Australian Government

Defence

X.509 Certificate Policy for the Australian Department of Defence Individual - Hardware Certificates (High Assurance)

Version 10.0
November 2023

Notice to all parties seeking to rely

Reliance on a Certificate issued under this Certificate Policy (CP) for Australian Department of Defence Individual - Hardware Certificates (High Assurance) , identified by subarcs of the object identifier **1.2.36.1.334.1.1.2.2**, 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 (GCA)

Change History

Version	Issue Date	Description/ Amendment	Changed by
1.0	17 May 2007	Released	
2.0	Nov 2011	Released (LoAs, new OIDs, hard tokens, PIV and CCEB compliance)	SJP
3.0	July 2012	Released	SJP
4.0	May 2014	Review for release	PKI Ops Man
5.0	Oct 2016-	Released	PKI Operations Manager
5.1	Dec 2016	Updated www.defence.gov.au to crl.defence.gov.au	Cogito Group (BB)
5.2	February 2018	Document Review	PKI Operator (LM)
5.3	Dec 2018	Document Review	PKI Operator (NA)
5.4	Jun 2019	Minor updates to align policies based on review of Mdm Assurance CP	GJF
6.0	July 2019	Published	PKI Ops Man
6.1	Sep 2020	Updates for GK review. Classification updated. Minor corrections and improvements. Variant OID for CST added to cert profiles.	CDMC (AKK)

Version	Issue Date	Description/ Amendment	Changed by
7.0	Oct 2020	Reviewed by DTA – Changes accepted - Released	CDMC (AKK)
7.1	Nov 2021	2021 updates. Removal of confidentiality certificates. Revocation process update. Other minor improvements.	CDMC (AKK)
8.0	Dec 2021	Reviewed by DTA – Changes accepted - Released	CDMC (AKK)
8.1	Oct 2022	2022 updates	CDMC (AKK)
9.0	Nov 2022	Reviewed by DTA – Changes accepted - Released	CDMC (AKK)
9.1	Nov 2022	Revision to accommodate split certificates – authentication and digital signing.	CDMC (AKK)
9.2	Oct 2023	2023 updates	CDMC (AKK)
10.0	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

1. INTRODUCTION 9
1.1 Overview 9
1.2 Document name and identification 10
1.3 PKI Participants 10
1.3.1 Certification authorities 10
1.3.2 Registration authorities 10
1.3.3 Subscribers 10
1.3.4 Relying Parties 10
1.3.5 Other participants 11
1.4 Certificate usage 11
1.4.1 Appropriate certificate uses 11
1.4.2 Prohibited certificate uses 12
1.5 Policy administration 12
1.5.1 Organisation administering the document 12
1.5.2 Contact person 12
1.5.3 Authority determining CPS suitability for the policy 12
1.5.4 CPS approval procedures 12
1.6 Definitions, acronyms and interpretation 12
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES 13
2.1 Repositories 13
2.2 Publication of certification information 13
2.3 Time or frequency of publication 13
2.4 Access controls on repositories 13
3. IDENTIFICATION AND AUTHENTICATION 13
3.1 Naming 13
3.1.1 Types of names 13
3.1.2 Need for names to be meaningful 13
3.1.3 Anonymity or pseudonymity of Subscribers 13
3.1.4 Rules for interpreting various name forms 14
3.1.5 Uniqueness of names 14
3.1.6 Recognition, authentication, and role of trademarks 14
3.2 Initial identity validation 14
3.2.1 Method to prove possession of private key 14
3.2.2 Authentication of organisation identity 14
3.2.3 Authentication of individual identity 14
3.2.4 Non-verified Subscriber information 15
3.2.5 Validation of authority 15
3.2.6 Criteria for interoperation 15
3.3 Identification and authentication for re-key requests 15
3.3.1 Identification and authentication for re-key 15
3.3.2 Identification and authentication for re-key after revocation 16
3.4 Identification and authentication for revocation request 16
4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 17
4.1 Certificate application 17
4.1.1 Who can submit a certificate application 17
4.1.2 Enrolment process and responsibilities 17
4.2 Certificate application processing 17
4.2.1 Performing identification and authentication functions 17

4.2.2 Approval or rejection of certificate applications 17
4.2.3 Time to process certificate applications 17
4.3 Certificate issuance 17
4.3.1 CA actions during certificate issuance 18
4.3.2 Notification to Subscriber by the CA of issuance of certificate 18
4.4 Certificate acceptance 18
4.4.1 Conduct constituting certificate acceptance 18
4.4.2 Publication of the certificate by the CA 18
4.4.3 Notification of certificate issuance by the CA to other entities 18
4.5 Key pair and certificate usage 18
4.5.1 Subscriber private key and certificate usage 18
4.5.2 Relying Party public key and certificate usage 18
4.6 Certificate renewal 18
4.7 Certificate re-key 19
4.7.1 Circumstance for certificate re-key 19
4.7.2 Who may request certification of a new public key 19
4.7.3 Processing certificate re-keying requests 19
4.7.4 Notification of new certificate issuance to Subscriber 19
4.7.5 Conduct constituting acceptance of a re-keyed certificate 19
4.7.6 Publication of the re-keyed certificate by the CA 19
4.7.7 Notification of certificate issuance by the CA to other entities 19
4.8 Certificate modification 19
4.9 Certificate revocation and suspension 19
4.9.1 Circumstances for revocation 19
4.9.2 Who can request revocation 20
4.9.3 Procedure for revocation request 20
4.9.4 Revocation request grace period 20
4.9.5 Time within which CA must process the revocation request 20
4.9.6 Revocation checking requirement for Relying Parties 20
4.9.7 CRL issuance frequency (if applicable) 20
4.9.8 Maximum latency for CRLs (if applicable) 20
4.9.9 On-line revocation/status checking availability 20
4.9.10 On-line revocation checking requirements 21
4.9.11 Other forms of revocation advertisements available 21
4.9.12 Special requirements re key compromise 21
4.9.13 Circumstances for suspension 21
4.9.14 Who can request suspension 21
4.9.15 Procedure for suspension request 21
4.9.16 Limits on suspension period 21
4.10 Certificate status services 21
4.11 End of subscription 21
4.12 Key escrow and recovery 21
4.12.1 Key escrow and recovery policy and practices 21
4.12.2 Session key encapsulation and recovery policy and practices 21
5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 21
5.1 Physical controls 21
5.2 Procedural controls 22
5.3 Personnel controls 22
5.4 Audit logging procedures 22
5.5 Records archival 22
5.6 Key changeover 22

