Australian Government

Defence

# X.509 Certificate Policy
# for the
# Australian Department of Defence
# Individual - Medium Assurance Certificate

Version 5.0
November 2023

# Notice to all parties seeking to rely

Reliance on a Certificate issued under this Certificate Policy for Australian Department of Defence Individual - Medium Assurance Certificates, identified by subarcs of the object identifier **1.2.36.1.334.1.1.2.1,** is only permitted as set forth in this document.

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

## Document Management

| | |
|---|---|
| **This document is controlled by:** | *Defence Public Key Infrastructure Policy Management Authority (PKI PMA)* |
| **Changes are authorised by:** | Defence Public Key Infrastructure Policy Management Authority (PKI PMA)<br>*Gatekeeper Competent Authority* (GCA) |

## Change History

| Version | Issue Date | Description/ Amendment | Changed by |
|---|---|---|---|
| 0.1 | June 2019 | Initial Draft – New policy to issue both medium assurance software and hardware tokens | GJF |
| 0.2 | June 2019 | Initial Version | GJF |
| 1.0 | July 2019 | Published. | PKI Ops Man |
| 1.1 | March 2020 | Edited subarc OID as it was incorrectly referencing<br>1.2.36.1.334.1.1.2.1 (software). Changed to<br>1.2.36.1.334.1.1.2.1.1 (software MAC) | Frankie Braybon (PKI Operator) |
| 1.2 | Sep 2020 | Updates and corrections.<br>OIDs re-adjusted to:<br>1.2.36.1.334.1.1.2.1 (CP)<br>1.2.36.1.334.1.1.2.1.1 (ID-MA SW variant)<br>1.2.36.1.334.1.1.2.1.2 (ID-MA HW variant)<br>Other minor corrections/improvements only. | CDMC (AKK) |
| 2.0 | Oct 2020 | Reviewed by DTA – Changes accepted - Released | CDMC (AKK) |
| 2.1 | Nov 2021 | 2021 updates. Removal of confidentiality certificate. Update of revocation processes. Other minor changes. | CDMC (AKK) |
| 3.0 | Dec 2021 | Reviewed by DTA – Changes accepted - Released | CDMC (AKK) |
| 3.1 | Oct 2022 | 2022 Updates | CDMC (AKK) |
| 4.0 | Nov 2022 | Reviewed by DTA – Changes accepted - Published | CDMC (AKK) |
| 4.1 | Nov 2022 | Draft with split cert changes (auth & signing) | CDMC (AKK) |
| 4.2 | Nov 2023 | 2023 updates. | CDMC (AKK) |

| Version | Issue Date | Description/ Amendment | Changed by |
|---|---|---|---|
| 5.0 | Nov 2023 | Published | CDMC (AKK) |

## Signatures

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

# Contents

## List of Tables

# 1. INTRODUCTION

*Certificate policies (CPs)* are, in the *X.509* version 3 digital certificate standard, the named set of rules regarding the applicability of a *certificate* to a particular community (e.g. *Defence*) and contain information about the specific structure of the relevant certificate type and grade.

This CP identifies the rules to manage the **Australian Department of Defence** ('Defence') **Individual – Medium Assurance Certificate (AD-ID-MAC).**

This CP includes the obligations of the *Public Key Infrastructure* (PKI) entities, and how they apply to the parties, indicated in section 1.3. In general, the rules in this CP identify the minimum standards in terms of security, process and auditing for the issuance and use of keys and certificates.

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

A document hierarchy applies:

1. The provisions of any applicable contract such as a *Subscriber Agreement*, Deed of Agreement, *Cross-certification Arrangement* (CCA) or other relevant contract override the provisions of this CP.
2. The provisions of this CP prevail over the provisions of CPS to the extent of any direct inconsistency.
3. The provisions of the 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

An **AD-ID-MAC** is used to identify an individual who has an affiliation with Defence (Active Military Member, Reservist Military Member, Australian Public Servant employed by the Australian Defence, Cadet, Contractor or Consultant etc.) and who has a requirement, which has been approved by Defence, to:

i. Interact directly with Defence assets or systems, using *Public Key Technology* (PKT);
ii. Authenticate with a third party, as an affiliate of Defence; or
iii. Provide a *digital signature*, as an individual *affiliated* with Defence.

AD-ID-MACs are issued either as:

i. Software (Authentication/Signing keys and certificates stored in the Subscriber's device/workstation software crypto store); or
ii. Hardware (Authentication and/or Digital Signing keys and certificates stored on the Subscriber's hard token, e.g. smart card)

No authority, or privilege, applies to an individual by becoming an approved AD-ID-MAC holder, other than confirming an affiliation with Defence.

## 1.2 Document name and identification

The title for this CP is "X.509 Certificate Policy for the Australian Department of Defence Individual – Medium Assurance Certificate".

The *Object Identifier* (OID) for this CP is **1.2.36.1.334.1.1.2.1** :

**{iso (1) iso-member (2) australia (36) government (1) department of defence (334) pki (1) public(1) individual (2) medium assurance cp (1)}**

Further variants may be created under this CP OID branch. Refer to certificate profiles in Appendix B. Each variant is assigned an OID to be asserted in certificates that comply with the policy stipulations and certificate profile related to that OID, e.g.:

|  |  |
|---|---|
| 1. AD-ID-MAC - Software variants | **1.2.36.1.334.1.1.2.1.1.n** |
| 2. AD-ID-MAC - Hardware variants | **1.2.36.1.334.1.1.2.1.2.n** |

## 1.3 PKI participants

### 1.3.1 Certification authorities

The *Certification Authorities* (CAs) that issue certificates under this CP are Defence Public CAs, which are Gatekeeper accredited. Defence Public CAs are managed by the Defence Certificate and Directory Management Centre (CDMC). Refer to [ADPRCA] for information about the Root CA and Issuing CAs.

The issuing CA can be found in the certificate "Issuer" field.

### 1.3.2 Registration authorities

The *Registration Authorities* (RAs) that perform the registration function under this CP are Gatekeeper accredited Defence RAs. AD-ID-MACs are issued using the *Defence Identity Management Environment*. For further information, see CPS.

### 1.3.3 Subscribers

The term *Subscriber* refers to the individual (person) whose name appears as the subject in an AD-ID-MAC, and includes any individual that has been approved as having a requirement to be authenticated as affiliated with Defence. Subscribers include:

i. Defence personnel (permanent and reserve members of the *Australian Defence Force* (ADF), and APS employees);
ii. Members of the ADF Cadets;
iii. Contractors, Consultants and Professional Service Providers (individuals); and
iv. Other individuals approved by Defence as having a requirement for an AD-ID-MAC.

A Subscriber issued a certificate under this CP does not automatically receive access, authority or privilege to Defence assets or systems. Defence assets and systems may act as a *Relying Party* granting access, authority or privilege to an individual.

### 1.3.4 Relying parties

A Relying Party may use an AD-ID-MAC to:

i. Verify the identity of a Subscriber;
ii. Validate a digital signature;
iii. Verify the integrity of a communication with the Subscriber; or
iv. Ensure the non-repudiation of a communication with a Subscriber.

Before relying on the Subscriber certificate, a Relying Party must:

i. Verify the validity of a digital certificate;

ii. Verify that the digital certificate is being used within the limits specified in the CP; and
iii. Promptly notify the RA in the event that it suspects that there has been a compromise of the Subscriber's *Private Keys*.

A Relying Party is responsible for deciding whether, and how, to establish:

i. The processes of checking validity of the Subscriber's certificate;
ii. Any authority, or privilege, of the Subscriber to act on behalf of Defence; and
iii. Any authority, access or privilege the Subscriber has to the Relying Party's assets or systems.

A Relying Party agrees to the conditions of this CP and the CPS. The use of a certificate, or associated revocation information, issued under this CP is the Relying Party's acceptance of the terms and conditions of this CP and CPS.

