

iii. Accreditation agencies – to provide independent assurance that the facilities, practices and procedures used to issue certificates comply with this CP, the CPS and other relevant documentation (policy and legal).

iv. Directory Service providers – to provide a repository for certificates and certificate status information issued under this CP.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

1.4.1.1 DIOCA-C

The certificates issued by the DIOCA under this CP, in conjunction with their associated private keys, allow the DIOCA to:

i. self-sign the DIOCA certificate;

ii. digitally sign a Peer CA’s public key to create a Principal Cross-Certificate;

iii. digitally sign the Defence Operational CAs public key to create a Secondary Cross-Certificate;

iv. sign the operational certificates required by the PKCSI;

v. sign its own internal log files.

1.4.1.2 DIOCA-PXC

Certificates issued by the DIOCA under this CP allow Defence to publish the cross-certificate to Defence end entities in order to provide a trusted certificate path validating the other CAs issued certificates.

1.4.1.3 DIOCA-SXC

Certificates issued by the DIOCA to Defence Operational CAs (cross-certificates) under this CP allow the cross-certified CA to publish the cross-certificate to its end entities in order to provide a trusted certificate path validating Defence issued certificates.

In addition, some PKI component certificates (e.g. CA operator, RA) may be issued by the DIOCA. These are only valid for use within the PKI and are used for the authentication and confidentiality (as appropriate) between PKI components.

1.4.2 Prohibited certificate uses

The prohibited uses for certificates issued under this CP are:

i. to sign certificates issued to end-entities;

ii. to sign the certificate of a non DPKIPB approved CA;

iii. to establish a subordinate CA (as opposed to signing an existing CAs certificate); and

iv. To conduct any transaction, or communication, which is any or all of the following:

   a) Unrelated to Defence business;
   b) Illegal;
   c) Unauthorised;
   d) Unethical, or
   e) Contrary to Defence policy.

---

2 This only refers to certificates directly associated with the management of the DIOCA. All other PKI component certificates are covered under the Defence Root CA and SubCA Certificate Policy [RCA CP].
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 the DIOCA-C, DIOCA-PXC and DIOCA-SXC and the DIOCA's latest CRL in its repository. This information is available to Relying Parties both internal and external of Defence.

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

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

2.3 Time or frequency of publication

Published documentation such as this CP and the CPS is updated on approved changes.

Defence CAs publish new certificates and CRLs as operationally required - see 4.9.7 (CRL issuance frequency) and relevant CP.
2.4 Access controls on repositories
See CPS.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names
The Distinguished Name (DN) is in the form of a X.501 printable string and is not blank.

A DIOCA-C issued under this CP must have:
   i. a clear distinguishable and unique DN in the certificate subjectName field;
   ii. a DN approved by the DPKIPB; and
   iii. a name composed of "Australian Defence Interop CA ([Gen])" where the optional CA Generation ([Gen]) field is comprised of G<integer> and is only used for subsequent generations of the CA.

A DIOCA-PXC issued under this CP must have:
   i. a clear distinguishable and unique DN in the certificate subjectName field;
   ii. a common name whose components of the name are unique to the PKI name space of the Peer PKI; and
   iii. a DN approved by the Peer PKIs Policy Governance Body.

A DIOCA-SXC issued under this CP must have:
   i. a clear distinguishable and unique DN in the certificate subjectName field;
   ii. a DN approved by the DPKIPB; and
   iii. a name composed of "Australian Defence Interop CA ([Gen])" where the optional CA Generation ([Gen]) field is comprised of G<integer> and is only used for subsequent generations of the CA.

3.1.2 Need for names to be meaningful
The DPKIPB shall ensure that the DN in subjectName field used to identify the Subject of a certificate is:
   i. Meaningful; and
   ii. Relates directly to the identity of the Subject

Names used to identify the DIOCA PKI core components are based on their PKI role and serial number. Additionally, names are used to identify individual operators to allow for system auditing.

3.1.3 Anonymity or pseudonymity of Subscribers
Not applicable.

3.1.4 Rules for interpreting various name forms
No stipulation as there is only one form.
3.1.5 Uniqueness of names
DIOCA-C and DIOCA-SXC: Names are unique within the Defence PKI name space.
DIOCA-PXC: Names are unique within the Peer 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

3.2.1.1 DIOCA-C
*Private Key* generation of the DIOCA is performed using a *Hardware Security Module* (HSM) that has undergone a security evaluation though an *Australian Signals Directorate* (ASD) recognised evaluation program. (evaluated product) 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* (KMP).

3.2.1.2 DIOCA-PXC
A certificate signing request for a DIOCA-PXC must be submitted in the format of a PKCS#10 request signed with the corresponding private key. The generation of the PKCS#10 file must be witnessed by authorised representatives of each of the CAs to cross-certify.

3.2.1.3 DIOCA-SXC
A certificate signing request for a DIOCA-SXC must be submitted in the format of a PKCS#10 request signed with the corresponding private key. The generation of the PKCS#10 file must be witnessed by a representative of the DPKIPB and the *PKI Operations Manager*.

3.2.2 Authentication of Organisation Identity

3.2.2.1 DIOCA-C
To establish the DIOCA, the DPKIPB and the Gatekeeper Competent Authority must grant approval prior to the key generation ceremony.

Generation of DIOCA 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.

Before issuing certificates to PKI Operators, the operator is required to perform a face-to-face identity verification that complies with the Gatekeeper *Evidence of Identity* (EOI) policy for a High Assurance
X.509 Certificate Policy

IDENTIFICATION AND AUTHENTICATION
certificate and be cleared to a minimum level of NV1\(^3\). In addition, the operator will need to be validated as being affiliated with Defence by confirmation of their existence in the Defence Directory.

3.2.2.2 DIOCA-PXC
In order to issue a DIOCA-PXC, the two PKIs must enter into a formal CCA. A representative for the CA to be cross-certified must be formally authorised in writing by the Peer PKI prior to attending the cross-certification ceremony

At the time of the cross-certification ceremony, the PKI Operations Manager shall:

i. Authenticate the representative of the CA to be cross-certified and verify their affiliation with the organisation they represent.

ii. Verify the representative's authority to request a cross-certificate.

iii. Verify the certificate signing request details are as per the relevant CCA.

3.2.2.3 DIOCA-SXC
Issuing of a DIOCA-SXC does not require check of affiliation with Defence, as both parties are core components within the Defence PKI. However, generation of a DIOCA-SXC must comply with the processes dictated in the KMP, which indicates that the process includes:

i. identification of the infrastructure elements;

ii. witnessed generation of cross-certification request;

iii. witnessed generation of cross-certificate;

iv. verification by the PKI Operator and witnesses that the generation process was successful; and

v. publishing of cross-certificate.

3.2.3 Authentication of individual identity

Authentication of authorised representatives of the CA will take place during the cross certification ceremony for DIOCA-PXC.

3.2.4 Non-verified Subscriber information

Non-verified Subscriber information shall not be included in certificates.

3.2.5 Validation of authority

3.2.5.1 DIOCA-C

The DPKIPB is responsible for nominating all parties involved in the initial key signing ceremony and ensuring that they are suitable for their role in the creation of the DIOCA. Any non-Defence representatives (see 1.3.5 Other parties) must be formally appointed in writing by their organisation prior to the key signing ceremony.

3.2.5.2 DIOCA-PXC

Prior to a cross-certification ceremony taking place, the DPKIPB is responsible for:

i. ensuring that a CCA has been completed between the parties;

ii. nominating all Defence representatives involved in the cross-certification ceremony and ensuring that they are suitable for their role in the creation of the DIOCA-PXC; and

---

\(^3\) Negative Vetting level 1 permits ongoing access to Australian Government information and assets that are security classified up to and including SECRET.
iii. ensuring that non-Defence representatives (see 1.3.5 Other parties) have been nominated formally and in writing by their organisation.

The authority of the participants shall be verified by the PKI Operations Manager prior to commencement of the cross-certification ceremony.

3.2.5.3 DIOCA-SXC

The DPKIPB is responsible for nominating all parties involved in the cross-certification of two Defence CAs and ensure that they are suitable for their role in the creation of the cross-certificate.

The authority of the participants shall be verified by the PKI Operations Manager prior to commencement of the cross-certification ceremony.

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

3.3.1.1 DIOCA-C

The minimum identification and authentication requirements for routine re-key are as per 3.2.2.1 (Authentication of Organisation identity - sections relevant to DIOCA-C).

