Australian Government

Defence

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

Version 9.0
November 2023

X.509 Certificate Policy

Notice to all parties seeking to rely

Reliance on a Certificate issued under this Certificate Policy (CP) for the **Defence Interoperability CA (DIOCA)**, identified by subarcs of the object identifier **1.2.36.1.334.1.1.1.3,** is only permitted as set forth in this document.

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

Document Management

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

Change History

Version	Issue Date	Description/ Amendment	Changed by
0.1	June 2011	Initial Draft	AKK
1.0	4 Aug 2011	Released	SJP
2.0	July 2012	Released	SJP
3.0	May 2014	Reviewed for release	PKI Ops Man
4.0	Oct 2016	Released	PKI Operations Manager
4.1	Nov 2016	Updated SHA2 certificate profile	Cogito Group (BB)
4.2	Sep 2017	CSO review	CSO
4.3	February 2018	Reviewed	PKI Operator (LM)
4.4	Dec 2018	Reviewed for GK	Ops Man
5.0	July 2019	Published	PKI Ops Man
5.1	Sep 2020	Removed SHA-1 cert profiles. Other minor updates incl. classification.	CDMC (AKK)
6.0	Oct 2020	Reviewed by DTA – Changes accepted - Released	CDMC (AKK)
6.1	Nov 2021	2021 updates.	CDMC (AKK)
7.0	Dec 2021	Reviewed by DTA – Changes accepted - Released	CDMC (AKK)
7.1	Oct 2022	2022 updates.	CDMC (AKK)
8.0	Nov 2022	Reviewed by DTA – Changes accepted - Published	CDMC (AKK)
8.1	Oct 2023	2023 updates	CDMC (AKK)
9.0	Nov 2023	Published	CDMC (AKK)

Signatures

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

Contents

Table of Tables

Table of Figures

1. INTRODUCTION

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

This CP identifies the rules to manage the *Australian Government Department of Defence* ("Defence") **Interoperability Certificate Authority (DIOCA)** certificates.

This CP includes 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] In general, the rules in this CP identify the minimum standards in terms of security, process, and auditing, for the issuance and use of keys and certificates.

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

A document hierarchy applies:

1. The provisions of any applicable contract, such as a *Cross-certification Arrangement* (CCA), or other relevant contract, will override the provisions of this CP.
2. The provisions of this CP prevail over the provisions of CPS to the extent of any direct inconsistency.
3. The provisions of CPS govern any matter on which this CP is silent.

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

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

1.1 Overview

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.

[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.

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 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.