### 1.3.5 Other participants

Other participants include:

i. The *Defence PKI Policy Management Authority (PKI PMA*) - refer to the CPS for the PKI PMA's responsibilities, which include, but are not limited to:

   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/RA); and
   d) Approval of operational standards and guidelines to be followed.

ii. *Accreditation Agencies* – to provide independent assurance that the facilities, practices and procedures used to issue AD-ID-MACs comply with this CP, the CPS and other relevant documentation (policy and legal).
iii. *Directory Service* providers – to provide a *repository* for certificates and certificate status information issued under this CP.

## 1.4 Certificate usage

Certificates issued under this CP, in conjunction with their associated private keys, allow a Subscriber to:

i. Authenticate themselves to a Relying Party electronically in online transactions; and
ii. Digitally sign electronic documents, transactions and communications.

### 1.4.1 Appropriate certificate uses

Certificates issued under this CP, in conjunction with their associated private key, and in accordance with the certificate profile (key usage), may be used:

i. For the authentication of the identity of a Subscriber, during the conduct of any lawful business with that individual, as an individual affiliated with Defence and for which the *level of assurance* has been assessed as sufficient by the PKI PMA and the Relying Party organisation;
ii. To provide accountability and non-repudiation[1] of AD-ID-MAC Subscriber transactions or communication; and
iii. To verify the integrity of a communication from a Subscriber to a Relying Party.

[1] Acceptable for non-repudiation of Routine Orders, administrative processes and minor value financial transactions other than transactions involving issuance or acceptance of contracts or contract modifications.

Relying Parties should note any risks identified as per Appendix D in relation to the Defence requirements of Individual - Medium Assurance certificates.

### 1.4.2 Prohibited certificate uses

The prohibited uses for certificates issued under this CP are:

i. To use the certificate in a way that represents that the certificate possesses any authority, access, privilege or delegations that may be afforded to the Subscriber.
ii. To use the certificate in a way that represents that communications and transactions can only occur over certain specified infrastructure for that transaction or communication.
iii. To use the certificate and keys in a way that is not in accordance with the specified key usage.
iv. For a Subscriber 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;
c) Unauthorised;
d) Unethical, or
e) Contrary to Defence policy.

The acceptance of a certificate by a Relying Party for a prohibited purpose is at the Relying Party's risk. Engaging in a prohibited certificate use is a breach of the responsibilities and obligations agreed to by the Subscriber, 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 (B.3) also applies to this CP.

# 2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

## 2.1 Repositories

See CPS.

## 2.2 Publication of certificate information

Defence publishes the issuing CA certificate, and the issuing CA's latest *Certificate Revocation List* (CRL) in its repository. This information is available to Relying Parties internal and external to Defence.

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

i. this CP; and
ii. the CPS.

## 2.3 Time or frequency of publication

Published documentation is updated on approved change.

The issuing CA publishes new certificates and CRLs at least once every *Operational Day*.

## 2.4 Access controls on repositories

See CPS.

# 3. IDENTIFICATION AND AUTHENTICATION

## 3.1 Naming

### 3.1.1 Types of names

Every certificate issued under this CP must have:

i. a clear distinguishable and unique *Distinguished Name* (DN) in the certificate subjectName field;
ii. as an alternative name in the subjectAlternativeName field; the Subscriber's Defence email address, as well as their Microsoft *Unique Principal Name* (UPN);
iii. common name components of the name, for both the subjectName and subjectAlternativeName, that are unique to the individual within the Defence name space; and
iv. the DN in the form of a X.501 printable string and not blank.

To achieve a unique DN the *Common Name* (CN) component is based on the Subscriber's name derived from the Defence Identity Management environment.

### 3.1.2 Need for names to be meaningful

Names used to identify the Subscriber are to be based on the Subscriber's Defence email address and:

i. Relate to identity of the Subscriber as provided by the *Defence Directory* entry;
ii. Must not identify the Subscriber by role or position; and
iii. *Evidence of Identity* (EOI) information verifying the identity of the Subscriber must relate to the Subscriber's Defence Directory entry.

### 3.1.3 Anonymity or pseudonymity of Subscribers

This CP prohibits using an anonymous or pseudonymous Subscriber name.

However, the Subscriber's common name as identified in the Defence Directory may be used if it is their Defence email address as well.

### 3.1.4 Rules for interpreting various name forms

Names must be compliant with the standard used (e.g. X.500 for DNames or RFC822 for email addresses.)

### 3.1.5 Uniqueness of names

Names must be unique within the Defence name space. Names used in certificates must be unique to the individual and valid for that individual irrespective of their affiliation or relative location to, or within, Defence. A name issued to an individual is permanent, even after the Subscriber's affiliation expires, and this CP prohibits the re-use of that name by another individual as a Subscriber name.

### 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 AD-ID-MAC soft token*

A soft token containing the *key pair* is generated for the individual on the workstation the first time the user logs in to their account. To prove possession of the private key, a digitally-signed certificate request is submitted to the RA. The submission is made using the credentials supporting access to the individual's account within the *Defence Single Information Environment* (SIE).

#### *3.2.1.2 AD-ID-MAC hard token*

Following authentication of the Subscriber by the *Token Management System* (TMS), the Subscriber's hard token generates the private and *public* keys, and submits a digitally signed certificate request to the RA via the TMS. The RA validates the certificate request prior to submitting it to the CA for issuance. To activate key usage, the Subscriber must enter their token's passphrase, thereby proving the Subscriber has possession of the token with the generated private key.

### 3.2.2 Authentication of organisation identity

To be identified as *affiliated* with Defence the Subscriber must be identified in the *Defence Directory*. This identification is validated by aligning their unique identifier during the enrolment process.

### 3.2.3 Authentication of individual identity

Applicants must have an account within the SIE and their affiliation to Defence verified by reference to the Defence Directory prior to issue of a certificate (soft or hard token).

Prior to certificate issuance the individual's identity is authenticated to obtain a Defence network account which generally includes the following processes:

i. The Subscriber undergoes the Defence security clearance process that confirms the Subscriber's security status and identity.
ii. The Subscriber's identity is re-validated as part of the process to issue a Defence facility access card (positive face-to-face identification using a government issued token with photograph).
iii. The Subscriber's identity attributes are registered in the Defence Identity Management environment depending on the Subscriber's role within Defence (whether Defence personnel or other individual), the Subscriber is:

   a) Registered within the *Personnel Management Key Solution* (PMKeyS) system for Defence personnel; or

b) Registered within the *Other Defence Support* (ODS) system for other approved Defence affiliated individuals.

iv. Once registered in Defence's Identity Management environment, the Subscriber's identity attributes are populated into the Defence Directory.

v. To obtain a network account, the Subscriber's sponsor validates the Subscriber's security clearance, positively identifies the applicant using a government issued token with photograph (Drivers Licence, Passport etc.), confirms the Defence Directory entry and submits a network access request.

vi. Upon receiving a valid network access request, an account is created for the Subscriber. The Defence Directory is used as the authoritative source when creating a user's account within the SIE.

#### *3.2.3.1 AD-ID-MAC soft token*

A soft token is issued automatically to the known Subscriber upon successful authentication to their network account.

#### *3.2.3.2 AD-ID-MAC hard token*

The Subscriber, while logged in to their network account, can access the Token Management System (TMS) Self Service client. The TMS verifies the Subscriber's identity by checking that the account details and the token serial number align with the data derived from the *Defence Directory*. Upon authentication, the Subscriber is able to activate their token and request a certificate, using the key pair generated on the hard token in the activation process. The PKI PMA may approve alternative methods to verify a Subscriber's identity for special circumstances.

### 3.2.4 Non-verified subscriber information

All Subscriber information contained in a certificate is verified against the Defence Directory.

