X.509 Certification Practice Statement (CPS)

Cogito PKI as a Service Root and Shared Certificate Authorities

27 September 2021

Version 1.0

Owner:	Cogito Governance Risk and Compliance Group
Contact details:	Telephone: +61 2 6140 4494 Email: Security.services@cogitogroup.net
Document status:	RELEASED

Document Management

This document is controlled by:	Cogito Governance Risk and Compliance Group (GRCG)
Changes are authorised by:	Cogito Governance Risk and Compliance Group Gatekeeper Competent Authority (GCA)

Revision history

Revision date	Version No.	Author	Description of changes
2021-09-16	1.0	Brad Fardig	Released

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.

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

This section identifies and introduces the set of provisions and indicates the types of entities and applications to which this Cogito PKI as a Service (PKIaaS) X.509 CPS applies.

1.1 Overview

The purpose of this CPS is to provide a common framework under which the Cogito PKIaaS, Certificate Authority (CA) and Registration Authority (RA), services are provided.

As such, this CPS sets out a number of policy and operational matters related to the services, including the practices that Cogito employs in issuing, revoking and managing certificates for subscribers to the PKIaaS within the Gatekeeper PKI Framework

This CPS is to 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 provisions of the relevant CP prevail over the provisions of the Cogito PKIaaS X.509 CPS to the extent of any direct inconsistency.

Cogito operates a PKI that 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:

- The Australian Government Protective Security Policy Framework (PSPF) – Attorney General's Department; and
- The Australian Government Information Security Manual – Australian Signals Directorate.

The Cogito PKIaaS conducts its role in accordance with the Approved Documents.

The following documents are Approved Documents:

- This CPS;

- The X.509 Certificate Policy for the Cogito PKIaaS Root Certificate Authorities and Subordinate Certificate Authorities;
- The X.509 Certificate Policy for Cogito PKIaaS - Individual Hardware Certificates (ECC/RSA);
- The X.509 Certificate Policy for Cogito PKIaaS - Individual Software Certificates (ECC/RSA);
- The X.509 Certificate Policy for Cogito PKIaaS –Resource Certificates (ECC/RSA);
- The X.509 Certificate Policy for Cogito PKIaaS – Validation Authority Certificates (ECC/RSA); and
- The Cogito PKIaaS Subscriber Agreement.

The following non-public documents are also approved documents:

- Cogito Information Security Policy (ISP)
- Cogito PKIaaS System Security Plan (SSP)
- Cogito Security Risk Management Plan (SRMP)
- Cogito Cryptographic Key Management Plan (CKMP)
- Cogito Disaster Recovery and Business Continuity Plans (DRBCP)
- Cogito Incident Response Plan (IRP)
- Cogito RA Operations Manual

Non-public documents may be cited in this CPS, but their contents are not disclosed publicly for security reasons.

Cogito Group operates and manages PKI facilities on behalf of subscribers to support:

- Interaction directly with a Subscribers assets or systems, using Public Key Technology (PKT);
- Authentication with third parties as a subscriber of Cogito services; and
- Provision of digital signatures to entities affiliated with subscribers of Cogito Services.

The Governance and Policy Board responsible for ensuring operation within the Gatekeeper PKI Framework is the Cogito Governance, Risk and Compliance Group (GRCG). The GRCG is responsible for the approval of updates to this CPS to support any additional certificate types and ensuring that the CPS is suitable to support the certificates issued by the Cogito PKIaaS.

The GRCG is responsible for Cogito PKI Facilities with operation responsibility residing with Cogito PKI Operations. The Cogito PKIaaS provides certificate management covering:

- Identity certificates;
- Resource certificates;
- PKI infrastructure certificates (CA, RA, CRLs etc.); and

- Additional certificate types approved by the GRCG.

1.2 Document Name and Identification

The title for this CPS is X.509 Certification Practice Statement (CPS) Cogito PKI as a Service Root and Shared Certificate Authorities.

1.3 PKI Participants

1.3.1 Certification Authorities

The Certificate Authority(ies) (CA or CAs) that issue certificates under this CPS are the Cogito PKIaaS CAs subordinate to a Cogito PKIaaS Root CA. Appendix A provides a list of the CAs operated by Cogito under this CPS.

1.3.2 Registration Authorities

The Registration Authority(ies) (RA or RAs) that perform the registration functions under this CPS are Cogito RAs or 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 Cogito Group.

Only Gatekeeper accredited RAs may be used by Gatekeeper Accredited CAs

1.3.3 Subscribers

A Subscriber within the context of this CPS is defined as an organisation or agency whose Distinguished Name appears in the “Subject Distinguished Name” on the relevant CA certificate, or the legal entity that applied for the certificate, and/or entered into the Subscriber Agreement in respect to that certificate.

Note that “Individual” CPs provide the definition of a subscriber relevant to that CP. Typically Individual CPs will define a subscriber as the entity (e.g., an individual, device, web site, application or resource) whose Distinguished Name appears as the "Subject Distinguished Name" on the relevant end Certificate; and/or the person or legal entity that applied for that Certificate or entered into the Subscriber Agreement in respect of that Certificate.

1.3.4 Relying Parties

In general, a Relying Party uses a Cogito PKIaaS certificate to:

- Verify the identity of an entity;
- Verify the integrity of a communication with an entity;
- Establish confidential communications with an entity; and
- 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, the Cogito PKIaaS 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 Cogito PKIaaS by Relying Parties is governed by the conditions set out in the Cogito PKIaaS policies 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 Cogito PKIaaS for the purpose of establishing trust and validating a certificate.

Relying Parties are hereby notified that no financial liability is associated with this CPS or associated CPs, or CA and RA service providers.

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

- The validity of the entity's certificate using certificate status information;
- Any authority, or privilege, of the entity to act on behalf of the Subscriber or Cogito Group;
- Any authority, access or privilege the entity has to the Relying Party's assets or systems; and
- Any liability arising from relying on the Cogito PKIaaS.

