Australian Government

Defence

X.509 Certification Practice Statement for the Australian Department of Defence

Version 11.0
November 2023

Document Management

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

Change History

Version	Issue Date	Description/ Amendment	Changed by
1.0	17 May 2007	Initial Release	GJF
2.0	23 Nov 09	Release (add T3 device certs, legal)	GJF
3.0	Nov 2011	Released (minor amendments, hard tokens, PIV & CCEB compliance)	SJP
4.0	July 2012	Released	SJP
5.0	May 2014	Review for release	PKI Ops Man
6.0	Oct 2016	Released	PKI Ops Manager
6.1	Nov 2016	CA name change	CogitoGroup (CJP)
6.2	Sep 2017	CSO review	CSO
6.3	Feb 2018	GK Review	Ops Manager
7.0	July 2019	Published	PKI Ops Man
7.1	Sep 2019	Edits	PKI Ops Man
7.2	Sep 2020	Update classification (new scheme), change to Subscriber definition, rename CMS (to TMS), contact email, other minor improvements	CDMC (AKK)
8.0	Oct 2020	Reviewed by DTA – Changes accepted - Released	CDMC (AKK)
8.1	Jan 2021	Updated contact details (PO Box)	CDMC (AKK)
8.2	Nov 2021	2021 updates. Name change RCs -> TAs. Other minor edits,	CDMC (AKK)
9.0	Nov 2021	Reviewed by DTA – Changes accepted - Released	CDMC (AKK)
9.1	Jan 2022	Very minor legal change 9.12.3 and added definition of “Confidential information” – Released. Addition of ICTSB to authorised revocation requestors (4.9.2)	CDMC (AKK)
9.2	Oct 2022	Annual review and update	CDMC (AKK)
10.0	Nov 2022	Reviewed by DTA. Changes accepted - Published	CDMC (AKK)
10.1	Nov 2023	2023 updates	CDMC (AKK)
11.0	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

In general, a *Certification Practice Statement* (CPS) is a statement of the practices that a *Certification Authority* (CA) employs for all *certificate* lifecycle services (e.g. issuance, management, revocation, and renewal or re-keying) and provides details concerning other business, legal, and technical matters. A *Certificate Policy* (CP) is a named set of rules that indicates the applicability of a Certificate to a particular community and/or class of applications with common security requirements.

The headings in this CPS follow the framework set out in the *Internet Engineering Task Force (IETF) Request for Comment* (RFC) 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. The CPS is closely related to the corresponding CPs, and the documents are frequently cross-referenced. Where the CPS or the CP is silent on a subject, it may refer to the other and omit sub headings.

A document hierarchy applies:

1. The provisions of any applicable contract such as a *Subscriber Agreement*, Deed of Agreement or other relevant contract override the provisions of a CP.
2. The provisions of a CP prevail over the provisions of this CPS to the extent of any direct inconsistency.
3. The provisions of this CPS govern any matter on which a CP is silent.

This section identifies and introduces the set of provisions, and indicates the types of entities and applications to which this Australian Government *Department of Defence* (*Defence*) X.509 CPS applies.

1.1 Overview

The purpose of this CPS is to provide a common framework under which Defence *Public Key Infrastructure* (*PKI*), CAs and *Registration Authorities* (RA), services are provided. As such, it sets out a number of policy and operational matters related to the services, including the practices that Defence employs in issuing, revoking and managing certificates.

This CPS should be read in conjunction with the relevant CP, which sets out the rules regarding the applicability of a certificate to a particular community and contains information about the specific structure of the relevant certificate type and assurance level.

The Defence PKI operates and complies with this CPS and the PKI is capable of supporting multiple CAs to provide different certificate types.

The principal documents referenced by this CPS and the entities responsible for them are:

i. the Australian Government *Protective Security Policy Framework* (PSPF) – Attorney General's Department;
ii. the Australian Government *Information Security Manual* (ISM) – *Australian Cyber Security Centre (ACSC);* and
iii. the *Defence Security Principles Framework* (DSPF) – Defence Security and Vetting Service.

The Defence PKI conducts its role in accordance with the *Approved Documents*.

The following public documents are Approved Documents:

i. this CPS;
ii. the X.509 Certificate Policy for the Australian Department of Defence **Public Root Certificate Authority and Subordinate Certificate Authorities**;
iii. the X.509 Certificate Policy for the Australian Department of Defence **Interoperability Certificate Authority;**

iv. the X.509 Certificate Policy for the Australian Department of Defence **Individual – Hardware Certificates (High Assurance)**;
v. the X.509 Certificate Policy for the Australian Department of Defence **Individual – Medium Assurance Certificate;**
vi. the X.509 Certificate Policy for the Australian Department of Defence **Secure Communications Certificates**;
vii. the X.509 Certificate Policy for the Australian Department of Defence **Validation Authority;**
viii. the X.509 Certificate Policy for the Australian Department of Defence **Digital Signing Certificates; and**
ix. the Defence PKI Subscriber Agreement.

The following classified documents are also Approved Documents:

i. Certificate and Directory Management Centre Information Communications Technology Security Policy (CDMC ICTSP);
ii. PKI System Security Plan (PKI SSP);
iii. PKI Security Risk Management Plan (PKI SRMP);
iv. PKI Key Management Plan (PKI KMP);
v. PKI Disaster Recovery and Business Continuity Plan (PKI DRBCP);
vi. PKI Incident Response Plan (PKI IRP)
vii. PKI Operations Manual (PKI Operations Manual);
viii. PKI Registration Authority Operations Manual (RA Manual); and
ix. Gatekeeper Memorandum of Agreement (MOA).

Whilst the classified documents are named in this CPS, the contents are not disclosed publicly for security reasons.

In addition, there are other Approved Documents for CAs that are used internally only, which are not publicised outside of Defence.

Defence operates and manages PKI facilities to support:

i. interaction directly with Defence assets or systems, using Public Key Technology (PKT);
ii. authentication with third parties as an affiliate of Defence; or
iii. provision of digital signatures to entities affiliated with Defence.

The Management Board accountable for Defence PKI facilities is the Defence PKI Policy Management Authority (PKI PMA), with operational responsibility residing with ICT Operations Division. The Defence PKI operates at an enterprise level across Defence (with public and enterprise CAs) and it provides certificate management covering:

i. Identity certificates;
ii. Resource certificates;
iii. PKI Infrastructure certificates (CAs, RAs, CRLs etc.); and
iv. Additional certificates types as approved by the PKI PMA.

It is the responsibility of the PKI PMA to ensure that this CPS is suitable to support the certificates issued by the Defence PKI, and to update the CPS as necessary to support any additional certificates types.

Any entity within Defence running or planning to provide a PKI service outside of the Defence PKI service requires approval from the PKI PMA to operate a facility for their specific application area, and this service is to be constrained to that specific applications area and not to offer a more generic service.

1.2 Document name and identification

The title for this CPS is "X.509 Certification Practice Statement for the Australian Department of Defence". This CPS does not require an *Object Identifier* (OID).

1.3 PKI participants

1.3.1 Certification authorities

The CAs that issue certificates under this CPS are Defence CAs. Appendix A provides a list of Public CAs operated by Defence under this CPS. Public CAs are Gatekeeper accredited and audited to be trusted externally to Defence. Details of CAs approved by the PKI PMA to operate internally are not externally published.

1.3.2 Registration authorities

The *Registration Authority* (RA), or RAs, that perform the registration function under this CPS are Defence RAs or Defence approved "Third party" RAs (Authorised RAs). An RA is formally bound to perform the registration functions in accordance with the applicable CP and other relevant documentation via an appropriate agreement with Defence. All:

i. Gatekeeper accredited CAs must only use Gatekeeper accredited RAs; and
ii. non-Gatekeeper accredited CAs may use Defence RAs, Authorised RAs or Gatekeeper accredited RAs as approved by the PKI PMA.

1.3.3 Subscribers

A *Subscriber* is, as the context allows:

i. for Identity Certificates, i.e. those issued to Person Entities (PE); the person whose Distinguished Name appears as the "Subject Distinguished Name" on the relevant Certificate;
ii. for Resource Certificates, i.e. those issued to Non-Person Entities (NPE); the person or legal entity that applied for that Certificate, and/or administers the system that utilises the Certificate.

Individual CPs provide context for the definition of Subscriber relevant to that CP.

1.3.4 Relying parties

In general, a *Relying Party* uses a Defence certificate to:

i. verify the identity of an entity;
ii. verify the integrity of a communication with an entity;
iii. establish confidential communications with an entity; and
iv. ensure the non-repudiation of a communication with an entity.

In order to give uninhibited access to revocation information and subsequently invoke trust in its own services, Defence refrains from implementing an agreement with the Relying Party with regard to controlling the validity of certificate services with the purpose of binding Relying Parties to their obligations.

Use of the Defence PKI by Relying Parties is governed by the conditions set out in the Defence PKI policy framework consisting of the Approved Documents.

Relying Parties are hereby notified that the conditions prevailing in the CPS, and relevant CP, are binding upon them when they consult the Defence PKI for the purpose of establishing trust and validating a certificate.

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

i. the validity of the entity's certificate using certificate status information;
ii. any authority, or privilege, of the entity to act on behalf of Defence; and
iii. any authority, access or privilege the entity has to the Relying Party's assets or systems.

A Relying Party agrees to the conditions of the relevant CP and must:

i. verify the validity of a digital certificate i.e. verify that the digital certificate is current and has not been revoked or suspended, in the manner specified in the CP under which the digital certificate was issued;
ii. verify that the digital certificate is being used within the limits specified in the CP under which the digital certificate was issued; and
iii. promptly notify the Defence PKI in the event that it suspects that there has been a compromise of the Subscriber's Private Keys.

1.3.5 Other participants

Other participants include:

i. the **PKI PMA** – which owns the overarching policy under which this CPS operates, and:
   a) reviews and approves this CPS and relevant CPs;
   b) ensures that the infrastructure remains compliant at all times within the terms of its accreditation;
   c) presides over the PKI audit process;
   d) defines rules, and approves agreements, for interoperation with other PKIs;
   e) approves mechanisms and controls for the management of the PKI;
   f) approves operational standards and guidelines to be followed;
   g) provides strategic direction for PKT addressing Defence, National and International issues;
   h) monitors the governance and performance of the Defence PKI; and
   i) authorises establishing the PKT infrastructure to support PKI within Defence;
ii. **Accreditation agencies** – to provide independent assurance that the facilities, practices and procedures used to issue Defence certificates comply with the relevant accreditation frameworks (policy, security and legal);
iii. **Directory Service providers** – to provide a repository for certificates and certificate status information issued under the CP; and
iv. **Defence system administrators** – to act as trusted installers/key custodians for Defence Resource certificates.

1.4 Certificate usage

Certificates issued under this CPS, in conjunction with their associated private *keys*, allow an entity to:

i. authenticate to a Relying Party electronically in online transactions;
ii. digitally sign electronic documents, transactions, application code, timestamps and communications; and/or
iii. confidentially communicate with a Relying Party.

1.4.1 Appropriate certificate uses

See relevant CP.

1.4.2 Prohibited certificate uses

See relevant CP.

1.5 Policy administration

This section defines the administrative details for all aspects of this CPS and any applicable CPs.

1.5.1 Organisation administering the document

Defence, through the PKI PMA, is the endorsing organisation for this CPS and applicable CPs, and any amendments. Additional organisations, through agreement with the PKI PMA may also endorse this CPS as satisfying their requirements for a specific CP. Defence will maintain a list of organisations and certificate types for which such agreements exists.

1.5.2 Contact person

Contact details for PKI PMA:

Email	pki.ops@defence.gov.au
Postal address	Defence PKI Policy Management Authority c/o CDMC R8-LG-014 Department of Defence PO Box 7909 CANBERRA BC ACT 2610

To report a problem with a certificate issued by the Defence PKI, send an email to pki.ops@defence.gov.au with details of the Issuing CA, certificate serial number or full Subject DName, and the nature of the issue, e.g. suspected Private Key compromise, certificate misuse, or other types of fraud, compromise or inappropriate conduct.

1.5.3 Authority determining CPS suitability for the policy

The PKI PMA is the authority responsible for determining if this CPS is suitable for a CP.

1.5.4 CPS approval procedures

This CPS is approved by the PKI PMA and the Gatekeeper Competent Authority.

Before accepting changes to this document, or associated CP:

i. the proposed changes are to be integrated into a draft document and submitted to the PKI PMA;
ii. the proposed changes are reviewed by the PKI PMA;
iii. once the proposed changes are acceptable, the PKI PMA will endorse the changes and forward the endorsed changes to external parties who perform any PKI accreditation or cross certification process with Defence; and
iv. upon acceptance by all applicable parties, the PKI PMA will approve for publication, and implementation, the proposed changes.