### 3.2.5 Validation of authority

No authority, or privilege, applies to an individual by becoming an approved AD-ID-MAC holder, other than confirming an affiliation with Defence. The Subscriber's affiliation with Defence is validated by ensuring they have an account within the SIE and by reference to the Defence Directory prior to issuance of a certificate.

### 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

A Subscriber authenticates to the network (soft token) or to the TMS (hard token) prior to routine *re-key*. No additional identification is required.

#### *3.3.1.1 AD-ID-MAC soft token*

For soft tokens, where required, authentication to the network automatically generates a routine re-key.

#### *3.3.1.2 AD-ID-MAC hard token*

For hard tokens, routine re-key is normally managed via the TMS User Self Service client prior to the original certificate expiring. In such cases, there is no need to re-identify the Subscriber using other methods, as they must authenticate to the TMS with their hard token, using their *Personal Identification Number* (PIN). They will then follow the TMS processes for replacing their certificate, during which time the new key pair will be generated.

### 3.3.2 Identification and authentication for re-key after revocation

See 3.2 (Initial Identity Validation).

## 3.4 Identification and Authentication for Revocation Requests

Revocation of certificates is in accordance with this section and 4.9 (Certificate revocation and suspension) of this CP and the CPS.

### 3.4.1 AD-ID-MAC soft token - Subscriber request

Soft tokens are normally not revoked; if there is an actual or suspected compromise, it is likely the account is compromised and will be disabled, or deleted and subsequently recreated. If the Subscriber's subscription is ended, as per 4.11 (End of subscription) the account is disabled or deleted.

If a Subscriber knows or suspects that their Windows login has been compromised, they must contact SIE support immediately. Identification for such a support call follows normal Defence procedures.

Should revocation nevertheless be required, the Subscriber may request it by sending a digitally signed email from their Defence email account to:

pki.ops@defence.gov.au

### 3.4.2 AD-ID-MAC hard token - Subscriber request

Subscribers may request a certificate's revocation using the TMS User Self Service client. Authentication to the TMS may be achieved by using their Authentication certificate and private key, regardless of the compromise status of the private key. Where multiple keys are stored on the token (e.g. separate Authentication and Signing keys), all should be revoked if one is suspected compromised.

Alternatively, the Subscriber may request revocation of their own certificate(s) by sending a digitally signed email from their Defence email account to:

smartcard.level2support@defence.gov.au

Signing of the email may be achieved by using their Signing certificate and private key, regardless of the compromise status of the private key.

### 3.4.3 Revocation Requests from other parties

In addition, revocation requests can be submitted and authenticated by any authorised requestor (see CPS section 4.9.2 Who can request revocation) - in the following ways:

i. By digitally signed email from a valid Defence account to smartcard.level2support@defence.gov.au ; or

ii. In person, to an RO. The RO must verify the identity and authority of a requestor before carrying out a revocation, e.g. by sighting a Defence issued token with photograph and checking their entry in the Defence Directory.

In exceptional or emergency circumstances, a verbal revocation request can be processed at the discretion of *PKI Operations Manager* or Defence Executive.

A *PKI operator* or *Registration Officer* (RO) must verify the identity and authority of a requestor before carrying out a revocation on behalf of someone else.

The relationship to the Subscriber for revocation requests by the Subscriber's chain of command are to be verified via the Defence Directory.

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 RO; 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

An individual who has an approved affiliation with Defence, and who has been assigned a user account in a SIE network is eligible for an AD-ID-MAC.

### 4.1.2 Enrolment process and responsibilities

#### *4.1.2.1 AD-ID-MAC soft token*

Once an applicant has been granted a network user account, the act of the applicant logging on for the first time initiates the certificate application process for a soft token. This process is automated, using the operating systems auto-enrol features integrated with the Defence PKI.

#### *4.1.2.2 AD-ID-MAC hard token*

Having been issued a network account and a hard token, the applicant can authenticate to the TMS Self Service client. The TMS verifies the Subscriber's identity by checking that the account details and the token serial number align with the data derived from the Defence Identity Management Environment. Upon authentication, the Subscriber is able to activate their token and request a certificate, using the key pair generated in the activation process.

## 4.2 Certificate application processing

### 4.2.1 Performing identification and authentication functions

See 3.2.3 (Authentication of individual identity)

### 4.2.2 Approval or rejection of certificate applications

All **soft token** requests that meet the conditions of the policy permissions in *Active Directory* (AD) will be approved and passed to the RA; others are rejected.

All **hard token** requests submitted from the SIE from applicants that have been validated as per 3.2.3 (Authentication of individual identity) will be approved and passed to the RA; others are rejected.

The RA signs and forwards the certificate request to the CA. The CA only certifies certificate requests that are signed by an approved Defence RA.

### 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

For **soft tokens,** the auto-enrolment process returns the certificate directly to the Subscriber's certificate store within the specific network that the Subscriber is connected to.

For **hard tokens,** notification to the Subscriber occurs for a certificate request either when it succeeds or fails.

There is no other notification.

## 4.4 Certificate acceptance

### 4.4.1 Conduct constituting certificate acceptance

The Subscriber is deemed to have accepted the certificate when they have *exercised* the private key.

### 4.4.2 Publication of the certificate by the CA

The CA will publish all certificates.

### 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

Subscriber private key and certificate usage is defined above in 1.4 (Certificate Usage). Subscriber responsibilities are described below in 9.6.3 (Subscriber Representations and Warranties).

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

### 4.5.2 Relying party public key and certificate usage

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

The interpretation and compliance with extended KeyUsage attributes, and any associated limitations on the use of the certificate and/or private key, is in accordance with RFC5280.

## 4.6 Certificate renewal

Renewal of a certificate indicates creating a new certificate with an existing key pair, i.e. re-using a previously generated CSR. Certificate renewal is not permitted under this CP, certificates must be re-keyed, see 4.7 Certificate *re-key*.

## 4.7 Certificate re-key

### 4.7.1 Re-key of a certificates indicates renewing a certificate with a new key pair, creating a new CSR which is submitted to the RA.Circumstance for certificate re-key

This CP permits certificate re-key. See CPS for relevant circumstances.

### 4.7.2 Who may request certification of a new public key

Certificate re-key may be requested by the:

i. PKI PMA; or
ii. Subscriber.

### 4.7.3 Processing certificate re-keying requests

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

### 4.7.4 Notification of new certificate issuance to subscriber

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

### 4.7.5 Conduct constituting acceptance of a re-keyed certificate

See 4.4.1 (Conduct constituting certificate acceptance).

### 4.7.6 Publication of the re-keyed certificate by the CA

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

### 4.7.7 Notification of certificate issuance by the CA to other entities

No stipulation.

## 4.8 Certificate modification

Certificate modification is a method to re-issue a certificate with changes to certificate details.

Certificate modification is not permitted under this CP. If a change is required in a certificate, the certificate must be revoked and a new certificate issued, as per “Certificate Issuance” section 4.3..

## 4.9 Certificate revocation and suspension

### 4.9.1 Circumstances for revocation

#### *4.9.1.1 AD-ID-MAC soft token*

If a Subscriber’s account has been compromised, is suspected to be compromised, or the identification of the Subscriber changes, they are obliged to report this to the relevant SIE support channel. The account itself will then be disabled or re-keyed, requiring the Subscriber to create a new account password. The Subscriber’s AD-ID-MAC will not normally be revoked – the new account will be provisioned with a new certificate.

See CPS for other circumstances for revocation.

#### *4.9.1.2 AD-ID-MAC hard token*

See CPS.

### 4.9.2 Who can request revocation

See CPS.

### 4.9.3 Procedure for revocation request

#### *4.9.3.1 AD-ID-MAC soft token*

Where used, revocation requests received by *PKI operators* are to be verified on receipt in accordance with 3.4 (Identification and authentication for revocation request) and processed in priority order.

#### *4.9.3.2 AD-ID-MAC hard token*

Subscribers can request revocation of their own hard token certificate at any time, using the TMS User Self Service client.