5.7 Compromise and disaster recovery 22
5.8 CA or RA Termination 22
6. TECHNICAL SECURITY CONTROLS 22
6.1 Key pair Generation and Installation 22
6.1.1 Key pair generation 22
6.1.2 Private Key delivery to Subscriber 22
6.1.3 Public key delivery to certificate issuer 22
6.1.4 CA public key delivery to Relying Parties 23
6.1.5 Key sizes 23
6.1.6 Public key parameters generation and quality checking 23
6.1.7 Key usage purposes (as per X.509 v3 key usage field) 23
6.2 Private key protection and cryptographic module engineering controls 23
6.2.1 Cryptographic module standards and controls 23
6.2.2 Private Key (n out of m) multi-person control 23
6.2.3 Private Key escrow 23
6.2.4 Private Key backup 23
6.2.5 Private Key archival 23
6.2.6 Private Key transfer into or from a cryptographic module 23
6.2.7 Private Key storage on cryptographic module 24
6.2.8 Method of activating private key 24
6.2.9 Method of deactivating private key 24
6.2.10 Method of destroying private key 24
6.2.11 Cryptographic Module Rating 24
6.3 Other aspects of key pair management 24
6.3.1 Public key archival 24
6.3.2 Certificate operational periods and key pair usage periods 24
6.4 Activation data 24
6.4.1 Activation data generation and installation 24
6.4.2 Activation data protection 24
6.4.3 Other aspects of activation data 24
6.5 Computer security controls 25
6.5.1 Specific computer security technical requirements 25
6.5.2 Computer security rating 25
6.6 Life cycle technical controls 25
6.6.1 System development controls 25
6.6.2 Security management controls 25
6.6.3 Life cycle security controls 25
6.7 Network security controls 25
6.8 Time-stamping 25
7. CERTIFICATE, CRL AND OCSP PROFILES 25
7.1 Certificate profile 25
7.1.1 Version Numbers 25
7.1.2 Certificate Extensions 25
7.1.3 Algorithm Object Identifiers 25
7.1.4 Name Forms 26
7.1.5 Name Constraints 26
7.1.6 Certificate Policy Object Identifier 26
7.1.7 Usage of Policy Constraints Extension 26
7.1.8 Policy Qualifiers Syntax and Semantics 26
7.1.9 Processing Semantics for the Critical Certificate Policies Extension 27

7.2 CRL profile **27**
7.2.1 Version Numbers 27
7.2.2 CRL and CRL Entry Extensions 27
7.3 OCSP Profile **27**
7.3.1 Version Numbers 27
7.3.2 OCSP Extensions 27
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS **27**
8.1 Frequency or circumstances of assessment **27**
8.2 Identity/qualifications of assessor **27**
8.3 Assessor's relationship to assessed entity **27**
8.4 Topics covered by assessment **27**
8.5 Actions taken as a result of deficiency **27**
8.6 Communication of results **27**
9. OTHER BUSINESS AND LEGAL MATTERS **28**
9.1 Fees **28**
9.1.1 Certificate issuance or renewal fees 28
9.1.2 Certificate access fees 28
9.1.3 Revocation or status information access fees 28
9.1.4 Fees for other services 28
9.1.5 Refund policy 28
9.2 Financial responsibility **28**
9.2.1 Insurance coverage 28
9.2.2 Other assets 28
9.2.3 Insurance or warranty coverage for end-entities 28
9.3 Confidentiality of business information **28**
9.4 Privacy of personal information **28**
9.4.1 Privacy plan 28
9.4.2 Information treated as private 29
9.4.3 Information not deemed private 29
9.4.4 Responsibility to protect private information 29
9.4.5 Notice and consent to use private information 29
9.4.6 Disclosure pursuant to judicial or administrative process 29
9.4.7 Other information disclosure circumstances 29
9.5 Intellectual property rights **29**
9.6 Representations and warranties **29**
9.6.1 CA representations and warranties 29
9.6.2 RA representations and warranties 29
9.6.3 Subscriber representations and warranties 29
9.6.4 Relying Party representations and warranties 30
9.6.5 Representations and warranties of other participants 30
9.7 Disclaimers of warranties **30**
9.8 Limitations of liability **30**
9.9 Indemnities **30**
9.10 Term and termination **30**
9.10.1 Term 30
9.10.2 Termination 30
9.10.3 Effect of termination and survival 30
9.11 Individual notices and communications with participants **30**
9.12 Amendments **31**
9.13 Dispute resolution provisions **31**

9.14 Governing law 31
9.15 Compliance with applicable law 31
9.16 Miscellaneous provisions 31
9.17 Other provisions 31
APPENDIX A. REFERENCES 32
APPENDIX B. CERTIFICATE PROFILES 33
B.1 High Assurance Certificate (HAC) - dual purpose Authentication/Signing 34
B.2 Individual – Hardware - CST Authentication Certificate 37
B.3 Individual – Hardware - CST Digital Signing Certificate 40
B.4 High Assurance Certificate (HAC) - Authentication 43
B.5 Individual – Hardware - HAC Digital Signing Certificate 46
APPENDIX C. CRL FORMAT 49
APPENDIX D. LEVEL OF ASSURANCE MAPPING 50
D.1 Assurance Level 50
D.2 Risk Assessment 51

Table of Tables

Table 1 – Signature OIDs 25
Table 2 - Algorithm OIDs 26
Table 3 - References 32
Table 4 – Individual – Hardware - dual purpose Authentication/Signing Certificate Profile 36
Table 5 – Individual – Hardware - CST Authentication Certificate Profile 39
Table 6 – Individual – Hardware - CST Digital Signing Certificate Profile 42
Table 7 – Individual – Hardware - HAC Authentication Certificate Profile 45
Table 8 – Individual – Hardware - HAC Digital Signing Certificate Profile 48

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) **Individual – Hardware (High Assurance) Identity** certificates.

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

The headings in this CP follow the framework set out in 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 **Australian Defence Individual – High Assurance Certificate (AD-ID-HAC)** 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.

Certificates issued under this CP are signing and/or authentication certificates. No authority, or privilege, applies to an individual by becoming an approved AD-ID-HAC holder, other than confirming an affiliation with Defence.

This CP only allows *Subscribers*' keys and certificates to reside on a hardware based *token* with an embedded cryptographic engine. Before being issued with a token, the applicant is required to undergo

a face to face identity verification that complies with the *Gatekeeper Evidence of Identity* (EOI) policy for an *Identity - Hardware* (*High Assurance) certificate*.

1.2 Document name and identification

The title for this CP is the "X.509 Certificate Policy for the Australian Department of Defence Individual – Hardware (High Assurance) Certificates".

The *Object Identifier* (OID) for this CP is **1.2.36.1.334.1.1.2.2:**

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

Certificate variants may be created under this CP OID branch. Refer to certificate profiles in Appendix B.

1.3 PKI Participants

1.3.1 Certification authorities

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

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

1.3.2 Registration authorities

The *Registration Authorities* (RAs) that perform the registration function under this CP are Gatekeeper accredited Defence RAs. For further information, see CPS.

Registration Officers (ROs) authorised by the RAs perform the initial identity validation of applicants under this CP. ROs are required to undergo registration including Evidence of Identity (EOI) check and training prior to commencing their duties as ROs.

1.3.3 Subscribers

A *Subscriber* is the individual whose name appears as the subject in a certificate, having signed a *Subscriber Agreement*, asserting that their use of the *private key*s and associated certificate will be in accordance with this CP. The RA must formally verify the identity of the Subscriber and their requirement for an AD-ID-HAC. 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-HAC.