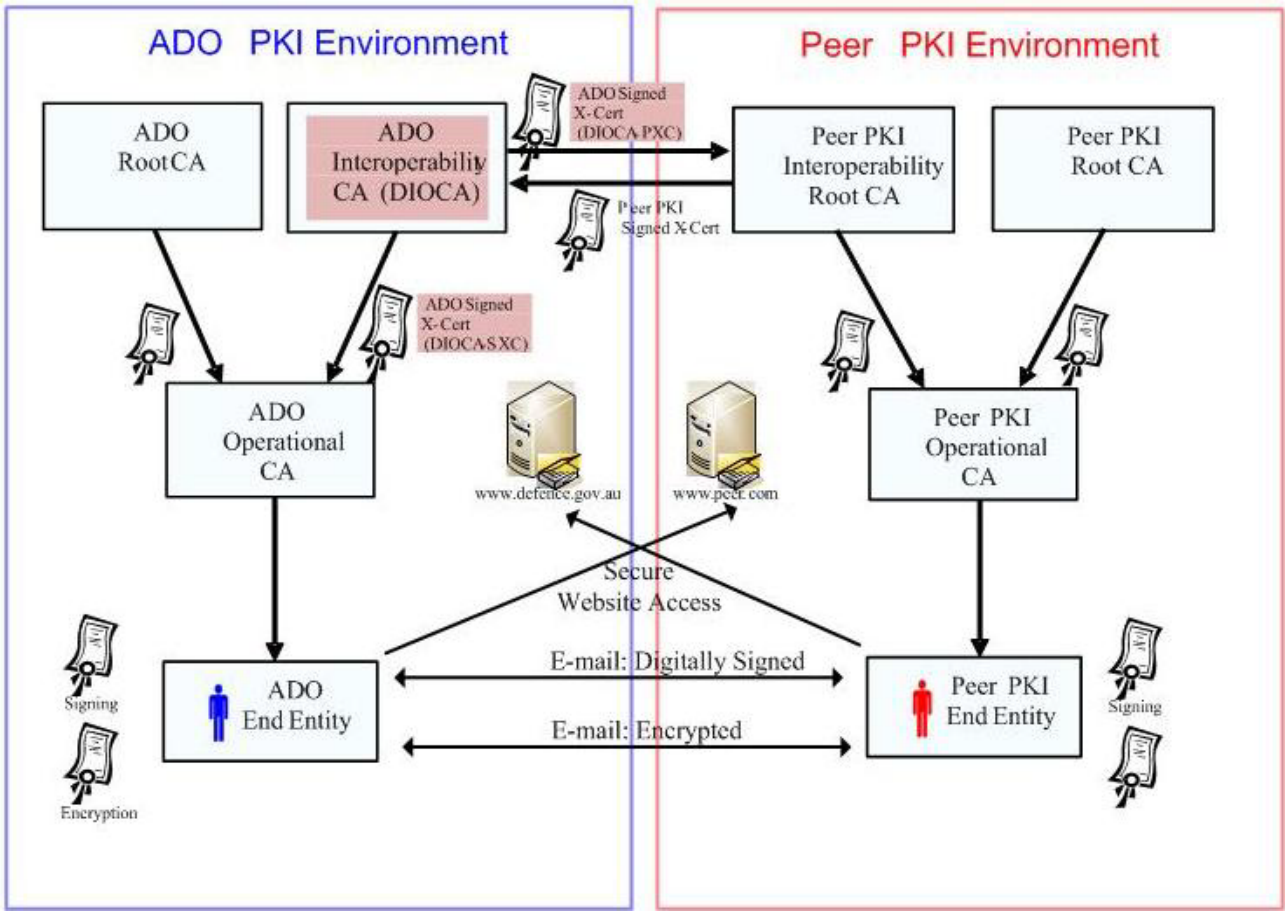

Figure 1 – Extended Bilateral Cross-certification model - example

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) public (1) CA - certificate policy (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-certificates* (DIOCA-PXC) - authentication certificates signed by the DIOCA and issued to Peer CAs;
iii. *Secondary Cross-certificates* (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

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). The CCA describes the full responsibilities of each party.
ii. the Defence PKI Policy Management Authority (PKI PMA)– refer to the Certification Practice Statement (CPS) for their responsibilities, which include, but are not limited to:

    a) the 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);
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[2]; and
v. sign its own internal log files.
vi. sign any CRLs it generates.

1.4.1.2 DIOCA-PXC

Certificates issued by the DIOCA under this CP allow Defence to publish the principal 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 secondary 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 PKI PMA 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 and/or the appropriate certificate uses;
b) Illegal;

[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].

c) Unauthorised;
d) Unethical, or
e) Contrary to Defence policy.

Refer to RCA CP for prohibited uses for *PKI Operator* and core component certificates. Engaging in a prohibited certificate use is a breach of the responsibilities and obligations agreed to by the PKI operators, and Defence disclaims any and all liability in such circumstances.

1.5 Policy administration

1.5.1 Organisation administering the document

See CPS.

1.5.2 Contact person

See CPS.

1.5.3 Authority determining CPS suitability for the policy

See CPS.

1.5.4 CPS approval procedures

See CPS.

1.6 Definitions, acronyms and interpretation

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

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

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

See CPS.

2.2 Publication of certification information

Defence publishes 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 PKI PMA; and
iii. a common 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 PKI PMA; and
iii. the name of the Defence CA that is being cross-signed.

3.1.2 Need for names to be meaningful

The PKI PMA 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, individual operators are identified by their names to allow for system auditing.

3.1.3 Anonymity or pseudonymity of Subscribers

Not applicable.

3.1.4 Rules for interpreting various name forms

Names are compliant with the standard used (e.g. X.500 for DNames).

3.1.5 Uniqueness of names

DIOCA-C and DIOCA-SXC: Names must be unique within the Defence PKI name space.

DIOCA-PXC: Names must be 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 (CSR) for a DIOCA-PXC must be submitted in the format of a PKCS#10 request signed by 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 by the corresponding private key. The generation of the PKCS#10 file must be witnessed by a representative of the PKI PMA and the *PKI Operations Manager*.