Revocation requests by other authorised parties are validated in accordance with 3.4.3 (Identification and authentication for revocation requests – other parties) and processed in priority order. Prior to revocation, the request is verified and the requestor and reasons documented.

After verification, the operator processes revocation requests by using the TMS/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 PKI PMA, or an approved delegate, in exceptional circumstances (such as a security or law enforcement investigation), may approve a delay in the submission of a revocation request. An audit record of this approval is required, and must be submitted with the revocation request upon expiry of the approved delay.

### 4.9.5 Time within which CA must process the revocation request

A CA shall process revocation requests for certificates issued under this CP promptly after receipt.

### 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.

Certificates issued under this CP are unsuitable for a Relying Party's use if the requirements for revocation checking conflict with the clauses in 4.9 of this CP.

### 4.9.7 CRL issuance frequency (if applicable)

CRL issuance frequency for certificates under this CP are published on each certificate revocation or at intervals no longer than 24 hours if there are no updates.

### 4.9.8 Maximum latency for CRLs (if applicable)

The maximum latency between the generation and publication of CRLs is 3 days.

### 4.9.9 On-line revocation/status checking availability

*Online Certificate Status Protocol service* (OCSP) is available at http://ocsp.defence.gov.au

Refer to the relevant Certificate Profile in Appendix B - if the certificate is issued with an OCSP access location reference (Authority Information Access extension), OCSP is available to the Relying Party as a certificate status checking method.

The latest CRL is available from the published repositories; refer to 2.1 (Repositories) and the certificates CRL Distribution Point for further information.

### 4.9.10 On-line revocation checking requirements

See 4.9.6. (Revocation checking requirement for Relying Parties)

### 4.9.11 Other forms of revocation advertisements available

See CPS.

### 4.9.12 Special requirements re key compromise

See CPS section 5.7 Compromise and disaster recovery.

### 4.9.13 Circumstances for suspension

This CP does not support certificate suspension.

### 4.9.14 Who can request suspension

This CP does not support certificate suspension.

### 4.9.15 Procedure for suspension request

This CP does not support certificate suspension.

### 4.9.16 Limits on suspension period

This CP does not support certificate suspension.

## 4.10 Certificate status services

See CPS.

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

### 4.10.1 Operational characteristics

See CPS.

### 4.10.2 Service availability

See CPS.

### 4.10.3 Optional features

No stipulation.

## 4.11 End of subscription

See CPS.

In addition, when the Subscribers account is disabled or deleted.

## 4.12 Key escrow and recovery

### 4.12.1 Key escrow and recovery policy and practices

Escrow, backup and archiving of private Authentication or Signing keys issued is not permitted under this CP.

### 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

**Soft token** Subscriber keys are generated in the operating system's cryptographic *application programming interface* (API) during the requesting process based on rules defined by the account creation policy.

**Hard tokens** utilise the tokens' technology to generate and securely store private Authentication and Signing keys, with passphrase access controls. The individual receiving the hard token is responsible for the security and usage of this hard token. Under no circumstances will copies of private Authentication or Signing keys be kept, or be capable of recovery.

See CPS for more detail.

### 6.1.2 Private key delivery to subscriber

**Soft token** key generation is performed on the Subscriber's workstation and stored directly in the Subscriber's operating system certificate store, so no delivery is required.

**Hard token** private Authentication and Signing keys are always generated within the hard token. Where private keys are generated on the Subscriber's hard token at the time of enrolment, no additional delivery process is required.

Where the hard token is not personalised at the time of enrolment, it will be securely delivered to the Subscriber. Activation information is delivered separately and securely, using a mechanism for both deliveries that ensures that the private key(s) can only be accessed by the correct Subscriber.

### 6.1.3 Public key delivery to certificate issuer

The Subscriber's public key is provided to the CA in a PKCS#10 certificate request file signed with the corresponding private key.

### 6.1.4 CA public key delivery to relying parties

See CPS.

### 6.1.5 Key sizes

See Appendix B.

### 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)

Subscriber key and certificate usage is defined above in 1.4 (Certificate Usage).

Subscriber certificates include key usage extension fields to specify the purposes for which the keys may be used, and also to technically limit the functionality of the certificate when used with *X.509v3* compliant software. Reliance on key usage extension fields is dependent on correct software implementations of the X.509v3 standard and is outside of the control of the Defence PKI.

Keys issued under this CP contain Key Usage and Extended Key Usage extensions allowing Client Authentication and/or Digital Signing.

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

## 6.2 Private key protection and cryptographic module engineering controls

### 6.2.1 Cryptographic module standards and controls

**Soft token** Subscriber keys are stored in the user account certificate store, protected by the Subscriber's user account password. The operating system of the certificate store is listed on the Defence Approved Software List.

**Hard token** cryptographic modules meet the evaluation requirements of:

i. Common Criteria *Evaluation Assurance Level* (EAL) of a minimum of 2; and/or
ii. FIPS 140-2 Level 3 certified cards; and
iii. FIPS 201 compliant for *Personal Identity Verification* (PIV) cards.

All PKI core component cryptographic modules have undergone a security evaluation through an ASD recognised evaluation program and approved for the uses intended in this CP by the *National Cryptographic Authority* (NCA).

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

See CPS.

### 6.2.3 Private key escrow

Escrow of private Authentication or Signing keys does not occur.

### 6.2.4 Private key backup

See CPS.

### 6.2.5 Private key archival

See CPS.

### 6.2.6 Private key transfer into or from a cryptographic module

See CPS.

### 6.2.7 Private key storage on cryptographic module

See CPS.

### 6.2.8 Method of activating private key

To activate private keys on **soft tokens** the Subscriber must authenticate into their SIE account, which gives the Subscriber access to the token associated with the Subscriber's key pair.

Activating private keys on **hard tokens** occurs by the Subscriber authenticating to the cryptographic module. The session stays live until deactivated (see 6.2.9).

### 6.2.9 Method of deactivating private key

The Subscriber's **soft token** private key will be deactivated when they log out of the network account to which the certificate has been issued.

Deactivation of the **hard token** can be achieved by:

i. Shut down or restart of the system it is connected to;
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 of this CP.

## 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 Subscriber certificate has a maximum validity period of 2 years to limit the key lifetime. See also Appendix B and CPS.

## 6.4 Activation data

### 6.4.1 Activation data generation and installation

Lifecycle management of passphrases and other activation data is in accordance with the Defence PKI Key Management Plan (KMP) and Defence policy.

### 6.4.2 Activation data protection

All passphrases used to activate the private key shall be kept in accordance with Defence security policy for the applicable network.

### 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 the formats for the certificates, and CRL profiles and formats relative to this CP.

## 7.1 Certificate profile

### 7.1.1 Version number(s)

All certificates are X.509 Version 3 certificates.

### 7.1.2 Certificate extensions

See Appendix B.

### 7.1.3 Algorithm object identifiers

Certificates under this CP will use the following OID for signatures.

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

**Table 1 - Signature OIDs**

Certificates under this CP will use one of the following OIDs for identifying the algorithm for which the subject key was generated.

| | |
|---|---|
| id-ecPublicKey | {iso(1) member-body(2) us(840) ansi-x9-62(10045) public-key-type (2) 1} |
| rsaEncryption | {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1} |
| Dhpublicnumber | {iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1} |
| id-keyExchangeAlgorithm | {joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) algorithms(1) 22} |

**Table 2 - Algorithm OIDs**

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, CRL*s* and any other PKI product, including other forms of revocation information, such as OCSP responses.

### 7.1.4 Name forms

The Common Name (CN) component is based on the Subscriber's Defence email address and defined as <firstname> <lastname> <serial[2]>. It is encoded as an X.501 printable string where possible, and using UTF-8 otherwise.

[2] In some instances the 'serial' is blank

The Subject Alternative Name extension contains an identifier which binds the certificate to a specific account.