3.3.1.2 DIOCA-PXC

A DIOCA-PXC may be re-issued upon the re-keying of either the cross-certified CAs in question. The minimum identification and authentication requirements for such re-issue are as per 3.2.2.2 (Authentication of Organisation identity - sections relevant to DIOCA-PXC).

3.3.1.3 DIOCA-SXC

A DIOCA-SXC may be re-issued upon the re-keying of either of the cross-certified CAs in question. The minimum identification and authentication requirements for such re-issue are as per 3.2.2.3 (Authentication of Organisation identity - sections relevant to DIOCA-SXC).

3.3.2 Identification and authentication for re-key after revocation

Re-key is not allowed after revocation for CAs.

For PKI 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 (3.4) and section 4.9 of this CP and the CPS.

The DPKIPB must approve all requests for revocation of Defence CAs and cross-certificates. Revocation of other PKI core components, including operator certificates, can be approved by the PKI Operations Manager or the CDMC Security Officer (SO).

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

The revocation process provides an auditable record of this process, which includes at a minimum:
4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate application

4.1.1 Who can submit a certificate application

4.1.1.1 DIOCA-C

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

4.1.1.2 DIOCA-PXC and DIOCA-SXC

Anyone wishing to enter into a CCA with Defence can apply for cross-certification, however only the DPKIPB (and the PKI Policy board of the Peer PKI) can approve the decision to cross-certify.

4.1.2 Enrolment process and responsibilities

4.1.2.1 DIOCA and DIOCA-SXC

The enrolment process and responsibilities for a CA and secondary cross-certificates are outlined in the PKI Operations Manual and KMP.

4.1.2.2 DIOCA-PXC

The enrolment process and responsibilities for principal cross-certificates are detailed in the relevant CCA.

4.2 Certificate application processing

DIOCA-PXC: Cross-certification of external CA by DIOCA

The process of cross-certification with a Peer PKI (principal cross-certificate, i.e. DIOCA-PXC) is carried out as follows, in broad steps (individual CCAs may provide more detail):

i. The Peer PKI arranges for the cross-certificate signing request generation at a mutually agreed date, time and place. A representative of the Defence PKI must be able to be present to witness the generation.

ii. At a formal ceremony, a cross-certificate signing request in the format of a PKCS#10 file is generated in view of both CAs' representatives.

iii. Both CA representatives record the requesting CA's thumbprint, e.g. a SHA-1 hash of its public key. Optionally, a hash is also produced of the PKCS#10 file (using an agreed 3rd party tool) and recorded.
iv. The PKCS#10 file is saved to disk and to removable media, e.g. CD, which is safe-handed to the Defence PKI by its representative.

v. Prior to issuing the cross-certificate, the PKI Operations Manager or a delegate checks that the PKCS#10 file has not been tampered with by re-creating the hash of the PKCS#10 file which was created and recorded in step (iii). The two hashes are compared.

vi. After checking that the PKCS#10 file is correct (incl. certificate details), a cross-certificate is issued by DIOCA.

vii. The cross-certificate is inspected and the CAs thumbprint checked against the one recorded in step (iii).

viii. The cross-certificate is returned to the requesting CA by email or other method. Once the certificate has been checked and accepted in writing by the cross-certified CA, it is published in a location that is accessible by the cross-certifying CA’s Subscribers (Relying Parties in terms of the cross-certified CA).

A cross-certification ceremony script is prepared in advance, and during the event, records are made which are signed by the witnesses. This provides an audit record of the cross-certification.

DIOCA-SXC (Cross-certification of internal Defence CA by DIOCA)

i. DPKIPB arranges for the cross-certificate signing request generation. A minimum of two representatives of the DPKIPB must be able to be present to witness the generation. Other parties may also be required at the generation, e.g. Accreditation agencies.

ii. At a formal ceremony, a cross-certificate signing request in the format of a PKCS#10 file is generated in view of witnesses.

iii. The PKCS#10 file is saved to removable media, e.g. CD, and copied onto the DIOCA server.

iv. After checking that the PKCS#10 file is correct (incl. certificate details), a cross-certificate is issued by DIOCA.

v. The cross-certificate is returned to the requesting CA. Once the certificate has been checked and accepted, it is published in Defence repositories and provided to Peer PKI for publishing to its Subscribers.

A cross-certification ceremony script is prepared in advance, and during the event, records are made which are signed by the witnesses. This provides an audit record of the cross-certification.

4.2.1 Performing identification and authentication functions

4.2.1.1 DIOCA

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 DIOCA creation; and

ii. validation of all information to be included in the certificate.

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

4.2.1.2 DIOCA-PXC

The DPKIPB is responsible for ensuring that a CCA has been completed and that representatives and witnesses required to attend the cross-certification ceremony have been nominated by the legal entity they are representing formally and in writing.

* Alternatively, by diplomatic bag, or sent in a email signed with a trusted certificate.
The PKI Operations Manager is responsible for ensuring that representatives and witnesses participating in the cross-certification ceremony have been identified and authenticated to the level of Gatekeeper LOA 3 (high confidence). (See [EOI])

4.2.1.3 DIOCA-SXC
The DPKIPB is responsible for ensuring that representatives and witnesses required to attend the cross-certification ceremony have been nominated by the legal entity they are representing formally and in writing.

The PKI Operations Manager is responsible for ensuring that representatives and witnesses participating in the cross-certification ceremony have been identified and authenticated to the level of Gatekeeper LOA 3 (high confidence). (See [EOI])

4.2.2 Approval or rejection of certificate applications
The DPKIPB approves or rejects CA certificate and cross-certificate

4.2.3 Time to process certificate applications
No stipulation.

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.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance
The DIOCA, DIOCA-SXC, and any PKI core components are deemed to have accepted a certificate when they exercise the private key.

The DIOCA-PXC is accepted when the cross-certified external CA advises Defence in writing that the certificate has been accepted.

4.4.2 Publication of the certificate by the CA
Certificates (except DIOCA operator certificates) will be published to the Defence repository and external repositories as per the CPS.

See Appendix B - Certificate Profiles (CRL Distribution Point) for exact location.

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
There are no end entity Subscribers to this CP. Certificate usage is defined above in 1.4 (Certificate Usage) and as such core components, other than CAs, may only be used within the PKI.
Custodians shall protect private keys from access by other parties in accordance with the KMP.
If the extended key usage extension is present and implies any limitation on the use of the certificate and/or private key, the certificates must be used within those limitations.

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

4.6  Certificate renewal
The DIOCA certificates cannot be renewed; however, associated core components can be renewed.
Cross-certificates (DIOCA-PXC and DIOCA-SXC) may be renewed.

4.6.1  Circumstance for certificate renewal
The CPS defines the criteria for certificate renewals.
Renewal of revoked certificates is not permitted regardless of the reason for revocation.

4.6.2  Who may request renewal
Same as per applications - see 4.1.1 (Who can submit a certificate application).

4.6.3  Processing certificate renewal requests
The process for certificate renewal is consistent with the enrolment process defined in 4.1 (Certificate Application), 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
Cross-certificates will be delivered to the cross-certified CA upon issuance.
Operators shall be notified when a “renewal” certificate has been issued, and of any requirements necessary to update the operators token.

4.6.5  Conduct constituting acceptance of a renewal certificate
See 4.4.1 (Conduct constituting certificate acceptance).

4.6.6  Publication of the renewal certificate by the CA
See 4.4.2 (Publication of certificate by the CA)

4.6.7  Notification of certificate issuance by the CA to other entities
Not applicable.
4.7 Certificate re-key

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
See 4.1.1 (Certificate application).

4.7.3 Processing certificate re-keying requests
The process for certificate re-keying is consistent with the enrolment process defined in 4.1 (Certificate Application), 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 DPKIPB receives notification of progress, issues and completion of DPKIPB initiated certificate re-keys.
Cross-certificates are delivered to the cross-certified CA upon issuance.
The operator receives notification when a re-keyed certificate is issued, or if a certificate request for re-key is rejected.

4.7.5 Conduct constituting acceptance of a re-keyed certificate
See 4.4.1 (Conduct constituting certificate acceptance).

4.7.6 Publication of the re-keyed certificate by the CA
See 4.4.2 (Publication of certificates by the CA)

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 (but may not be limited to):

i. Details in the certificate relevant to an 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 DPKIPB will determine other circumstances as appropriate.