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

- 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;
- Verify that the digital certificate is being used within the limits specified in the CP under which the digital certificate was issued; and
- Promptly notify the Cogito PKIaaS 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:

- The Cogito GRCG – which owns the overarching policy under which this CPS operates and:
    - Reviews and approves the CPS and relevant CPs;
    - Ensures that the infrastructure remains compliant within the terms of its accreditation;
    - Presides over the PKI audit process;
    - Defines rules and approves agreements for interoperability with other PKIs;
    - Approves mechanisms and controls for the management of the PKI;
    - Approves the operational standards and guidelines to be followed;
    - Monitors the governance and performance of the Cogito PKIaaS; and
    - Authorises the establishment of the infrastructure to support the Cogito PKIaaS

- Accreditation Agencies – to provide independent assurance that the facilities, practices, and procedures used to issue certificates comply with the relevant accreditation frameworks (policy, security, legal);
- Directory Service Providers – to provide a repository for certificates and certificate status information issued under the CP; and
- Subscriber System Administrators – to act as trusted installers or key custodians for Cogito PKIaaS issued resource certificates.

1.4 Certificate Usage

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

- Authenticate to a Relying Party electronically in online transactions;
- Digitally sign electronic documents, transactions, application code, timestamps and communications; and/or
- 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 aspects of this CPS and any applicable CPs.

1.5.1 Organisation Administering the Document

Cogito Group, through the GRCG, is the endorsing organisation for this CPS and applicable CPs and any amendments.

1.5.2 Contact Person

Contact details for the GRCG:

Email: security.services@cogitogroup.net

Postal Address: GRCG

Suite 3, 9 Sydney Ave

Barton ACT 2600

1.5.3 Authority determining CPS suitability for the policy

The GRCG 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 GRCG.

Before accepting changes to this document, or associated CP:

- The proposed changes are to be made to a draft document and submitted to the GRCG;
- The proposed changes are reviewed by the GRCG;
- Once the proposed changes are acceptable the GRCG will endorse the changes and forward the endorsed changes to any external parties that perform PKI accreditation; and
- Once accepted by all applicable parties the GRCG will approve the publication and implementation of proposed changes.

1.6 Definitions, acronyms and interpretation

See Appendix B – Definitions Acronyms and Interpretation

2 Publication and Repository Responsibilities

2.1 Repositories

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

The external online repository of information from the Cogito PKIaaS is accessible at: http://pki.gatekeeper.securesme.com/

2.2 Publication of certification information

Cogito publishes to its internal repository all CA certificates, relevant to subscriber certificates and Certificate Revocation Lists (CRLs).

External online certificate, CP, and CRL repository is accessible at: http://pki.gatekeeper.securesme.com/

Additional repository for this CPS, relevant CPs and PKI related information, resources, service, compromise notices and any other PKIaaS collateral will be accessible at: http://pki.gatekeeper.securesme.com/

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 Cogito PKIaaS Operations 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 for details.

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 are to 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 Section 4.9 of this CPS.

It is not anticipated that trademarks or other intellectual property rights will exist in personal names used within Cogito PKIaaS certificates. If a Subscribing organisation's legal name is also a trademark, use of the name is authorised by virtue of the organisation's signing of the Subscriber Agreement and acceptance of this CPS.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

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

3.2.2 Authentication of organisation entity

Cogito will take reasonable steps to ensure that the Organisation is verified prior to the creation of CAs or the issuance of a certificate containing an Organisation Identity.

Documents presented for the establishment of an Organisations identity must:

i. Identify the organisation;

ii. Confirm that the applicant/authoriser is a member of the organisation (via an ASIC check, an ABR search and/or an out of band check such as a phone verification);

iii. Confirm that the applicant/authoriser is authorised to act on behalf of the organisation; and

iv. Indicate the applicant/authoriser has approved a certificate manager for the organisation.

The Organisation identity must comprise either of the options shown in the table below:

Options	Organisation Identity Documentation Requirement
Option 1	• An original or certified copy of the notice issued by the Registrar of the ABR bearing the business entity's name and ABN. If either the owner, chief capacity or other officer or employee with clear capability to commit the business entity is named as the Public Officer on the document issued by the Registrar of the ABR, then this document only will suffice; and • Online verification with the ABR to link the Organisation's ABN to its business name.
Option 2	• If the notice issued by the Registrar of the ABR cannot be provided, then a legal or regulatory document binding either the individual or the Authoriser to the business entity; and • Online verification with the ABR to link the Organisation's ABN to its business name.

3.2.3 Authentication of individual identity

Applications can be made for certificates by individuals as their own identity or as the representative of an organisation. Applicants will be authenticated through binding the physical entity to the documented identity. The RA should sight a document containing a signature or a photograph as part of the authentication of an identity.

The individual shall undergo identity verification by an accredited RA in accordance with the gatekeeper LOA policy

3.2.4 Non-Verified Subscriber information

Business or organisational units within an Organisation will not be verified. Devices and application names and locations supplied to the RA to be used in device common names will not be validated.

3.2.5 Validation of authority

See relevant CP.

3.2.6 Criteria for interoperation

The decision to cross certify, cross recognise, mutually recognise, or other form of interoperation of the PKIaaS with a third-party PKI resides with the GRCG and the third party.

The GRCG 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 as also compatible.

3.3 Identification and authentication for re-key requests

See relevant CP.

3.4 Identification and authentication for revocation requests

See relevant CP.

4 Certificate Lifecycle Operational Requirements

4.1 Certificate Application

4.1.1 Who can submit a certificate application

Individuals affiliated with a Cogito PKIaaS subscriber can request a certificate for either themselves or a resource (non-person entity). Subscriber affiliations are validated in the registration process.

Where a relevant CP permits, an authorised resource can submit an application for a certificate from the Cogito PKIaaS.

The GRCG determines which types of affiliations with the subscriber organisation are appropriate for a certificate issued under the relevant CP.