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-HAC 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)* – previously known as the *Defence PKI Policy Board* (DPKIPB) – refer to the CPS for their responsibilities which specifically include:

   a) Review and approval of this CP;
   b) Presiding over the PKI audit process;
   c) Approving mechanisms and controls for the management of the accredited infrastructure (CA/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-HACs 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 the 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 authenticate to Defence assets and systems to which the Subscriber has the requisite privileges.

iii. To provide accountability and non-repudiation of AD-ID-HAC Subscriber transactions or communications; and
iv. To verify the integrity of a communication from a Subscriber to and a Relying Party.

Relying Parties should note any risks identified as per Appendix D in relation to the Defence requirements for Identity – Hardware (High 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 certification 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 both internal and external of 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. 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.

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 are 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

Following authentication of the Subscriber by a Registration Officer (RO), a token is issued to the Subscriber. The token, generating the private and *public keys,* submits a digitally signed certificate request to the RA. 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

The RO, on behalf of the RA, must verify a Subscriber's identity before issuing a certificate and token. This must:

i. Occur face to face[1];
ii. Involve the presentation of EOI documents as required by the Gatekeeper EOI policy for Level of Assurance (LOA) 4 Identity certificates (see [GK2015]); and
iii. Total evidence presented must meet the following requirements:

   a) the applicant's name is on every document. Where the EOI documents bear a different name, then the linkage between that EOI document, the name to be registered and the applicant must be clearly established;
   b) the applicant's date of birth is on at least one of the documents; and
   c) a recognisable photograph of the applicant is on at least one of the documents.

The authentication process provides an audit record containing at a minimum:

i. The identity of the applicant;
ii. Document types, name as on document, and document unique identifier which were presented as EOI;
iii. The identity of the RO;

[1] If necessary, registration can be done remotely over video link. In this case, a person local to the Applicant (e.g. supervisor/Security Officer/Defence member) must evaluate the EOI being presented and advise the RO (via email) that to the best of their ability they have verified the documents to be authentic and original.

iv. The CA name and serial numbers of certificates issued, or the reason for rejection of application; and
v. The Subscriber's read and acknowledged Subscriber Agreement, which includes an affirmation that the Subscriber's identity matches the documentation presented.

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

i. Locations where sufficient EOI is unavailable (e.g. Theatre of Operation, or exercises); or
ii. If such individuals do not have sufficient EOI documentation due to genuine difficulty such as loss, theft or destruction of EOI documentation; or
iii. Individuals who, for legitimate reasons, have not been issued sufficient EOI documentation.

Certificates issued under special circumstances will require authorisation by the PKI Operations Manager (or their delegate) based on the risks associated with the circumstances. This authorisation may impose a limit on the reuse of the method by the Subscriber before reverting to standard method of verification (or for re-key requests listed below). In addition, such certificates may have a defined validity period that is less than the normal certificate life.

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-HAC holder, other than confirming an affiliation with Defence. All Subscribers have their affiliation to Defence verified, prior to issue of a certificate, by reference to the Defence Directory.

3.2.6 Criteria for interoperation

See CPS.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for re-key

3.3.1.1 Routine re-key

Routine re-key is normally managed via the *Token Management System* (TMS) prior to the original certificate expiring, and provided the applicant's EOI is less than 5 years old. In such cases, the Subscriber must authenticate to the TMS User Self Service client with their hard token (using their valid certificate and Personal Identification Number – PIN) and follow the TMS processes for replacing their certificate, during which time the new key pair will be generated.

3.3.1.2 Non Routine re-key

The minimum requirements for identification and authentication of other *re-key* activities are as follows:

i. A face to face presentation of the Subscriber to the RO is required for all re-keys where the previous certificate has expired and/or their EOI has expired;
ii. A Subscriber's affiliation shall be verified prior to performing a re-key; and
iii. The RO verifies the Subscriber's identity.

In the event the Subscriber's certificate was originally issued under a PKI PMA approved alternative method, the Subscriber will need to either:

- Request re-key of the certificate from the PKI Operations Manager (or their delegate); or

- Revalidate their identify based upon the presentation of EOI documents as required by the Gatekeeper EOI policy for LOA 4 Identity certificates.

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

i. As per initial enrolment; or
ii. Use of a PKI PMA approved biometric. (Only if biometric was recorded during initial enrolment); or
iii. Proof of possession, and ability to exercise, a current private key, from a token that was issued by the Defence PKI/TMS. This method can only be used provided no more than 5 years has passed since the Subscriber has been identified using the Gatekeeper High Assurance requirements for EOI, or uses an approved biometric.

3.3.2 Identification and authentication for re-key after revocation

Re-key after revocation shall occur in the same manner as for Non Routine re-key (see 3.3.1.2), or the use of a PKI PMA approved biometric (only if the biometric was recorded during the initial enrolment).

3.4 Identification and authentication for revocation request

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

Subscribers may request revocation of their own certificate via the TMS User Self Service client. Authentication to the TMS may be achieved by using the Authentication private key, regardless of the compromise status of the private key.

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 for DRN users; 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.

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

Any individual who has an approved affiliation with Defence, and has a valid requirement, can submit an application for a certificate. Such an application can only be submitted via the accredited RA.

An individual's affiliation with Defence is determined by reference to the Defence Directory.

4.1.2 Enrolment process and responsibilities

Upon receiving a request to issue a certificate to a Subscriber, the RA must ensure that each certificate application undergoes:

i. Confirmation of approval for the individual to hold a certificate;
ii. Validation of all information to be included in certificate request; and
iii. Confirmation of the individual's identity before issuing a token.

The Subscriber is required to present their EOI to an RO for verification. The RO then confirms affiliation with Defence and upon verifying the EOI registers the Subscriber application with the RA.

The RA forwards valid certificate requests to the CA for actioning.

The CA actions requests after confirming that the certificate request originated from a Gatekeeper accredited RA and the details in the certificate request conforms with the CP profile for the requested certificate.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

A summary of the process is as follows:

i. The RO verifies the affiliation and identity of the Subscriber at a face to face interview, as per requirements outlined in section 3.2 (Initial identity validation).
ii. The Subscriber reads and acknowledges the Subscriber Agreement.
iii. The RO enters identifying information for the Subscriber into the applicable certificate application form in the PKI software.
iv. The Subscriber token, keys and certificates are issued either at the time of enrolment, or at a later stage – see section 4.3 (Certificate Issuance).

4.2.2 Approval or rejection of certificate applications

A RO may reject or approve a certification application. Reasons for rejection could include insufficient affiliation with Defence, or the provision of incorrect or insufficient identification details.

4.2.3 Time to process certificate applications

Processing for certificate applications will occur in a timely manner.