4.8.2 Who may request certificate modification
Certificate modification may be requested by:

i. the DPKIPB, or
ii. Operator
4.8.3 Processing certificate modification requests

The process for certificate modification is consistent with the enrolment process defined in 4.1 (Certificate Application). The identification and authentication procedures comply with 3.3 (Identification and Authentication for Re-Key Requests).

4.8.4 Notification of new certificate issuance to Subscriber

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

Cross-certificates are delivered to the cross-certified CA upon issuance.

The operator or key custodian receives notification when issued a modified certificate, or if rejection of a modification request occurs.

4.8.5 Conduct constituting acceptance of modified certificate

See 4.4.1 (Conduct constituting certificate acceptance)

4.8.6 Publication of the modified certificate by the CA

See 4.4.2 (Publication of the certificate by the CA)

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

4.9.1.1 DIOCA-C

See CPS, section 4.9.1.

4.9.1.2 DIOCA-PXC and DIOCA-SXC

See CPS, in addition to the circumstances for revocation of cross-certificates as specified in the relevant CCA and ACP185.

4.9.2 Who can request revocation

4.9.2.1 DIOCA-C

See CPS, section 4.9.2.

4.9.2.2 DIOCA-PXC and DIOCA-SXC

See CPS, section 4.9.2. In addition to the parties listed in the CPS, the authorised representative of a cross-certified CA may request revocation.

4.9.3 Procedure for revocation request

Revocation requests must be validated by the PKI Operations Manager prior to initiation. The Disaster Recovery and Business Continuity Plan (DRBCP) details the revocation process for the DIOCA in the event of an emergency.

After verification, a PKI operator processes the revocation request using the PKI software, which captures an auditable record of the process.
After a certificate is revoked, the CA includes the applicable certificate (certificate serial number) in the CRL that is signed by the CA and published in the repositories.

4.9.4 Revocation request grace period
A grace period of one Operational Day is permitted.

The DPKIPB, 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
The DIOCA shall process revocation requests for certificates issued under this CP promptly after receipt.

4.9.6 Revocation checking requirement for Relying Parties
Before using a certificate, the Relying Party must validate it against the CRL. 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 DIOCA are published when a cross-certificate is revoked or monthly.

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
No stipulation.

4.9.11 Other forms of revocation advertisements available
See CPS.

4.9.12 Special requirements re key compromise
Peer PKIs must be advised of any compromise affecting cross-certificates.

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. However, operator 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 session key encapsulation and 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. DIOCA's keys are generated within a HSM;
ii. operators generate keys within a hard token or using ASD recognised security evaluated software; and
iii. non-critical core components (e.g. Certificate Status Server) 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
DIOCA public keys are self generated and do not require delivery.

Operational CA or Cross-certified CA public key delivery to the DIOCA are witnessed events, 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 or 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 will support either SHA1 or SHA2 for signing and RSA public key algorithm. The key sizes for:

i. DIOCA is a minimum of 2048 bits; and
ii. Operators are a minimum 1024 bits.

DIOCA-PXC and DIOCA-SXC key sizes are determined by the key sizes of the CAs that issued them.

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)
In addition to the key usage defined in 1.4, certificates include key usage extension fields to specify the purposes for which the Certificate may be used 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 are specified in the Certificate Profile set forth in Appendix B.

6.2 Private key protection and cryptographic module engineering controls
This section does not apply to DIOCA-PXC and DIOCA-SXC.

6.2.1 Cryptographic module standards and controls
All cryptographic modules used with PKI core components have undergone a security evaluation though an ASD recognised evaluation program and approved for the uses intended in this CP by the NCA.

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

6.2.3 Private Key escrow
Escrow of private keys is permitted and occurs in accordance with the KMP and the 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 KMP and the DRBCP.

6.2.6 Private Key transfer into or from a cryptographic module
See CPS.

6.2.7 Private Key storage on cryptographic module
See CPS.
6.2.8 Method of activating private key
Activating private keys occurs by the PKI Operator 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 DIOCA certificate validity has a maximum period of 20 years to limit the key lifetime. DIOCA-PXC and DIOCA-SXC lifetimes have a maximum of three years. Operator certificates have a maximum validity period of two years.

6.4 Activation data
This section does not apply to DIOCA-PXC and DIOCA-SXC.

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 KMP and Defence policy.

6.4.2 Activation data protection
All passphrases used to activate core components are kept in accordance with KMP and Defence policy.

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**
Appendix B contains certificates and CRL profiles and formats relative to this CP. The four certificates issued under this CP are:

i.  the Defence Interoperability Certificate Authority certificate;

ii.  Principal Cross-certificate (DIOCA signing another PKI’s CA);

iii. Secondary Cross-certificate (DIOCA signing Defence Operational CAs’ certificates); and

iv.  Certificates issued to the operators of the DIOCA to ensure their abilities to undertake administrative activities. Certificate profiles for these certificates are not published.

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 one of the following OIDs for signatures.

<table>
<thead>
<tr>
<th>Algorithm Object Identifier</th>
<th>OID Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>sha1WithRSAEncryption</td>
<td>(iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5)</td>
</tr>
<tr>
<td>sha256WithRSAEncryption</td>
<td>(iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11)</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Algorithm Object Identifier</th>
<th>OID Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>rsaEncryption</td>
<td>(iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1)</td>
</tr>
<tr>
<td>Id-ecPublicKey</td>
<td>(iso(1) member-body(2) us(840) ansi-x9-62(10045) public-key-type(2) 1)</td>
</tr>
<tr>
<td>rsaEncryption</td>
<td>(iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1)</td>
</tr>
<tr>
<td>Dhpublicnumber</td>
<td>(iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1)</td>
</tr>
<tr>
<td>Id-keyExchangeAlgorithm</td>
<td>(joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) algorithms(1) 22)</td>
</tr>
</tbody>
</table>

**Table 2 – Algorithm OIDs**
7.1.4 Name Forms

7.1.4.1 DIOCA-C and DIOCA-SXC
The Common Name (CN) component is based on the name assigned by the DPKIPB to the CA being created and is presented as a printable string.
All other DN components are fixed and defined in Appendix B.

7.1.4.2 DIOCA-PXC
The Common Name (CN) component is based on the name assigned by the Peer PKIs Policy Governance Body to the CA being created and is presented as a printable string.
All other DN components are fixed and defined in Appendix B.

7.1.5 Name Constraints
Name constraints may be present. See Appendix B.

7.1.6 Certificate Policy Object Identifier
CA Certificates issued under this policy shall assert the OID \{1.2.36.1.334.1.1.1.3\}.
The DIOCA certificate shall also assert the anyPolicy OID of \{2.5.29.32.0\}.
Cross-certificates shall also assert the following OIDs representing Levels of Assurance of certificates issued:

<table>
<thead>
<tr>
<th>Level</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual</td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td>1.2.36.1.334.1.2.1.1</td>
</tr>
<tr>
<td>Medium</td>
<td>1.2.36.1.334.1.2.1.2</td>
</tr>
<tr>
<td>High</td>
<td>1.2.36.1.334.1.2.1.3</td>
</tr>
<tr>
<td>Very High</td>
<td>1.2.36.1.334.1.2.1.4</td>
</tr>
<tr>
<td>Resources</td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td>1.2.36.1.334.1.2.2.1</td>
</tr>
<tr>
<td>Medium</td>
<td>1.2.36.1.334.1.2.2.2</td>
</tr>
<tr>
<td>High</td>
<td>1.2.36.1.334.1.2.2.3</td>
</tr>
</tbody>
</table>

Table 3 – Levels of Assurance

N.B. Resource Levels of Assurance OIDs should only be asserted in cross-certificates which map to a policy OID that is only for Resources (See ACP185).

7.1.7 Usage of Policy Constraints Extension

7.1.7.1 DIOCA-C
Policy constraints are not present.

7.1.7.2 DIOCA-PXC
A Principal Cross-certificate shall contain the policyConstraints extension with inhibitPolicyMapping field with a skipCerts value of zero, and with requiredExplicitPolicy with a skipCerts value of zero. It shall contain the inhibitAnyPolicy extension with a skipCerts value of zero.
7.1.7.3 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 shall be X.509 version 2 CRLs.

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 2560.

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 (Cth)) will be collected during the creation of the DIOCA 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).