4.1.2 Enrolment process and responsibilities

The relevant CP will describe unique conditions, though the following is the overarching process for all CPs issued under the Cogito PKIaaS.

For RCA and CA certificates, a formal key generation and signing ceremony is scripted prior to the event. Highly trusted from subscriber organisations will fill participant roles (such as PKI trusted custodians and official witnesses), along with PKI operational and co-ordination staff from Cogito as the PKI Service Provider who provide technical support for conducting the ceremony.

Registration for Subscribers may vary according to certificate type:

- Generally, individuals requiring keys and certificates are to submit an application in accordance with individual Subscriber processes through the Registration Authority;
- Applications are to contain information that is accurate, complete, and up to date;
- Subscribers will, be bound by contract, or equivalent arrangement for trusted agents and partners. This is in addition to their use being subject to the provisions of the applicable CP and this CPS;
- The agency Subscriber is responsible for:
    - Confirming the Entity's identity, ensuring the certificate request form is approved, [or];
    - Confirming that the Entity has an existing entry in the Subscriber's corporate directory, [and];
    - Forwarding the certificate request to the RA Operator and maintaining a record of the request.
- The RA Operator is responsible for ensuring the certificate application documentation is complete and conduct internal procedures to issue the certificate (as per the RA Operations Manual).

See relevant CP for further details of enrolment processes and responsibilities.

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:

- Authenticate a certificate request, to ensure it has come from an accredited or approved source;
- Verify the request is properly formed;
- Perform any additional process specified as part of the PKI operations;
- Compose and sign the certificate;
- Provide the certificate to the entity; and
- Publish the certificate in accordance with this CPS and relevant CP.

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

- Details of the certificate request;
- The success, or rejection (with reason), of the certificate request; and
- The entity that submitted the certificate request.

The CA is not bound to issue keys and certificates to any entity despite the 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.

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 will be published to Hyper Text Transfer Protocol (HTTP) and Lightweight Directory Access Protocol (LDAP) repositories (see also Section 2). 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 Keypair and certificate usage

See relevant CP.

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

This CPS permits certificate renewal. Certificate renewal is not the preferred process to issue a replacement certificate within the Cogito PKIaaS. The preferred process is certificate rekey, see Section 4.7.1.

The minimum defined criteria for certificate renewals is:

- The entity is an approved affiliation with the PKI subscriber; and
- The new validity period will not extend beyond the 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 permitted by the relevant CP, and the parties that may request renewal are not defined in the CP, then renewal requests may only be undertaken by the parties identified in Section 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

Certificate re-key is permitted by this CPS. Certificate re-key rather than renewal is the preferred process to issue a replacement certificate within the Cogito PKIaaS. Re-key indicates issuance of completely new keys and certificates. Where allowed by respective CP and Section 4.3.1 of this CPS, the circumstances for certificate re-key include:

- Normal certificate expiration;
- Certificate revocation;
- Usable life of the current key material has been reached; or
- Change in algorithm, or key length required.

The GRCG 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

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

See relevant CP for further details.

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 Section 4.4.1 (Conduct constituting certificate acceptance).

4.8.6 Publication of the modified certificate by the CA

See Section 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:

- Upon suspected or known compromise of the private key;
- Upon suspected or known loss or compromise of the media holding the private key;
- When a certificate has been issued erroneously or with incorrect content and needs to be reissued;
- When an entity (Subscriber) ceases to be employed or function within the terms and conditions of the original certificate request (e.g. Subscriber is dismissed or moves departments.);
- When an entity fails to comply with obligations set out in the CPS, the relevant CP, or any other agreement or applicable law; or
- If the Gatekeeper Framework or associated services are terminated.

RCA, CA and RA certificates are to be immediately revoked under any of the above conditions.

Revocation would also occur in the event of PKI termination.

Expiry of a certificate shall not require revocation of the certificate.

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 of the RCA or CA certificates due to a business decision to terminate the PKI would be a significant event requiring formal consultation, documentation, and contingency planning. This would be managed by Cogito Group.

Certificate revocation requests may be submitted by the following authorised parties:

- GRCG;
- The Subscriber's CSO, CISO, or ITSM;
- A PKI Operator (for core components);
- A Registration Officer (RO); and
- A subscriber.

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 the 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)

See relevant CP.

4.9.8 Maximum latency for CRLs

All Cogito PKIaaS 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:

- Generate the CRL;
- Transfer the CRL from the CA to the master repository;
- Replicate the master repository to subordinate repositories; and
- Scheduled periods of system unavailability.

4.9.9 Online 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 Section 8.1 (Repositories) and the certificate's CRL Distribution Point in the respective CP for further information.

4.9.10 On-line revocation checking requirements

See relevant CP, otherwise 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, the relevant external parties are to be informed using the mechanisms identified in the arrangement.

4.9.12 Special requirements re key compromise

See 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 Cogito PKIaaS shall store in its internal repository and make available via its internal web site:

- The Root CAs, and all SubCA certificates;
- All valid individual (human) and applicable non-person entity (resource) certificates and cross-certificates; and
- The most up-to-date CRL(s).

Externally, the Cogito PKIaaS 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 Cogito PKIaaS repositories. 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 requires a 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 that have been revoked due to key compromise or have been issued to unauthorised persons must be maintained in the CA's public revocation database for at least 20 years.

Revocation of a CA certificate will require an immediate out-of-sequence CRL publication. Such CRL releases will be notified to subscribers immediately by out-of-band processes e.g. via email distribution list, telephone contact list.

4.10.2 Service availability

The Cogito PKIaaS shall make this service available continuously, except for unavoidable activities. Due to the nature of the internet this service cannot be guaranteed to always accessible.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

A subscription for a certificate ends:

- When a certificate is revoked or allowed to expire;
- When all tokens containing a certificates matching private key have been surrendered to an RA and destroyed in an appropriate manner; or
- 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, recover the entities private confidentiality key and decrypt any data encrypted with the corresponding public key.