3.2.2 Authentication of Organisation Identity

3.2.2.1 DIOCA-C

To establish the DIOCA, the PKI PMA 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

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 PKI PMA 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 PKI PMA 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, ensuring that they are suitable for their role in the creation of the DIOCA-PXC;

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

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:

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

4. 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 PKI PMA. 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 PKI PMA (and the PKI Policy Management Authority (PKI PMA) 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 in the following 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 drive and to removable media, e.g. CD, which is safe-handed to the Defence PKI by its representative[4].
v. Prior to issuing the cross-certificate, the PKI Operations Manager (or their appointed 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). They compare the two hashes.
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.

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. PKI PMA arranges for the cross-certificate signing request generation. A minimum of two representatives of the PKI PMA 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 PKI PMA are required to witness the generation of CA keys.

4.2.1.2 DIOCA-PXC

The PKI PMA 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.

The PKI Operations Manager is responsible for ensuring the external parties nominated representatives/witnesses participating in the cross-certification ceremony are validated, prior to the ceremony, by verifying a Government issued photo ID that matches the name and biometric image.

[4] Alternatively, by diplomatic bag, or sent in an email signed with a trusted certificate.

4.2.1.3 DIOCA-SXC

The PKI PMA 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.

The PKI Operations Manager is responsible for ensuring that external (to Defence) representatives and witnesses participating in the cross-certification ceremony are validated, prior to the ceremony, by verifying a Government issued photo ID that matches the name and biometric image.

4.2.2 Approval or rejection of certificate applications

The PKI PMA approves or rejects the CA certificate and cross-certificate.

4.2.3 Time to process certificate applications

Processing for certificate applications will occur in a timely manner.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

See CPS.

4.3.2 Notification to Subscriber by the CA of issuance of certificate

See CPS.

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.

The DIOCA-PXC is also published in a location that is accessible by the cross-certifying CA's Subscribers (Relying Parties in terms of the cross-certified CA).

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.

Key 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 use of such certificates must not exceed 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 PKI PMA receives notification of progress, issues and completion of PKI PMA 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 PKI PMA will determine other circumstances as appropriate.

4.8.2 Who may request certificate modification

Certificate modification may be requested by:

i. the PKI PMA, 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 PKI PMA receives notification of progress, issues and completion of PKI PMA 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 from the time a Subscriber or Key Custodian becomes aware of a reason for revocation, until submitting a revocation request.

The PKI PMA, or an approved delegate, in exceptional circumstances (such as a security or law enforcement investigation), 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 or OCSP. It is the Relying Party's responsibility to determine their requirement for revocation checking.

4.9.7 CRL issuance frequency (if applicable)

CRLs for the 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

See 4.9.6 (Revocation checking requirement for Relying Parties)

4.9.11 Other forms of revocation advertisements available

See CPS.

4.9.12 Special requirements re key compromise

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 is to 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. DIOCAs 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 air gap 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 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 2048 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 required 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)
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 for Defence certificate profiles.

Refer to [ACP 185] for requirements.

7.1.3 Algorithm Object Identifiers

7.1.3.1 Signature algorithms

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

sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12}
sha512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13}
ecdsa-with-SHA256	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)}
ecdsa-with-SHA384	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(3)}
ecdsa-with-SHA512	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(4)}

Table 1 – Signature Algorithm OIDs

7.1.3.2 Subject Public Key cryptographic algorithms

Certificates under this CP will use one of the following OIDs for identifying the algorithm for which the subject key was generated. (See Subject Public Key Information in certificate profile).

rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
Id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-x9-62(10045) public-key-type (2) 1}
Dhpublicnumber	{iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}
Id-ecDH	{iso(1) identified-organization(3) certicom(132) schemes(1) ecdh(12)}

Table 2 – SPKI Algorithm OIDs

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

7.1.3.3 Elliptic curve public key curve

Where certificates contain an elliptic curve public key, the parameters must be specified as one of the following named curves.

ansip256r1	{iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 7}
ansip384r1	{iso(1) identified-organization(3) certicom(132) curve(0) 34}
ansip521r1	{iso(1) identified-organization(3) certicom(132) curve(0) 35}

Table 3 – Elliptic Curve parameters

7.1.4 Name Forms

7.1.4.1 DIOCA-C and DIOCA-SXC

The *Common Nam*e (CN) component is based on the name assigned by the PKI PMA 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:

Individual:	Low	1.2.36.1.334.1.2.1.1
	Medium	1.2.36.1.334.1.2.1.2
	High	1.2.36.1.334.1.2.1.3

	Very High	1.2.36.1.334.1.2.1.4
Resources: (see note below)	Low	1.2.36.1.334.1.2.2.1
	Medium	1.2.36.1.334.1.2.2.2
	High	1.2.36.1.334.1.2.2.3

Table 4 – 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

As per ACP 185 section 7.1.7:

A Principal Cross-Certificate issued to a bridge PKI shall contain the policyConstraints extension with inhibitPolicyMapping field omitted, and with requiredExplicitPolicy field with a skipCerts value of zero. It shall contain the inhibitAnyPolicy extension with a skipCerts value of zero.

A Principal Cross-Certificate issued to a non-Bridge (e.g., Enterprise) PKI 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 DIOCA-SXC

Policy constraints are not present.

7.1.8 Policy Qualifiers Syntax and Semantics

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

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

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

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

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

7.2 CRL profile

7.2.1 Version Numbers

CRLs issued 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 6960.

7.3.2 OCSP Extensions

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

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

See CPS.

8.2 Identity/qualifications of assessor

See CPS.

8.3 Assessor's relationship to assessed entity

See CPS.

8.4 Topics covered by assessment

See CPS.

8.5 Actions taken as a result of deficiency

See CPS.

8.6 Communication of results

See CPS.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

No stipulation.

9.1.2 Certificate access fees

There is no fee for accessing Certificates from approved repositories.

9.1.3 Revocation or status information access fees

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

9.1.4 Fees for other services

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

9.1.5 Refund policy

See CPS.

9.2 Financial responsibility

See CPS.

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

9.2.1 Insurance coverage

No stipulation.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

No stipulation.

9.3 Confidentiality of business information

See CPS.

9.4 Privacy of personal information

9.4.1 Privacy plan

No Personal Information (as defined in the *Privacy Act 1988 (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)

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

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 Agency is not responsible and cannot be held liable for any loss of any kind in relation to the use of digital keys and certificates issued by a Gatekeeper accredited Service Provider. By granting a Service Provider Gatekeeper Accreditation the Digital Transformation Agency makes no representation and gives no warranty as to the:

- Accuracy of any statements or representations made in, or suitability of, the Approved Documents of a Gatekeeper accredited Service Provider;
- Accuracy of any statement or representation made in, or suitability of, the documentation of a Service Provider in a Gatekeeper recognised PKI domain; or

- Standard or suitability of any services thereby provided by any Subscriber or Relying Party or application.

9.9 Indemnities

See CPS.

9.10 Term and termination

9.10.1 Term

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

9.10.2 Termination

See CPS. 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 PKI PMA 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:

[6960]	RFC6960 Internet X.509 Public Key Infrastructure On-line Certificate Status Protocol (ocsp), Internet Engineering Task Force, available at https://www.ietf.org/rfc/rfc6960.txt
[3647]	RFC3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Internet Engineering Task Force, available at https://www.ietf.org/rfc/rfc3647.txt
[5280]	RFC5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Internet Engineering Task Force, available at https://www.ietf.org/rfc/rfc5280.txt
[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.)
[CPS]	X.509 Certification Practice Statement for the Australian Department of Defence, available at https://defence.gov.au/pki/cps/Defence-CPS.pdf
[DRBCP]	Australian Department of Defence Public Key Infrastructure Disaster Recovery and Business Continuity Plan (classified)
[EOI]	Gatekeeper Evidence of Identity (EOI) policy available at https://www.dta.gov.au/standard/design-guides/authentication-frameworks/national-e-authentication-framework
[GK2015]	Digital Transformation Office, Gatekeeper PKI Framework v3.1 Dec 2015, available at https://www.dta.gov.au/standard/design-guides/authentication-frameworks/gatekeeper-public-key-infrastructure-framework/
[KMP]	Australian Department of Defence Public Key Infrastructure Key Management Plan (classified)
[LOA]	Department of Defence Public Key Infrastructure Assurance Level Requirements document, available at https://defence.gov.au/pki/_lib/doc_pdf/LOA.pdf
[RCA CP]	X.509 Certificate Policy for the Australian Department of Defence Root Certification Authority and Subordinate Certificate Authorities, available at https://defence.gov.au/pki/_lib/doc_pdf/Defence-ADPRCA-CP.pdf
[VA CP]	X.509 Certificate Policy for the Australian Department of Defence Validation Authority Certificates, available at https://defence.gov.au/pki/_lib/doc_pdf/Defence-Validation-Authority-CP.pdf

Table 5 - References

APPENDIX B. CERTIFICATE, CRL AND OCSP PROFILES AND FORMATS

B.1 DIOCA certificate [DIOCA-C]

This is the Defence Interoperability Root CA, a self-signed certificate used to sign other CA certificates to create a trusted certificate chain.