9.4.2 Information treated as private

Not applicable for core components other than Operators. The PKI will only retain details of EOI documentation presented and the unique document identifiers. This information will be stored by the CMDC Security Officer in accordance with Defence requirements and protected in accordance with the requirements of the PKI Privacy Notice. Personal Information of Operators will not 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.

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 Office 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 Office 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. Further requirements in relation to each cross-certification may be detailed in the relevant CCA.

9.10.3 Effect of termination and survival

See CPS. Further requirements in relation to each cross-certification may be detailed in the relevant CCA.

9.11 Individual notices and communications with participants

See CPS. Further requirements in relation to each cross-certification may be detailed in the relevant CCA.
9.12 Amendments

9.12.1 Procedure for amendment
See CPS. Further requirements in relation to each cross-certification may be detailed in the relevant CCA.

9.12.2 Notification mechanism and period
See CPS. Further requirements in relation to each cross-certification may be detailed in the relevant CCA.

9.12.3 Circumstances under which OID must be changed.
If an OID relevant to this CP must be changed, the DPKIPB shall notify Peer PKIs to make appropriate updates to cross-certificates.

9.13 Dispute resolution provisions
See CPS. Further requirements in relation to each cross-certification may be detailed in the relevant CCA.

9.14 Governing law
See CPS. Further requirements in relation to each cross-certification may be detailed in the relevant CCA.

9.15 Compliance with applicable law
See CPS. Further requirements in relation to each cross-certification may be detailed in the relevant CCA.

9.16 Miscellaneous provisions
See CPS. Further requirements in relation to each cross-certification may be detailed in the relevant CCA.

9.17 Other provisions
For a Relying Party who is a member of a nation that is a signatory of the Combined Joint Multilateral Master Military Information Exchange Memorandum of Understanding (CJM3IEM) the conditions of the CJM3IEM in relation to Settlement of Disputes and Claims and Liabilities will apply, otherwise no stipulation. See also relevant CCA.
APPENDIX A. REFERENCES

The following documents are referenced in this CP:


[ACP185] Public Key Infrastructures (PKI) Cross-Certification Between Combined Communications-Electronics Board (CCEB) Nations (Nov 2011)

[CCA] Cross-certification Arrangement (one per cross-certification). (As represented as certificate profiles in Appendix B of this CP.)


[DRBCP] Australian Department of Defence Public Key Infrastructure Disaster Recovery and Business Continuity Plan (classified)


[KMP] Australian Department of Defence Public Key Infrastructure Key Management Plan (classified)


Table 4 - References
APPENDIX B.  CERTIFICATE, CRL AND OCSP PROFILES AND FORMATS

B.1  DIOCA SHA1 certificate [DIOCA-C]

Defence has now established a SHA2 Interoperability PKI. The SHA1 references remain in this policy document as a reference to the certificate profiles created at the time of the original Cross Certification between PKIs. The SHA1 CA’s remain in operation presently providing CRLs only.

<table>
<thead>
<tr>
<th>Field</th>
<th>Critical</th>
<th>Defence Certificate Value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td></td>
<td>V3 (2)</td>
<td>Version 3 of X.509</td>
</tr>
<tr>
<td>Serial</td>
<td></td>
<td>&lt;octet string&gt;</td>
<td>Unique value generated by the issuing CA</td>
</tr>
<tr>
<td>Issuer Signature Algorithm</td>
<td></td>
<td>sha-1WithRSAEncryption</td>
<td>Minimum cryptographic level – SHA-1 (ADOCA03) for Legacy purposes only; SHA-2 for new requests</td>
</tr>
<tr>
<td>Issuer Distinguished Name</td>
<td></td>
<td>CN= ADODCA03 or CN= Australian Defence Interop CA ([Gen])</td>
<td>The Serial number (03) is for the existing SHA1 Interop CA. The ([Gen]) field is an optional Generation field to be added for future implementations of the CA, comprised of G&lt; integer&gt;.</td>
</tr>
<tr>
<td>Issuer Distinguished Name</td>
<td></td>
<td>OU= CAs</td>
<td></td>
</tr>
<tr>
<td>Issuer Distinguished Name</td>
<td></td>
<td>OU= PKI</td>
<td></td>
</tr>
<tr>
<td>Issuer Distinguished Name</td>
<td></td>
<td>OU= DoD</td>
<td></td>
</tr>
<tr>
<td>Issuer Distinguished Name</td>
<td></td>
<td>O= GOV</td>
<td></td>
</tr>
<tr>
<td>Issuer Distinguished Name</td>
<td></td>
<td>C= AU</td>
<td></td>
</tr>
<tr>
<td>Validity Period</td>
<td></td>
<td>Not before &lt;UTCtime&gt;</td>
<td>Maximum 10 years from date of issue</td>
</tr>
<tr>
<td>Validity Period</td>
<td></td>
<td>Not after &lt;UTCtime&gt;</td>
<td></td>
</tr>
<tr>
<td>Subject Distinguished Name</td>
<td></td>
<td>CN= ADODCA03 or CN= Australian Defence Interop CA ([Gen])</td>
<td>Self-signed. Encoded as printable string.</td>
</tr>
<tr>
<td>Subject Distinguished Name</td>
<td></td>
<td>OU= CAs</td>
<td></td>
</tr>
<tr>
<td>Subject Distinguished Name</td>
<td></td>
<td>OU= PKI</td>
<td></td>
</tr>
<tr>
<td>Subject Distinguished Name</td>
<td></td>
<td>OU= DoD</td>
<td></td>
</tr>
<tr>
<td>Subject Distinguished Name</td>
<td></td>
<td>O= GOV</td>
<td></td>
</tr>
<tr>
<td>Subject Distinguished Name</td>
<td></td>
<td>C= AU</td>
<td></td>
</tr>
<tr>
<td>Subject Public Key Information</td>
<td></td>
<td>Minimum 2048 bit RSA key modulus, rsaEncryption</td>
<td></td>
</tr>
<tr>
<td>Issuer Unique Identifier</td>
<td></td>
<td>-</td>
<td>Not Present</td>
</tr>
<tr>
<td>Subject Unique Identifier</td>
<td></td>
<td>-</td>
<td>Not Present</td>
</tr>
<tr>
<td>Subject Key Identifier</td>
<td></td>
<td>&lt;octet string&gt;</td>
<td></td>
</tr>
<tr>
<td>Authority Key Identifier</td>
<td>No</td>
<td>&lt;octet string&gt;</td>
<td>The value of this field is the 160 bit SHA-1 or 256 bit SHA-2 hash of the binary DER encoding of the signing CA’s public key information.</td>
</tr>
<tr>
<td>Subject Key Identifier</td>
<td>No</td>
<td>&lt;octet string&gt;</td>
<td>The value of this field is the 160 bit SHA-1 or 256 bit SHA-2 hash of the binary DER encoding of the signing CA’s public key information.</td>
</tr>
<tr>
<td>Field</td>
<td>Critical</td>
<td>Defence Certificate Value</td>
<td>Notes</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Key usage</td>
<td>Yes</td>
<td>Certificate signing, CRL signing, digitalSignature, nonRepudiation</td>
<td>Digital signature and non-repudiation key usages are only used for the signing of the CA's own log entries.</td>
</tr>
<tr>
<td>Extended key usage</td>
<td>-</td>
<td>-</td>
<td>Not Present</td>
</tr>
<tr>
<td>Private key usage period</td>
<td>-</td>
<td>-</td>
<td>Not Present</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[2] Policy OID: (2.5.29.32.0)</td>
<td>anyPolicy OID</td>
</tr>
<tr>
<td>Policy Mapping</td>
<td>-</td>
<td>-</td>
<td>Not Present</td>
</tr>
<tr>
<td>Subject Alternative Name</td>
<td>-</td>
<td>-</td>
<td>Not Present</td>
</tr>
<tr>
<td>Issuer Alternative Name</td>
<td>-</td>
<td>-</td>
<td>Not Present</td>
</tr>
<tr>
<td>Subject Directory Attributes</td>
<td>-</td>
<td>-</td>
<td>Not Present</td>
</tr>
<tr>
<td>Basic Constraints</td>
<td>Yes</td>
<td>CA=True, path length constraint=none</td>
<td></td>
</tr>
<tr>
<td>Name Constraints</td>
<td>-</td>
<td>-</td>
<td>Not Present</td>
</tr>
<tr>
<td>Policy Constraints</td>
<td>-</td>
<td>-</td>
<td>Not Present</td>
</tr>
<tr>
<td>Authority Information Access</td>
<td>-</td>
<td>-</td>
<td>Not Present</td>
</tr>
<tr>
<td>CRL Distribution Points</td>
<td>-</td>
<td>-</td>
<td>Not Present</td>
</tr>
</tbody>
</table>

Table 5 – DIOCA SHA1 Certificate [DIOCA-C] Profile
B.2 Principal SHA1 Cross Certificate [DIOCA-PXC]

This certificate is issued by the DIOCA to another PKI's chosen Interoperability CA to provide a trusted certificate path for another PKI's Subscribers to the Defence PKI.