Authorised Key Retrievers (AKRs) are either:

i. Subscriber;

ii. A RO who may request key retrieval on behalf of a Subscriber; or

iii. Authorised government officials where criminal or national security matters are involved.

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

The GRCG is to approve any process that provides for the escrow, back-up or archiving and subsequent recovery of private keys, see also Section 6.2.3 (Private key escrow). Documentation of these processes is summarised in the 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

All Cogito PKIaaS approved PKI Facilities are located, constructed, and controlled in accordance with Australian Government PSPF and ISM requirements for PROTECTED protection. Approved government datacentre facilities are used whenever possible.

Section 8 details the responsibilities for Certification and Accreditation (C&A) of PKI facilities.

All PKI facilities (CAs, RAs) are to be operated in suitably controlled environments.

5.1.2 Physical Access

Access to Cogito PKIaaS PKI Facilities is to be restricted to authorised people, and all access monitored and logged.

Datacentre facility staff are not to have access to Cogito PKIaaS PKI assets at any time.

All PKI Core components except the RA operate in No Lone Zone mode.

5.1.3 Power and Air Conditioning

Datacentre facility providers provide all power and air conditioning services and are responsible for facility management.

5.1.4 Water Exposures

Protection from exposure to water is in accordance with datacentre facility standards.

5.1.5 Fire prevention and protection

Prevention and protection from fire is in accordance with datacentre facility 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 the guidance provided in the Protective Security Policy Framework (PSPF) commensurate with the information stored on the media.

5.1.7 Waste disposal

Disposal of waste is in accordance with the Information Security Manual (ISM) commensurate with the information contained upon or within the waste

5.1.8 Off-site backup

Off-site backups are in accordance with the Cogito PKIaaS Disaster Recovery and Business Continuity Plan (DRBCP)

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 Cogito policy for IT systems personnel with special privileges.

The PKI Operations trusted roles include:

- the Operations Manager;
- PKI Operators;
- RA Operators;
- Registration Officer(s) (RO); and
- Security Officer (SO).

For operational management of the Root CA and Subscriber CAs, with the exception of the ROs, each of the above positions requires access to the secure PKI operations facility. Privilege to access this area is controlled by the Operations Manager, based on a number of factors including the risks of human error, theft, fraud, or facilities misuse. The GRCG can authorise the Operations Manager the right to limit, restrict, or extend access privileges to PKI resources. These access privileges include to 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 person control:

- PKI Servers;
- Workstations with administrative or cryptographic administrative access to PKI servers;
- Removeable and portable storage media (data and configuration backups, system images); and
- Removable media containing key material.

Backup, restore, and key recovery tasks, for PKI entities, will be subject to two person control.

RO operations will not be subject to two person control.

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

Any area containing Hardware Security Modules (HSM), servers or other hardware relating to 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, authentication and appropriate security clearance 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 from auditing or authorising a task that they were responsible for.

All tasks accessing the Root CA require multiple operators; including tasks that access the Root CA private keys or HSM.

A RO cannot authorise their own application for a certificate. A single PKI Operator cannot carry out the recovery of a subscriber's private keys.

A PKI Operator carrying out SO duties cannot conduct an audit on work they carried out.

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 the PSPF and are to be appropriately qualified and experienced for their roles.

Any clearance requirements are detailed in the SSP.

5.3.2 Background check procedures

Background checks are performed as part of the Cogito employment process in accordance with the PSPF.

5.3.3 Training requirements

All PKI personnel will be suitably trained in the relevant policy, procedures, and technology required to perform the tasks required of their roles. 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 within the PKI.

PKI and RA operators are to develop and maintain an awareness of security policies. Specific training requirements are detailed in the SSP. In general PKI personnel are to complete training in:

- Basic PKI components;
- Use and operation of PKI hardware, software and associated applications;
- Computer security and procedures;
- Privacy procedures and considerations;
- Disaster recovery and business continuity procedures;
- Risk management procedures; and
- PKI operational policies, plans and procedures.

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

Training will occur:

- When personnel commence their employment;
- Whenever new policies and or procedures are implemented; and
- Whenever the SO or Operations Manager deem that remedial or other training is necessary.

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 Operations Manager may allocate and assign staff members to any suitable training activity, such as:

- Training on the use and features of new/latest release of PKI application software, and the associated database software;
- Training on new/latest release security tools (such as firewalls, routers, application platform security, intrusion detection systems, footprint analysis tools, backup utilities etc.);
- Training on PKI internal processes and procedures; and
- Training on internet security, PKI, and similar topics.

Note: Training topics are to be related to the PKI business plans and activities.

5.3.4 Retraining frequency and requirements

All PKI personnel require ongoing assessments and training updates 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 Operation 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 line managers, who may take administrative or disciplinary action, if appropriate.

Sanctions against contract employees, or other third-party providers (e.g. Data centre facility providers), are to be in accordance with the terms and conditions of their contract, or equivalent SLA or other agreement.

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

In the most extreme of cases, unauthorised actions may constitute terrorist or criminal activity and result in criminal proceedings under appropriate Australian legislation.

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 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 are to include:

- All successful and rejected network connection requests;
- All successful and unsuccessful logins;
- All certificate requests received, accepted and rejected;
- Administering and configuring the PKI system components;
- Administering and configuring privileged user accounts (including permission changes); and
- Significant certificate lifecycle events.

Significant certificate lifecycle events include, but not necessarily limited to:

- Root CA and Subordinate CA Key generation;
- Root CA private key use;
- Signing-key generation requests (new CA accounts);
- Certificate generation requests;
- Certificate propagation to PKI Service Providers and other bilateral interoperability partners;

- Key destruction requests;
- Key destruction verification reports;
- CRL notifications;
- Bilateral (interoperability) certificate revocation notifications;
- Private key removal;
- Tamper detection with private key devices (e.g. HSMs);
- Certificate signer and RO console access; and
- Certificate signer and RO private key use.