1.6 Definitions, acronyms and interpretation

See Appendix B – Definitions, Acronyms and Interpretation. Note that all defined terms in this CPS appear in italics the first time they are used and otherwise are not identified in this manner when appearing later throughout the CPS.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

Defence operates repositories supporting the Defence PKI and its operations. Only Defence operated repositories hold authoritative Defence PKI related information (Certificates, CRLs, etc.).

The external online repository of information from the Defence PKI is accessible at http://crl.defence.gov.au/pki/

2.2 Publication of certification information

Defence publishes to its internal repository all CA certificates, relevant *Subscriber* certificates and *Certificate Revocation Lists* (CRL). Externally, Defence provides a repository of relevant PKI information for Relying Parties either directly or via "proxy" repositories at the borders of Defence networks. CA Certificates, Entity Certificates and CRLs that are not required for external use or external Relying Parties, will not be published in external repositories. Resource certificates for non-person entities such as Defence applications, servers, routers and so forth may be published to a certificate store within an application as an alternative to publication within the repository.

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

i. this CPS; and
ii. relevant CPs.

2.3 Time or frequency of publication

The prompt publishing of information in the repository is required after such information becomes available. This CPS specifies the minimum performance standards applicable to the various types of information in section 4 (Certificate Life-cycle Operational Requirements).

Public documents are published/updated promptly on approved change.

Publication frequencies for certificates and CRLs are detailed in the applicable CP, where they differ from the minimum standards defined above.

2.4 Access controls on repositories

Repository information requires protection from unauthorised disclosure or modification, appropriate for the classification of the information and its value to all parties.

There are no further access controls on read-only versions of public documents.

Appropriate access controls on the repositories are used to ensure that only personnel and processes authorised by the *Certificate and Directory Management Centre* (CDMC) are able to write to, or modify repository information.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

See Relevant CP

3.1.2 Need for names to be meaningful

See relevant CP.

3.1.3 Anonymity or pseudonymity of Subscribers

See relevant CP.

3.1.4 Rules for interpreting various name forms

See relevant CP.

3.1.5 Uniqueness of names

See relevant CP.

3.1.6 Recognition, authentication, and role of trademarks

Applicants for certificates must take all reasonable steps to ensure that subject names do not contain or comprise anything that might infringe a trademark.

The CA will not issue a certificate where it is aware that it would contain a name that infringes (or that the CA considers might infringe) a trademark.

Where the CA becomes aware subsequent to issuing that a name on the certificate contains or comprises anything that might infringe a trademark (and hence has been erroneously issued), the certificate may be revoked as provided for in 4.9 of this CPS.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

The PKI PMA endorses all methods used to prove possession by an entity or entity owner of the private key. See relevant CP for further details.

3.2.2 Authentication of organisation identity

See relevant CP.

3.2.3 Authentication of individual identity

See relevant CP.

3.2.4 Non-verified Subscriber information

See relevant CP.

3.2.5 Validation of authority

See relevant CP.

3.2.6 Criteria for interoperation

The decision to cross certify, cross recognise, mutually recognise, at Defence level, or other form of interoperation with a third party PKI resides with the PKI PMA and the third party.

The PKI PMA will inspect the third party CP, and the *X.509* Certificate Profiles, for compatibility and intended uses, as well as the CPS to ensure that the practice and procedures are also compatible.[1]

3.3 Identification and authentication for re-key requests

See relevant CP.

3.4 Identification and authentication for revocation requests

See relevant CP.

[1] This does not mean 100% equivalent, but more that for the intended purposes of interoperation the third party system and processes, are acceptable.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate application

4.1.1 Who can submit a certificate application

Individuals affiliated with Defence can submit a certificate application for either themselves or a resource (non-person entity). Defence affiliations are validated in the registration process.

If the relevant CP allows it, an authorised resource can submit an application for a Defence certificate.

The PKI PMA determines which types of affiliations with Defence are appropriate for a certificate issued under the relevant CP.

4.1.2 Enrolment process and responsibilities

See relevant CP.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

See relevant CP.

4.2.2 Approval or rejection of certificate applications

See relevant CP.

4.2.3 Time to process certificate applications

Processing for certificate applications will occur in a timely manner.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

The CA shall:

i. authenticate a certificate request, to ensure that it has come from an accredited or approved source[2];
ii. verify the request is correctly formed;
iii. perform any additional process as specified in the PKI Operations manual;
iv. compose and sign the certificate;
v. provide the certificate to the entity; and
vi. publish the certificate in accordance with this CPS and relevant CP.

The certificate issuance process provides an auditable record containing at a minimum:

i. details of the certificate request;
ii. the success, or rejection (with reason), of the certificate request; and
iii. the entity that submitted the certificate request.

The CA is not bound to issue keys and certificates to any entity despite receipt of an application.

4.3.2 Notification to Subscriber by the CA of issuance of certificate

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

[2] For Gatekeeper accredited CAs it must come from a Gatekeeper accredited RA

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

See relevant CP.

4.4.2 Publication of the certificate by the CA

Certificates may be published to *Hyper Text Transfer Protocol* (HTTP) and *Lightweight Directory Access Protocol* (LDAP) repositories. Resource certificates may be published to the relevant entity certificate store as an alternative to publication in a repository. Individual CPs may have additional detail.

4.4.3 Notification of certificate issuance by the CA to other entities

No stipulation.

4.5 Key pair and certificate usage

See relevant CP.

4.6 Certificate renewal

Renewal of a certificate indicates creating a new certificate with an existing key pair, i.e. re-using a previously generated CSR.

4.6.1 Circumstance for certificate renewal

This CPS permits certificate *renewal* only where permitted by the relevant CP. The minimum PKI PMA defined criteria for certificate renewals is:

i. the entity has an approved affiliation with Defence; and
ii. the new validity period will not extend beyond the approved cryptographic life of the private keys.

Renewal of revoked certificates is not permitted regardless of the reason for revocation.

The relevant CP may define additional criteria.

4.6.2 Who may request renewal

If renewal is authorised by the relevant CP, and the parties that may request renewal are not defined in the CP, then renewal requests may be undertaken by the parties identified in 4.1.1 (Who can submit a certificate application).

4.6.3 Processing certificate renewal requests

See relevant CP.

4.6.4 Notification of new certificate issuance to Subscriber

See relevant CP.

4.6.5 Conduct constituting acceptance of a renewal certificate

See relevant CP.

4.6.6 Publication of the renewal certificate by the CA

See relevant CP.

4.6.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

This CPS permits certificate *re-key.* Certificate re-key, rather than renewal is the preferred process to issue a replacement certificate in the Defence PKI. Where allowed by the CP, the circumstances for certificate re-key include:

i. normal certificate expiration;
ii. certificate revocation;
iii. useable life of current key material has been reached; or
iv. change in algorithm, or key length, required.

The PKI PMA may define other circumstances that initiate certificate re-key. When these circumstances are defined they will be published in the relevant CP.

4.7.2 Who may request certification of a new public key

See relevant CP.

4.7.3 Processing certificate re-keying requests

See relevant CP.

4.7.4 Notification of new certificate issuance to Subscriber

See relevant CP.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

See relevant CP.

4.7.6 Publication of the re-keyed certificate by the CA

See relevant CP.

4.7.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

See relevant CP.

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

4.8.2 Who may request certificate modification

See relevant CP.

4.8.3 Processing certificate modification requests

See relevant CP.

4.8.4 Notification of new certificate issuance to Subscriber

See relevant CP.

4.8.5 Conduct constituting acceptance of modified certificate

See 4.4.1 (Conduct constituting certificate acceptance).

4.8.6 Publication of the modified certificate by the CA

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

4.8.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

Unless otherwise stated in the relevant CP, a certificate must be *revoked* if one of the following conditions applies:

i. The Subscriber notifies the CA that the original certificate request was not authorised and does not retrospectively grant authorisation.
ii. The CA obtains evidence that the Subscriber's private key corresponding to the public key in the certificate suffered a key compromise or no longer complies with the requirements outlined in the CP.
iii. The CA obtains credible evidence any certificate it has issued has been misused.
iv. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or other contractual or terms of use agreements that apply.
v. The CA is made aware that the certificate was not issued in accordance with its CP or CPS.
vi. The CA determines that any of the information appearing in the certificate is inaccurate or misleading.
vii. The Subscriber's affiliation has changed so that they are no longer entitled to the certificate.
viii. The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the certificate.
ix. The CA obtains credible evidence of a possible compromise of a Subordinate CA's private key.
x. Upon suspected or known loss or compromise of the media holding the private key.

A revoked certificate must be included on all new publications of the CRL until the certificate expires.

4.9.2 Who can request revocation

Revocation requests may be submitted by any of the following authorised parties:

i. PKI PMA;
ii. Head of *Defence Security and Vetting Service* (DS&VS);
iii. Member of Information and Communications Technology Security Branch (ICTSB)
iv. Subscriber's direct or indirect supervisor (e.g. Chain of command or management);
v. a PKI Operator (for PKI core components), RO or TA; or
vi. the Subscriber.

Relevant CP may have other requirements.

In addition, any person may raise a certificate problem or suspicions of private key compromise by contacting Defence PKI Operations at pki.ops@defence.gov.au.

4.9.3 Procedure for revocation request

The procedure for revoking certificates is set out in the relevant CP. The revocation process that applies will depend on the type of certificate being revoked.

4.9.4 Revocation request grace period

See relevant CP.

4.9.5 Time within which CA must process the revocation request

See relevant CP.

4.9.6 Revocation checking requirement for Relying Parties

It is the Relying Parties responsibility to determine their requirement for revocation checking.

4.9.7 CRL issuance frequency (if applicable)

Refer to the issuing CA's CP for CRL issuance frequency.

4.9.8 Maximum latency for CRLs

All Defence repositories responsible for providing CRLs to Relying Parties shall be updated within the time frame specified in the CP.

The latency time in each CP must account for the time to:

i. generate the CRL;
ii. transfer the CRL from the CA to the master repository;
iii. replicate the master repository to subordinate repositories; and
iv. scheduled periods of system unavailability.

4.9.9 On-line revocation/status checking availability

Online Certificate Status Protocol service (*OCSP*) is available for some certificate types; refer to the relevant CP.

The latest CRL is available from the published repositories; refer to 2.1 (Repositories) and the certificate's CRL Distribution Point in the respective CP for further information.

4.9.10 On-line revocation checking requirements

No stipulation.

4.9.11 Other forms of revocation advertisements available

In the event of the need to revoke a CA certificate, if the CA is involved in any form of external recognition arrangement, Defence will notify the relevant external parties using the "out of band" mechanisms identified in the arrangement.

4.9.12 Special requirements re key compromise

See section 5.7 and the relevant CP.

4.9.13 Circumstances for suspension

See relevant CP.

4.9.14 Who can request suspension

See relevant CP.

4.9.15 Procedure for suspension request

See relevant CP.

4.9.16 Limits on suspension period

See relevant CP.

4.10 Certificate status services

4.10.1 Operational characteristics

The Defence PKI shall store in its internal repository and make available via its internal web site:

i. all CA certificates;
ii. all relevant valid individual (person) and applicable resource (non-person) certificates and cross-certificates where required; and
iii. the most up-to-date CRL(s).

Externally, the Defence PKI will provide relevant PKI information for Relying Parties. The CP will define what information is provided.

Once a certificate has been revoked, the CA will write the certificate serial number to the CRL, which is published periodically to the Defence repository. While the certificate is revoked immediately after the CA processes the revocation request, any end user checking the validity of a certificate will not be able to detect the revocation until the next CRL posting or their application retrieves the new CRL. The details of CRL publishing frequency is documented in the CP of the issuing CA.

Information exchanged between the CA and the Validation Authority shall be authenticated and protected from modification using mechanisms commensurate with the requirements of the data to be protected by the certificates being issued.

Code signing certificates used externally, that have been revoked due to key compromise or have been issued to unauthorised persons must be included in the relevant CRL made available to relying parties for at least 20 years.

4.10.2 Service availability

Defence shall make this service available continuously, except for unavoidable activities. Due to the nature of the Internet and internal Defence communications this service cannot be guaranteed to be always accessible.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

A subscription for a certificate ends:

i. when a certificate is revoked or allowed to expire; or
ii. when all tokens containing the certificates matching private key have been surrendered to an RA and destroyed or zeroised in an approved manner; or
iii. when the PKI is terminated.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

Key escrow and recovery is supported when dual *key pairs* and certificates are issued, one for authentication and one for confidentiality. Key escrow is permitted for end entity confidentiality private keys but not for end entity signature/authentication private keys.

Recovery of end entity confidentiality keys is overseen by personnel in a PKI *Trusted Role*.

Key escrow and recovery is used to support certificate renewal/re-key/modification functions where they are authorised by the CP. In addition, the CA may, as required by law or authorised Defence officials, recover the entities private confidentiality key and decrypt any data encrypted with the corresponding *public key*.

Authorised Key Retrievers (AKRs) are either:

i. the Subscriber;
ii. a Trusted Role who may request key retrieval on behalf of a Subscriber;
iii. the Subscriber's direct or indirect supervisor (e.g. Chain of command or management); or
iv. the Head DS&VS.