4.3 Certificate issuance

Depending on the facilities available to the RO, a token can be issued to the Subscriber at the time of enrolment or at a later stage:

Option 1 – Issuance at the time of enrolment:

If the enrolment is done at a facility where the RO is able to personalise hard tokens, the keys and certificates are issued at the time of enrolment. The *PKI software* initiates the private and public key generation on the Subscriber's hard token.

The token is protected with a passphrase to protect the private key(s) .

Option 2 – Issuance at a later date:

If the enrolment is done at an RO facility without token personalisation capability, the hard token is personalised centrally and securely delivered to the Subscriber, who is then able to access the PKI software to exercise private and public key usage on the token using the passphrase (Section 6.1.2).

In either case, the public keys for the Subscriber are validated by an RA and sent to the CA to be digitally signed. The signed certificates are returned and stored on the Subscriber's hard token.

4.3.1 CA actions during certificate issuance

See CPS.

4.3.2 Notification to Subscriber by the CA of issuance of certificate

Notification to the Subscriber occurs for a certificate request either when it succeeds or fails.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

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

4.4.2 Publication of the certificate by the CA

See CPS.

4.4.3 Notification of certificate issuance by the CA to other entities

No stipulation.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

Subscriber private key and certificate usage is defined above in 1.4 (Certificate Usage). Subscriber responsibilities are described above in 1.3.3 (Subscribers) and in the Subscriber Agreement.

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) details the Relying Party 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. This CP does not permit certificate *renewal*. See 4.7 Certificate Re-key.

4.7 Certificate re-key

Re-key of a certificates indicates creating a certificate with a new key pair, i.e. generating a new key pair on the token, using the identifying information from the old certificate.

4.7.1 Circumstance for certificate re-key

This CP permits 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

Certificate re-key may be requested by the:

i. PKI PMA; or
ii. Subscriber

4.7.3 Processing certificate re-keying requests

To perform a routine certificate re-key, the Subscriber uses the TMS User Self Service client (where the Subscriber's certificate has not yet expired, and their EOI is less than 5 years old).

Where the old certificate has expired, or the Subscriber's EOI has not been validated in the last 5 years, the process is consistent with the enrolment process 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

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

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

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

The CPS defines circumstances for revocation.

4.9.2 Who can request revocation

See CPS.

4.9.3 Procedure for revocation request

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

Alternatively, a digitally signed email from a valid Defence email account may be sent to TMS operations at smartcard.level2support@defence.gov.au for DRN users.

Revocation requests received by ROs are to be verified on receipt in accordance with 3.4 (Identification and authentication for revocation request) and processed in priority order.

After verification, the RO processes revocation requests by using the TMS software, which captures an auditable record of the process.

PKI Operators are also able to revoke an AD-ID-HA certificate through the PKI software if necessary.

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 becomes aware of a reason for revocation, until submitting a revocation request.

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

4.9.5 Time within which CA must process the revocation request

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

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.

4.11 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 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

All Subscribers use hard token technology to generate and securely store private 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

Private authentication or signing keys are always generated within the hard token.

Where private keys are generated on the Subscriber's token at the time of enrolment, no additional delivery process is required.

Where the token is not personalised at the time of enrolment, it will be securely delivered to the Subscriber. Activation information will be 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 through a secure channel.

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).

Keys issued under this CP allow a Subscriber to:

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

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.

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

Cryptographic modules used in the hard tokens 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 compliance for *Personal Identity Verification* (PIV) cards.

HSMs used with the PKI core components have undergone a security evaluation though an ASD recognised evaluation program.

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

Activating private keys 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

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 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.

NB. Subscriber certificates issued in special circumstances (section 3.2) will have a defined validity period that is less than the normal certificate life of two years (eg.1 year for deployed Subscribers with minimum EOI).

6.4 Activation data

6.4.1 Activation data generation and installation

When the certificate and associated key pairs are installed on the hard token during the certificate issuance, the system generates a passphrase. The Subscriber is requested to insert this passphrase when activating their card. They must then change it.

The passphrase is used as the activation data and must be in accordance with Defence policy, which complies with the ISM. 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 policy for the applicable network.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

See CPS.

6.5.2 Computer security rating

See CPS.

6.6 Life cycle technical controls

6.6.1 System development controls

See CPS.

6.6.2 Security management controls

See CPS.

6.6.3 Life cycle security 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 Numbers

All certificates are X.509 Version 3 certificates.

7.1.2 Certificate Extensions

See Appendix B.

7.1.3 Algorithm Object Identifiers

Certificates under this Policy 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}

Table 1 – Signature OIDs

Certificates under this Policy 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.

All other DN components are fixed and defined in Appendix B.

7.1.5 Name Constraints

Refer to the Issuing CA's CP.

7.1.6 Certificate Policy Object Identifier

Highly Trusted Token (HTT) Certificates issued under this policy shall assert this CP's OID:

{1.2.36.1.334.1.1.2.2}

Coalition Security Token (CST) Certificates issued under this policy shall assert this CP's OID with an added '.1' to assist in identifying certificates issued between the two different tokens:

{1.2.36.1.334.1.1.2.2.1}

Certificates issued under this policy shall also assert the appropriate 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:

{1.2.36.1.334.1.2.1.3} Level of Assurance – High (Individual)

{1.2.36.1.334.1.2.1.3.1} Level of Assurance – High (Individual) - CST

{1.2.36.1.334.1.2.1.2} Level of Assurance – Medium (Individual)

{1.2.36.1.334.1.2.1.2.1} Level of Assurance – Medium (Individual) - CST

{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.

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

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 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

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 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 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

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 will only retain details of *Evidence of Identity* (EOI) documentation presented and the unique document identifiers. This information is recorded in the RA and is protected in accordance with the requirements of the Privacy Act, the Information privacy Act 2015 (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 signing the Subscriber Agreement.

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

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, as part of acknowledging the Subscriber Agreement, 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 Disclaimers of warranties

See CPS.

9.8 Limitations of liability

See CPS.

In Addition: GATEKEEPER ACCREDITATION DISCLAIMER

The Gatekeeper Competent Authority is responsible for ensuring that the accreditation process is conducted with due care and in accordance with published Gatekeeper Criteria and Policies. The Gatekeeper Competent Authority is not liable for any errors and/or omissions in the final Approved Documents, which remain the responsibility of the accredited Service Provider. The Digital Transformation Agency is not responsible and cannot be held liable for any loss of any kind in relation to the use of digital keys and certificates issued by a Gatekeeper accredited Service Provider. By granting a Service Provider Gatekeeper Accreditation the Digital Transformation Agency makes no representation and gives no warranty as to the:

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

9.9 Indemnities

See CPS.

9.10 Term and termination

9.10.1 Term

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

9.10.2 Termination

See CPS.

9.10.3 Effect of termination and survival

See CPS.

9.11 Individual notices and communications with participants

See CPS.

9.12 Amendments

See CPS.

9.13 Dispute resolution provisions

See CPS.

9.14 Governing law

See CPS.

9.15 Compliance with applicable law

See CPS.

9.16 Miscellaneous provisions

See CPS.