The recorded log information shall include a minimum of:

- Date/time stamp;
- Event target;
- Event source;
- Event description; and
- CA/RA event status (Success or 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 National Archive policy.

5.4.4 Protection of audit log

Protection of audit log information is in accordance with the Cogito policy for the protection of security log information for systems processing, commensurate with the level of data being protected.

5.4.5 Audit log backup procedures

Backup of audit logs occur daily. Where log information processing into a common format for analysis occurs, both raw and processed log data are backed up.

5.4.6 Audit collection system (internal vs external)

The audit collection system is a combination of automated and manual processes performed by the operating system and operational personnel.

Audit logs are to be exportable from the host system and able to be manually reviewed (human readable), but not altered.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

Vulnerability assessments are in accordance with the requirements of the Gatekeeper framework commensurate with the level of data being processed.

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.

5.5.2 Retention period for archive

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

5.5.3 Protection of archive

Archive media is protected by physical security and cryptographic protection commensurate with the contents and in accordance with the provisions of the PSPF and ISM.

5.5.4 Archive backup procedure

Archive backup is in accordance with the Cogito PKI backup procedures and technical guides. The archive backup procedures are in accordance with the DRBCP.

5.5.5 Requirements for timestamping 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)

Archiving is performed by PKI Operations personnel.

Key pairs will be archived and retrieved using the procedures documented in the CKMP.

5.5.7 Procedures to obtain and verify archive information

Digital signatures are applied to provide authentication and integrity confirmation of the archive records.

5.6 Key changeover

The 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 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:

- Key or CA systems compromise has occurred, is suspected, or cannot be discounted;
- The incident was deliberate or accidental;
- Procedures require to be modified, to address the circumstances that enabled the incident to occur; and
- 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.

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:

- Physical investigation of disaster and collection of necessary evidence to complete investigation - sign off as required by GRCG;
- Re-establishment of secure environment for PKI operations - temporary measures are acceptable but require detailing in the DRBCP or sign off by the GRCG;

- Reconstitute the ability to issue CRLs and process revocation requests - this includes audit functionality;
- Reconstitute the ability to receive, process and issue certificates;
- Return to stable operating conditions;
- Update documentation to reflect any changes as a result of recovery - including to processes, procedures and configuration; and
- Provide an incident closure report to the GRCG.

5.8 CA or RA termination

In the event of a CA or RA termination or a CA or RA ceasing operation, and its certificate requires revocation (i.e. it cannot be allowed to expire or has not already expired) it will be revoked. Self-signed CAs shall follow notification procedures equivalent to key compromise (if required. Termination of CAs, where possible, should minimise impact on subordinate certificates. The GRCG receives notification of planned and actual terminations.

Should revocation or notification be required, the Cogito PKIaaS CA will give as much notice as is possible in the relevant circumstances and the actions of the Cogito PKIaaS CA proposes for the benefit of all Subscribers and all Relying Parties of which the Cogito PKIaaS CA is aware. Where the Cogito PKIaaS intends to terminate its own services, it will attempt to give a minimum of 3 months notice to affected parties, including the Gatekeeper Competent Authority.

Where possible Cogito as the operator of the Cogito PKIaaS RA and CA services, will endeavour to continue the maintenance of a CRL or OCSP service in accordance with contractual arrangements with agencies and any relevant Approved documents.

Cogito will work with the DTA and other Service Providers to achieve a migration of agencies and subscribers to a new Gatekeeper accredited CA if this is requested by the customer and can be supported by Cogito.

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:

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

See relevant CP for description of key pair generation.

The PKI CKMP details the products, processes and procedures and the approved combinations, that are valid.

6.1.2 Private key delivery to the 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 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 GRCG to third party CAs, where a cross certification (or equivalent) agreement is in place.

6.1.5 Key Sizes

Key sizes are defined in the CKMP 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. Public key parameters shall be generated in accordance with NCA approved guidelines. Parameter quality checking (including primarily testing for prime numbers) shall be performed in accordance with NCA approved guidelines.

6.1.7 Key usage (as per X.509 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.509 v3 compliant software. The correct values for key usage are set in these fields in accordance with the X.509 v3 standard but Cogito 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.509 v3 standard and is outside of the control of the Cogito PKIaaS.

See the relevant CP for key usages.

6.2 Private key production and cryptographic module engineering controls

6.2.1 Cryptographic module standards and controls

All cryptographic modules used with PKI core components comply with ISM requirements, specifically in complying the Common Criteria scheme Evaluation Assurance Level 4 (EAL4) and US Federal Information Processing Standard Publication 140-3 (FIPS-140-3) requirements.

6.2.2 Private key (n of m) control

All CA and RA operations involving generation of Private Keys require a minimum of 2 persons and a minimum of two m-of-n access factors to private keys (on HSMs) each with unique passcodes.

A minimum of two passwords, passphrases, or passcodes are required to access all critical PKI components handling private keys (e.g. HSM, CA servers, etc.), and are to comply with, or exceed, ISM password structure and management requirements.

All CA and RA operations involving generation of Private Keys by the Root CAs and Sub CAs, require a minimum of 2 persons, and access to private keys (on HSMs) requires 2-of-6 smart card token authorisation, each with unique passcodes.

The PKI Operations Manual and SSP are to ensure that CA and RA key certification requests require two authorised operators to generate. Key generation of PKI entities (CA and RA components) are to be conducted in a suitable secure area, requiring multiple personnel to fulfil specific roles for key ceremony.

Root CAs are to be offline at all times. Access to a Root CA for CA key generation requests and self-certification requests require a minimum of 2 personnel.

Sub CA systems are to have a minimum of 2 personnel trained and authorised in PKI.

No single person is to be able to fully access and operate any components of the PKI systems that contain or generate Private Keys, Root CA or Sub CA Certificates, and Root CA CRL generation.