Escrow, backup and archive of PKI *core component* keys is permitted to facilitate key recovery in a disaster recovery situation. However, cloning of *hard tokens* is not permitted.

The PKI PMA must approve any process that provides for the escrow, back-up or archiving and subsequent recovery of private keys, see also 6.2.3 (Private key escrow). Documentation of these processes is detailed in internal procedures and summarised in the relevant CP.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

5.1.1 Site location and construction

PKI Facilities are located and constructed in accordance with Defence and Australian Government policy and legislation, for the use of:

i. systems classified up to and including the national security classification of SECRET; and
ii. the transmission, processing and storage of national security classified SECRET information (electronic and hard copy).

Note. This clause specifies the standard required, and not the classification of any systems or information. The PKI *Security Classification Grading Guide* (SCGG) records the security classification of systems and information.

5.1.2 Physical access

Physical access to PKI Facilities is in accordance with Defence[3] and Australian Government policy and legislation, for the use of:

i. systems classified up to and including the national security classification of SECRET; and
ii. the transmission, processing and storage of national security classified SECRET information (electronic and hard copy).

Access to the PKI Facilities is restricted to authorised people and is logged.

All PKI Core components except the Token Management System (TMS) and Web RA Operator (WebRAO) operate in *No-Lone Zone* (NLZ) mode.

5.1.3 Power and air conditioning

Defence provides the PKI facilities for use with all "housekeeping" activities, such as maintaining power and air conditioning, and Defence is responsible for the facilities management. This includes the use of *Uninterruptible Power Supplies* (UPS), and air conditioning to maintain ambient temperatures within equipment operating conditions and temperature threshold controls implemented on all servers.

[3] Such access meets or exceeds physical access requirements for Gatekeeper *High Assurance certificates*.

5.1.4 Water exposures

Protection from exposure to water is in accordance with national and Defence standards.

5.1.5 Fire prevention and protection

Protection and prevention from fire is in accordance with national and Defence standards. This includes the use of fire detection and backup procedures to provide for disaster recovery.

5.1.6 Media storage

All PKI media is stored in accordance with Defence and Australian Government policy for the "Security Classification" of the information stored on the media.

5.1.7 Waste disposal

Disposal of classified waste is in accordance with Defence and Australian Government policy for "Product Sanitisation and Disposal".

5.1.8 Off-site backup

Defence maintains a PKI *Backup Operational Centre* (BOC). Off-site backups are in accordance with the PKI *Disaster Recovery and Business Continuity Plan* (DRBCP) and comply with Defence and National security policy.

5.2 Procedural controls

5.2.1 Trusted roles

This CPS identifies which roles are "*Trusted roles*". Personnel occupying trusted roles will require security clearances in accordance with Defence policy for IT systems personnel with special privileges.

The PKI trusted roles include:

i. the *PKI Operations Manager*;
ii. *PKI Operators*;
iii. *PKI System Administrators (Third Party)*;
iv. *Registration Officer(s)* (RO);
v. *Trusted Agent(s)* (TA);
vi. *Code Signing Key Custodian;* and
vii. *Certificate and Directory Management Centre* (CDMC) *Security Officer* (CSO).

With the exception of ROs, TAs and Code Signing Key Custodians, each of the above positions requires access to the PKI operations facility. Privilege to access this area is controlled by the PKI Operations Manager, based on a number of factors including the risks of human error, theft, fraud, or facilities misuse. The PKI Operations Manager reserves the right to limit, restrict, or extend access privileges to PKI resources. These access privileges include the PKI rooms and facilities, network resources, and infrastructure components.

5.2.2 Number of persons required per task

Access and use of the following items will be subject to "two party" control:

i. PKI Servers;
ii. Workstations with administrative or cryptographic administrative access to PKI servers; and
iii. Storage media (data and configuration backups, and key material).

Backup, restore and key recovery tasks (for PKI component entities) will be subject to "two party" control.

RO and TA operations are not subject to two party control.

Audit logs are maintained and reviewed for unauthorised or inappropriate activity.

The PKI Operations Facilities contain classified work areas. Some of these areas require the enforcement of No-Lone Zones to comply with security policy. Any area containing *Hardware Security Modules* (HSM), servers or other hardware relating to the critical PKI system components are contained in a No-Lone Zone.

5.2.3 Identification and authentication for each role

Irrespective of the role or the tasks performed all access to PKI facilities and systems require identification and authentication of the individual(s) involved in accordance with the *Information and Communications Technology Security Policy* (ICTSP) and *System Security Plan* (SSP). Once authenticated, the appropriate facility or system controls will determine the role, or roles, permitted for the individual(s).

The relevant CP identifies the method of identification and authentication of the end entity.

5.2.4 Roles requiring separation of duties

This CPS prohibits personnel responsible for the auditing of a task to carry responsibility for the performance of that task.

The same person cannot hold the roles of PKI Operations Manager and the SO. The same person cannot hold the PKI Operator role and the SO role.

An RO or TA cannot authorise their own application for a certificate.

The duties of each role are documented in the PKI Operations Manual.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

All personnel in PKI positions of trust require clearances in accordance with Defence security clearance policy and are to be appropriately qualified and experienced for their roles.

Clearance requirements are detailed in the SSP.

5.3.2 Background check procedures

Background checks are part of the Defence security clearance process, which is required for all trusted roles.

5.3.3 Training requirements

All PKI personnel will be suitably trained in relevant policy, procedure and technology. The PKI Operations Manager will maintain competence in all operations areas.

Specific training for the SO will focus on security management, system auditing and system specific security applications employed in the PKI (surveillance, access systems, etc.).

PKI Operators must develop and maintain an awareness of security policies. Specific training requirements are detailed in the PKI SSP. In general, PKI personnel must complete training in:

i. basic PKI concepts;
ii. use and operation of PKI software, hardware and associated applications;
iii. computer security awareness and procedures;
iv. privacy procedures and considerations;
v. disaster recovery and business continuity procedures;
vi. risk management procedures; and
vii. the PKI operational policies, plans and procedures.

RO and TA training will focus on affiliation and *Evidence of Identity* (EOI) validation, registration software operation and procedures.

Training will occur:

i. when personnel commence their employment;
ii. whenever new policies and/or procedures are implemented; and
iii. whenever remedial or other training is deemed necessary by the SO and/or the PKI Operations Manager.

PKI staff are encouraged to undertake training activities that will assist them to carry out their duties and improve the security and integrity of PKI operations. The PKI Operations Manager may allocate and assign staff members to any suitable training activity, such as:

i. training on the use and features of new/latest release of PKI application software, and the associated database software;
ii. training on new/latest release security tools (such as firewalls, routers, application platform security, intrusion detection systems, foot print analysis tools, backup utilities etc.);
iii. training on PKI internal processes and procedures; and
iv. training on internet security, PKI, and similar topics conducted by Gatekeeper Evaluators, the ASD, the *Digital Transformation Agency* (DTA), the *Australian Government Solicitor* (AGS), authorised legal evaluator or private enterprises with relevant expertise.

Note that the training topics should be related to the PKI business plans and activities.

5.3.4 Retraining frequency and requirements

All PKI personnel require retraining as required to maintain currency with policy, procedure and technology. Training on the security policy and procedures occurs annually for all trusted roles. Refer to SSP for more information.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorised actions

Unauthorised actions are identified in the Approved Documents.

The PKI Manager's response to unauthorised actions is to take into account whether the misuse was an accident, omission, or malicious act.

Where a staff member has been found to have seriously misused the resources to which they have been granted access, these actions are to be documented and passed to senior Defence personnel, who may wish to take administrative or disciplinary action, if appropriate.

Sanctions against contract employees are to be in accordance with the terms and conditions of their contract.

Depending on the nature of the actions, sanctions will comply with Defence policy for administrative or disciplinary action and may range from counselling and/or suspension of access rights, through to dismissal and/or legal action.

5.3.7 Independent contractor requirements

All contractors with physical or logical administrative access to the PKI facilities must either have appropriate clauses in their contract or sign a Confidentiality/Non-disclosure Agreement before they are allowed access to PKI systems. Casual PKI staff and third party access that are not already covered by an existing contract (containing the Confidentiality Agreement) may be required to sign a Confidentiality Agreement before being granted limited access to information processing facilities.

5.3.8 Documentation supplied to personnel

For each role, the personnel performing duties, procedures and responsibilities receive access to the necessary documentation for that role. All documentation will be available within the PKI facilities for access by operational staff.

ROs and TAs will only be supplied with relevant documentation for the registration of Subscribers.

Access to data and reports will be subject to normal security classification controls.

5.4 Audit logging procedures

5.4.1 Types of events recorded

Records of RA and CA infrastructure events include:

i. all successful and rejected network connection requests;
ii. all logins and certificate requests received; and
iii. administering and configuring.

The recorded information shall include:

i. date/time stamp;
ii. event target;
iii. event source;
iv. event description; and
v. CA/RA event status (Success/Failure).

5.4.2 Frequency of processing log

Audit logs require processing at least monthly for anomalous and unauthorised events. Processing is to include searches for anomalous patterns across more than one month. Additional processing will be performed as required if an incident occurs warranting an investigation of events leading up to incident.

5.4.3 Retention period for audit log

Backups of audit logs are retained for 12 months. Archives of audit logs are retained in accordance with *National Archive of Australia* (NAA) legislation and policy including the *Archives Act 1983 (Cth).*

Audit retention/ backup and archival policies are to ensure that together a complete record of all audit material is maintained, and recoverable for the period specified within Defence and National Archive policy.

5.4.4 Protection of audit log

Protection of Audit log information is in accordance with Defence policy for the protection of security log information for systems processing up to and including SECRET information.

5.4.5 Audit log backup procedures

Backups of audit logs occur daily. Where log information processing into a common format for analysis occurs, both raw and processed log data require backing up. Backup policy includes off-site storage as per Defence policy for systems processing data up to and including SECRET information.

5.4.6 Audit collection system (internal vs. external)

The audit collection system is compliant with Defence policy for systems processing up to and including SECRET information.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

Vulnerability assessments are in accordance with Defence policy for systems processing up to and including SECRET information. These assessments include off-site and archival data/systems.

5.5 Records archival

5.5.1 Types of records archived

All audit log records for CA and RA infrastructure require archival. To minimise the duplication of records duplicated archives are destroyed, whilst maintaining a full record of all auditable events.

Archiving of key material is required for specific components to support the archiving requirements for the PKI. That is, in order to access information from archived PKI databases, a set of specific key material is required to be archived and stored securely along with the archived PKI databases.

The specific components of key material generated for archive includes:

i. archive CA Operator (CAO) token when a CA database is archived;
ii. archive RA Auditor (RAA) token when a RA database is archived;
iii. archive Key Archive Server (KAS), including the KAS' Long Term Storage Key (LTSK) and Key Archive Operator (KAO) token, when a KAS database is archived;
iv. archive Timestamp Server (*TSS) Administrator* token when a TSS database is archived; and
v. archive *TMS Auditor* token when a TMS database is archived.

5.5.2 Retention period for archive

Retention period for archive records is in accordance with Defence and National Archive policy. This retention period is also required for systems and applications necessary to process the archived records.

5.5.3 Protection of archive

Archives protection occurs in accordance with Defence policy for the protection of systems processing up to and including SECRET information.

During copying or generation of the archive key material, the resultant media is placed into tamper evident envelopes, and an entry is to be made in the Trusted Element Register.

Archive key material is to be transported in accordance with Defence SECRET COMSEC transport procedures to a secure facility, with the receipt being included in the CDMC *Classified Document Register* (CDR). NB: the corresponding passphrase for the archived key material is to be stored and transported separately to that of the private key.

5.5.4 Archive backup procedures

Archive data backup is in accordance with Defence and National Archive policy.

5.5.5 Requirements for time-stamping of records

Individual events shall be time stamped with the timing of the event. Audit logs shall also be time stamped with the time of archival, and if via a backup process a timestamp of the relevant backup.

5.5.6 Archive collection system (internal or external)

No stipulation.

5.5.7 Procedures to obtain and verify archive information

To provide authentication and integrity confirmation of the archive records digital signatures are applied.

5.6 Key changeover

The Defence PKI ensures that the key changeover process and procedures will provide for uninterrupted operation of the CA, and will also ensure that subordinate certificates do not become invalid as a result of CA key changeover.

Key changeover periods will be in accordance with Defence policy, and prior to normal certificate/key expiry.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

All security incidents (as per the SSP) are to be logged, and an investigation of the incident is to be undertaken, to determine if:

i. key compromise has occurred, is suspected, or cannot be discounted;
ii. the incident was deliberate or accidental;
iii. procedures should be modified to address the circumstances that enabled the incident to occur; and
iv. any further action is required.

If it is possible that a key compromise has occurred, the certificate requires revocation. All cross-certified CAs are to be informed if an applicable CA is compromised.