9.17 Other provisions

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/_lib/doc_pdf/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 will 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
(No ext)	High Assurance Certificate (HAC) (Auth+Sign)	1.2.36.1.334.1.1.2.2.[4]			
1[5]	CST Authentication	1.2.36.1.334.1.1.2.2.1			Nov 2022
2	CST Digital Signing	1.2.36.1.334.1.1.2.2.2			Nov 2022
3[6]	High Assurance Certificate (HAC) - Authentication	1.2.36.1.334.1.1.2.2.3			Nov 2022
4	High Assurance Certificate (HAC) - Digital Signing	1.2.36.1.334.1.1.2.2.4			Nov 2022

[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] Used for dual purpose HACs, i.e. authentication and signing, until such time split keys have been implemented

[5] Prev. used for CST auth *and* signing.

[6] The HAT certificate used OID 1.2.36.1.334.1.1.2.2. prior to Nov 2022. It was then a multipurpose (auth and sign) certificates.

B.1 High Assurance Certificate (HAC) - dual purpose Authentication/Signing

This profile allows dual purpose keys (Auth & Sign) and is used until such time split certs (Authentication & Signing) have been fully implemented. N.B. this variant has **no** extension to the CP OID (1.2.36.1.334.1.1.2.2).
"HAC" replaces the terms "HTT" or "HAT" that were used in the past when they were issued on a separate token to the DCAC.

Field	Critical	Identity Certificate Value	Notes
Version		V3 (2)	Version 3 of X.509
Serial		<octet string>	Must be unique within Defence namespace
Issuer Signature Algorithm		SHA2WithRSAEncryption	
Issuer Distinguished Name		CN= <subCAIssuer> OU= CAs OU= PKI OU= DoD O= GOV C= AU	Encoded as printable string. See Defence-ADPRCA-CP for the Issuing SubCA naming convention.
Validity Period		Not before <UTCtime> Not after <UTCtime>	▪ Maximum 2 years from date of issue. ▪ Maximum 1 year from date of issue for Subscribers under PKI PMA approved special circumstances.
Subject Distinguished Name		CN= <Defence common name> OU= Personnel OU= PKI OU= DoD O= GOV C= AU	CN consists of the subject's common name as described in the Defence Corporate Directory, or where 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" Encoded as printable string where possible, and otherwise using UTF-8
Subject Public Key Information		2048 bit RSA key modulus, rsaEncryption	
Issuer Unique Identifier		Not Present	
Subject Unique Identifier		Not Present	

Field	Critical	Identity Certificate Value	Notes
X.509 V3 extensions:			
Authority Key Identifier	No	<octet string>	160 bit SHA-1 hash of binary DER encoding of the issuing CA's public key[7]
Subject Key Identifier	No	<octet string>	160 bit SHA-1 hash of binary DER encoding of subject's public key
Key Usage	Yes	digitalSignature nonRepudiation	
Extended key usage	No	{1.3.6.1.5.5.7.3.2} Microsoft Client Authentication {1.3.6.1.4.1.311.20.2.2} Microsoft Smart Card Logon {1.3.6.1.5.5.7.3.4} Secure email protection	
Private key usage period		Not Present	
Certificate policies	No	[1] Policy OID: {1.2.36.1.334.1.1.2.2} Policy Qualifier – User Notice: "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 Certificate Policy" Policy Qualifier - CPS pointer: http://crl.defence.gov.au/pki/	▪ The OID of this CP 1.2.36.1.334.1.1.2.2 ▪ UserNotice shall use explicitText field.
		[2] Policy OID: {1.2.36.1.334.1.2.1.3.} or 1.2.36.1.334.1.2.1.3.1 (See Notes)	HAC: 1.2.36.1.334.1.2.1.3 - Level of Assurance – High (Individual); or CST: 1.2.36.1.334.1.2.1.3.1- Level of Assurance – High (Individual) SC650 (CST)
		[3] Policy OID: {1.2.36.1.334.1.2.1.2.1} or {1.2.36.1.334.1.2.1.3.1} (See Notes)	HAC: 1.2.36.1.334.1.2.1.2 - Level of Assurance – Medium (Individual); or CST: 1.2.36.1.334.1.2.1.2.1- Level of Assurance – Medium (Individual) SC650 (CST) Included to allow the certificate to be used in lower assurance contexts. Applicable OID will be below the OID expressed above.
		[4] Policy OID: {1.2.36.1.334.1.2.1.1}	1.2.36.1.334.1.2.1.1 – Level of Assurance – Low (Individual) Included to allow the certificate to be used in lower assurance contexts. Applicable OID will be below the OID expressed above.
Policy Mapping		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	Identity Certificate Value	Notes
Subject Alternative Name	No	rfc822Name: <Defence RFC822 email address> OtherName: <Defence User Principal Name>	Contains the Subject's Defence principal email address. Contains the Subject's Defence User Principal Name.
Issuer Alternative Name		Not Present	
Subject Directory Attribute		Not Present	
Basic Constraints		Not Present	
Name Constraints		Not Present	
Policy Constraints		Not Present	
Subject Information Access		Not Present	
Authority Information Access	No	[1] Access method: OCSP {1.3.6.1.5.5.7.48.1} Access location: http://ocsp.defence.gov.au [2] Access method: CAIssuer{1.3.6.1.5.5.7.48.2} Access location: http://crl.defence.gov.au/pki/Certificates/<subCAIssuer> [3]Access method: CA Issuer {1.3.6.1.5.5.7.48.2} Access location: ldap://dir.defence.gov.au/cn=<subCAIssuer>,ou=CAs,ou=PKI,ou=DoD,o=GOV,c=AU?cACertificate;binary,crossCertificatePair;binary	Defence uses a URL rewrite (redirection) rule in the Web Server to ensure that AIA urls without a file extension are assigned the correct filetype (.crt or .p7c)
CRL Distribution Points	No	[1] Distribution Point Name (http): http://crl.defence.gov.au/pki/crl/<subCAIssuer>.crl [2] Distribution Point Name (ldap): ldap://dir.defence.gov.au/cn=<subCAIssuer>,ou=CAs,ou=PKI,ou=DoD,o=GOV,c=AU?certificateRevocationList	▪ The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension). ▪ 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).