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 Key Archive Server (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. Where such keys must be transferred to other media for 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. Where these keys are stored on hard tokens, the archive copy is also to be a hard token.

All components of the backed-up key are to be stored in a separate, geographically dispersed site.

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

Key components and access codes are to be stored and transported separately in individual sealed envelopes, within approved security containers or safe-hand bags.

Backup key components will be retrieved from storage upon expiry of their key usage period, securely erased and destroyed under supervision by the PKI Auditor and/or subscriber representatives.

6.2.5 Private key archive

Archive of end entity private authentication keys does not occur.

Private keys will not be archived upon expiry of their key usage period, and devices containing backup key components will be destroyed.

6.2.6 Private key transfer into or from a cryptographic module

The transfer of private authentication keys from, or into, a cryptographic module does not occur except for the duplication of keys for the PKI core components. Where this occurs, it is done by a product on the ASD Evaluated Product List.

Any confidentiality keys that are transported into or from the cryptographic module are transferred using the PKI Software confidentiality key(s).

RA Operator and subscriber keys cannot be exported from hardware tokens.

6.2.7 Private key storage on cryptographic module

All private keys will be generated and stored by dedicated and ASD approved cryptographic modules, commensurate with the data to be protected by the CA and Certificates associated with the private keys.

Within the PKI environment in general, private keys are either stored encrypted, stored protected by a password, or stored password protected in hardware (such as an HSM, USB token, or smart card).

The private keys are stored in a protected secure facility and only accessible with the cryptographic module (i.e. HSM).

6.2.8 Method of activating private key

See relevant CP.

6.2.9 Method of deactivating private key

Deactivation of private keys is in accordance with a method approved by the NCA and summarised in the relevant CP.

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 CKMP.

6.2.10 Method of destroying private keys

PKI positions of trust can destroy private keys. HSMs and hard tokens will be re-initialised to destroy the stored private keys.

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 Section 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 Section 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. 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 CKMP and the applicable CP.

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 the CKMP.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

The Cogito PKIaaS has established an ICTSP and SSP for computer security technical requirements for PKI operations. These documents are only available to Cogito personnel on a need-to-know basis.

Appropriate levels of trustworthiness and security exist throughout the PKI. Security meets or exceeds the requirements mandated under Gatekeeper for a High Assurance service. Controls in place include:

- A configuration baseline and a configuration change control process;
- Performance of regular and frequent systems operability tests to prove the correct operation of critical PKI components;
- Strong authentication required for core PKI system access;
- Proactive user account management including comprehensive auditing and timely removal of access;
- Role segregation and No-Lone Zone procedures;
- Restrictions and controls on the use of system utilities;
- Secure deletion of cryptographic material in accordance with COMSEC requirements;
- The use of monitoring and alarm systems to detect and warn of unauthorised access to computer system resources; and
- Logging of all system access and use.

6.5.2 Computer security rating

All facilities and equipment have been constructed or selected to satisfy appropriate PSPF and ISM security requirements, as per Section 6.5.1.

6.6 Life cycle technical controls

6.6.1 System development controls

The software development controls applied in the development of the CA software has been evaluated and certified to meet or exceed the requirements of ITSEC E3 or Common Criteria EAL4.

Changes in the production environment are tested in the Cogito PKIaaS test environment, which is operated and maintained within a physically secure environment. Proposed changes are then approved for deployment under the PKIaaS Change Control Management Procedures.

6.6.2 Security management controls

Security management controls exist to ensure that PKI systems are operating correctly and 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 Operations Manager is responsible for maintaining the configuration baseline and for managing any changes in accordance with the SSP. The SO 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 SSP.

Regular audits are conducted to check the baseline configuration matches the actual system components deployed and the change control register.

6.6.3 Lifecycle security controls

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

6.7 Network security controls

The Cogito PKIaaS network security controls include:

- Firewalls;
- Strong authentication;
- Physical access controls;
- Mechanisms to prevent denial-of-service attacks; and
- Password and other logical access control.

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. The PKI network is a discrete network, strictly controlled by Cogito Group. The only network traffic allowed is from authorised PKI entities and essential core services such as directories, validation, time and synchronisation with any back-up or alternate sites. All other traffic is denied by default. Direct access to networks external to Cogito Group (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

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. Directories use the DN for lookups. Names are to be meaningfully related to the identity presented for EOI check and relate directly to the identity of the subscriber, 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

Refer to relevant CP for details.

7.1.7 Usage of policy constraints extension

See relevant CP.

7.1.8 Policy qualifiers syntax and semantics

The certificate policies extension will be used to clearly indicate the policy under which the Root CA and CA certificates have been issued and the purposes for which the certificates may be used.

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 a version number as described in the X.509 standard [ISO/IEC 9594-8:2014]. CRLs shall assert Version 2.

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 Cogito PKIaaS Validation Authority Certificates for a full OCSP profile.

8 Compliance Audit and Other Assessments

All infrastructure elements in the Cogito PKIaaS, including the 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 PKIaaS 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).

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 GRCG to assure that they comply with this CPS and relevant CPs.

In accordance with Gatekeeper requirements, the Cogito PKIaaS must undergo an annual compliance audit.

8.2 Identity/qualifications of assessor

Auditors receive approval by the GRCG (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:

- Maintains compliance with Accreditation criteria and policies; and
- 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 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 GRCG. The GRCG 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 GRCG. 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 DTA.

9 Other business and Legal Matters

9.1 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.

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

Cogito Group has sufficient resources to meet their perceived obligations under this CPS. The associated PKIaaS services are to be made 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 Cogito PKIaaS and an end entity, or Relying Party.

The Cogito PKIaaS 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 Confidentially of business information

9.3.1 Scope of Confidential information

The following information is considered confidential and protected against disclosure using a reasonable degree of care:

- Private Keys;
- Activation data used to access Private Keys or to gain access to the CA system;
- Business continuity, incident response, contingency, and disaster recovery plans;
- Other security practices used to protect the confidentiality, integrity, or availability of information;
- Information held by Cogito Group as private information in accordance with Section 9.4;
- Audit logs and archive records; and
- Transaction records, financial audit records, audit trail records, and any audit reports (with the exception of an auditor's letter confirming the effectiveness of the controls set forth in this CP/CPS).