See also Appendix B.

### 7.1.5 Name constraints

Refer to the Issuing CA's CP.

### 7.1.6 Certificate policy object identifier

Certificates issued under this policy shall assert this CP's OID plus a variant number (refer to Appendix B):

{**1.2.36.1.334.1.1.2.1.n}**

Certificates issued under this policy shall also assert the following LoA OID and, to enable the use of the certificate at lower Levels of Assurance, this policy enables the additional assertion of the lower (or 'stacked') LoA OIDs. LoA OIDs able to be asserted under this policy include:

**{1.2.36.1.334.1.2.1.2} Level of Assurance – Medium (Individual)**

**{1.2.36.1.334.1.2.1.1} Level of Assurance – Low (Individual)**

See also Appendix B.

### 7.1.7 Usage of policy constraints extension

Refer to the Issuing CA's CP.

### 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 CPS published by the CA, or to a webpage from which the CPS can then be downloaded.

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

### 7.1.9 Processing semantics for the critical certificate policies extension

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

## 7.2 CRL profile

### 7.2.1 Version number(s)

CRLs shall be X.509 version 2.

### 7.2.2 CRL and CRL entry extensions

See Appendix C.

## 7.3 OCSP profile

### 7.3.1 Version Numbers

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

### 7.3.2 OCSP Extensions

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

# 8. Compliance Audit and Other Assessments

## 8.1 Frequency or circumstances of assessment

See CPS.

## 8.2 Identity/qualifications of assessor

See CPS.

## 8.3 Assessor's relationship to assessed entity

See CPS.

## 8.4 Topics covered by assessment

See CPS.

## 8.5 Actions taken as a result of deficiency

See CPS.

## 8.6 Communication of results

See CPS.

# 9. Other Business and Legal Matters

## 9.1 Fees

### 9.1.1 Certificate issuance or renewal fees

No stipulation.

### 9.1.2 Certificate access fees

There is no fee for accessing Certificates from approved repositories.

### 9.1.3 Revocation or status information access fees

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

### 9.1.4 Fees for other services

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

### 9.1.5 Refund policy

See CPS.

## 9.2 Financial responsibility

See CPS.

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

### 9.2.1 Insurance

No stipulation.

### 9.2.2 Other assets

No stipulation.

### 9.2.3 Insurance or warranty coverage for end-entities

No stipulation.

## 9.3 Confidentiality of business information

See CPS.

## 9.4 Privacy of personal information

### 9.4.1 Privacy plan

In order to provide an audit and evidentiary trail of the verification process, and documentation presented to confirm an individual's identity, Defence is required to collect Personal Information (as defined in the *Privacy Act 1988 (Cth)*). The collection, use and disclosure of such information is governed by the Privacy Act 1988 (Cth) (Privacy Act).

At enrolment, applicants agree to the terms and conditions of being given an account on a Defence system, acknowledging that Defence may collect, use or disclose Personal Information about them, for the purposes discussed below.

The Defence PKI Privacy Notice is available from http://crl.defence.gov.au/pki and contains information on the collection, use and disclosure of personal information associated with the PKI. In addition, the Notice also details how individuals can access their personal information in the PKI.

### 9.4.2 Information treated as private

Personal Information, other than the name and e-mail address of the applicant, is not published in the Digital Certificate and is treated as private. The Defence PKI relies on the Subscriber being given an account within the Defence network, and relies on the Evidence of Identity (EOI) documentation presented to the Subscriber's network account sponsor and the unique identity attributes registered in the Defence Identity Management environment. This information is protected in accordance with the requirements of the Privacy Act and the PKI Privacy Notice.

### 9.4.3 Information not deemed private

See CPS.

### 9.4.4 Responsibility to protect private information

See CPS.

### 9.4.5 Notice and consent to use private information

Consent by the Subscriber to the use of Personal Information is given by acknowledging the conditions associated with their network account.

### 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.

### 9.6.1 CA representations and warranties

See CPS.

### 9.6.2 RA representations and warranties

See CPS.

### 9.6.3 Subscriber representations and warranties

The Subscriber, in obtaining access to the Defence network, warrants that the information provided by them is true to the best of their knowledge. In addition, Subscribers warrant to:

i. only use Keys and digital certificates within the limits specified in this CP;
ii. take all reasonable measures to protect their Private Key(s) from compromise and take all necessary precautions to prevent loss, disclosure, modification, or unauthorised use of their Private Key(s);
iii. promptly notify the RA in the event that they consider or suspect there has been a compromise of their Private Key(s); and
iv. promptly notify the RA in the event that they consider the EOI information provided by them is or may be incorrect.

### 9.6.4 Relying party representations and warranties

See CPS.

### 9.6.5 Representations and warranties of other participants

No Stipulation.

## 9.7 Disclaimer of warranties

See CPS.

## 9.8 Limitations of liability

See CPS.

In Addition: GATEKEEPER ACCREDITATION DISCLAIMER

The Gatekeeper Competent Authority is responsible for ensuring that the accreditation process is conducted with due care and in accordance with published Gatekeeper Criteria and Policies.

The Gatekeeper Competent Authority is not liable for any errors and/or omissions in the final Approved Documents, which remain the responsibility of the accredited Service Provider.

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

- Accuracy of any statements or representations made in, or suitability of, the Approved Documents of a Gatekeeper accredited Service Provider;

- Accuracy of any statement or representation made in, or suitability of, the documentation of a Service Provider in a Gatekeeper recognised PKI domain; or
- Standard or suitability of any services thereby provided by any Subscriber or Relying Party or application.

## 9.9 Indemnities

See CPS.

## 9.10 Term and termination

### 9.10.1 Term

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

### 9.10.2 Termination

See CPS.

### 9.10.3 Effect of termination and survival

See CPS.

## 9.11 Individual notices and communications with participants

See CPS.

## 9.12 Amendments

See CPS.

## 9.13 Dispute resolution provisions

See CPS.

## 9.14 Governing Law

See CPS.

## 9.15 Compliance with Applicable Law

i. See CPS.

## 9.16 Miscellaneous provisions

See CPS.

## 9.17 Other provisions

See CPS.

# APPENDIX A. REFERENCES

The following documents are referenced in this CP:

| | |
|---|---|
| [6960] | RFC6960 Internet X.509 Public Key Infrastructure On-line Certificate Status Protocol (ocsp), Internet Engineering Task Force, available at https://www.ietf.org/rfc/rfc6960.txt |
| [3647] | RFC3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Internet Engineering Task Force, available at https://www.ietf.org/rfc/rfc3647.txt |
| [5280] | RFC5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Internet Engineering Task Force, available at https://www.ietf.org/rfc/rfc5280.txt |
| [CPS] | X.509 Certification Practice Statement for the Australian Department of Defence, available at https://defence.gov.au/pki/cps/Defence-CPS.pdf |
| [GK2015] | Australian Government, Gatekeeper PKI Framework v3.1 Dec 2015, available at https://www.dta.gov.au/standard/design-guides/authentication-frameworks/gatekeeper-public-key-infrastructure-framework/ |
| [ISM] | Australian Signals Directorate, Australian Government Information Security Manual Controls, available at https://www.asd.gov.au/infosec/ism/index.htm |
| [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/documents/LOA.pdf |
| [OID Register] | Defence Object Identifier (OID) register. Not available externally. |
| [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 3 - References**

# APPENDIX B. CERTIFICATE PROFILES

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

## Certificate profile summary

| **Variant No. (OID extension)[3]** | **Name/description** | **Variant OID** | **RP Name/ID** | **Customer** | **Month/year implemented** |
|---|---|---|---|---|---|
| 1 | ID-MA Software Authentication and Digital Signing[4] | 1.2.36.1.334.1.1.2.1.1. | | | |
| 2 | ID-MA Hardware Authentication and Digital Signing | 1.2.36.1.334.1.1.2.1.2. | | | |
| 3 | ID-MA Hardware Authentication | 1.2.36.1.334.1.1.2.1.3. | | | |
| 4 | ID-MA Hardware Digital Signing | 1.2.36.1.334.1.1.2.1.4. | | | |
| | | | | | |
| | | | | | |
| | | | | | |

[3] N.B. These are not always sequential, as OIDs must not be re-used, and certificate profiles that are no longer in use are removed from the CP. Refer to [OID Register] for a full list of OIDs used.