Table 4 – Individual – Hardware - dual purpose Authentication/Signing Certificate Profile

B.2 Individual – Hardware - CST Authentication Certificate

This certificate is issued onto a Subscriber's DCAC and has CP OID 1.2.36.1.334.1.1.2.2.1

Field	Critical	Identity Certificate Value	Notes
Version		V3 (2)	Version 3 of X.509
Serial		<octet string>	Must be unique within Defence namespace
Issuer Signature Algorithm		SHA2WithRSAEncryption	
Issuer Distinguished Name		CN= <subCAIssuer> OU= CAs OU= PKI OU= DoD O= GOV C= AU	Encoded as printable string. See Defence-ADPRCA-CP for the Issuing SubCA naming convention.
Validity Period		Not before <UTCtime> Not after <UTCtime>	▪ Maximum 2 years from date of issue. ▪ Maximum 1 year from date of issue for Subscribers under PKI PMA approved special circumstances.
Subject Distinguished Name		CN= <Defence common name> OU= Personnel OU= PKI OU= DoD O= GOV C= AU	CN consists of the subject's common name as described in the Defence Corporate Directory, or where 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" Encoded as printable string where possible, and otherwise using UTF-8
Subject Public Key Information		2048 bit RSA key modulus, rsaEncryption	
Issuer Unique Identifier		Not Present	
Subject Unique Identifier		Not Present	
X.509 V3 extensions:			
Authority Key Identifier	No	<octet string>	160 bit SHA-1 hash of binary DER encoding of the issuing CA's public key[8]

[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	Identity Certificate Value	Notes
Subject Key Identifier	No	<octet string>	160 bit SHA-1 hash of binary DER encoding of subject's public key
Key Usage	Yes	digitalSignature	N.B. Existing/older CST certs for dual auth+sign use may also have NonRepudiation
Extended key usage	No	{1.3.6.1.5.5.7.3.2} Microsoft Client Authentication {1.3.6.1.4.1.311.20.2.2} Microsoft Smart Card Logon	N.B. Existing/older CST certs for dual auth+sign use may also have {1.3.6.1.5.5.7.3.4} Secure email protection
Private key usage period		Not Present	
Certificate policies	No	[1] Policy OID: {1.2.36.1.334.1.1.2.2.1} Policy Qualifier – User Notice: "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 Certificate Policy" Policy Qualifier - CPS pointer: http://crl.defence.gov.au/pki/	▪ The OID of this CP is 1.2.36.1.334.1.1.2.2 plus the CST variant – Authentication (1) N.B. The OID for this certificate may also being used for CST dual purpose certificates (auth + sign) until split certs are implemented. ▪ UserNotice shall use explicitText field.
		[2] Policy OID: {1.2.36.1.334.1.2.1.3.1}	1.2.36.1.334.1.2.1.**3.1**- Level of Assurance – High (Individual) SC650 (CST)
		[3] Policy OID: {1.2.36.1.334.1.2.1.2.1	1.2.36.1.334.1.2.1.**2.1** - Level of Assurance – Medium (Individual) SC650 (CST) Included to allow the certificate to be used in lower assurance contexts. Applicable OID will be below the OID expressed above.
		[4] Policy OID: {1.2.36.1.334.1.2.1.1}	1.2.36.1.334.1.2.1.1 – Level of Assurance – Low (Individual) Included to allow the certificate to be used in lower assurance contexts. Applicable OID will be below the OID expressed above.
Policy Mapping		Not Present	
Subject Alternative Name	No	rfc822Name: <Defence RFC822 email address> OtherName: <Defence User Principal Name>	Contains the Subject's Defence principal email address. Contains the Subject's Defence User Principal Name.
Issuer Alternative Name		Not Present	
Subject Directory Attribute		Not Present	
Basic Constraints		Not Present	
Name Constraints		Not Present	
Policy Constraints		Not Present	

Field	Critical	Identity Certificate Value	Notes
Subject Information Access		Not Present	
Authority Information Access	No	[1] Access method: OCSP {1.3.6.1.5.5.7.48.1} Access location: http://ocsp.defence.gov.au [2] Access method: CAIssuer{1.3.6.1.5.5.7.48.2} Access location: http://crl.defence.gov.au/pki/Certificates/<subCAIssuer> [3]Access method: CA Issuer {1.3.6.1.5.5.7.48.2} Access location: ldap://dir.defence.gov.au/cn=<subCAIssuer>,ou=CAs,ou=PKI,ou=DoD,o=GOV,c=AU?cACertificate;binary,crossCertificatePair;binary	Defence uses a URL rewrite (redirection) rule in the Web Server to ensure that AIA urls without a file extension are assigned the correct filetype (.crt or .p7c)
CRL Distribution Points	No	[1] Distribution Point Name (http): http://crl.defence.gov.au/pki/crl/<subCAIssuer>.crl [2] Distribution Point Name (ldap): ldap://dir.defence.gov.au/cn=<subCAIssuer>,ou=CAs,ou=PKI,ou=DoD,o=GOV,c=AU?certificateRevocationList	▪ The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension). ▪ 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).

Table 5 – Individual – Hardware - CST Authentication Certificate Profile

B.3 Individual – Hardware - CST Digital Signing Certificate

This certificate is issued onto a Subscriber's DCAC and has CP OID 1.2.36.1.334.1.1.2.2.2

Field	Critical	Identity Certificate Value	Notes
Version		V3 (2)	Version 3 of X.509
Serial		<octet string>	Must be unique within Defence namespace
Issuer Signature Algorithm		SHA2WithRSAEncryption	
Issuer Distinguished Name		CN= <subCAIssuer> OU= CAs OU= PKI OU= DoD O= GOV C= AU	Encoded as printable string. See Defence-ADPRCA-CP for the Issuing SubCA naming convention.
Validity Period		Not before <UTCtime> Not after <UTCtime>	▪ Maximum 2 years from date of issue. ▪ Maximum 1 year from date of issue for Subscribers under PKI PMA approved special circumstances.
Subject Distinguished Name		CN= <Defence common name> OU= Personnel OU= PKI OU= DoD O= GOV C= AU	CN consists of the subject's common name as described in the Defence Corporate Directory, or where 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" Encoded as printable string where possible, and otherwise using UTF-8
Subject Public Key Information		2048 bit RSA key modulus, rsaEncryption	
Issuer Unique Identifier		Not Present	
Subject Unique Identifier		Not Present	
X.509 V3 extensions:			
Authority Key Identifier	No	<octet string>	160 bit SHA-1 hash of binary DER encoding of the issuing CA's public key[9]

[9] 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	Identity Certificate Value	Notes
Subject Key Identifier	No	<octet string>	160 bit SHA-1 hash of binary DER encoding of subject's public key
Key Usage	Yes	digitalSignature nonRepudiation	
Extended key usage	No	{1.3.6.1.5.5.7.3.4} Secure email protection	
Private key usage period		Not Present	
Certificate policies	No	[1] Policy OID: {1.2.36.1.334.1.1.2.2.2} Policy Qualifier – User Notice: "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 Certificate Policy" Policy Qualifier - CPS pointer: http://crl.defence.gov.au/pki/	▪ The OID of this CP is 1.2.36.1.334.1.1.2.2 plus the CST variant – Digital Signing (2) ▪ UserNotice shall use explicitText field.
		[2] Policy OID: {1.2.36.1.334.1.2.1.3.1}	1.2.36.1.334.1.2.1.**3.1**- Level of Assurance – High (Individual) SC650 (CST)
		[3] Policy OID: {1.2.36.1.334.1.2.1.2.1	1.2.36.1.334.1.2.1.**2.1** - Level of Assurance – Medium (Individual) SC650 (CST) Included to allow the certificate to be used in lower assurance contexts. Applicable OID will be below the OID expressed above.
		[4] Policy OID: {1.2.36.1.334.1.2.1.1}	1.2.36.1.334.1.2.1.1 – Level of Assurance – Low (Individual) Included to allow the certificate to be used in lower assurance contexts. Applicable OID will be below the OID expressed above.
Policy Mapping		Not Present	
Subject Alternative Name	No	rfc822Name: <Defence RFC822 email address> OtherName: <Defence User Principal Name>	Contains the Subject's Defence principal email address. Contains the Subject's Defence User Principal Name.
Issuer Alternative Name		Not Present	
Subject Directory Attribute		Not Present	
Basic Constraints		Not Present	
Name Constraints		Not Present	
Policy Constraints		Not Present	