<table>
<thead>
<tr>
<th>Field</th>
<th>Critical</th>
<th>Identity Certificate Value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>V3 (2)</td>
<td></td>
<td>Version 3 of X.509</td>
</tr>
<tr>
<td>Serial</td>
<td></td>
<td>&lt;octet string&gt;</td>
<td>Unique value generated by the issuing CA</td>
</tr>
<tr>
<td>Issuer Signature Algorithm</td>
<td></td>
<td>Sha-1WithRSAEncryption</td>
<td>SHA-1 for Legacy purposes only;</td>
</tr>
<tr>
<td>Issuer Distinguished Name</td>
<td></td>
<td>CN= ADOCA03 OU= CAs OU= DoD O= GOU C= AU</td>
<td>Encoded as printable string. ADCA03 is the issuing Defence Interoperability CA.</td>
</tr>
<tr>
<td>Validity Period</td>
<td></td>
<td>Not before &lt;UTCtime&gt; Not after &lt;UTCtime&gt;</td>
<td>Maximum 3 years from date of issue.</td>
</tr>
<tr>
<td>Subject Distinguished Name</td>
<td></td>
<td>&lt;Distinguished name of cross certified CA&gt;</td>
<td>In accordance with Cross Certification Arrangement.</td>
</tr>
<tr>
<td>Subject Public Key Information</td>
<td></td>
<td>2048 bit RSA key modulus, rsaEncryption</td>
<td></td>
</tr>
<tr>
<td>Issuer Unique Identifier</td>
<td></td>
<td>-</td>
<td>Not Present</td>
</tr>
<tr>
<td>Subject Unique Identifier</td>
<td></td>
<td>-</td>
<td>Not Present</td>
</tr>
<tr>
<td>Authority Key Identifier</td>
<td>No</td>
<td>&lt;octet string&gt;</td>
<td>The value of this field is the 160 bit SHA-1 or 256 bit SHA-2 hash of the binary DER encoding of the signing CA's public key.</td>
</tr>
<tr>
<td>Subject Key Identifier</td>
<td>No</td>
<td>&lt;octet string&gt;</td>
<td>The value of this field is the 160 bit SHA-1 or 256 bit SHA-2 hash of the binary DER encoding of the subject's public key.</td>
</tr>
</tbody>
</table>
### UNCLASSIFIED (PUBLIC DOMAIN)

#### X.509 Certificate Policy

<table>
<thead>
<tr>
<th>Field</th>
<th>Critical</th>
<th>Identity Certificate Value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>[3] Policy OID: {1.2.36.1.334.1.2.1.3}</td>
<td>Level of Assurance – Individual – High</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[4] Policy OID: {1.2.36.1.334.1.2.1.2}</td>
<td>Level of Assurance – Individual – Medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[5] Policy OID: {1.2.36.1.334.1.2.1.1}</td>
<td>Level of Assurance – Individual – Low</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[6] Policy OID: {1.2.36.1.334.1.2.2.3}</td>
<td>Level of Assurance – Resource – High^5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[7] Policy OID: {1.2.36.1.334.1.2.2.2}</td>
<td>Level of Assurance – Resource – Medium^4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[8] Policy OID: {1.2.36.1.334.1.2.2.1}</td>
<td>Level of Assurance – Resource – Low^4</td>
</tr>
<tr>
<td>Policy Mapping</td>
<td>No</td>
<td>Sequence of one or more pairs of OIDs; each pair includes an issuerDomainPolicy and a subjectDomainPolicy</td>
<td>In accordance with Cross Certification Arrangement.</td>
</tr>
<tr>
<td>Subject Alternative Name (Email)</td>
<td>-</td>
<td></td>
<td>Not Present</td>
</tr>
<tr>
<td>Subject Alternative Name (Microsoft UPN)</td>
<td>-</td>
<td></td>
<td>Not Present</td>
</tr>
<tr>
<td>Issuer Alternative Name</td>
<td>-</td>
<td></td>
<td>Not Present</td>
</tr>
<tr>
<td>Subject Directory Attributes</td>
<td>-</td>
<td></td>
<td>Not Present</td>
</tr>
<tr>
<td>Basic Constraints</td>
<td>Yes</td>
<td>Subject Type=CA Path Length Constraint=None</td>
<td></td>
</tr>
<tr>
<td>Policy Constraints</td>
<td>No</td>
<td>Explicit Policy Skip Certs = 0 Inhibit Policy Mapping Skip Certs = 0</td>
<td></td>
</tr>
<tr>
<td>Authority Information Access</td>
<td>No</td>
<td>[1] Access method=OCSP (1.3.6.1.5.5.7.48.1): Access location: <a href="http://ocsp.defence.gov.au">http://ocsp.defence.gov.au</a></td>
<td>The AIA is to reference a location containing the cross-certificates for ADOCA03.</td>
</tr>
</tbody>
</table>

^5 A Device OID shall only be used in cross certificates which map to a member policy OID that is only for devices (ACP185).
<table>
<thead>
<tr>
<th>Field</th>
<th>Critical</th>
<th>Identity Certificate Value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRL Distribution Points</td>
<td>No</td>
<td>[1] Distribution Point Name (http): <a href="http://crl.defence.gov.au/pki/crl/ADOCA03.crl">http://crl.defence.gov.au/pki/crl/ADOCA03.crl</a></td>
<td>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).</td>
</tr>
</tbody>
</table>

Table 6 - DIOCA SHA1 Principal Cross-Certificate [DIOCA-PXC] Profile
### B.3 DIOCA SHA1 Secondary Cross Certificate [DIOCA-SXC]

This certificate is issued by the DIOCA to a Defence Operational CA to provide a trusted certification path for Defence PKI Subscribers to another PKI.