[4] Prior to Nov 2022, the description was ID-MA Software

## B.1 Individual – Medium Assurance Software Certificate – Authentication and Signing

This certificate is issued to the Subscriber's workstation through Microsoft Auto-Enrolment.

| Field | Critical | Value | Notes |
|---|---|---|---|
| Version | | V3 (2) | |
| Serial | | Randomly Generated Number | Unique value generated by the issuing CA |
| Issuer signature algorithm | | sha-2WithRSAEncryption | |
| Issuer distinguished name | | CN= <subCAIssurer><br>OU= CAs<br>OU= PKI<br>OU= DoD<br>O= GOV<br>C= AU | See Defence-ADPRCA-CP for the Issuing subCA naming convention. |
| Validity period | | Not before <UTCtime><br>Not after <UTCtime> | 2 years from date of issue |
| Subject distinguished name | | CN=<LHS of Defence email alias><br>OU=Personnel<br>OU=PKI<br>OU=DoD<br>O=GOV<br>C=AU | CN consists of the left hand side of the Subject's Defence email address, e.g. "Rob.Smith7" for a subject with the principal email address "rob.smith7@defence.gov.au"<br>Encoded as printable string where possible, and otherwise using UTF-8 |
| Subject public key information | | 2048 bit RSA key modulus | |
| Issuer unique identifier | | - | Not Present |
| Subject unique identifier | | - | Not Present |
| X.509 V3 extensions: | | | |
| Authority key identifier | No | <octet string> | 160 bit SHA-1 hash of binary DER encoding of signing CA's public key[5] |
| Subject key identifier | No | <octet string> | 160 bit SHA-1 hash of binary DER encoding of subject's public key |
| Key usage | Yes | digitalSignature<br>nonRepudiation | |
| Extended key usage | No | {1.3.6.1.5.5.7.3.2} Microsoft Client Authentication<br>{1.3.6.1.5.5.7.3.4} Secure email protection | |
| Private key usage period | | - | Not Present |
| Certificate policies | No | [1] Policy ID:{ 1.2.36.1.334.1.1.2.1.1.}<br><br>Policy Qualifier: | The OID of CP for - AD-ID-MAC-Software<br><br>UserNotice shall use explicitText field. |

[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 | Value | Notes |
|---|---|---|---|
| | | User Notice: explicitText, <"Other than confirming affiliation with the Department of Defence, the Defence PKI infers no authority or privilege to the Subscriber of this certificate. Certificates must not be used for any purpose not permitted by the CP"<br>CPS Pointer: http://crl.defence.gov.au/pki | |
| | | [2] Policy OID: {1.2.36.1.334.1.2.1.2} | Level of Assurance – Medium<br>The Level of Assurance of this certificate |
| | | [3] Policy OID: {1.2.36.1.334.1.2.1.1} | Level of Assurance – Low<br>Included to allow the certificate to be used in lower assurance context. |
| Policy mapping | | - | Not Present |
| Subject Alternative Name | | RFC822 Name (email address)<br>Other Name: Principal Name | Defence Email address and Defence User Principal Name (UPN) |
| Issuer alternative name | | - | Not Present |
| Subject directory attributes | | - | Not Present |
| Basic constraints | | - | Not Present |
| Name constraints | | - | Not Present |
| Policy constraints | | - | Not Present |
| Subject Information Access | | - | Not Present |
| Authority Information Access | No | [1] Access method=OCSP {1.3.6.1.5.5.7.48.1}:<br>Access location: http://ocsp.defence.gov.au<br>[2] Access method: CAIssuer{1.3.6.1.5.5.7.48.2}<br>Access location: http://crl.defence.gov.au/pki/Certificates/<subCAIssuer><br>[3] Access method=CAIssuer {1.3.6.1.5.5.7.48.2}:<br>Access location:<br>ldap://dir.defence.gov.au/cn=<subCAIssuerCN>,ou=CAs,ou=PKI,ou=DoD,o=GOV,c=AU?crossCertificatePair;binary | ▪ Defence uses a URL rewrite (redirection) rule in the Web Server to ensure the CDP URLs without a file extension are assigned to the correct file type (.crt). |
| CRL Distribution Point | No | [1] Distribution Point Name (http):<br>http://crl.defence.gov.au/pki/crl/ <subCAIssuer>.crl<br>[2] Distribution Point Name (ldap): ldap://dir.defence.gov.au/cn=<subCAIssuerCN>,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). |
| Microsoft Certificate Template | | User Authentication | |
| 1.3.6.1.4.1.311.25.2 | No | <octet string> | This field is the **Microsoft SID Extension** which stores the unique AD Security Identifier for a user |

**Table 4 – AD-ID-MAC Software Certificate Profile ADO User Authentication and Signing**

## B.2 Individual – Medium Assurance Hardware Token Certificate – Authentication and Signing

This certificate is issued onto a Subscriber's DCAC and has CP OID 1.2.36.1.334.1.1.2.1.2

| Field | Critical | Value | Notes |
|---|---|---|---|
| Version | | V3 (2) | |
| Serial | | Randomly Generated Number | Unique value generated by the issuing CA |
| Issuer signature algorithm | | sha-2WithRSAEncryption | |
| Issuer distinguished name | | CN= <subCAIssuer><br>OU= CAs<br>OU= PKI<br>OU= DoD<br>O= GOV<br>C= AU | Encoded as printable string.<br>See Defence-ADPRCA-CP for the Issuing subCA naming convention. |
| Validity period | | Not before <UTCtime><br>Not after <UTCtime> | 2 years from date of issue |
| Subject distinguished name | | CN=<Defence commonname><br>OU=Personnel<br>OU=PKI<br>OU=DoD<br>O=GOV<br>C=AU | CN consists of the subject's common name as described in the Defence Corporate Directory, or where the an entry is not present, the left hand side of the Subject's Defence User Principal Name, e.g. "Rob.Smith7" for a subject with the user principal name "rob.smith7@defence.gov.au".<br>Encoded as printable string where possible, and otherwise using UTF8. |
| Subject public key information | | 2048 bit RSA key modulus | |
| Issuer unique identifier | | - | Not Present |
| Subject unique identifier | | - | Not Present |
| **X.509 V3 extensions:** | | | |
| Authority key identifier | No | <octet string> | 160 bit SHA-1 hash of binary DER encoding of signing CA's public key[6] |
| Subject key identifier | No | <octet string> | 160 bit SHA-1 hash of binary DER encoding of subject's public key |
| Key usage | Yes | digitalSignature<br>nonRepudiation | |
| Extended key usage | No | {1.3.6.1.5.5.7.3.2} Microsoft Client Authentication<br>{1.3.6.1.4.1.311.20.2.2} Microsoft Smart Card Logon<br>{1.3.6.1.5.5.7.3.4} Secure Email | |
| Private key usage period | | - | Not Present |