The decision to revoke the certificates subordinate to the compromised entity is optional however; the PKI Operations Manual describes the necessary processes. Where a *superior CA* is compromised, ALL immediately *subordinate CAs* are effectively revoked.

The PKI PMA receives notification of all incidents where the continued integrity of service is impacted, and will provide a formal notice to cross-certified entities, and accrediting bodies, indicating the proposed corrective action and the estimated schedule for implementation.

5.7.2 Computing resources, software, and/or data are corrupted

The DRBCP details the restoration strategy. The backup of *private signing keys* for CAs occurs only if appropriate protection applies, and is only used as part of a rebuild if compromise has not occurred or is not suspected.

5.7.3 Entity private key compromise procedures

If the entity private key is compromised it is revoked and the entity must re-apply for registration.

5.7.4 Business continuity capabilities after a disaster

Priorities for Business Continuity are in the following order:

i. physical investigation of disaster and collection of necessary evidence to complete investigation – sign off as required by PKI PMA;
ii. re-establishment of secure environment for PKI operations – temporary measures are acceptable but require detailing in the DRBCP or sign off by the PKI PMA.
iii. reconstitute the ability to issue CRLs and process revocation requests – this includes audit functionality;
iv. reconstitute the ability to receive, process and issue certificates;
v. return to stable operating conditions;
vi. update documentation to reflect any changes as a result of recovery – including to processes, procedures and configuration; and
vii. provide an incident closure report to the PKI PMA.

5.8 CA or RA termination

In the event of a CA or RA termination, or a CA or RA ceasing operation, its certificate requires revocation. Self-signed CAs shall follow notification procedures equivalent to key compromise. Termination of CAs, where possible, should minimise impact on subordinate certificates.

The PKI PMA receives notification of planned and actual terminations.

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

Key pair generation is to be via a combination of product and process approved by the *National Cryptographic Authority* (*NCA*) to provide keys suitable:

i. for use in PKI based authentication, non-repudiation and integrity services for systems and data classified up to and including the SECRET classification; and
ii. for use in PKI based confidential communications capable of protecting symmetric (Private Key encryption) keys used to protect data up to and including the PROTECTED classification over publicly accessible data networks (e.g. the Internet).

See relevant CP for description on key pair generation.

The PKI KMP details the products, process and procedures and the approved combinations, which are valid.

6.1.2 Private key delivery to Subscriber

Private key delivery is defined in the relevant CP.

6.1.3 Public key delivery to certificate issuer

Public key delivery is defined in the relevant CP.

6.1.4 CA public key delivery to relying parties

Public keys for a CA in a certificate chain for entity certificates will be accessible to Relying Parties using the approved repositories.

In addition CA certificates in the chain which are self-signed (the "Root" CA) will be delivered, using secure methods approved by the PKI PMA to third party CAs, where a cross certification (or equivalent) agreement is in place.

Internal Defence infrastructure will have relevant certificate chains installed into the Certificate store on workstations and servers.

6.1.5 Key sizes

Key sizes are defined in the KMP and relevant CP.

6.1.6 Public key parameters generation and quality checking

Public key parameters shall always be generated and checked in accordance with the standard that defines the cryptographic algorithm in which the parameters are to be used.

Parameter quality checking (including primarily testing for prime numbers) shall be performed in accordance with the approved certification programs and their guidelines.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

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. The correct values for key usage are set in these fields in accordance with the X.509v3 standard but Defence cannot control how third-party software applications interpret or act upon these. 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.

See the relevant CP for key usages.

6.2 Private key protection and cryptographic module engineering controls

6.2.1 Cryptographic module standards and controls

Core component cryptographic modules require evaluation under NCA agreed standards and/or certification programs and approval for the uses intended in the CP from the PKI PMA.

All cryptographic modules, including those used by subscribers, are Defence approved prior to use (i.e. on the Defence Approved Software/Hardware List etc.).

The PKI Build and Configuration documentation details the products used for core components.

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

Private Key (n out of m) multi-person control does not occur. However, the key generation of PKI entities (CA and RA components) is conducted in a No-lone Zone.

6.2.3 Private key escrow

Escrow of end entity private authentication keys does not occur.

The relevant CP details whether private confidentiality keys are subject to escrow.

A copy of every private confidentiality key that is stored in escrow is kept in the KAS, encrypted under a KAS *Long Term Storage Key* (LTSK). The KAS is located within the PKI facilities (No-Lone Zone) and access is restricted to PKI *trusted roles*.

6.2.4 Private key backup

Back up of end entity private authentication keys does not occur, however, where the private confidentiality key is escrowed, it is backed up as part of the KAS backup process. Where such keys must be transferred to other media for backup and disaster recovery purposes, they are transferred and stored in an encrypted form protected by the HSM keys.

Critical PKI components, such as CAs and RAs, have duplicate private keys created and archived. Where these keys are stored on hard tokens, the archive copy is also a hard token.

Duplicated hardware security tokens are recorded within tamper evident envelopes and signed by the SO.

6.2.5 Private key archival

Archive of end entity private authentication keys does not occur, however, where the private confidentiality key is escrowed it is archived as part of the KAS archive process, section 5.5 (Records archival) defines the controls surrounding the archive of private keys.

Archive of PKI core component keys is permitted.

6.2.6 Private key transfer into or from a cryptographic module

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

6.2.7 Private key storage on cryptographic module

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

6.2.8 Method of activating private key

See relevant CP.

6.2.9 Method of deactivating private key

Cryptographic modules that have been activated shall be protected against unauthorized access. After use, the cryptographic module shall be deactivated (e.g. via a manual logout procedure or automatically after a period of inactivity by a passive timeout). Hardware cryptographic modules shall be removed and stored in accordance with Section 5.1.2 when not in use.

Private keys stored in HSMs are deactivated when the HSM is powered down. Operator hard tokens are removed from the token reader (deactivating access) and stored in accordance with the PKI ICTSP, PKI SSP and PKI KMP.

6.2.10 Method of destroying private key

PKI Trusted Roles can destroy private keys in accordance with COMSEC requirements. HSMs and hard tokens will be re-initialised to destroy the stored private keys. Destroying CA keys requires a witnessed and documented process.

Subscribers may destroy their own authentication private keys when no longer needed either by securely erasing/destroying the token, or by having their hard token re-initialised.

6.2.11 Cryptographic module rating

See 6.2.1 (Cryptographic module standards and controls) of this CPS.

6.3 Other aspects of key pair management

6.3.1 Public key archival

The CA archives all certificates it generates. CA archival is part of the archival process which requires the storage of software and hardware to allow the reconstitution of the CA if required.

The public keys of certificates are archived in accordance with 5.5 (Records archival).

6.3.2 Certificate operational periods and key pair usage periods

Within the PKI, certificate lifetimes are nested and as such the key lifetime is dependent on the certificate life. In other words, an issued certificate (of an end entity or a CA) expires before the certificate of the CA that issued it. Otherwise, after the CAs expiration, the issued certificate becomes invalid, even if it has not expired[4].

Key lifetimes are set as a matter of policy and will depend on a number of factors, not the least of which includes the size of the key. As such the key lifetimes within the PKI are detailed in the PKI KMP and the applicable CP.

[4] If there is an alternative certificate validation path because of cross-certification, the certificate may still validate.

6.4 Activation data

6.4.1 Activation data generation and installation

See relevant CP.

6.4.2 Activation data protection

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

6.4.3 Other aspects of activation data

See relevant CP.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

The Defence PKI has established an ICTSP and SSP for computer security technical requirements for PKI operations. These documents carry a National Security classification and are only available to appropriately cleared personnel on a need- to- know basis.

Appropriate levels of trustworthiness and security exist throughout the PKI. Security meets Defence requirements for systems cleared to store and process data that is classified up to and including SECRET, which meets or exceeds the requirements mandated under Gatekeeper for a *High Assurance* service.

Controls in place include:

i. a configuration baseline and a configuration change control process;
ii. performance of regular and frequent systems operability tests to prove the correct operation of critical PKI components;
iii. strong authentication required for core PKI system access;
iv. proactive user account management including comprehensive auditing and timely removal of access;
v. role segregation and No-Lone Zone procedures;
vi. restrictions and controls on the use of system utilities;
vii. secure deletion of cryptographic material in accordance with COMSEC requirements;
viii. the use of monitoring and alarm systems to detect and warn of unauthorised access to computer system resources; and
ix. logging of all system access and use.

6.5.2 Computer security rating

All facilities and equipment have been constructed or selected to satisfy the requirements for a system handling or processing information classified up to and including SECRET. Typically, products in use within the Defence PKI have undergone a security evaluation though an ASD recognised evaluation program.

6.6 Life cycle technical controls

6.6.1 System development controls

The software development controls applied in the development of the CA and RA software have undergone a security evaluation though a Defence recognised evaluation program.

Changes in the production environment are tested in the PKI test environment, which is operated and maintained within a physically secure environment. Proposed changes are then approved for deployment by the PKI PMA.

6.6.2 Security management controls

Security management controls exist to ensure that PKI systems are operating correctly and in a manner consistent with the PKI configuration baseline. The configuration baseline document includes a schedule of configured items, including details of the hardware and software configuration parameters and a mechanism for identifying appropriate documentation and known security flaws for each item.

The PKI Operations Manager is responsible for maintaining the configuration baseline and for managing any changes in accordance with the SSP. The PKI Security Officer is responsible for maintaining a change control process at the PKI that records all changes to the PKI configuration, including all hardware and software changes.

Security management controls are described in further detail in the PKI SSP.

6.6.3 Life cycle security controls

No specific life cycle security ratings were sought in the development of the CA and RA software.

6.7 Network security controls

The Defence PKI network security controls include:

i. firewalls;
ii. strong authentication;
iii. physical access controls;
iv. mechanisms to prevent denial-of-service attacks; and
v. passwords and other logical access controls.

The network security controls were developed after conducting a comprehensive threat and risk assessment.

PKI network services are operated and maintained within the physically secure environment of the PKI.

In addition to meeting Gatekeeper requirements, the PKI network conforms to the Information Systems Security measures outlined in the ISM for the protection of systems cleared to process data that is classified up to and including SECRET.

The PKI network is a discrete network, strictly controlled by CDMC. The only network traffic allowed is from authorised PKI entities and essential core services such as directories, validation, time, monitoring and synchronisation with any back-up or alternate sites. All other traffic is denied by default. Direct access to networks external to Defence (e.g. Internet) is not available from the PKI network.

6.8 Time-stamping

Asserted times in certificates shall be accurate to within +/- 5 seconds of UTC.

All hosts and workstations within the facility are to be synchronised with a reliable time source, disseminating UTC. Local network time is to be accurate within +/-5 seconds of UTC.

7. CERTIFICATE, CRL, AND OCSP PROFILES

Appendix C contains a list of OIDs for Public CPs approved to operate under this CPS[5]. The relevant CP details the specific Certificate, CRL and OCSP profiles. Accreditation processes ensure that this CPS is suitable for a CP, prior to the CP being approved for use by the PKI PMA.

[5] This CPS also covers various internal CPs, not published externally.

7.1 Certificate profile

7.1.1 Version number(s)

CAs operating under this CPS shall only issue X.509 Version 3 certificates.

7.1.2 Certificate extensions

See relevant CP.

7.1.3 Algorithm object identifiers

See relevant CP.

7.1.4 Name forms

Distinguished Names (DN) will be used by the CAs in the issuer and in subject fields of the certificates. The DN shall not be blank. Names must be meaningfully related to the identity presented for EOI check and relate directly to the identity of the subscriber or resource, except as otherwise provided in the relevant CP. Some communities or installations may choose to use other names, for example, certificates used to implement a hardware protocol, where device addresses are more useful. In this case, an alternate name form may be included in the subjectAltName extension. Use of alternate name forms shall be in accordance with the CP, including criticality, types, and name constraints. The combination of DN and subjectAltName must be unique within the PKI.

See relevant CP for name forms.

7.1.5 Name constraints

See relevant CP.

7.1.6 Certificate policy object identifier

See relevant CP.

7.1.7 Usage of policy constraints extension

See relevant CP.

7.1.8 Policy qualifiers syntax and semantics

See relevant CP.

7.1.9 Processing semantics for the critical certificate policies extension

See relevant CP.

7.2 CRL profile

7.2.1 Version number(s)

CRLs for certificates issued under this CPS shall assert Version 2 as described in the X.509 standard [ISO9594-8].

7.2.2 CRL and CRL entry extensions

See relevant CP.

7.3 OCSP profile

7.3.1 Version number(s)

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

7.3.2 OCSP extensions

All OCSP extensions are to comply with RFC 6960.

OCSP certificates are issued with the no-check extension (id-pkix-ocsp-nocheck), negating the need of the relying party to validate the OCSP responder's certificate through another source such as the CRL. This extension will not be marked critical.