Field	Critical	Defence Certificate Value	Notes
Version		V3 (2)	Version 3 of X.509
Serial		<octet string>	
Issuer Signature Algorithm		SHA-2WithRSAEncryption	
Issuer Distinguished Name		CN= Australian Defence Interoperability CA [G<integer>] OU= CAs OU= PKI OU= DoD O= GOV C= AU	Encoded as printable string. [G<integer>] is an optional extension for future generations of the Interop CA.
Validity Period		Not before <UTCtime> Not after <UTCtime>	Maximum 20 years from date of issue
Subject Distinguished Name		CN= Australian Defence Interoperability CA [G<integer>] OU= CAs OU= PKI OU= DoD O= GOV C= AU	Self-signed. Encoded as printable string. [G<integer>] is an optional extension for future generations of the Interop CA.
Subject Public Key Information		Minimum 2048 bit RSA key modulus, rsaEncryption	
Issuer Unique Identifier		-	Not Present
Subject Unique Identifier		-	Not Present
X.509 V3 extensions:			
Authority Key Identifier	No	<octet string>	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.[5]
Subject Key Identifier	No	<octet string>	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.

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

Field	Critical	Defence Certificate Value	Notes
Key usage	Yes	Certificate Signing CRL Signing Off-line CRL Signing Digital Signature Non-Repudiation	Digital signature and non-repudiation key usages are only used for the signing of the CA's own log entries.
Extended key usage		-	Not Present
Private key usage period		-	Not Present
Certificate policies	No	[1] Policy OID: {1.2.36.1.334.1.1.1.3} Policy Qualifier - CPS pointer: http://crl.defence.gov.au/pki	The OID of this CP (DIOCA)
		[2] Policy OID: {2.5.29.32.0}	anyPolicy OID
Policy Mapping		-	Not Present
Subject Alternative Name		-	Not Present
Issuer Alternative Name		-	Not Present
Subject Directory Attributes		-	Not Present
Basic Constraints	Yes	CA=True, path length constraint=none	
Name Constraints		-	Not Present
Policy Constraints		-	Not Present
Subject Information Access		-	Not Present
Authority Information Access		-	Not Present
CRL Distribution Points		-	Not Present

Table 6 – DIOCA Certificate [DIOCA-C] Profile

B.2 Principal Cross Certificate [DIOCA-PXC]

This is the profile of a Principal Cross Certificate issued by DIOCA, where the Subject is the external party's interoperability CA. The Principal Cross Certificate provides a trusted certificate path for Defence PKI's Subscribers to the other parties PKI's subscribers (i.e. the other PKI's CA is now signed by a trusted Defence CA). The Principal cross certificate contains the Policy Mapping extension.

Field	Critical	Req'd	Identity Certificate Value	Notes
Version		Yes	V3 (2)	Version 3 of X.509
Serial		Yes	<octet string>	Unique value generated by the issuing CA
Issuer Signature Algorithm		Yes	SHA-2WithRSAEncryption	
Issuer Distinguished Name		Yes	CN= Australian Defence Interoperability CA [G<integer>] OU= CAs OU= PKI OU= DoD O= GOV C= AU	Encoded as printable string. [G<integer>] is an optional extension for future generations of the Interop CA.
Validity Period		Yes	Not before <UTCtime> Not after <UTCtime>	Maximum 3 years from date of issue. Note: the notBefore component will be the certificate's issue date. The notAfter component is the day ending the validity period.
Subject Distinguished Name		Yes	<Distinguished name of cross certified CA>	In accordance with Cross Certification Arrangement.
Subject Public Key Information (SPKI)		Yes	RsaEncryption {1 2 840 113549 1 1 1} Minimum 2048 bit RSA key modulus	
Issuer Unique Identifier			-	Not Present
Subject Unique Identifier			-	Not Present
X.509 V3 extensions:				
Authority Key Identifier	No	Yes	<octet string>	The value of this field is the 160 bit SHA-1 hash of the binary DER encoding of the signing CA's public key.[6]
Subject Key Identifier	No	Yes	<octet string>	The value of this field is the 160 bit SHA-1 hash of the binary DER encoding of the subject's public key.
Key Usage	Yes	Yes	Certificate Signing, Off-line CRL Signing, CRL Signing	