[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 | Value | Notes |
|---|---|---|---|
| Certificate policies | No | [1] Policy ID:{1.2.36.1.334.1.1.2.1.2 }<br>Policy Qualifier – User Notice: explicitText, <"Other than confirming affiliation with the Department of Defence, the Defence PKI infers no authority or privilege to the Subscriber of this certificate. Certificates must not be used for any purpose not permitted by the CP"<br>Policy Qualifier - CPS Pointer: https://crl.defence.gov.au/pki | The OID of CP for - AD-ID-MAC-Hardware (Variant 2)<br>UserNotice shall use explicitText field. |
| | | [2] Policy OID: {1.2.36.1.334.1.2.1.2} | Level of Assurance – Medium<br>The Level of Assurance of this certificate |
| | | [3] Policy OID: {1.2.36.1.334.1.2.1.1} | Level of Assurance – Low<br>Included to allow the certificate to be used in lower assurance context. |
| Policy mapping | | - | Not Present |
| Subject Alternative Name | | RFC822 Name (email address)<br>Other Name: Principal Name | |
| Issuer alternative name | | - | Not Present |
| Subject directory attributes | | - | Not Present |
| Basic constraints | | - | Not Present |
| Name constraints | | - | Not Present |
| Policy constraints | | - | Not Present |
| Subject Information Access | | - | Not Present |
| Authority Information Access | No | [1] Access method=OCSP {1.3.6.1.5.5.7.48.1}:<br>Access location: http://ocsp.defence.gov.au<br>[2] Access method: CAIssuer{1.3.6.1.5.5.7.48.2}<br>Access location: http://crl.defence.gov.au/pki/Certificates/<subCAIssuer><br>[3] Access method=CAIssuer {1.3.6.1.5.5.7.48.2}:<br>Access location:<br>ldap://dir.defence.gov.au/cn=<subCAIssuerCN>,ou=CAs,ou=PKI,ou=DoD,o=GOV,c=AU?crossCertificatePair;binary | Defence uses a URL rewrite (redirection) rule in the Web Server to ensure the CDP URLs without a file extension are assigned to the correct file type (.crt). |
| CRL Distribution Point | No | [1] Distribution Point Name (http):<br>http://crl.defence.gov.au/pki/crl/ <subCAIssuer>.crl<br>[2] Distribution Point Name (ldap): ldap://dir.defence.gov.au/cn=<subCAIssuerCN>,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). |

**Table 5 – AD-ID-MAC Hardware Certificate Profile ADO User Authentication and Signing**

## B.3 Individual – Medium Assurance Hardware Token Certificate – Authentication

This certificate is issued onto a Subscriber's DCAC and has CP OID 1.2.36.1.334.1.1.2.1.3

| Field | Critical | Value | Notes |
|---|---|---|---|
| Version | | V3 (2) | |
| Serial | | Randomly Generated Number | Unique value generated by the issuing CA |
| Issuer signature algorithm | | sha-2WithRSAEncryption | |
| Issuer distinguished name | | CN= <subCAIssurer><br>OU= CAs<br>OU= PKI<br>OU= DoD<br>O= GOV<br>C= AU | Encoded as printable string.<br>See Defence-ADPRCA-CP for the Issuing subCA naming convention. |
| Validity period | | Not before <UTCtime><br>Not after <UTCtime> | 2 years from date of issue |
| Subject distinguished name | | CN=<Defence commonname><br>OU=Personnel<br>OU=PKI<br>OU=DoD<br>O=GOV<br>C=AU | CN consists of the subject's common name as described in the Defence Corporate Directory, or where the an entry is not present, the left hand side of the Subject's Defence User Principal Name, e.g. "Rob.Smith7" for a subject with the user principal name "rob.smith7@defence.gov.au".<br>Encoded as printable string where possible, and otherwise using UTF8. |
| Subject public key information | | 2048 bit RSA key modulus | |
| Issuer unique identifier | | - | Not Present |
| Subject unique identifier | | - | Not Present |
| **X.509 V3 extensions:** | | | |
| Authority key identifier | No | <octet string> | 160 bit SHA-1 hash of binary DER encoding of signing CA's public key[7] |
| Subject key identifier | No | <octet string> | 160 bit SHA-1 hash of binary DER encoding of subject's public key |
| Key usage | Yes | digitalSignature | |
| Extended key usage | No | {1.3.6.1.5.5.7.3.2} Microsoft Client Authentication<br>{1.3.6.1.4.1.311.20.2.2} Microsoft Smart Card Logon | |
| Private key usage period | | - | Not Present |

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

| Field | Critical | Value | Notes |
|---|---|---|---|
| Certificate policies | No | [1] Policy ID:{1.2.36.1.334.1.1.2.1.3 }<br>Policy Qualifier – User Notice: explicitText, <"Other than confirming affiliation with the Department of Defence, the Defence PKI infers no authority or privilege to the Subscriber of this certificate. Certificates must not be used for any purpose not permitted by the CP"<br>Policy Qualifier - CPS Pointer: http://crl.defence.gov.au/pki | The OID for AD-ID-MAC-Hardware-Authentication (Variant 3)<br>UserNotice shall use explicitText field. |
| | | [2] Policy OID: {1.2.36.1.334.1.2.1.2} | Level of Assurance – Medium<br>The Level of Assurance of this certificate |
| | | [3] Policy OID: {1.2.36.1.334.1.2.1.1} | Level of Assurance – Low<br>Included to allow the certificate to be used in lower assurance context. |
| Policy mapping | | - | Not Present |
| Subject Alternative Name | | RFC822 Name (email address)<br>Other Name: Principal Name | |
| Issuer alternative name | | - | Not Present |
| Subject directory attributes | | - | Not Present |
| Basic constraints | | - | Not Present |
| Name constraints | | - | Not Present |
| Policy constraints | | - | Not Present |
| Subject Information Access | | - | Not Present |
| Authority Information Access | No | [1] Access method=OCSP {1.3.6.1.5.5.7.48.1}:<br>Access location: http://ocsp.defence.gov.au<br>[2] Access method: CAIssuer{1.3.6.1.5.5.7.48.2}<br>Access location: http://crl.defence.gov.au/pki/Certificates/<subCAIssuer><br>[3] Access method=CAIssuer {1.3.6.1.5.5.7.48.2}:<br>Access location:<br>ldap://dir.defence.gov.au/cn=<subCAIssuerCN>,ou=CAs,ou=PKI,ou=DoD,o=GOV,c=AU?crossCertificatePair;binary | ▪ Defence uses a URL rewrite (redirection) rule in the Web Server to ensure the CDP URLs without a file extension are assigned to the correct file type (.crt). |
| CRL Distribution Point | No | [1] Distribution Point Name (http):<br>http://crl.defence.gov.au/pki/crl/ <subCAIssuer>.crl<br>[2] Distribution Point Name (ldap): ldap://dir.defence.gov.au/cn=<subCAIssuerCN>,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). |

**Table 6 – AD-ID-MAC Hardware Certificate Profile - Authentication**

## B.4 Individual – Medium Assurance Hardware Token Certificate – Digital Signing

This certificate is issued onto a Subscriber's DCAC and has CP OID 1.2.36.1.334.1.1.2.1.4

| Field | Critical | Value | Notes |
|---|---|---|---|
| Version | | V3 (2) | |
| Serial | | Randomly Generated Number | Unique value generated by the issuing CA |
| Issuer signature algorithm | | sha-2WithRSAEncryption | |
| Issuer distinguished name | | CN= <subCAIssurer><br>OU= CAs<br>OU= PKI<br>OU= DoD<br>O= GOV<br>C= AU | Encoded as printable string.<br>See Defence-ADPRCA-CP for the Issuing subCA naming convention. |
| Validity period | | Not before <UTCtime><br>Not after <UTCtime> | 2 years from date of issue |
| Subject distinguished name | | CN=<Defence commonname><br>OU=Personnel<br>OU=PKI<br>OU=DoD<br>O=GOV<br>C=AU | CN consists of the subject's common name as described in the Defence Corporate Directory, or where the an entry is not present, the left hand side of the Subject's Defence User Principal Name, e.g. "Rob.Smith7" for a subject with the user principal name "rob.smith7@defence.gov.au".<br>Encoded as printable string where possible, and otherwise using UTF8. |
| Subject public key information | | 2048 bit RSA key modulus | |
| Issuer unique identifier | | - | Not Present |
| Subject unique identifier | | - | Not Present |
| **X.509 V3 extensions:** | | | |
| Authority key identifier | No | <octet string> | 160 bit SHA-1 hash of binary DER encoding of signing CA's public key[8] |
| Subject key identifier | No | <octet string> | 160 bit SHA-1 hash of binary DER encoding of subject's public key |
| Key usage | Yes | digitalSignature<br>nonRepudiation | |
| Extended key usage | No | {1.3.6.1.5.5.7.3.4} Secure email protection | |
| Private key usage period | | - | Not Present |