<table>
<thead>
<tr>
<th>Field</th>
<th>Critical</th>
<th>Identity Certificate Value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td></td>
<td>V3 (2)</td>
<td>Version 3 of X.509</td>
</tr>
<tr>
<td>Serial</td>
<td></td>
<td>&lt;octet string&gt;</td>
<td>Unique value generated by the issuing CA</td>
</tr>
<tr>
<td>Issuer Signature Algorithm</td>
<td></td>
<td>Sha-1 WithRSAEncryption</td>
<td>SHA-1 for Legacy purposes only;</td>
</tr>
<tr>
<td>Issuer Distinguished Name</td>
<td></td>
<td>CN= ADOCA03</td>
<td>Encoded as printable string. Defence Interoperability CA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OU= CAs</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>OU= PKI</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>OU= DoD</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>O= GOV</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>C= AU</td>
<td></td>
</tr>
<tr>
<td>Validity Period</td>
<td></td>
<td>Not before &lt;UTCtime&gt;</td>
<td>Maximum 3 years from date of issue</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Not after &lt;UTCtime&gt;</td>
<td></td>
</tr>
<tr>
<td>Subject Distinguished Name</td>
<td></td>
<td>CN= ADOCA &lt;Serial&gt;</td>
<td>Encoded as printable string.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OU= CAs</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>OU= PKI</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>OU= DoD</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>O= GOV</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>C= AU</td>
<td></td>
</tr>
<tr>
<td>Subject Public Key Information</td>
<td></td>
<td>2048 bit RSA key modulus, rsaEncryption</td>
<td></td>
</tr>
<tr>
<td>Issuer Unique Identifier</td>
<td></td>
<td>-</td>
<td>Not Present</td>
</tr>
<tr>
<td>Subject Unique Identifier</td>
<td></td>
<td>-</td>
<td>Not Present</td>
</tr>
<tr>
<td>X.509 V3 extensions:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authority Key Identifier</td>
<td>No</td>
<td>&lt;octet string&gt;</td>
<td>The value of this field is the 160 bit SHA-1 hash of the binary DER encoding of the signing CA's public key information.</td>
</tr>
<tr>
<td>Subject Key Identifier</td>
<td>No</td>
<td>&lt;octet string&gt;</td>
<td>The value of this field is the 160 bit SHA-1 or 256 bit SHA-2 hash of the binary DER encoding of the subject's public key information.</td>
</tr>
<tr>
<td>Key Usage</td>
<td>Yes</td>
<td>keyCertSign cRLSign</td>
<td>Digital signature and non-repudiation key usages are only used for the signing of the CA's own log entries.</td>
</tr>
<tr>
<td>Extended key usage</td>
<td>-</td>
<td></td>
<td>Not Present</td>
</tr>
<tr>
<td>Field</td>
<td>Critical</td>
<td>Identity Certificate Value</td>
<td>Notes</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------</td>
<td>---------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Private key usage period</td>
<td>-</td>
<td></td>
<td>Not Present</td>
</tr>
<tr>
<td>Certificate policies</td>
<td>No</td>
<td>[1] Policy OID: {1.2.36.1.334.1.1.1.3}</td>
<td>The OID of this CP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[2] Policy OID: {1.2.36.1.334.1.2.1.4}</td>
<td>Level of Assurance - Individual - Very High</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[3] Policy OID: {1.2.36.1.334.1.2.1.3}</td>
<td>Level of Assurance - Individual - High</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[4] Policy OID: {1.2.36.1.334.1.2.1.2}</td>
<td>Level of Assurance - Individual - Medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[5] Policy OID: {1.2.36.1.334.1.2.1.1}</td>
<td>Level of Assurance - Individual - Low</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[6] Policy OID: {1.2.36.1.334.1.2.2.3}</td>
<td>Level of Assurance - Resource - High</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[7] Policy OID: {1.2.36.1.334.1.2.2.2}</td>
<td>Level of Assurance - Resource - Medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[8] Policy OID: {1.2.36.1.334.1.2.2.1}</td>
<td>Level of Assurance - Resource - Low</td>
</tr>
<tr>
<td>Policy Mapping</td>
<td>-</td>
<td></td>
<td>Not Present</td>
</tr>
<tr>
<td>Subject Alternative Name</td>
<td>-</td>
<td></td>
<td>Not Present</td>
</tr>
<tr>
<td>Email</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subject Alternative Name</td>
<td>-</td>
<td></td>
<td>Not Present</td>
</tr>
<tr>
<td>Microsoft UPN</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Issuer Alternative Name</td>
<td>-</td>
<td></td>
<td>Not Present</td>
</tr>
<tr>
<td>Subject Directory Attributes</td>
<td>-</td>
<td></td>
<td>Not Present</td>
</tr>
<tr>
<td>Basic Constraints</td>
<td>Yes</td>
<td>Subject Type=CA</td>
<td></td>
</tr>
<tr>
<td>Path Length Constraint=None</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name Constraints</td>
<td>-</td>
<td></td>
<td>Not Present</td>
</tr>
<tr>
<td>Policy Constraints</td>
<td>-</td>
<td></td>
<td>Not Present</td>
</tr>
<tr>
<td>Authority Information Access</td>
<td>No</td>
<td>[1] Access method=OCSP (1.3.6.1.5.5.7.48.1): Access location: <a href="http://ocsp.defence.gov.au">http://ocsp.defence.gov.au</a></td>
<td>The AIA is to reference a location containing the cross-certificates for ADOCA03.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[2] Access method=CAIssuer (1.3.6.1.5.5.7.48.2): Access location:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>[3] Access method=CAIssuer (1.3.6.1.5.5.7.48.2): Access location:</td>
<td></td>
</tr>
</tbody>
</table>
### X.509 Certificate Policy

#### OTHER BUSINESS AND LEGAL MATTERS

<table>
<thead>
<tr>
<th>Field</th>
<th>Critical</th>
<th>Identity Certificate Value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRL Distribution Points</td>
<td>No</td>
<td>[1] Distribution Point Name (http): <a href="http://crl.defence.gov.au/pki/crl/ADOCA03.crl">http://crl.defence.gov.au/pki/crl/ADOCA03.crl</a></td>
<td>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). The missing &quot;;binary&quot; at the end of the LDAP URI is a Unicert limitation.</td>
</tr>
</tbody>
</table>

**Table 7 –DIOCA SHA1 Secondary Cross-Certificate [DIOCA-SXC] Profile**
## B.4 DIOCA SHA2 certificate [DIOCA-C]

<table>
<thead>
<tr>
<th>Field</th>
<th>Critical</th>
<th>Defence Certificate Value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial</td>
<td></td>
<td>&lt;octet string&gt;</td>
<td></td>
</tr>
<tr>
<td>Issuer Signature Algorithm</td>
<td></td>
<td>SHA-2WithRSAEncryption</td>
<td></td>
</tr>
<tr>
<td>Issuer Distinguished Name</td>
<td></td>
<td>CN= Australian Defence Interoperability CA [G&lt;integer&gt;]</td>
<td>Encoded as printable string. [G&lt;integer&gt;] is an optional extension for future generations of the Interop CA.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OU = CAs</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>OU = PKI</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>OU = DoD</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>O= GOV</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>C= AU</td>
<td></td>
</tr>
<tr>
<td>Issuer Distinguished Name</td>
<td></td>
<td>CN= Australian Defence Interoperability CA [G&lt;integer&gt;]</td>
<td>Encoded as printable string. [G&lt;integer&gt;] is an optional extension for future generations of the Interop CA.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OU = CAs</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>OU = PKI</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>OU = DoD</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>O= GOV</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>C= AU</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Validity Period</td>
<td></td>
<td>Not before &lt;UTCtime&gt;</td>
<td>Maximum 20 years from date of issue</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Not after &lt;UTCtime&gt;</td>
<td></td>
</tr>
<tr>
<td>Subject Distinguished Name</td>
<td></td>
<td>CN= Australian Defence Interoperability CA [G&lt;integer&gt;]</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>OU = CAs</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>OU = PKI</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>OU = DoD</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>O= GOV</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>C= AU</td>
<td></td>
</tr>
<tr>
<td>Subject Public Key Information</td>
<td></td>
<td>Minimum 2048 bit RSA key modulus, rsaEncryption</td>
<td></td>
</tr>
<tr>
<td>Issuer Unique Identifier</td>
<td></td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Subject Unique Identifier</td>
<td></td>
<td>-</td>
<td>Not Present</td>
</tr>
<tr>
<td>X.509 V3 extensions:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authority Key Identifier</td>
<td>No</td>
<td>&lt;octet string&gt;</td>
<td>The value of this field is the 160 bit SHA-1 hash of the binary DER encoding of the signing CA’s public key information.</td>
</tr>
<tr>
<td>Subject Key Identifier</td>
<td>No</td>
<td>&lt;octet string&gt;</td>
<td>The value of this field is the 160 bit SHA-1 hash of the binary DER encoding of the signing CA’s public key information.</td>
</tr>
<tr>
<td>Key usage</td>
<td>Yes</td>
<td>Certificate Signing</td>
<td>Digital signature and non-repudiation key usages are only used for the signing of the CA’s own log entries.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CRL Signing</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Off-line CRL Signing</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Digital Signature</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Non-Repudiation</td>
<td></td>
</tr>
<tr>
<td>Extended key usage</td>
<td></td>
<td>-</td>
<td>Not Present</td>
</tr>
<tr>
<td>Private key usage period</td>
<td></td>
<td>-</td>
<td>Not Present</td>
</tr>
<tr>
<td>Certificate policies</td>
<td>No</td>
<td>Policy OID: 1.2.36.1.334.1.1.1.3</td>
<td>The OID of this CP (DIOCA)</td>
</tr>
<tr>
<td>Field</td>
<td>Critical</td>
<td>Defence Certificate Value</td>
<td>Notes</td>
</tr>
<tr>
<td>----------------------------</td>
<td>----------</td>
<td>----------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Policy Mapping</td>
<td>-</td>
<td>[2] Policy OID: (2.5.29.32.0)</td>
<td>anyPolicy OID</td>
</tr>
<tr>
<td>Subject Alternative Name</td>
<td>-</td>
<td>Not Present</td>
<td></td>
</tr>
<tr>
<td>Issuer Alternative Name</td>
<td>-</td>
<td>Not Present</td>
<td></td>
</tr>
<tr>
<td>Subject Directory Attributes</td>
<td>-</td>
<td>Not Present</td>
<td></td>
</tr>
<tr>
<td>Basic Constraints</td>
<td>Yes</td>
<td>CA=True, path length constraint=none</td>
<td></td>
</tr>
<tr>
<td>Name Constraints</td>
<td>-</td>
<td>Not Present</td>
<td></td>
</tr>
<tr>
<td>Policy Constraints</td>
<td>-</td>
<td>Not Present</td>
<td></td>
</tr>
<tr>
<td>Authority Information Access</td>
<td>-</td>
<td>Not Present</td>
<td></td>
</tr>
<tr>
<td>CRL Distribution Points</td>
<td>-</td>
<td>Not Present</td>
<td></td>
</tr>
</tbody>
</table>

Table 8 – DIOCA SHA2 Certificate [DIOCA-C] Profile
### B.5 Principal SHA2 Cross Certificate [DIOCA-PXC]

This certificate is issued by the DIOCA to another PKI's chosen Interoperability CA to provide a trusted certificate path for another PKI's Subscribers to the Defence PKI.