9.3.2 Information not within the scope of confidential information

Any information not listed as confidential is considered public information. Published certificate and revocation data is considered public information.

9.3.3 Responsibility to protect confidential information

Cogito Group's employees, agents, and contractors are responsible for protecting confidential information and are contractually obligated to do so. Employees receive training on how to handle confidential information. RAs are contractually required to protect confidential information.

9.4 Privacy of personal information

9.4.1 Privacy Plan

The Cogito PKIaaS Privacy Notice conforms to the requirements of the Privacy Act 1988(Cth) (Privacy Act) and Information Privacy Act 2014(Cth). The Privacy Notice is posted on the Cogito Group website at: https://www.cogitogroup.net/privacy/

9.4.2 Information treated as private

Cogito Group treats all personal information about an individual that is not publicly available in the contents of a certificate or CRL as private information. Cogito Group protects private information using appropriate safeguards and a reasonable degree of care.

9.4.3 Information not deemed private

Subscribers (Identity Certificates) using the Cogito PKIaaS 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 Cogito 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 Cogito PKIaaS 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 entity is disclosed to any external entities to Cogito Group unless the disclosure is in accordance with the Privacy Act (including APP 6). Cogito Group personnel are entitled to access Personal Information about themselves in the PKI in accordance with APP 12 of the Privacy Act.

Only authorised PKI staff, under two party control, are permitted to access data about individual entities. 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 individual 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 (email 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:

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

9.6 Representations and Warranties

9.6.1 CA representations and warranties

Except as expressly stated in this CP/CPS or in a separate agreement with a Subscriber, Cogito Group does not make any representations regarding its products or services. Cogito Group represents, to the extent specified in this CP/CPS, that Cogito Group:

- Complies, in all material aspects, with this CP/CPS and all applicable laws and regulations;
- Publishes and updates CRLs and OCSP responses on a regular basis;
- Does not warrant the accuracy, authenticity, completeness, or fitness of any unverified information;
- Is not responsible for information contained in a certificate except as stated in this CP/CPS;
- Does not warrant the quality, function, or performance of any software or hardware device; and
- Is not responsible for failing to comply with this CP/CPS because of circumstances outside of Cogito Group's control.

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:

- 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;
- Verify that the digital certificate is being used within the limits specified in the CP under which the digital certificate was issued; and

- Promptly notify the Cogito PKIaaS 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 COGITO GROUP 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 Cogito PKIaaS 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 Cogito PKIaaS 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 Cogito Group is not liable for:

- Any use of certificates, other than uses specified in this CPS or the relevant CP;
- Falsification of transactions;
- Improper use or configuration of equipment, not operated under the responsibility of the PKI, used in transactions involving certificates;
- Compromise of private keys associated with the certificates;
- Loss, exposure, or misuse of PIN code(s) etc. protecting private keys associated with the certificates;
- Erroneous or incomplete requests for operations on certificates;
- Delays arising from Force Majeure;
- The use of public or private keys of cross certified (non-subordinate) CAs and their Relying Parties; and
- Any termination of the PKI or any related contract by Cogito Group.

In the absence of any documented contractual relationship between the CA and a Subscriber (other than a Subscriber Agreement) and/or Relying Party, Cogito Group does not accept any

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

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

9.9 Indemnities

By using or accepting a certificate, each Subscriber and Relying Party agrees to indemnify and hold Cogito Group, 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 Cogito Group, 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:

- Misrepresentation or omission of material fact in order to obtain or use a Certificate, whether or not such misrepresentation or omission was intentional;
- Violation of the Subscriber Agreement, Relying Party Agreement, this CPS, the relevant CP, or any applicable law;
- Compromise or unauthorised use of a Certificate or Private Key caused by the negligence of that party and not by Cogito (unless prior to such unauthorised use Cogito has received an authenticated request to revoke the Certificate);
- Use or reliance on a Certificate or Private Key; or
- Misuse of a Certificate or Private Key.

The Subscriber and its affiliated entities and individuals recognise that Cogito Group 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

Cogito), 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 Cogito Group, 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 notice of their termination is communicated by the Cogito PKIaaS on its repository or website.

The CPS is available at: http://pki.gatekeeper.securesme.com/

9.10.2 Termination

The entire PKI may be terminated at any time by Cogito Group. All existing certificates expired or unexpired, revoked, or active, will be deemed unfit for further use. Cogito Group is not required to revoke existing certificates in this event. All CRLs may only be used for historic or evidentiary purposes upon CA termination. Cogito Group is not required to give any notice to end entities before or after CA termination, however, before the Cogito PKIaaS terminates its services, it will attempt to:

- Inform entities and subordinate RAs;
- Make widely available information of its termination; and
- Stop issuing certificates and CRLs.

In accordance with the Gatekeeper Memorandum of Agreement, Cogito Group will inform the Gate Keeper 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:

- Intellectual Property Rights;
- Confidential Information;
- The protection of Personal Information; or
- 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 Cogito PKIaaS 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:

- It is hand-delivered to a physical address - at the time of delivery whether or not any person is there to receive it;
- 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;
- It is transmitted by facsimile - when the sending machine produces a report showing the transmission was successful;
- It is sent by e-mail - when it enters a system under the control of the addressee; or
- 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 Section 1.5.4). Rephrasing provisions to improve their clarity as well as and typographical corrections, changes to contact details are not considered amendments, however, any change must be brought to the attention of the GRCG and Gatekeeper Competent Authority to seek their concurrence.

9.12.2 Notification mechanism and period

The amended CPS and/or a CP shall be published on the Cogito PKIaaS 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 change (editorial changes etc. see 9.12.1 are not amendments).