Field	Critical	Identity Certificate Value	Notes
Subject Information Access		Not Present	
Authority Information Access	No	[1] Access method: OCSP {1.3.6.1.5.5.7.48.1} Access location: http://ocsp.defence.gov.au [2] Access method: CAIssuer{1.3.6.1.5.5.7.48.2} Access location: http://crl.defence.gov.au/pki/Certificates/<subCAIssuer> [3]Access method: CA Issuer {1.3.6.1.5.5.7.48.2} Access location: ldap://dir.defence.gov.au/cn=<subCAIssuer>,ou=CAs,ou=PKI,ou=DoD,o=GOV,c=AU?cACertificate;binary,crossCertificatePair;binary	Defence uses a URL rewrite (redirection) rule in the Web Server to ensure that AIA urls without a file extension are assigned the correct filetype (.crt or .p7c)
CRL Distribution Points	No	[1] Distribution Point Name (http): http://crl.defence.gov.au/pki/crl/<subCAIssuer>.crl [2] Distribution Point Name (ldap): ldap://dir.defence.gov.au/cn=<subCAIssuer>,ou=CAs,ou=PKI,ou=DoD,o=GOV,c=AU?certificateRevocationList	▪ The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension). ▪ 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).

Table 6 – Individual – Hardware - CST Digital Signing Certificate Profile

B.4 High Assurance Certificate (HAC) - Authentication

This certificate is issued onto a Subscriber's DCAC and has CP OID 1.2.36.1.334.1.1.2.2.3

Field	Critical	Identity Certificate Value	Notes
Version		V3 (2)	Version 3 of X.509
Serial		<octet string>	Must be unique within Defence namespace
Issuer Signature Algorithm		SHA2WithRSAEncryption	
Issuer Distinguished Name		CN= <subCAIssuer> OU= CAs OU= PKI OU= DoD O= GOV C= AU	Encoded as printable string. See Defence-ADPRCA-CP for the Issuing SubCA naming convention.
Validity Period		Not before <UTCtime> Not after <UTCtime>	▪ Maximum 2 years from date of issue. ▪ Maximum 1 year from date of issue for Subscribers under PKI PMA approved special circumstances.
Subject Distinguished Name		CN= <Defence common name> OU= Personnel OU= PKI OU= DoD O= GOV C= AU	CN consists of the subject's common name as described in the Defence Corporate Directory, or where 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" Encoded as printable string where possible, and otherwise using UTF-8
Subject Public Key Information		2048 bit RSA key modulus, rsaEncryption	
Issuer Unique Identifier		Not Present	
Subject Unique Identifier		Not Present	
X.509 V3 extensions:			
Authority Key Identifier	No	<octet string>	160 bit SHA-1 hash of binary DER encoding of the issuing CA's public key[10]

[10] 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	Identity Certificate Value	Notes
Subject Key Identifier	No	<octet string>	160 bit SHA-1 hash of binary DER encoding of subject's public key
Key Usage	Yes	digitalSignature	
Extended key usage	No	{1.3.6.1.5.5.7.3.2} Microsoft Client Authentication {1.3.6.1.4.1.311.20.2.2} Microsoft Smart Card Logon	
Private key usage period		Not Present	
Certificate policies	No	[1] Policy OID: {1.2.36.1.334.1.1.2.2.**3**} Policy Qualifier – User Notice: "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 Certificate Policy" Policy Qualifier - CPS pointer: http://crl.defence.gov.au/pki/	▪ The OID of this CP is 1.2.36.1.334.1.1.2.2 plus the HAC–Authentication variant number (3) ▪ UserNotice shall use explicitText field.
		[2] Policy OID: {1.2.36.1.334.1.2.1.**3**}	The LoA of this certificate. 1.2.36.1.334.1.2.1.**3** - Level of Assurance – High (Individual)
		[3] Policy OID: {1.2.36.1.334.1.2.1.2}	1.2.36.1.334.1.2.1.**2** - Level of Assurance – Medium (Individual) Included to allow the certificate to be used in lower assurance contexts. Applicable OID will be below the OID expressed above.
		[4] Policy OID: {1.2.36.1.334.1.2.1.1}	1.2.36.1.334.1.2.1.1 – Level of Assurance – Low (Individual) Included to allow the certificate to be used in lower assurance contexts. Applicable OID will be below the OID expressed above.
Policy Mapping		Not Present	
Subject Alternative Name	No	rfc822Name: <Defence RFC822 email address> OtherName: <Defence User Principal Name>	Contains the Subject's Defence principal email address. Contains the Subject's Defence User Principal Name.
Issuer Alternative Name		Not Present	
Subject Directory Attribute		Not Present	
Basic Constraints		Not Present	
Name Constraints		Not Present	
Policy Constraints		Not Present	
Subject Information Access		Not Present	

Field	Critical	Identity Certificate Value	Notes
Authority Information Access	No	[1] Access method: OCSP {1.3.6.1.5.5.7.48.1} Access location: http://ocsp.defence.gov.au [2] Access method: CAIssuer{1.3.6.1.5.5.7.48.2} Access location: http://crl.defence.gov.au/pki/Certificates/<subCAIssuer> [3]Access method: CA Issuer {1.3.6.1.5.5.7.48.2} Access location: ldap://dir.defence.gov.au/cn=<subCAIssuer>,ou=CAs,ou=PKI,ou=DoD,o=GOV,c=AU?cACertificate;binary,crossCertificatePair;binary	Defence uses a URL rewrite (redirection) rule in the Web Server to ensure that AIA urls without a file extension are assigned the correct filetype (.crt or .p7c)
CRL Distribution Points	No	[1] Distribution Point Name (http): http://crl.defence.gov.au/pki/crl/<subCAIssuer>.crl [2] Distribution Point Name (ldap): ldap://dir.defence.gov.au/cn=<subCAIssuer>,ou=CAs,ou=PKI,ou=DoD,o=GOV,c=AU?certificateRevocationList	▪ The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension). ▪ 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).