Refer to the X.509 Certificate Policy for the Australian Department of Defence Validation Authority Certificates [VA CP] for a full OCSP profile.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

All infrastructure elements in the Defence PKI, including the off-line Root CAs, require auditing on a regular basis to ensure that they comply with this CPS and the relevant CP. The process of such audits is not publicly disclosed.

In addition to the CPS requirements, Gatekeeper accreditation for the Public PKI requires the conduct of annual audits to ensure compliance with the Gatekeeper policies and criteria (refer to https://www.dta.gov.au for Gatekeeper Compliance Audit directions). Where possible, other external accreditations or cross certification requirements are aligned with the Gatekeeper annual audits.

The PKI PMA gives further consideration to the results of such audits before possibly implementing any recommendations[6].

8.1 Frequency or circumstances of assessment

Each CA and RA requires an annual audit, more frequently if required, by an auditor appointed by the PKI PMA to assure that they comply with this CPS and relevant CPs.

In accordance with Gatekeeper requirements, the Defence Public PKI must undergo an annual compliance audit.

8.2 Identity/qualifications of assessor

Auditors receive approval by the PKI PMA (and where applicable, the Gatekeeper Competent Authority) based on expertise in relation to electronic signature technology, IT security procedures or any other relevant areas of expertise required of an evaluator to perform an evaluation properly and expertly against the Accreditation Criteria.

8.3 Assessor's relationship to assessed entity

Auditors must be independent of the audited entity and have no actual, or potential, conflict of interest during the period of the audit.

8.4 Topics covered by assessment

The purpose of audits is to ensure that each CA and RA:

i. maintains compliance with Accreditation criteria and policies; and
ii. continues to operate in accordance with the Approved Documents.

Topics covered by the assessment are based on the Gatekeeper PKI Framework, and where applicable other external accreditation or cross certification requirements, which identifies a series of compliance

[6] Note: The Gatekeeper CA is subject to direction by the Gatekeeper Competent Authority in relation to maintaining accreditation.

audit activities that must be performed to ensure the operational integrity and suitability of the infrastructure.

8.5 Actions taken as a result of deficiency

Auditor identified deficiencies will be presented to the PKI PMA[7]. The PKI PMA will determine actions to be taken in relation to any deficiency. Where this deficiency affects accredited systems authorised representatives of Accreditation Agencies will be included in the review and determination of the solution.

Any deficiency that impacts upon continued accreditation is to be remedied to the standard required by the Accreditation Agency(s).

Failure to adequately address deficiencies identified in an audit in an agreed timeframe may result in withdrawal of the entity's accreditation and/or termination of the Gatekeeper Memorandum of Agreement.

The PKI Operations Manager is responsible for the on-going management of the PKI accreditation.

8.6 Communication of results

The results of an audit are confidential and require the auditor to communicate them only to authorised representatives of Accrediting bodies and the audited entity. Results of the compliance audit against Gatekeeper, or other external accreditation or cross certification, may be released at the discretion of the PKI PMA.

All required corrective action must be verified to have been completed within the agreed timeframe.

The PKI Operations Manager has the responsibility for correspondence of results of PKI audits between the PKI and other entities, for example DSA, ASD, and DTA.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

See relevant CP.

9.1.2 Certificate access fees

See relevant CP.

9.1.3 Revocation or status information access fees

See relevant CP.

9.1.4 Fees for other services

No fee is levied for access to this CPS, or relevant CP via the approved repositories. Printed copies may be made available for a fee.

See relevant CP for any other service fees.

[7] In relation to Gatekeeper accreditation audits the report will also be submitted to the Gatekeeper Competent Authority at the same time as submission to the PKIPB.

9.1.5 Refund policy

Where a fee is charged for a certificate, once that certificate is issued a refund will not be provided. The relevant CA will issue a new certificate free of charge if, through the fault of the CA, an erroneous certificate was issued.

9.2 Financial responsibility

Defence has sufficient resources to meet its perceived obligations under this CPS. Defence makes this service available on an 'as available' basis.

Nothing in this CPS, or relevant CP, or the issuing of Key Pairs and Certificates under it, establishes a fiduciary relationship between the Defence PKI and an end entity, or Relying Party.

The Defence PKI is not liable for any loss or damage arising from any delay or failure to perform its obligations described in this CPS. Relying Parties assume responsibility for any financial losses due to transactions authenticated using certificates issued under this CPS.

9.2.1 Insurance coverage

See relevant CP.

9.2.2 Other assets

See relevant CP.

9.2.3 Insurance or warranty coverage for end-entities

See relevant CP.

9.3 Confidentiality of business information

Information requires classification and handling, storing and processing in accordance with Defence Security policy. Public Access is only to information classified as "OFFICIAL". Release of all other information will be subject to satisfying security clearance requirements and a demonstrated "need-to-know".

PKI related document classifications are recorded in the PKI Security Classification Grading Document.

9.3.1 Scope of confidential information

No stipulation.

9.3.2 Information not within the scope of confidential information

No stipulation.

9.3.3 Responsibility to protect confidential information

Whilst the keys provided are suitable for use in PKI confidential communications capable of protecting symmetric (PKI Key encryption) keys used to protect data up to and including PROTECTED information over publicly accessible data networks (e.g. the Internet), the sending party in any communication is responsible for complying with the Defence Security policy.

Where in connection with the use of the Defence PKI, *confidential information* is provided or produced, the relevant party shall ensure that any person receiving or producing the information protects the confidential nature of the information, except:

i. where disclosure of the information is required by law or statutory or portfolio duties;
ii. where disclosure of the information is made to the responsible Minister or in response to a request by a House or Committee of the Parliament of the Commonwealth of Australia; or

iii. to the extent that Defence would be prevented from exercising its Intellectual Property rights under a Contract.

The Subscriber shall not, in marking information supplied to Defence, misuse the term confidential or the end entities equivalent. The marking of information as confidential shall not affect the legal nature and character of the information.

9.4 Privacy of personal information

9.4.1 Privacy plan

The Defence PKI Privacy Notice conforms to the requirements of the *Privacy Act 1988 (Cth)* (Privacy Act) and *Information Privacy Act 2014 (Cth).* The Privacy Notice is available internally from Defence repositories and externally at:
https://defence.gov.au/pki/_lib/doc_pdf/DefencePKIPrivacyStatement.pdf

9.4.2 Information treated as private

See relevant CP.

9.4.3 Information not deemed private

Subscribers (Identity Certificates) using the Defence PKI will be required to acknowledge that Personal Information (as defined in the Privacy Act*)* published in the certificate, primarily the name and email address of the applicant, may be collected, used or disclosed as necessary for the efficient functioning of the PKI system.

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

The relevant CP will detail any other information that may be treated in this manner in respect of that CP.

9.4.4 Responsibility to protect private information

Information collected as part of the entities' interaction with the PKI operation that is Personal Information, other than that which forms part of the *Certificate Information,* will be protected in accordance with the requirements of the Privacy Act.

Information held in the PKI can only be used by other areas within Defence where the individual, the subject of the Personal Information, has consented or where one of the exceptions in the Privacy Act, including those in Australian Privacy Principle 6 (APP 6) apply.

Given there may be a requirement to access Personal Information as part of the verification procedure, management of the access, storage, use and disclosure of information in the PKI will be in accordance with the *Australian Privacy Principles* (APPs). Access to this information is restricted to PKI *trusted roles*.

In keeping with the requirements of the Privacy Act, the PKI implements physical and logical access control mechanisms to protect the sensitive information from unauthorised access.

The Defence PKI encrypts communications of confidential information including the communications links between the CAs and the point of registration.

9.4.5 Notice and consent to use private information

Subscribers are to be informed of any Personal Information collected and its use and/or distribution. Refer to relevant CP for notice and consent arrangements.

9.4.6 Disclosure pursuant to judicial or administrative process

No Personal Information contained in the PKI, other than that which forms part of the Certificate Information, that relates to an identifiable Defence entity is disclosed to any external entities to Defence unless the disclosure is in accordance with the Privacy Act (including APP 6).

Defence personnel are entitled to access Personal Information about themselves in the PKI in accordance with APP 12 of the Privacy Act. This information can be obtained by sending a signed and dated minute to the PKI Operations Centre, requesting the relevant data. The minute should include the person's full name, organisation unit and contact details and PKI staff will action the request.

Only authorised PKI staff, under two party control, are permitted to access data about individual personnel. Access by these authorised persons will be in accordance with the appropriate APPs of the Privacy Act. The Privacy Commissioner has the right under the Privacy Act to conduct audits to ascertain whether Personal Information records are being maintained in accordance with the APPs.

Any Defence person is able to request changes to their own information in the PKI. Changes will, however, be subject to verification of the identity of the person requesting the change, preventing unauthorised persons from accessing or altering information.

Where changes to Personal Information (e-mail address and name) affect the contents of digital certificates, revocation and reissue of the affected certificates is required.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual property rights

Unless otherwise agreed between the relevant parties:

i. *Intellectual Property Rights* (IPR) in the Approved Documents, the Certificate Directory and the CRL are owned by Defence;
ii. IPR in Certificates are owned by Defence, subject to any pre-existing IPR which may exist in the Certificates or the Certificate Information;
iii. the entity generating the key pairs own any IPR in the key pairs; and
iv. the Distinguished Names of all CAs of the Defence PKI remain the sole property of Defence.

The IPR owners of Certificates, *Distinguished Names* and key pairs (IP Owner) grants to any other relevant entity, which has a requirement under this CPS, the CP or the other Approved Documents to use that intellectual property, the rights it reasonably requires to perform that entity's roles, functions and obligations under this CPS, the CP or the Approved Documents.

Where an entity is required under this CPS, the CP or another Approved Document to use any software or other item owned by, or licensed to, a PKI Service Provider, that PKI Service Provider grants to the relevant entity any rights it reasonably requires to use that software or other item for the purposes of discharging that requirement.

The IPR owner warrants that:

i. it has all the rights necessary to grant the licences described in this 9.5; and
ii. use by relevant entities of the relevant IPR pursuant to this CPS, the CP or other Approved Documents will not infringe the IPR of a third party.

The Subscriber Agreement and any other relevant documents must include intellectual property rights arrangements that are consistent with this section.

9.6 Representations and warranties

Defence uses this CPS, associated CPs and Subscriber Agreements to convey conditions of usage of Defence certificates to Subscribers and Relying Parties.

Participants that may make representations and warranties include Defence CAs, RAs, Subscribers, Relying Parties, and any other participants as it may become necessary.

All parties in the Defence PKI domain, including Defence CAs and RAs and Subscribers warrant the integrity of their respective private key(s). If any such party suspects that a private key has been compromised they will promptly notify the appropriate RA or the CDMC.

9.6.1 CA representations and warranties

The CA warrants:

i. the certificate information provided to it has been accurately transcribed into the certificate;
ii. all other certificate information it generates itself is accurate;
iii. the digital certificate operates with functional key pairs; and
iv. that at the time it issues a certificate, the certificate contains all the elements required by the Certificate Profile as detailed in the relevant CP.

9.6.2 RA representations and warranties

The RA warrants the information in the certificate is true to the best of the RAs knowledge after performing identity authentication (registration) procedures with due diligence.

9.6.3 Subscriber representations and warranties

See relevant CP.

9.6.4 Relying party representations and warranties

Relying Parties warrant that they will:

i. verify the validity of a digital certificate i.e. verify that the digital certificate is current and has not been revoked or suspended, in the manner specified in the CP under which the digital certificate was issued;
ii. verify that the digital certificate is being used within the limits specified in the CP under which the digital certificate was issued; and
iii. promptly notify the Defence PKI in the event that they suspect that there has been a compromise of the Subscriber's Private Keys.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

EXCEPT FOR ANY WARRANTIES EXPRESSLY GIVEN IN ACCORDANCE WITH THIS CPS OR IN A CP. NO IMPLIED OR EXPRESS WARRANTIES ARE GIVEN BY DEFENCE OR BY ANY OTHER ENTITY WHO MAY BE INVOLVED IN THE ISSUING OR MANAGING OF KEY PAIRS AND/OR CERTIFICATES ISSUED UNDER THIS CPS AND ALL STATUTORY WARRANTIES ARE TO THE FULLEST EXTENT PERMITTED BY LAW EXPRESSLY EXCLUDED.

The Defence PKI uses software and procedures for the authentication of entities that, to the best of its knowledge, perform as required by this CPS and relevant CP. However, it gives no warranty as to their full correctness. Also, the Defence PKI cannot be held responsible for any misuse of its certificate by a Subscriber or any other party in possession of the corresponding private key, and of any unchecked acceptance of any of its certificates by a Relying Party.

Any Relying Party that accepts a certificate for any usage for which it was not issued does so at its own risk and responsibility.

The Subscriber Agreement must include a disclaimer that is consistent with the above disclaimer.