<table>
<thead>
<tr>
<th>Field</th>
<th>Critical</th>
<th>Identity Certificate Value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td></td>
<td>V3 (2)</td>
<td>Version 3 of X.509</td>
</tr>
<tr>
<td>Serial</td>
<td></td>
<td>&lt;octet string&gt;</td>
<td>Unique value generated by the issuing CA</td>
</tr>
<tr>
<td>Issuer Signature Algorithm</td>
<td></td>
<td>SHA-2WithRSAEncryption</td>
<td></td>
</tr>
<tr>
<td>Issuer Distinguished Name</td>
<td></td>
<td>CN= Australian Defence Interoperability CA [G&lt;integer&gt;]</td>
<td>Encoded as printable string. [G&lt;integer&gt;] is an optional extension for future generations of the Interop CA.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OU= CAs</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>OU= PKI</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>OU= DoD</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>O= GOV</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>C= AU</td>
<td></td>
</tr>
<tr>
<td>Validity Period</td>
<td></td>
<td>Not before &lt;UTCtime&gt;</td>
<td>Maximum 3 years from date of issue</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Not after &lt;UTCtime&gt;</td>
<td></td>
</tr>
<tr>
<td>Subject Distinguished Name</td>
<td></td>
<td>&lt;Distinguished name of cross certified CA&gt;</td>
<td>In accordance with Cross Certification Arrangement.</td>
</tr>
<tr>
<td>Subject Public Key Information</td>
<td></td>
<td>Minimum 2048 bit RSA key modulus, rsaEncryption</td>
<td></td>
</tr>
<tr>
<td>Issuer Unique Identifier</td>
<td></td>
<td>-</td>
<td>Not Present</td>
</tr>
<tr>
<td>Subject Unique Identifier</td>
<td></td>
<td>-</td>
<td>Not Present</td>
</tr>
<tr>
<td>X.509 V3 extensions:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authority Key Identifier</td>
<td>No</td>
<td>&lt;octet string&gt;</td>
<td>The value of this field is the 160 bit SHA-1 hash of the binary DER encoding of the signing CA's public key.</td>
</tr>
<tr>
<td>Subject Key Identifier</td>
<td>No</td>
<td>&lt;octet string&gt;</td>
<td>The value of this field is the 160 bit SHA-1 hash of the binary DER encoding of the subject's public key.</td>
</tr>
<tr>
<td>Key Usage</td>
<td>Yes</td>
<td>Certificate Signing, Off-line CRL Signing, CRL Signing</td>
<td></td>
</tr>
<tr>
<td>Extended key usage</td>
<td></td>
<td>-</td>
<td>Not Present</td>
</tr>
<tr>
<td>Private key usage period</td>
<td></td>
<td>-</td>
<td>Not Present</td>
</tr>
<tr>
<td>Certificate policies*</td>
<td>No</td>
<td>[1] Policy OID: {1.2.36.1.334.1.1.1.3}</td>
<td>The OID of this CP.</td>
</tr>
</tbody>
</table>

*Certificate policies may vary based upon the Cross Certification Agreement requirements.
<table>
<thead>
<tr>
<th>Field</th>
<th>Critical</th>
<th>Identity Certificate Value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Mapping</td>
<td>No</td>
<td>Sequence of one or more pairs of OIDs; each pair includes an issuerDomainPolicy and a subjectDomainPolicy</td>
<td>In accordance with Cross Certification Arrangement.</td>
</tr>
<tr>
<td>Subject Alternative Name</td>
<td>-</td>
<td>Not Present</td>
<td></td>
</tr>
<tr>
<td>Issuer Alternative Name</td>
<td>-</td>
<td>Not Present</td>
<td></td>
</tr>
<tr>
<td>Subject Directory Attributes</td>
<td>-</td>
<td>Not Present</td>
<td></td>
</tr>
<tr>
<td>Basic Constraints</td>
<td>Yes</td>
<td>Subject Type=CA</td>
<td>In accordance with Cross Certification Arrangement requirements</td>
</tr>
<tr>
<td>Path Length Constraint</td>
<td>1 or 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name Constraints</td>
<td>Yes</td>
<td>Permitted: directoryName</td>
<td>In accordance with Cross Certification Arrangement. (Optional) If included, it shall contain permittedSubtrees or excludedSubtrees field. Recommend that if asserted it be marked critical.</td>
</tr>
<tr>
<td>Policy Constraints</td>
<td>Yes</td>
<td>Explicit Policy Skip Certs = 0</td>
<td></td>
</tr>
<tr>
<td>Inhibit Any Policy</td>
<td>Yes</td>
<td>02 01 00</td>
<td></td>
</tr>
<tr>
<td>CRL Distribution Points</td>
<td>No</td>
<td>[1] Distribution Point Name (http): <a href="http://crl.defence.gov.au/pki/crl/DIOCA%5B">http://crl.defence.gov.au/pki/crl/DIOCA[</a>&lt;integer&gt;]-1.crl</td>
<td>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). The missing &quot;;binary&quot; at the end of the LDAP URI is a Unicert limitation.</td>
</tr>
</tbody>
</table>

Table 9 - DIOCA SHA2 Principal Cross-Certificate [DIOCA-PXC] Profile
## B.6 DIOCA SHA2 Secondary Cross Certificate [DIOCA-SXC]

This certificate is issued by the DIOCA to a Defence Operational CA to provide a trusted certification path for Defence PKI Subscribers to another PKI.