If a change in Cogito Group's CPS or CP is determined by the GRCG to warrant a change in the currently specified OID for a particular type of certificate, the revised version of the CP will also contain an revised OID for that type of certificate.

9.13 Dispute resolution provisions

Parties are required to notify Cogito Group and attempt to resolve disputes directly with Cogito Group before resorting to any dispute resolution mechanism, including adjudication or any type of alternate dispute resolution.

Nothing in this clause prevents Cogito Group from preventing a party from accessing the Cogito PKIaaS or commencing proceedings against a Subscriber for a breach of the Subscriber agreement.

9.14 Governing law

The governance of 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 Cogito PKIaaS 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 of this CPS and any relevant CP must comply with all relevant:

- Laws; and
- Australian Government security policies, such as the Protective Security Policy Framework (PSPF), Information Security Manual (ISM), Gatekeeper PKI Framework along with policies embedded within the overarching Frameworks.

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, 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 Cogito Group's prior written approval.

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.

9.16.6 Other provisions

No stipulation unless otherwise specified in relevant legal agreements.

APPENDIX A. CAs Operating Under this CPS

The CAs operating under this CPS are listed below:

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 certificates comply with the relevant accreditation frameworks (policy, security and legal). Principally these will consist of the DTA.
Application (Request)	A formal request to be considered for a position or to be allowed to do or have something, submitted to an authority, institution, or organization.
Application (Software)	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 GRCG 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	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 for the whole of the Australian Capital Territory. Traditionally such days are from 0900 to 1700.
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; and 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 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 file which lists the Digital Certificates that have been revoked by the Issuing CA before their scheduled expiration.
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.
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 "Application Web Handler". Where technically required, the Common Name can be the resources domain name.
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.

Custodian	A person who has custody of something, a keeper or guardian; in the context of PKI, usually a Key Custodian.
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)	A 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.
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.cyber.gov.au/acsc/view-all-content/epl-products 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	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. See also Protection Profile.

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. An act of employing or putting into play.
Gatekeeper	The Commonwealth Government strategy to develop Public Key Infrastructure to facilitate Government online service delivery and electronic 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.
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.
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 the subscriber.
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 PKIaaS. 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).
Operational CA	A CA that issues and manages end-entity certificates.
Operator	Any individual who is assigned keys and certificates to perform functions within the PKI. They are not regarded as either Subscribers or Relying Parties for the purposes of the PKIaaS.
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.
PKI Operations Manager	Manages PKI Operations of the PKIaaS.
PKI Operator	PKI Operators perform day to day operations, maintenance and support of the PKI systems managed as part of the PKIaaS.

PKI Software	Software programs that manage digital certificate lifecycle operations and token management.
PKI Systems Administrator	A PKI Systems Administrator performs system administration tasks on the PKIaaS systems.
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 an asymmetric key pair that must be kept secret to ensure confidentiality, integrity authenticity and non-repudiation.
Private Signing Key	A private key used to digitally sign messages on behalf of the relevant certificate Subject.
Protection Profile	A document that stipulates the security functionality that must be included in Common Criteria evaluation to meet a range of defined threats. Protection Profiles also define the activities to be taken to assess the security function of an evaluated product.
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.
Public Key Technology (PKT)	Public Key Technology is the hardware and software used for encryption, signing and 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 Registration Authority (RA) to perform RA functions in accordance with this CPS, the relevant Certificate Policy and other applicable documentation.
Re-Key	A Subscriber or other participant generating a new keypair 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 Network Resource, Application, code, electronic service or process, Device, or data object that is capable of utilising a Certificate.
Resource Administrator	The Resource 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 resource.
Revoke	To terminate a certificate prior to the end of its operational period.
Root CA	A CA that is the top of a certificate chain, i.e. its own certificate is self-signed.
Subordinate CA (SubCA)	A CA which has been established under the certificate path of a Root CA. A SubCA usually issues certificates to end entities and manages those certificates. 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; or 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.
Token	A hardware security device containing a user's Private Key(s), and Public Key Certificate.
Transport Layer Security (TLS)	A cryptographic protocol that provides security for communications over networks such as the Internet. TLS encrypts the segments of network connections at the Transport Layer end-to-end.
Universally Unique Identifier (UUID)	A universally unique identifier is a 128-bit label used for information in computer systems. The term globally unique identifier is also used, often in software created by Microsoft (GUID). When generated according to the standard methods, UUIDs are, for practical purposes, unique. See RFC 4122.
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 PKIaaS Validation Authority provides certificate status information through the provision of OCSP responders.

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 GRCG is the authoritative source of definitions relating to the Cogito PKIaaS, any requirement for clarification can be referred to the GRCG.

B.2 Acronyms

ACT	Australian Capital Territory

AKR	Authorised Key Retriever
ASD	Australian Signals Directorate
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
DRBCP	Disaster Recovery and Business Continuity Plan
DTA	Digital Transformation Agency
EAL	Evaluated Assurance Level
EOI	Evidence of Identity
EPL	Evaluated Products List
GRCG	Governance Risk and Compliance Group
HSM	Hardware Security Module
ICTSP	Information and Communication Technology Security Plan
IEC	International Electrotechnical Commission
IETF	Internet Engineering Taskforce
IP	Intellectual Property
IPR	Intellectual Property Rights
ISM	Australian Government Information Security Manual
ISO	International Standards Organisation
ITSEC	Information Technology Security Evaluation Critieria
KAS	Key Archive Server
KMP	Key Management Plan
LTSK	Long Term Key Storage
NCA	National Cryptographic Authority

OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKT	Public Key Technology
PSPF	Protective Security Policy Framework
RA	Registration Authority
RCA	Root Certification Authority
RFC	Request for Comment
RO	Registration Officer
SO	Security Officer
SRMP	Security Risk Management Plan
SSP	System Security Plan
URI	Uniform Resource Identifier
UTC	Coordinated Universal Time

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.