9.8 Limitations of liability

To the extent permitted by law Defence is not liable for:

i. any use of certificates, other than uses specified in this CPS or the relevant CP;
ii. falsification of transactions;
iii. improper use or configuration of equipment, not operated under the responsibility of the PKI, used in transactions involving certificates;
iv. compromise of private keys associated with the certificates;
v. loss, exposure or misuse of PIN code(s) etc., protecting private keys associated with the certificates;
vi. erroneous or incomplete requests for operations on certificates;
vii. delays arising from Force Majeure;
viii. the use of public or private keys of cross–certified (non-subordinate) CAs and their Relying Parties; and
ix. any termination of the PKI or any related contract by Defence.

In the absence of any documented contractual relationship between the CA and a Subscriber (other than a Subscriber Agreement) and/or Relying Party, Defence does not accept any liability regarding the operations of the Defence PKI associated with certificates issued under this CPS.

Relevant contractual documents define any limitations to the extent of the liability of parties with regards to certificate use.

9.8.1 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

By using or accepting a certificate, each Subscriber and Relying Party agrees to indemnify and hold Defence, as well as any of its officers, employees, agents, and contractors harmless from any acts or omissions resulting in liability, any loss or damage, and any costs or expenses of any kind, including legal fees (on a solicitor or own basis), that Defence, as well as any of its officers, employees, agents, and contractors may incur, that are caused by the use or publication of a certificate, and that arises from that party's:

i. misrepresentation or omission of material fact in order to obtain or use a Certificate, whether or not such misrepresentation or omission was intentional;
ii. violation of the Subscriber Agreement, Relying Party Agreement, this CPS, the relevant CP, or any applicable law;
iii. compromise or unauthorised use of a Certificate or Private Key caused by the negligence of that party and not by Defence (unless prior to such unauthorised use Defence has received an authenticated request to revoke the Certificate);
iv. use or reliance on a Certificate or Private Key; or
v. misuse of a Certificate or Private Key.

The Subscriber and its affiliated entities and individuals recognise that Defence relies solely on the representations, warranties, undertakings and the information contained in the application (along with such other certificates, statements or documents as may be required or demanded by Defence), to make a determination on recommending/not recommending the issuance of a digital certificate to the Subscriber and its affiliated entities and individuals and any misrepresentation thereof shall make the Subscriber and its affiliated entities and individuals liable, inter alia, for exemplary damages.

The indemnities contained herein shall be in addition to any other indemnities available generally in law or under the CPS or Subscriber Agreement and shall survive the termination of relationship between the Subscriber and Defence, including as a result of suspension/revocation of the certificate.

9.10 Term and termination

9.10.1 Term

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

The CPS is available at https://crl.defence.gov.au/pki.

9.10.2 Termination

The entire PKI may be terminated at any time by Defence. All existing certificates, expired or unexpired, revoked, or active, will be deemed unfit for further use. Defence is not required to revoke existing certificates in this event. All CRLs may only be used for historic or evidentiary purposes upon CA termination.

Defence is not required to give any notice to end entities before or after CA termination, however, before the Defence PKI terminates its services, it will attempt to:

i. inform entities and subordinate RAs;
ii. make widely available information of its termination; and
iii. stop issuing certificates and CRLs.

In accordance with the Gatekeeper Memorandum of Agreement, Defence will inform the Gatekeeper Competent Authority of its intention to terminate the CA and/or RA.

9.10.3 Effect of termination and survival

Unless the contrary intention appears, the expiry or termination of a contractual relationship between PKI entities which imports the terms of this CPS or a relevant CP, will not affect the continued application to those entities of any provision in this CPS or a relevant CP relating to:

i. Intellectual Property Rights;
ii. Confidential Information;
iii. the protection of Personal Information; or
iv. an indemnity,

or any other provision which is expressly stated to or by implication from its nature or its context is intended to continue after termination of the relevant contractual relationship.

9.11 Individual notices and communications with participants

A notice or other communication (Notice) from one entity to another in relation to this CPS or a relevant CP requires signing by the sending entity. If the Notice delivery is electronic, it requires the sender's digital signature.

Notices to Organisations requires delivery to the physical, postal, facsimile or e-mail address of the Organisation, which is included in its Registration Information, or to another address, which the Organisation has specified to the sender.

Notices to Subscribers will be posted to the Defence PKI web page and where appropriate will be sent to the address within the certificate.

Unless otherwise specified in this CPS or a relevant CP, a Notice sent as required under this section is satisfied if:

i. it is hand-delivered to a physical address - at the time of delivery whether or not any person is there to receive it;
ii. it is posted by prepaid post - at 5pm on the third day after it is posted even if the Notice is returned to the sender;
iii. it is transmitted by facsimile - when the sending machine produces a report showing the transmission was successful;
iv. it is sent by e-mail - when it enters a system under the control of the addressee; or
v. by posting on the agreed web site - seven days after the date of posting.

If a Notice delivery occurs outside normal business hours at the addressee's place of business, the parties agree in these circumstances that formal receipt occurs at 9 am on the next *business day* at that place.

9.12 Amendments

9.12.1 Procedure for amendment

Amendments to this CPS or a relevant CP must undergo the same procedures as for the initial approval (see 1.5.4). Rephrasing provisions to improve their clarity as well as editorial and typographical corrections, changes to contact details are not considered amendments, however any change must be brought to the attention of the PKI PMA and (for Gatekeeper Approved documents) the Gatekeeper Competent Authority, to seek their concurrence.

9.12.2 Notification mechanism and period

The amended CPS and/or a relevant CP shall be published on the Defence PKI web site prior to it becoming effective. There is no fixed notice and comment period. Editorial and typographical corrections, changes to contact details and other minor changes that do not materially impact the parties may be changed without notice and are not subject to the notification requirements herein.

9.12.3 Circumstances under which OID must be changed

Where a CP is amended, the OID for the relevant CP must not be changed without PKI PMA approval. A change history will be maintained within the document (editorial changes etc., see 9.12.1, are not amendments).

If a change in Defence's CPS or CP is determined by the PKI PMA to warrant a change in the currently specified OID for a particular type of certificate, then the revised version of the document will also contain a revised OID for that type of certificate.

9.13 Dispute resolution provisions

If a dispute arises between Defence and an employee of the Department of Defence under the *Public Service Act 1999 (Cth)* (APS employee), or a member of the Australian Defence Force (ADF member), such dispute must be resolved through normal departmental mechanisms.

If a dispute arises between Defence and any party other than an APS employee or ADF member (Dispute), written notice must be provided so that the parties can meet to negotiate in good faith to resolve the Dispute (Dispute Notice). Should the Dispute remain unresolved 30 days after receipt of the Dispute Notice, the parties may seek mediation in accordance with the mediation rules of the *Australian Disputes Centre*[8] (ADC), or if the ADC no longer exists, such other organisation as determined by Defence. The mediation will be held in the *Australian Capital Territory* (ACT) and subject to the laws of the ACT. Legal representation is permissible by either party to the mediation. . Each party will bear its own costs of resolving the Dispute and the parties must bear equally the cost of any third person appointed as mediator.

Nothing in this clause prevents Defence from preventing a party from accessing the Defence PKI, or commencing proceedings against a Subscriber for a breach of the Subscriber Agreement.

9.14 Governing law

The governance for this CPS and any relevant CP is by, and construed to be in accordance with, the laws from time to time in force in the Australian Capital Territory.

All parties in the Defence PKI domain agree to irrevocably and unconditionally submit to the exclusive jurisdiction of the Supreme Court of the Australian Capital Territory and waive any rights to object to any proceedings brought in that court.

9.15 Compliance with applicable law

All parties to this CPS and any relevant CP must comply with all relevant:

i. laws;
ii. Australian Government policies, such as the *Protective Security Policy Framework* (PSPF), *Information Security Manual* (ISM), *Gatekeeper PKI Framework along with policies embedded within the overarching Frameworks;* ,and
iii. Defence policies, such as the *Defence Security Principles Framework* (DSPF) and Defence *CDMC ICT Security Policy* (ICTSP).

9.16 Miscellaneous provisions

9.16.1 Entire agreement

Each Subscriber Agreement must include a clause that provides that the CPS, any relevant CP and the Subscriber Agreement supersedes any prior agreements or representations, written or oral, between the parties to the Subscriber Agreement and records the entire agreement between the parties in relation to its subject matter.

9.16.2 Assignment

No party may assign its obligations or rights under this CPS, or any relevant CP, without Defence's prior written approval.

[8] https://disputescentre.com.au

9.16.3 Severability

If any provision of this CPS and/or relevant CP is or becomes invalid, illegal or unenforceable then that provision will, so far as possible, be read down to the extent necessary to ensure that it is not illegal, invalid or unenforceable.

If the reading down of any provision, or part of the provision, is unachievable, then the provision or part of it will be void and severable, without impairing or affecting the remaining provisions of the CPS or CP (as the case may be) in any way.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Failure by either party to enforce a provision of this CPS or any relevant CP shall not be construed as in any way affecting the enforceability of that provision or the CPS or CP (as the case may be) as a whole.

9.16.5 Force Majeure

A PKI Entity is not liable for any loss or damage arising from any delay or failure to perform its obligations described in this CPS or relevant CP if such delay is due to Force Majeure (See Appendix B).

If a delay or failure by a PKI Entity to perform its obligations is due to a Force Majeure event, the performance of that PKI Entity's obligations is suspended to the extent and for the duration caused by the Force Majeure event.

If delay or failure by a PKI Entity to perform its obligations due to Force Majeure exceeds 10 days, the PKI Entity affected by the failure to perform the obligations may terminate the arrangement, agreement or contract it has with the non-performing PKI Entity on providing notice to that Entity in accordance with this CPS or the CP.

If the arrangement, agreement or contract terminates pursuant to this section, the non-performing PKI Entity must refund any money (if any) paid by the terminating Entity to the non-performing Entity for services not provided by the non-performing PKI Entity.

9.17 Other provisions

For a Relying Party who is a member of a nation that is a signatory of the *Combined Joint Multilateral Master Military Information Exchange Memorandum of Understanding* (CJM3IEM) the conditions of the CJM3IEM in relation to Settlement of Disputes and Claims and Liabilities will apply, otherwise no stipulation.

APPENDIX A. CAs OPERATING UNDER THIS CPS

Facility Name	CA Identification	Address	Contact Name
Certificate and Directory Management Centre (CDMC)	Australian Defence Public Root Certificate Authority Australian Defence Public Identity Certificate Authority Australian Defence Public Device Certificate Authority Australian Defence OSN Identity Certificate Authority Australian Defence OSN Device Certificate Authority Australian Defence Enterprise Certification Authorities	pki.ops@defence.gov.au PKI Operations Manager c/o CDMC (R8-LG-014) Department of Defence PO Box 7909 CANBERRA BC ACT 2610	PKI PMA Secretariat

APPENDIX B. DEFINITIONS, ACRONYMS AND INTERPRETATION

B.1 Definitions

Accreditation Agencies	Those agencies that provide independent assurance that the facilities, practices and procedures used to issue Defence certificates comply with the relevant accreditation frameworks (policy, security and legal). Principally these will consist of DTA, ASD, DSVS and ICTSB.
Active Directory	Microsoft product used in network and identity management. It uses the Lightweight Directory Access Protocol and typically stores information about all resources on the network. It also provides authentication services and can store PKI certificates.
Affiliated	An entity that is associated with Defence.
Application	A computer application or relevant component of one (including any object, module, function, procedure, script, macro or piece of code)
Approved Documents	The Approved Documents are those approved by the PKI PMA and include those approved by the Gatekeeper Competent Authority. E.g. CPS, CPs, ICTSP, SSP, KMP, DRBCP, IRP and PKI Operations Manual.
Authorised Key Retriever (AKR)	An AKR is a RO who is authorised to retrieve confidentiality keys from the Key Archive Server (KAS).
Authorised RA	Has the meaning given to it in paragraph 1.3.2 of this CPS.
Business Day	Any day other than a Saturday, Sunday or public holiday (including public service holidays) for the whole of the Australian Capital Territory. Traditionally such days are from 0800 to 1600.
Central RO (CRO)	Centrally located ROs, who in addition to managing smartcards (revoke, activate and unblock cards centrally, retire and unregister) also have permissions to print smartcards and authorise access to the TMS. See also Site RO (SRO)
Certificate	An electronic document signed by the Certification Authority which: i. Identifies a Subscriber by way of a Subject Distinguished Name (Identity certificates) and a Resource by way of a Subject Distinguished Name and/or Subject Alternative Name (Resource certificates) ii. Binds the Subject to a Key Pair by specifying the Public Key of that Key Pair iii. Contains the information required by the Certificate Profile.
Certificate Assurance Level	See Level of Assurance.
Certificate Information	Information needed to generate a digital certificate as required by the Certificate Profile.
Certificate Policy	Means the definition adopted by RFC3647, which defines a Certificate Policy as "A named set of rules that indicates the applicability of a Certificate to a particular community and/or class of applications with common security requirements".