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

| Field | Critical | Value | Notes |
|---|---|---|---|
| Certificate policies | No | [1] Policy ID:{1.2.36.1.334.1.1.2.1.4 }<br>Policy Qualifier – User Notice: explicitText, <"Other than confirming affiliation with the Department of Defence, the Defence PKI infers no authority or privilege to the Subscriber of this certificate. Certificates must not be used for any purpose not permitted by the CP"<br>Policy Qualifier - CPS Pointer: http://crl.defence.gov.au/pki | The OID for AD-ID-MAC-Hardware-DigSig (Variant 4)<br>UserNotice shall use explicitText field. |
| | | [2] Policy OID: {1.2.36.1.334.1.2.1.2} | Level of Assurance – Medium<br>The Level of Assurance of this certificate |
| | | [3] Policy OID: {1.2.36.1.334.1.2.1.1} | Level of Assurance – Low<br>Included to allow the certificate to be used in lower assurance context. |
| Policy mapping | | - | Not Present |
| Subject Alternative Name | | RFC822 Name (email address)<br>Other Name: Principal Name | |
| Issuer alternative name | | - | Not Present |
| Subject directory attributes | | - | Not Present |
| Basic constraints | | - | Not Present |
| Name constraints | | - | Not Present |
| Policy constraints | | - | Not Present |
| Subject Information Access | | - | Not Present |
| Authority Information Access | No | [1] Access method=OCSP {1.3.6.1.5.5.7.48.1}:<br>Access location: http://ocsp.defence.gov.au<br>[2] Access method: CAIssuer{1.3.6.1.5.5.7.48.2}<br>Access location: http://crl.defence.gov.au/pki/Certificates/<subCAIssuer><br>[3] Access method=CAIssuer {1.3.6.1.5.5.7.48.2}:<br>Access location:<br>ldap://dir.defence.gov.au/cn=<subCAIssuerCN>,ou=CAs,ou=PKI,ou=DoD,o=GOV,c=AU?crossCertificatePair;binary | Defence uses a URL rewrite (redirection) rule in the Web Server to ensure the CDP URLs without a file extension are assigned to the correct file type (.crt). |
| CRL Distribution Point | No | [1] Distribution Point Name (http):<br>http://crl.defence.gov.au/pki/crl/ <subCAIssuer>.crl<br>[2] Distribution Point Name (ldap): ldap://dir.defence.gov.au/cn=<subCAIssuerCN>,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). |

**Table 7 – AD-ID-MAC Hardware Certificate Profile - Digital Signing**

# APPENDIX C. CRL FORMAT

Please refer to the issuing CA’s Certificate Policy.

# APPENDIX D. LEVEL OF ASSURANCE MAPPING

## D.1 Assurance Level

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

| | |
|---|---|
| **CP's Level of Assurance:** | Medium Assurance {1.2.36.1.334.1.2.1.2}. **As documented in section 7.1.6 above.** |

| REQUIREMENT | CP'S MAPPING TO REQUIREMENT |
|---|---|
| IDENTITY PROOFING | |
| EOI | The Subscriber must have an account on a Defence network, as well as have a current Security Clearance, where the Subscriber must prove their identity, as covered in section 3.2 above. |
| Evidence of Relationship | Subscriber must be identified in the Defence directory, as covered in section 3.2.3 above. |
| Location | As documented in section 3.2.3, a Subscriber must have their Security Clearance validated, and then present locally to receive their Defence facility access card into a Defence site, and if authorised, will additionally be given access to a Defence network, this can occur locally or remotely, through the use of a split initial passphrase. Once authenticated into a Defence network, the operating system will automatically provide the Subscriber with their soft token stored within the operating system certificate store. Hardware tokens can only be requested either in person or by the validation of the applicant's ownership of their private key, which must be at least at the same Level of Assurance of that being issued. |
| CREDENTIAL STRENGTH | |
| Token Protection | As documented in section 6.2, the certificates supported by this CP is stored within the Subscriber's certificate store within the Defence network where the account resides, or in the Subscribers hard token.<br>Access to the certificate store is protected by access to the Subscriber's account within the Defence network, which is password protected in alignment with the Defence security requirements. As documented in section 6.2, the AD-ID-MAC hard token will be a hard token which has been evaluated under Common Criteria and/or FIPS 140-2 or PIV 201. |
| Token Activation | As documented in section 6.2.8, access to the soft token is activated on authentication to the Subscriber's account within the relevant Defence network. For the hard token activation of private keys occurs by the Subscriber authenticating to the cryptographic module. |

| | |
|---|---|
| Life (Time) of Key Strength | As documented in Appendix B, the Key Strength will be SHA-2, with at least 128 security bits (SHA-256) and a RSA key size of at least 2048 bits are suitable for protecting classified, confidential and secret information from 2010 to 2030 and available for legacy use post 2030. [ISM] 2015, [GK2015] |
| CERTIFICATE MANAGEMENT | |
| CA Protection | The CA is both physically and logically secure from the unauthorised access. The CA protection requirements are documented in the CPS and sections 5 and 6 of this CP. |
| Binding | As documented in section 4, the issuance of the AD-ID-MAC soft token through the operating systems auto enrol process binds the certificate issuance to the Subscriber's access to their Defence network account. Hard tokens are bound via either an in person request, where the certificate is issued in the presence of the RO, or the validation of the applicant's ownership of a private key, prior to the generation of a CSR from the hard token.<br>While the issuance process is not necessarily contiguous, the identity of the Subscriber is bound to their Defence email address, their affiliation in the Defence Directory, the account creation process and validation of the applicants use of a Defence issued private key |
| Revocation (Publication) | As covered in section 4.9.7, the CRL is published daily, or on a certificate revocation, which exceeds the requirements. This is as a result of issuing from the High Assurance CA. |
| Compliance | The Compliance requirements are covered in the CPS and section 8. The Defence PKI environment is certified under the Australian Government Gatekeeper program, to support the issuance of up to a High Assurance level. |

## D.2 Risk Assessment

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

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

The following risks were identified and managed in the alignment of the AD-ID-MAC with the requirements for Medium Assurance. The PKI PMA has accepted the risks through the appropriateness of the controls listed.

| LOA Requirement | Identified Risk | Mitigation / Controls |
|---|---|---|
| Identity Proofing | There is a risk that a Subscriber may not be correctly identified (as the EOI validated is limited and the account controls are not audited) | • At least one government issued photographic document is required<br>• Defence network account processes are well documented and responsibilities have to be consciously invalidated when not followed |
| Token Protection | There is a risk that the soft token can be used by other parties. (The soft token containing the Subscriber's key pair is stored within the operating system's certificate store within the Subscriber's Defence account.) | • The Defence network administrators must have a security clearance to at least the level of the Defence network, and they are educated on their responsibilities with regard to need-to-know.<br>• Defence has auditing of administration activity as described in the Defence Security Principles Framework.<br>• Access to a Subscribers network account is protected with a passphrase, which meets the complexity requirements as specified by Defence Security. |
| Token Activation | There is a risk that the soft token can be used by other parties. (The soft token containing the Subscriber's key pair doesn't require authentication for direct activation.) | • The soft token is stored within the Subscriber's operating system certificate store.<br>• Access to a Subscribers network account is protected with a passphrase, which meets the complexity requirements as specified by Defence Security.<br>• As per the network security requirements, the Subscriber is required to 'lock' their workstation if they leave it |