Table 7 – Individual – Hardware - HAC Authentication Certificate Profile

B.5 Individual – Hardware - HAC Digital Signing Certificate

This certificate is issued onto a Subscriber's DCAC and has CP OID 1.2.36.1.334.1.1.2.2.4

Field	Critical	Identity Certificate Value	Notes
Version		V3 (2)	Version 3 of X.509
Serial		<octet string>	Must be unique within Defence namespace
Issuer Signature Algorithm		SHA2WithRSAEncryption	
Issuer Distinguished Name		CN= <subCAIssuer> OU= CAs OU= PKI OU= DoD O= GOV C= AU	Encoded as printable string. See Defence-ADPRCA-CP for the Issuing SubCA naming convention.
Validity Period		Not before <UTCtime> Not after <UTCtime>	▪ Maximum 2 years from date of issue. ▪ Maximum 1 year from date of issue for Subscribers under PKI PMA approved special circumstances.
Subject Distinguished Name		CN= <Defence common name> OU= Personnel OU= PKI OU= DoD O= GOV C= AU	CN consists of the subject's common name as described in the Defence Corporate Directory, or where 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" Encoded as printable string where possible, and otherwise using UTF-8
Subject Public Key Information		2048 bit RSA key modulus, rsaEncryption	
Issuer Unique Identifier		Not Present	
Subject Unique Identifier		Not Present	
X.509 V3 extensions:			
Authority Key Identifier	No	<octet string>	160 bit SHA-1 hash of binary DER encoding of the issuing CA's public key[11]

[11] 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	Identity Certificate Value	Notes
Subject Key Identifier	No	<octet string>	160 bit SHA-1 hash of binary DER encoding of subject's public key
Key Usage	Yes	digitalSignature nonRepudiation	
Extended key usage	No	{1.3.6.1.5.5.7.3.4} Secure email protection	
Private key usage period		Not Present	
Certificate policies	No	[1] Policy OID: {1.2.36.1.334.1.1.2.2.**4**} Policy Qualifier – User Notice: "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 Certificate Policy" Policy Qualifier - CPS pointer: http://crl.defence.gov.au/pki/	▪ The OID of this CP is 1.2.36.1.334.1.1.2.2 plus the HAC–Digital Signing number (4) ▪ UserNotice shall use explicitText field.
		[2] Policy OID: {1.2.36.1.334.1.2.1.3}	The LoA of this certificate. 1.2.36.1.334.1.2.1.**3** - Level of Assurance – High (Individual)
		[3] Policy OID: {1.2.36.1.334.1.2.1.2}	1.2.36.1.334.1.2.1.**2** - Level of Assurance – Medium (Individual) Included to allow the certificate to be used in lower assurance contexts. Applicable OID will be below the OID expressed above.
		[4] Policy OID: {1.2.36.1.334.1.2.1.1}	1.2.36.1.334.1.2.1.1 – Level of Assurance – Low (Individual) Included to allow the certificate to be used in lower assurance contexts. Applicable OID will be below the OID expressed above.
Policy Mapping		Not Present	
Subject Alternative Name	No	rfc822Name: <Defence RFC822 email address> OtherName: <Defence User Principal Name>	Contains the Subject's Defence principal email address. Contains the Subject's Defence User Principal Name.
Issuer Alternative Name		Not Present	
Subject Directory Attribute		Not Present	
Basic Constraints		Not Present	
Name Constraints		Not Present	
Policy Constraints		Not Present	
Subject Information Access		Not Present	

Field	Critical	Identity Certificate Value	Notes
Authority Information Access	No	[1] Access method: OCSP {1.3.6.1.5.5.7.48.1} Access location: http://ocsp.defence.gov.au [2] Access method: CAIssuer{1.3.6.1.5.5.7.48.2} Access location: http://crl.defence.gov.au/pki/Certificates/<subCAIssuer> [3]Access method: CA Issuer {1.3.6.1.5.5.7.48.2} Access location: ldap://dir.defence.gov.au/cn=<subCAIssuer>,ou=CAs,ou=PKI,ou=DoD,o=GOV,c=AU?cACertificate;binary,crossCertificatePair;binary	Defence uses a URL rewrite (redirection) rule in the Web Server to ensure that AIA urls without a file extension are assigned the correct filetype (.crt or .p7c)
CRL Distribution Points	No	[1] Distribution Point Name (http): http://crl.defence.gov.au/pki/crl/<subCAIssuer>.crl [2] Distribution Point Name (ldap): ldap://dir.defence.gov.au/cn=<subCAIssuer>,ou=CAs,ou=PKI,ou=DoD,o=GOV,c=AU?certificateRevocationList	▪ The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension). ▪ 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).

Table 8 – Individual – Hardware - HAC Digital Signing Certificate Profile

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 Levels of Assurance Requirements paper [LOA]:

CP's Highest Level of Assurance:	HIGH Assurance {1.2.36.1.334.1.2.1.3}. **As documented in section 7.1.6 above.**

REQUIREMENT	CP'S MAPPING TO REQUIREMENT
IDENTITY PROOFING	
EOI	The EOI is in accordance with the processes required for certification of a Gatekeeper High Assurance certificate, as covered in section 3.2 above. NB. Reduced EOI may be approved for special circumstances by the PKI PMA.
Evidence of Relationship	Subscriber must be identified in the Defence directory, as covered in section 3.2.2 above.
Location	As documented in section 3.2.3 the location of the identity proofing should be local, and must be face-to-face.

CREDENTIAL STRENGTH	
Token Protection	As documented in section 6.2, the AD-ID-HA-CP token will be a hard token, which has been evaluated under Common Criteria and/or FIPS 140-2 and PIV 201. The keys will not be allowed to be exported, and the token will include the capability to identity tamper evidence.
Token Activation	As documented in section 6.4, a passphrase is created during token issuance. This passphrase is securely communicated to the Subscriber and used as the activation data, and must be in accordance with Defence passphrase policy. Lifecycle management of passphrases and other activation data is in accordance with the PKI KMP and Defence Policy.
Life (Time) of Key Strength	The key strength is determined based on National Institute of Standards and Technology (NIST) SP 800-57-1 Rev 3. Refer to Annex B to determine the applicable algorithms and size. Certificates that make use of SHA-2, with at least 128 security bits (SHA-256) and a RSA key size of at least 2048 bits are suitable for protecting classified, confidential and secret information from 2010 to 2030 and available for legacy use post 2030. [ISM2015, GK2015]

CERTIFICATE MANAGEMENT	
CA Protection	As documented within section 5, the CA protection is aligned with the High Assurance requirements as documented in the Defence [LOA] paper.
Binding	As documented in section 4, the issuance of the AD-ID-HA certificate is tightly bound to the presentation of the EOI paperwork, during the presentation of the token storing the AD-ID-HA key pair. The issuance process is contiguous, and requires the identity of the Subscriber to be bound to their Defence email address.
Revocation (Publication)	As covered in section 4.9.7, the CRL is published every Operational day, day or at intervals no greater than once a week if there are no updates.
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-HA Certificate Policy has been aligned with an Australian Defence High Assurance, which as documented in the [LOA] paper should provide a relying party some assurance in the asserted identity.

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

No risks were identified and managed in the alignment of the AD-ID-HA-CP with the requirements for High Assurance.

LOA REQUIREMENT	IDENTIFIED RISK	MITIGATION / CONTROLS