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

Field	Critical	Req'd	Identity Certificate Value	Notes
Extended key usage			-	Not Present
Private key usage period			-	Not Present
Certificate policies[7]	No	Yes	[1] Policy OID: {1.2.36.1.334.1.1.1.3} Policy Qualifier - CPS pointer: http://crl.defence.gov.au/pki/	The OID of this CP.
			Additional Policies	In accordance with Cross Certification Arrangement. Sequence of one or more policy information terms, each of which consists of an object identifier (OID) and optionally id-qt-cps | id- qt-unotice qualifiers (ACP 185)
Policy Mapping	No	Yes	Sequence of one or more pairs of OIDs; each pair includes an issuerDomainPolicy and a subjectDomainPolicy	In accordance with Cross Certification Arrangement.
Subject Alternative Name			-	Not Present
Issuer Alternative Name			-	Not Present
Subject Directory Attributes			-	Not Present
Basic Constraints	Yes	Yes	Subject Type=CA Path Length Constraint=1 or 2	In accordance with Cross Certification Arrangement requirements
Name Constraints	Yes		Permitted: [1] directoryName	In accordance with Cross Certification Arrangement. (Optional) If included, it must contain permittedSubtrees or excludedSubtrees field. Recommend that if asserted it be marked critical.
Policy Constraints	Yes	Yes	Explicit Policy Skip Certs = 0 Inhibit Policy Mapping Skip Certs = 0	Refer to section 7.1.7 for rules specific to Principal Cross-certificates issued to a bridge PKI, versus one issued to a non-bridge PKI.
Inhibit Any Policy	No[8]	Yes	02 01 00	
Subject Information Access			-	Not Present See ACP 185 for requirements if included.

[7] Certificate policies may vary based upon the Cross Certification Agreement requirements.

[8] This is not conformant to the RFC due to application compatibility issues.

Field	Critical	Req'd	Identity Certificate Value	Notes
Authority Information Access	No	See Notes	[1] Access method=OCSP {1.3.6.1.5.5.7.48.1} Access location: http://ocsp.defence.gov.au [2] Access method=CAIssuer {1.3.6.1.5.5.7.48.2}: Access location: http://crl.defence.gov.au/pki/certificates/ADIOCA[G<integer>] [3] Access method=CAIssuer {1.3.6.1.5.5.7.48.2}: Access location: ldap://dir.defence.gov.au/cn=Australian Defence Interoperability CA [G<integer>],ou=CAs,ou=PKI,ou=DoD,o=GOV,c=AU? cACertificate;binary,crossCertificatePair;binary	The Cross Certification Agreement specifies only the ocsp access method for the principal cross-certificates. ACP185: - id-ad-ocsp is optional. - id-ad-caIssuer http URI is required. - id-ad-caIssuer ldap is optional.
CRL Distribution Points	No	Yes (http URI)	[1] Distribution Point Name (http): http://crl.defence.gov.au/pki/crl/ADIOCA[G<integer>].crl [2] Distribution Point Name (ldap): ldap://dir.defence.gov.au/cn=Australian Defence Interoperability CA [G<integer>],ou=CAs,ou=PKI,ou=DoD,o=GOV,c=AU?certificateRevocationList	The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the 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 ";binary" at the end of the LDAP URI is a Unicert limitation.

Table 7 - DIOCA Principal Cross-Certificate [DIOCA-PXC] Profile

B.3 DIOCA Secondary Cross Certificate [DIOCA-SXC]

A Secondary Cross Certificate is issued by DIOCA, where the Subject is a Defence Operational CA, to provide a trusted certification path for the other party's PKI Subscribers to the Defence PKI. To complete the trust chain, they also need *their* Principal Cross Certificate to top the chain, i.e. Defence PKI's DIOCA certificate signed by their trusted CA. A Secondary Cross-certificate does not contain the Policy Mapping extension.