Certificate Profile	A certificate profile provides details about the format and contents of a digital certificate, including, for a natural person, their Distinguished Name.
Certificate Repository	The Certificate Repository provides a scalable mechanism to store and distribute certificates, cross-certificates and CRLs to end users of the PKI.
Certificate Revocation List	The published directory which lists revoked Digital Certificates. The CRL may form part of the Directory or may be published separately.
Certificate Authority	A Certificate Authority (or Certification Authority) (CA) is an entity which issues digital certificates for use by other parties.
Certificate Store	Storage location for certificates on a computer or device.
Certification Practice Statement	A statement of the practices that a Certification Authority employs in managing the digital Certificates it issues (this includes the practices that a Registration Authority employs in conducting registration activities on behalf of that Certification Authority). These statements will describe the PKI certification framework, mechanisms supporting the application, insurance, acceptance, usage, suspension/revocation and expiration of Digital Certificates signed by the CA, and the CA's legal obligations, limitations and miscellaneous provisions.
Code	A contiguous set of bits , i.e. scripts or executables, that has been or can be digitally signed with a Private Key that corresponds to a Code Signing Certificate.
Code Signing	Process of digitally signing software code, i.e. scripts or executables, to attest to the authenticity and integrity of the code, and to the identity of the publisher.
Code Signing Certificate	A digital certificate issued by a CA that contains a code Signing EKU.
Code Signing Key Custodian	Person who is responsible for managing code signing keys and certificates.
Code Signing Token	A hardware security device containing a Code Signing Certificate and keys.
Commonwealth	Means the Commonwealth of Australia
Commonwealth Agency	An agency established by the Commonwealth or in which the Commonwealth has a controlling interest.
Common Name	Is the characteristic value within a Distinguished Name. Typically, it is a descriptive name of the user or service e.g. "Bruce Smith" or "CDMC Web Handler". Where technically required, the Common Name can be the resources domain name.
Confidential Information	Any information having a commercial value that would be, or could be, reasonably expected to be destroyed or diminished if the information was disclosed.

Core Components	Core components are those elements, and sub-components, of the PKI that are integral to its trust and enable the following aspects:
	• Certification,
	• Issuance; and
	• Validation.
	They include the following, as well as their associated sub-components, databases and/or operator trusted elements:
	• Certification Authorities
	• CA Operators (CAO)
	• Registration Authorities
	• Registration Exchanges (RAX)
	• Registration Authority Auditors (RAA)
	• Protocol handlers, such as:
	  ○ web Handler,
	  ○ email Handler,
	  ○ SCEP Handler,
	  ○ CMP Handler
	  ○ Autoenroll Handler
	• Web Registration Authority Operators (WebRAO)
	• Token Management System (TMS)
	• Card Management System (CMS)
	• Validation Authorities (VA)
	• Certificate Status Servers (CSS)
	• Timestamp Servers (TSS) [9]
	• Key Archive Servers (KAS) [9]
	• KAS Operators (KAO) [9]
	• Hardware Security Modules (HSM)

Cross-certification	The establishment of a trust relationship between two PKIs, where one CA signs another PKI's CA certificate. This creates a chain of trust allowing the subscribers of the cross-certifying CA to trust those of the cross-certified CA. If done two-ways (PKIs signing each other's CAs' certificates), mutual trust can be established.
Cross-certification ceremony	The event where a cross-certification agreement is executed, i.e. one CA creates a cross-certification request to another CA. The cross-signing CA creates and returns the cross-certificate, signed with its own private key. The "ceremony" is a formal event, and is witnessed by representatives of both CAs. Details of the event are recorded and signed by the witnesses to provide an audit record.
Critical Core Components	Those core components whereby regeneration is not possible, and therefore loss or damage would severely impact the operations of the PKI, e.g. CA, RA and KAS private keys (all held on HSMs)
Custodian	A person who has custody of something, a keeper or guardian; in the context of PKI, usually a *Key Custodian.*
Defence	A holistic term utilised to define the Commonwealth of Australia's Department of Defence and includes the Australian Defence Force (ADF).

[9] Not used at the time of writing (Nov 2023) – may be revived in future.

Defence Directory	Defence Directory refers to repositories within Defence (e.g. Active Directory or Defence Corporate Directory) which contain information relating to Defence staff, departments, divisions, groups and sections, units and resources. These repositories also contain digital certificates for individuals and/or resources.
Defence Identity Management Environment	A combination of systems that are used to manage identities within the Defence organisation.
Defence Interoperability Certificate Authority (DIOCA)	Defence Certificate Authority solely used for signing certificates required for cross-certification with Peer PKIs. The DIOCA is a root CA, meaning its certificate is self-signed. See [DIOCA CP] for more detail.
Defence PKI Policy Management Authority	The governing body for the Defence PKI. Approves policy under which Defence's PKIs operate, and is responsible for addressing policy issues that affect the strategic, tactical and operational levels of Defence.
Defence Root CA	A Defence operated CA that provides a self-signed certification authority (CA) certificate that identifies a CA. It is called a root CA because by definition there is no higher certifying authority within Defence to sign its CA certificate. (A CA can issue multiple certificates, which can be used to issue multiple certificates in turn, thus creating a tree).
Department of Defence	The Commonwealth of Australia represented by and acting through the Department of Defence.
Defence Single Information Environment (SIE)	The Defence Single Information Environment (SIE) encompasses the computing and communications infrastructure of Defence along with the management systems and people that deliver that infrastructure.
Device	Device means any computer hardware or other electronic device.
Digital Signature	An electronic signature created using a Private Signing Key.
Directory Service	A directory service is a software application – or a set of applications – that stores and organises information about a computer network's users and network resources, and that allows network administrators to manage users' access to the resources. Additionally, directory services act as an abstraction layer between users and shared resources. The X.500 and LDAP directory services are examples of general-purpose distributed hierarchical object-oriented directory technologies. Both offer complex searching and browsing capabilities are used for white pages, network information services, PKI, and a wide range of other applications.
Distinguished Name (DN)	An unique identifier assigned to, as relevant: i. the Subject identified by; and ii. the issuer of a Certificate, having the structure required by the Certificate Profile.
Electronic Network Access Request (eNAR)	Electronic business process for the request of Defence network access.

End Entity (EE)	An entity that is identified as the subject of a certificate at the end of a certification path or shares a symmetric key with other entities for communication. End entities make up the leaf nodes in the PKI and are not allowed to issue certificates to other entities.
Evaluated Product List (EPL)	The Evaluated Product List is produced to assist in the selection of products that will provide an appropriate level of information security. The list, maintained by ASD, is published at https://www.asd.gov.au/infosec/. The EPL lists products that: i. have completed *Common Criteria* (CC) or ITSEC certification, ii. are in evaluation within the AISEP, or iii. have completed some other recognised ASD evaluation methodology.
Evaluation Assurance Level (EAL)	The Evaluation Assurance Level (EAL1 through EAL7) of a computer product or system is a numerical grade assigned following the completion of a Common Criteria security evaluation, an international standard in effect since 1999. The increasing assurance levels reflect added assurance requirements that must be met to achieve Common Criteria certification. The intent of the higher levels is to provide higher confidence that the system's principal security features are reliably implemented.
Everybody Database (EBDb)	Defence database which combines PMKeyS and ODS and is considered the authoritative source for creation of network accounts in the DIE.
Evidence Of Identity	Evidence (e.g. in the form of documents) issued to substantiate the identity of the presenting party, usually produced at the time of Registration (i.e. when authentication credentials are issued).
Exercised	To discharge, or perform, a function. Or, an act of employing or putting into play.
Force Majeure	A Force Majeure event means any occurrence or omission that is beyond the reasonable control of a party that prevents that party from, or delays that party in, performing any of its obligations under this CPS, a CP or a Subscriber Agreement, including, where relevant, due to forces of nature, war, riot, civil commotion, failure of a public utility, or industrial action (other than industrial action specifically directed at a party).
Gatekeeper	The Commonwealth Government strategy to develop Public Key Infrastructure to facilitate Government online service delivery and e-procurement.
Hard Token	A hard token, sometimes called an "authentication token," is a hardware security device that is used to authorise a Subscriber. A common example of a hard token is a smartcard.
High Assurance Certificate (Gatekeeper)	A digital certificate issued by a Gatekeeper Accredited or Recognised Service Provider to Organisations and individuals for the purpose of transacting online with government agencies and whose risk and threat to data are assessed as high. This category is characterised by a requirement for a Formal Identity Verification Model *EOI* check by a Gatekeeper accredited Registration Authority. N.B. Defence's own Levels of Assurance definition of "High Assurance" is aligned to the Gatekeeper definition, however does not issue certificates to organisations.

Identity Certificate	An identity certificate is a certificate which uses a digital signature to bind together a public key with a human identity — information such as the name of a person, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual.
Interoperability CA	Root CA created specifically for signing cross-certificates between the Defence PKI and external PKIs with whom a cross-certification arrangement (CCA) has been entered into.
Key	A Key is a string of characters used with a cryptographic algorithm to encrypt and decrypt.
Key Custodian	A key custodian refers to the authorised person appointed to manage a key on behalf of Defence or PKI PMA, or Resource Administrator.
Key Pair	A pair of asymmetric cryptographic Keys (e.g. one decrypts messages which have been encrypted using the other) consisting of a Public Key and a Private Key.
Level of Assurance	Levels of trust associated with a credential as measured by the associated technology, processes, and policy and practice statements controlling the operational environment. In the context of this CPS, the term refers to four levels of assurance of certificates (low, medium, high, very high) defined for the Defence PKI. A "No Assurance" level OID is used for test certificates.
Network Resource	Network Resources (devices) are units that mediate data in a computer network. Computer networking devices are also called network equipment and commonly include routers, gateways, switches, hubs, repeaters and firewalls.
National Cryptographic Authority (NCA)	The NCA of Australia is the Australian Signals Directory (ASD). ASD also maintain a list of evaluated and approved security products for use by Australian Government agencies (Evaluated Products List – EPL).
No-Lone Zone	A physically secure area which has been defined as an area which when occupied must have 2 or more trusted personnel as occupants.
Non-Person Entity	An entity with a digital identity (for example an IP address or MAC address) that acts in cyberspace, but is not a legal entity. This can include web sites, hardware devices, software applications, and information artefacts.
Modification (of certificate)	Certificate modification means the issuance of a new certificate due to changes in the information in the certificate other than the Subscriber public key. (RFC3647)
Object Identifier	An OID is a string of decimal numbers that uniquely identifies an object. These objects are typically an object class or an attribute. It serves to name almost every object type in X.509 Certificates, such as components of Distinguished Names and Certificate Policies.
Online Certificate Status Protocol (OCSP)	Method of establishing the status of a certificate that has not expired. A PKI enabled client requests the status of a certificate from an OCSP responder. The responder provides a response ("good", "revoked" or "unknown") to the client. OCSP is a more bandwidth efficient method than the download of a full Certificate Revocation List (CRL).
Open PKI	Open PKI deployments anticipate the widespread acceptance of Digital Certificates where Relying Parties may not be known and where the parties are not generally contractually bound.

Operational CA	A CA that issues and manages end-entity certificates. See also "Subordinate CA".
Operational Day	Any day that the PKI facility (within CDMC) is manned. In this context it normally occurs in conjunction with a *Business Day*, however, Defence will operate 24*7 in some circumstances.
Operator	Any individual who performs a Trusted Role and is assigned keys and certificates to perform administrative or maintenance functions within the PKI. They are considered Privileged users (refer to ISM) for the purposes of the Defence PKI and the term collectively represents individuals who interface directly with Core Components for the purposes of undertaking their role, including PKI Operators and auditors, ROs, TAs, and Code Signing Key Custodians, and PKI System Administrators.
Other Defence Support (ODS)	Database of Defence affiliated staff that are not directly employed by DoD, e.g. contractors.
Peer PKI	Other PKI which Defence PKI has entered (or intends to enter) into a cross-certification arrangement with. See [DIOCA CP].
Personal Identity Verification (PIV)	Standard created by National Institute for Standards and Technology (NIST) in response to Homeland Security Presidential Directive 12 (HSPD 12) of Aug 2004. Full name "Personal Identity Verification of Federal Employees and Contractors". Also known as FIPS 201. Specifies interfaces, biometrics and algorithms for PIV compliant cards.
Personnel Management Key Solution (PMKeyS)	Database of Defence employees.
PKI Operations Manager	Manages PKI operations at the Certificate & Directory Management Centre (CDMC).
PKI Operator	PKI Operators perform day-to-day maintenance and support of the PKI systems managed by the CDMC.
PKI Systems Administrator	A PKI Systems Administrator performs systems administrations tasks on the PKI systems operated by the CDMC.
Private Certificate-Signing Key	The Private Key used by the CA to digitally sign Certificates.
Private Confidentiality Key	The Key used by the addressee to decrypt messages, which have been encrypted using the corresponding Public Confidentiality Key.
Private Key	The Private Key in asymmetric Key Pair that must be kept secret to ensure confidentiality, integrity, authenticity and non-repudiation, as the case may be.
Private Signing Key	A Private Key used to digitally sign messages on behalf of the relevant certificate Subject.
Public Key	The Key in an asymmetric Key Pair which may be made public.
Public Key Infrastructure (PKI)	The combination of hardware, software, people, policies and procedures needed to create, manage, store and distribute Keys and Certificates based on public Key cryptography.