<table>
<thead>
<tr>
<th>Field</th>
<th>Critical</th>
<th>Identity Certificate Value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial</td>
<td></td>
<td>&lt;octet string&gt;</td>
<td>Unique value generated by the issuing CA</td>
</tr>
<tr>
<td>Issuer Signature Algorithm</td>
<td></td>
<td>SHA-2WithRSAEncryption</td>
<td></td>
</tr>
<tr>
<td>Issuer Distinguished Name</td>
<td></td>
<td>CN= Australian Defence Interoperability CA [G&lt;integer&gt;]</td>
<td>Encoded as printable string. [G&lt;integer&gt;] is an optional extension for future generations of the Interop CA.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OU= CAs</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>OU= PKI</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>OU= DoD</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>O= GOV</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>C= AU</td>
<td></td>
</tr>
<tr>
<td>Validity Period</td>
<td></td>
<td>Not before &lt;UTCtime&gt;</td>
<td>Maximum 3 years from date of issue</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Not after &lt;UTCtime&gt;</td>
<td></td>
</tr>
<tr>
<td>Subject Distinguished Name</td>
<td></td>
<td>CN= &lt;subCAname&gt;</td>
<td>Encoded as printable string. The &lt;subCAname&gt; represents a unique name for the public sha2 subCA issuing infrastructure. (See Defence-ADPRCA-CP for detailed naming information).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OU= CAs</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>OU= PKI</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>OU= DoD</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>O= GOV</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>C= AU</td>
<td></td>
</tr>
<tr>
<td>Subject Public Key Information</td>
<td></td>
<td>Minimum 2048 bit RSA key modulus, rsaEncryption</td>
<td></td>
</tr>
<tr>
<td>Issuer Unique Identifier</td>
<td></td>
<td>-</td>
<td>Not Present</td>
</tr>
<tr>
<td>Subject Unique Identifier</td>
<td></td>
<td>-</td>
<td>Not Present</td>
</tr>
<tr>
<td>X.509 V3 extensions:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authority Key Identifier</td>
<td>No</td>
<td>&lt;octet string&gt;</td>
<td>The value of this field is the 160 bit SHA-1 hash of the binary DER encoding of the signing CA's public key information.</td>
</tr>
<tr>
<td>Subject Key Identifier</td>
<td>No</td>
<td>&lt;octet string&gt;</td>
<td>The value of this field is the 160 bit SHA-1 hash of the binary DER encoding of the subject's public key information.</td>
</tr>
<tr>
<td>Key Usage</td>
<td>Yes</td>
<td>digitalSignature, nonRepudiation, Certificate Signing, Off-line CRL Signing, CRL Signing</td>
<td>Digital signature and non-repudiation key usages are only used for the signing of the CA's own log entries.</td>
</tr>
<tr>
<td>Extended key usage</td>
<td>-</td>
<td></td>
<td>Not Present</td>
</tr>
<tr>
<td>Field</td>
<td>Critical</td>
<td>Identity Certificate Value</td>
<td>Notes</td>
</tr>
<tr>
<td>----------------------------</td>
<td>----------</td>
<td>---------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Private key usage period</td>
<td>[1]</td>
<td>Policy OID: {1.2.36.1.334.1.1.1.3}</td>
<td>The OID of this CP:</td>
</tr>
<tr>
<td></td>
<td>[4]</td>
<td>Policy OID: {1.2.36.1.334.1.2.1.3}</td>
<td>Level of Assurance – Individual – High</td>
</tr>
<tr>
<td></td>
<td>[5]</td>
<td>Policy OID: {1.2.36.1.334.1.2.1.2}</td>
<td>Level of Assurance – Individual – Medium</td>
</tr>
<tr>
<td></td>
<td>[6]</td>
<td>Policy OID: {1.2.36.1.334.1.2.1.1}</td>
<td>Level of Assurance – Individual – Low</td>
</tr>
<tr>
<td></td>
<td>[7]</td>
<td>Policy OID: {1.2.36.1.334.1.2.1.2.2}</td>
<td>Level of Assurance – Resource – High</td>
</tr>
<tr>
<td></td>
<td>[8]</td>
<td>Policy OID: {1.2.36.1.334.1.2.1.2.1}</td>
<td>Level of Assurance – Resource – Medium</td>
</tr>
<tr>
<td></td>
<td>[9]</td>
<td>Policy OID: {2.5.29.3.2}</td>
<td>any Policy OID</td>
</tr>
<tr>
<td>Policy Mapping</td>
<td>-</td>
<td>Subject Alternative Name (Email)</td>
<td>Not Present</td>
</tr>
<tr>
<td></td>
<td>-</td>
<td>Subject Alternative Name (Microsoft UPN)</td>
<td>Not Present</td>
</tr>
<tr>
<td>Issuer Alternative Name</td>
<td>-</td>
<td>Subject Directory Attributes</td>
<td>Not Present</td>
</tr>
<tr>
<td>Basic Constraints</td>
<td>Yes</td>
<td>Subject Type=CA, Path Length Constraint=None</td>
<td></td>
</tr>
<tr>
<td>Authority Constraints</td>
<td>-</td>
<td>Policy Constraints</td>
<td>Not Present</td>
</tr>
<tr>
<td>Authority Information Access</td>
<td>No</td>
<td>[1] Access method=OCSP {1.3.6.1.5.5.7.48.1}; Access location: <a href="http://ocsp.defence.gov.au">http://ocsp.defence.gov.au</a></td>
<td>The AIA is to reference a location containing the cross-certificates for the Australian [G&lt;integer&gt;] is an optional extension for future generations of the Interop CA. Defence uses a URL rewrite (redirection) rule in the Web Server to ensure that AIA urls without a file extension are assigned the correct filetype (.crt or .p7b) Must reference the issuing authority.</td>
</tr>
<tr>
<td>CRL Distribution Points</td>
<td>No</td>
<td>[1] Distribution Point Name (http): [<a href="http://crl.defence.gov.au/pki/crl/ADIDCA%5B">http://crl.defence.gov.au/pki/crl/ADIDCA[</a>&lt;integer&gt;]+crl](<a href="http://crl.defence.gov.au/pki/crl/ADIDCA%5B">http://crl.defence.gov.au/pki/crl/ADIDCA[</a>&lt;integer&gt;]+crl)</td>
<td>The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and CRL issuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension). The missing &quot;,binary&quot; at the end of the LDAP URI is a Unicert limitation.</td>
</tr>
</tbody>
</table>
## Table 10 – DIOCA SHA2 Secondary Cross-Certificate [DIOCA-SXC] Profile
B.7 DIOCA SHA1 CRL

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Critical</th>
<th>Defence Interoperability CA CRL Value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td></td>
<td>V2 (1)</td>
<td>X.509 Version 2 CRL profile</td>
</tr>
<tr>
<td>Issuer Signature Algorithm</td>
<td></td>
<td>SHA-1WithRSAEncryption</td>
<td></td>
</tr>
<tr>
<td>Issuer Distinguished Name</td>
<td></td>
<td>CN= ADOCA03</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>OU= CAs</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>OU= PKI</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>OU= DoD</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>O= GOV</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>C= AU</td>
<td></td>
</tr>
<tr>
<td>thisUpdate</td>
<td></td>
<td>&lt;UTCTime&gt;</td>
<td></td>
</tr>
<tr>
<td>nextUpdate</td>
<td></td>
<td>&lt;UTCTime&gt;</td>
<td>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 + 31 days</td>
</tr>
<tr>
<td>Revoked certificates list</td>
<td></td>
<td>0 or more 2-tuple of certificate serial number and revocation date (in UTCTime)</td>
<td></td>
</tr>
<tr>
<td>CRL extensions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CRL Number</td>
<td>No</td>
<td>&lt;Integer&gt;</td>
<td></td>
</tr>
<tr>
<td>Authority Key Identifier</td>
<td>No</td>
<td>&lt;Octet String&gt;</td>
<td>The value of this field is the 160 bit SHA-1 hash of the binary DER encoding of the CA public key information</td>
</tr>
<tr>
<td>CRL entry extensions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Invalidity Date</td>
<td>No</td>
<td>Optional</td>
<td>Date on which it is known or suspected that the private key was compromised or that the certificate otherwise became invalid.</td>
</tr>
<tr>
<td>Reason Code</td>
<td>No</td>
<td>Optional</td>
<td></td>
</tr>
</tbody>
</table>

Table 11 – DIOCA SHA1 CRL Profile
## B.8 DIOCA SHA2 CRL

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Critical</th>
<th>Defence Interoperability CA CRL Value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td></td>
<td>V2 (1)</td>
<td>X.509 Version 2 CRL profile</td>
</tr>
<tr>
<td>Issuer Signature Algorithm</td>
<td></td>
<td>SHA-2WithRSAEncryption</td>
<td></td>
</tr>
<tr>
<td>Issuer Distinguished Name</td>
<td></td>
<td>CN= Australian Defence Interoperability CA [G&lt;integer&gt;] OU= CAs OU= PKI OU= DoD O= GOV C= AU</td>
<td>[G&lt;integer&gt;] is an optional extension for future generations of the Interoperability CA.</td>
</tr>
<tr>
<td>thisUpdate</td>
<td></td>
<td>&lt;UTCTime&gt;</td>
<td></td>
</tr>
<tr>
<td>nextUpdate</td>
<td></td>
<td>&lt;UTCTime&gt;</td>
<td>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 + 31 days</td>
</tr>
<tr>
<td>Revoked certificates list</td>
<td></td>
<td>0 or more 2-tuple of certificate serial number and revocation date (in UTCTime)</td>
<td></td>
</tr>
<tr>
<td>CRL extensions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CRL Number</td>
<td>No</td>
<td>&lt;Integer&gt;</td>
<td></td>
</tr>
<tr>
<td>Authority Key Identifier</td>
<td>No</td>
<td>&lt;Octet String&gt;</td>
<td>The value of this field is the 160 bit SHA-1 hash of the binary DER encoding of the CA public key information</td>
</tr>
<tr>
<td>CRL entry extensions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Invalidity Date</td>
<td>No</td>
<td>Optional</td>
<td>Date on which it is known or suspected that the private key was compromised or that the certificate otherwise became invalid.</td>
</tr>
<tr>
<td>Reason Code</td>
<td>No</td>
<td>Optional</td>
<td></td>
</tr>
</tbody>
</table>

**Table 12 – DIOCA SHA2 CRL Profile**