Field	Critical	Identity Certificate Value	Notes
Version		V3 (2)	Version 3 of X.509
Serial		<octet string>	Unique value generated by the issuing CA
Issuer Signature Algorithm		SHA-2WithRSAEncryption	
Issuer Distinguished Name		CN= Australian Defence Interoperability CA [G<integer>] OU= CAs OU= PKI OU= DoD O= GOV C= AU	Encoded as printable string. [G<integer>] is an optional extension for future generations of the Interop CA.
Validity Period		Not before <UTCtime> Not after <UTCtime>	Maximum 3 years from date of issue
Subject Distinguished Name		CN= <subCAname> OU= CAs OU= PKI OU= DoD O= GOV C= AU	Encoded as printable string. The <subCAname> represents a unique name for the public sha2 subCA issuing infrastructure. (See Defence-ADPRCA-CP for detailed naming information).
Subject Public Key Information		Minimum 2048 bit RSA key modulus, rsaEncryption	
Issuer Unique Identifier		-	Not Present
Subject Unique Identifier		-	Not Present
X.509 V3 extensions:			
Authority Key Identifier	No	<octet string>	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.
Subject Key Identifier	No	<octet string>	The value of this field is the 160 bit SHA-1 hash of the binary DER encoding of the subject's public key information.
Key Usage	Yes	digitalSignature, nonRepudiation, Certificate Signing, Off-line CRL Signing, CRL Signing	Digital signature and non-repudiation key usages are only used for the signing of the CA's own log entries.
Extended key usage		-	Not Present
Private key usage period		-	Not Present
Certificate policies	No	[1] Policy OID: {1.2.36.1.334.1.1.1.3} Policy Qualifier - CPS pointer: http://crl.defence.gov.au/pki/	The OID of this CP.

Field	Critical	Identity Certificate Value	Notes
		[2] Policy OID: {1.2.36.1.334.1.2.1.4}	Level of Assurance – Individual – Very High
		[3] Policy OID: {1.2.36.1.334.1.2.1.3}	Level of Assurance – Individual – High
		[4] Policy OID: {1.2.36.1.334.1.2.1.2}	Level of Assurance – Individual – Medium
		[5] Policy OID: {1.2.36.1.334.1.2.1.1}	Level of Assurance – Individual – Low
		[6] Policy OID: {1.2.36.1.334.1.2.2.3}	Level of Assurance – Resource – High
		[7] Policy OID: {1.2.36.1.334.1.2.2.2}	Level of Assurance – Resource – Medium
		[8] Policy OID: {1.2.36.1.334.1.2.2.1}	Level of Assurance – Resource – Low
		[9] Policy OID: {2.5.29.32.0}	anyPolicy OID
Policy Mapping		-	Not Present
subject Alternative Name (Email)		-	Not Present
Subject Alternative Name (Microsoft UPN)		-	Not Present
Issuer Alternative Name		-	Not Present
Subject Directory Attributes		-	Not Present
Basic Constraints	Yes	Subject Type=CA Path Length Constraint=None	
Name Constraints		-	Not Present
Policy Constraints		-	Not Present
Subject Information Access		-	Not Present
Authority Information Access	No	[1] Access method=OCSP {1.3.6.1.5.5.7.48.1}: Access location: http://ocsp.defence.gov.au [2] Access method=CAIssuer {1.3.6.1.5.5.7.48.2}: Access location: http://crl.defence.gov.au/pki/certificates/ADIOCA[G<integer>] [3] Access method=CAIssuer {1.3.6.1.5.5.7.48.2}: Access location: ldap://dir.defence.gov.au/cn=Australian Defence Interoperability CA [G<integer>],ou=CAs,ou=PKI,ou=DoD,o=GOV,c=AU?cACertificate;binary,crossCertificatePair;binary	The AIA is to reference a location containing the cross-certificates for the Australian [G<integer>] 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.
CRL Distribution Points	No	[1] Distribution Point Name (http): http://crl.defence.gov.au/pki/crl/ADIOCA[G<integer>].crl [2] Distribution Point Name (ldap): ldap://dir.defence.gov.au/cn=Australian Defence Interoperability CA [G<integer>],ou=CAs,ou=PKI,ou=DoD,o=GOV,c=AU?certificateRevocationList	The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the 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 ";binary" at the end of the LDAP URI is a Unicert limitation.

Table 8 –DIOCA Secondary Cross-Certificate [DIOCA-SXC] Profile

B.4 DIOCA CRL

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

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

Table 9 – DIOCA CRL Profile