PKI Software	Software programs that manage digital certificate lifecycle operations and token management.
Public Key Technology	Public Key Technology is the hardware and software used for encryption, signing, verification as well as the software for managing Digital Certificates.
Registration Authority (RA)	A Registration Authority (RA) is an entity that is responsible for one or more of the following functions on behalf of a CA: i. processing certificate application; ii. processing requests to revoke certificates, and iii. processing requests to renew, re-key or modify certificates. Processing includes the identification and authentication of certificate applicants and approval or rejection of requests. See section 1.3.2 (Registration Authorities) of this CPS and the relevant Certificate Policy (CP) for more information about the applicable RA.
Registration Officer (RO)	A person authorised by a Defence Registration Authority (RA) or Defence approved "Third party" RA to perform RA functions in accordance with this CPS, the relevant Certificate Policy and other applicable documentation. See also Central RO (CRO) and Site RO (SRO).
Re-Key	A Subscriber or other participant generating a new key pair and applying for the issuance of a new certificate that certifies the new public key. Normally used at the time of expiry of the certificate. (RFC3647)
Relying Party	A recipient of a Certificate who acts in reliance on that Certificate and/or Digital Signatures verified using that Certificate.
Renewal (of certificate)	Renewal means the issuance of a new certificate to the Subscriber without changing the Subscriber's public key or any other information in the certificate. (RFC3647). The validity period and serial number will be different in the renewed certificate.
Repository	A database of information (e.g. Certificate status, evaluated documents) which is made accessible to users including the Relying Parties.
Resource	Includes any Non-Person Entity, such as Network Resource, *Application*, code, electronic service or process, *Device,* or data object, that is capable of utilising a Certificate.
Resource Administrator	Resources administrator has the day-to-day responsibility for a resource, and will in most cases be the person who requests, or installs, a certificate for the resource they are managing (also referred to as a Systems Administrator or Trusted Installer).
Resource Certificate	A Resource Certificate is a Certificate issued in respect of a Non-Person Entity/Resource.
Resource Custodian (RC)	See Trusted Agent
Revoke	To terminate a Certificate prior to the end of its operational period.
Root CA	A CA that is at the top of a certificate chain, i.e. its own certificate is self-signed.
Secure Sockets Layer	A protocol developed by Netscape for transmitting private documents via the Internet.

Site RO	ROs in regional/deployed areas, who carry out registration operations for their respective location. See also Central RO (CRO).
Software Publisher	The Defence responsible owner of the software, who ensure Defence has the licence to distribute and use, as well as develop/configure if applicable, the software.
Subordinate CA (SubCA)	A CA which is has been established under the certificate path of the Defence Root CA. A SubCA usually issues and manages certificates to end entities. See also Operational CA.
Subscriber	A Subscriber is, as the context allows: i. for Identity Certificates, i.e. those issued to Person Entities (PE); the person whose Distinguished Name appears as the "Subject Distinguished Name" on the relevant Certificate; ii. for Resource Certificates, i.e. those issued to Non-Person Entities (NPE); the person or legal entity that applied for that Certificate, and/or administers the system that utilises the Certificate. Individual CPs provide context for the definition of Subscriber relevant to that CP.
Subscriber Agreement	An agreement between the relevant Service Provider and a Subscriber, which sets out the respective rights, obligations and liabilities of those parties, and which legally, binds those parties to the relevant Certificate Policy and Certification Practice Statement.
Superior CA	A CA which establishes/signs the certificate of a Subordinate CA.
Timestamp (trusted)	PKI based technology providing a trusted timestamp over a datum or a digital signature. A timestamp server signs a hash of the datum to be timestamped, including the correct time from a trusted time source, providing proof that the datum existed at the time of timestamping.
Token	A hardware security device containing a user's Private Key(s), and Public Key Certificate.
Token Management System (TMS)	Also known as Card Management System (CMS). Hardware and software applications used to manage smartcards. Smartcards are used as hard tokens for Subscribers and Operators in the Defence PKI.
TMS Auditor	Role within the TMS that has read-only access to log files for auditing purposes.
Transport Layer Security	A cryptographic protocol that provides security for communications over networks such as the Internet. TLS and SSL encrypt the segments of network connections at the Transport Layer end-to-end.
Trusted Agent	A Trusted Agent is a Defence staff member that is responsible and accountable for the approval of resource certificates for use within the Defence Single Information Environment. They interface with the RA to process certificate applications, revocations, and where applicable, renewal or re-key of certificates.
Trusted Element	A transportable, secure, and tamper-resistant container that includes the private keys of PKI Core Components and/or Trusted Roles.
Trusted Installer	See Resource Administrator
Trusted Role	A role conducted within a RA/CA that has access to or control over cryptographic operations that may materially affect the issuance, use,

	suspension, or revocation of Certificates, including operations that restrict access to a repository. Personnel who perform this role are qualified to serve in it.
TSS Administrator	The TSS (Timestamp Server) Administrator performs maintenance tasks on the Timestamp Server. This role is usually performed by a PKI Operator,
Universally Unique Identifier	Used in computing to identify an entity or item in the format of a 128bit hexadecimal number, e.g. With a sufficiently random and generation process makes it 'practically unique' without the need for central management. See RFC4122.
Validation Authority	A Validation Authority (VA) is an entity that can perform one or more of the following functions: i. processing certificate status requests; ii. validating credentials and authentication requests; iii. validating signatures; and iv. other services related to PKI and online authentication. The Defence Validation Authority provides certificate status information through the provision of OCSP responders, and may expand its services in the future to include Server-based Certificate Validation Protocol (SCVP) services.
X.509 and X.509v3	The international standard for the framework for Public Key Certificates and attribute Certificates. It is part of wider group protocols from the International Telecommunication Union-T X500 Directory Services Standards.

Additional terms not defined in this Glossary but which may be relevant can be found in the Identity and Access Management Glossary (refer to https://www.dta.gov.au). Where terms are defined in both the Identity and Access Management Glossary and this Glossary then for the purpose of Gatekeeper accreditation the definition in the Identity and Access Management Glossary will be determinative. The PKI PMA is the authoritative source of definitions relating to the Defence PKI, any requirement for clarification can be referred to the PKI PMA.

B.2 Acronyms

ADC	Australian Disputes Centre
ACSI	Australian Government Information and Communications –Electronic Technology Security Manual Instruction
ACT	Australian Capital Territory
AD	Active Directory
AD-CPS	Australian Defence Certificate Practice Statement
ADF	Australian Defence Force
ADOCA	Australian Defence Organisation Certification Authority
ADPRCA	Australian Defence Public Root Certificate Authority
AGS	Australian Government Solicitor
AKR	Authorised Key Retriever
ASD	Australian Signals Directorate
BOC	Backup Operations Centre
CA	Certification Authority
CAL	Certificate Assurance Level
CAO	CA Operator
CCA	Cross-Certification Arrangement
CDMC	Certificate and Directory Management Centre
CJM3IEM	Combined Joint Multilateral Master Military Information Exchange Memorandum of Understanding
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSA	Certificate Status Authority – equivalent to Validation Authority (VA), found in ACP185
CSO	CDMC Security Officer
DIE	Defence Information Environment
DIOCA	Defence Interoperability CA
DLM	Dissemination Limiting Marker
DN	Distinguished Name
DPKIPB	Defence Public Key Infrastructure Policy Board (now known as the Policy Management Authority – PKI PMA)

DRBCP	Disaster Recovery and Business Continuity Plan
DRCA	Defence Root Certificate Authority
DRCAO	Defence Root Certificate Authority Operator
DRN	Defence RESTRICTED Network
DS&VS	Defence Security and Vetting Service
DSN	Defence SECRET Network
DSPF	Defence Security Protective Framework
DTA	Digital Transformation Agency
EAL	Evaluated Assurance Level
EBDb	Everybody Database
EE	End Entity
eNAR	electronic Network Access Request
EOI	Evidence of Identity
EPL	Evaluated Products List
HSM	Hardware Security Module
I&A	Identification and Authentication
ICTSB	ICT Security Branch
ICTSP	Information Communication Technology Security Plan
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IP	Intellectual Property
IPR	Intellectual Property Rights
ISM	Australian Government Information Security Manual
ISO	International Standards Organisation
ITSEC	Information Technology Security Evaluation Criteria
KAO	Key Archive Operator
KAS	Key Archive Server
KMP	Key Management Plan
LOA	Level of Assurance
LTSK	Long Term Storage Key
NCA	National Cryptographic Authority
NPE	Non-Person Entity

OCSP	Online Certificate Status Protocol
ODS	Other Defence Support
OID	Object Identifier
PED	Pin Entry Device
PIN	Personal Identification Number
PIV	Personal Identification Verification
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKI PMA	Defence PKI Policy Management Authority (previously known as the DPKIPB)
PKIX	Public Key Infrastructure (X.509) (IETF Working Group)
PKT	Public Key Technology
PMKeyS	Personnel Management Key Solution
POC	Primary Operations Centre
PSE	Personal Secure Environment
RA	Registration Authority
RAA	Registration Authority Auditor
RAO	Registration Authority Operator
RC	Resource Custodian (also known as Trusted Agent)
RFC	Request For Comment
RO	Registration Officer
SCEP	Simple Certificate Enrolment Protocol
SCVP	Server-based Certificate Validation Protocol
SO	Security Officer
SRMP	Security Risk Management Plan
SSL	Secure Sockets Layer
SSP	System Security Plan
SubCA	Subordinate Certificate Authority
SubCAO	Subordinate Certificate Authority Operator
TA	Trusted Agent
TCSEC	Trusted Computer System Evaluation Criteria
TLS	Transport Layer Security
TMS	Token Management System

TSA	Timestamp Authority
TSS	Timestamp Server
UPS	Uninterruptible Power Supplier
URI	Uniform Resource Identifier
UTC	Coordinated Universal Time
UUID	Universally Unique Identifier
VA	Validation Authority

B.3 Interpretation

In Approved Documents, unless the contrary intention appears:

i. a reference to the singular includes plural and vice versa;
ii. words importing a gender include any other gender;
iii. a reference to a person includes a natural person, partnership, body corporate, association, governmental or local authority or agency, or Device or Application or other entity;
iv. a reference to a document or instrument includes the document or instrument as altered, amended, supplemented or replaced from time to time;
v. a reference to a section is a reference to the relevant section of that document;
vi. an amendment or replacement of a document does not imply any consequent amendment or alteration to any other document;
vii. where a word or phrase is given a particular meaning, other parts of speech and grammatical forms of that word or phrase have corresponding meanings;
viii. the meaning of general words is not limited by specific examples introduced by 'including', 'for example' or similar expressions;
ix. the headings are for convenience only and are not to be used in the interpretation of an Approved Document; and
x. any appendix or attachment to an Approved Document (no matter how named) forms part of that document.

APPENDIX C. APPROVED PUBLIC CERTIFICATE POLICES

1.2.36.1.334.1.1.1.7	X.509 Certificate Policy for the Australian Department of Defence **Public Root Certificate Authority**	PKI PMA Secretariat PKI Operations Manager pki.ops@defence.gov.au
1.2.36.1.334.1.1.1.8	X.509 Certificate Policy for the Australian Department of Defence **Public Subordinate Certificate Authorities**	PKI PMA Secretariat PKI Operations Manager pki.ops@defence.gov.au
1.2.36.1.334.1.1.1.3	X.509 Certificate Policy for the Australian Department of Defence **Interoperability Certificate Authority**	PKI PMA Secretariat PKI Operations Manager pki.ops@defence.gov.au
1.2.36.1.334.1.1.2.1	X.509 Certificate Policy For Australian Department of Defence **Individual – (Medium Assurance) Certificates**	PKI PMA Secretariat PKI Operations Manager pki.ops@defence.gov.au
1.2.36.1.334.1.1.2.2	X.509 Certificate Policy For Australian Department of Defence **Individual – Hardware (High Assurance) Certificates**	PKI PMA Secretariat PKI Operations Manager pki.ops@defence.gov.au
1.2.36.1.334.1.1.3.1	X.509 Certificate Policy for the Australian Department of Defence **Secure Communications Certificates**	PKI PMA Secretariat PKI Operations Manager pki.ops@defence.gov.au
1.2.36.1.334.1.1.3.5	X.509 Certificate Policy for the Australian Department of Defence **Validation Authority Certificates**	PKI PMA Secretariat PKI Operations Manager pki.ops@defence.gov.au
1.2.36.1.334.1.1.3.9	X.509 Certificate Policy for the Australian Department of Defence **Digital Signature - Resources Certificates**	PKI PMA Secretariat PKI Operations Manager pki.ops@defence.gov.au