Australian Competition and Consumer Commission Certificate Policy (ACCC CP)

Version: 1.03

Date of Publication: 20 April 2023

TABLE OF CONTENTS

TABLE OF TABLES

Revision History

Date	Document Number	Revision Number	Updates
14 May 2020	1	1.01	Initial release
11 June 2020	1	1.02	Minor amendments to s9 and s2.1.1, correction of reference errors in s5.5.1 and s9.13.2
20 April 2023	1	1.03	Minor amendment to s1.1.1 to specify that DigiCert has been engaged as a certificate authority service, and not the sole certificate authority.

1. INTRODUCTION

1.1 OVERVIEW

A Certificate issued in accordance with this Certificate Policy (CP) conveys a level of digital identity assurance associated with the Subject of the Certificate. A Certificate Subject may be an individual person; a role; a Server, application, or Device, subject to the rules concerning each described in this CP. Entities adopting this standard Certificate Policy as their own do so to ensure interoperability between their Entities and other Entities within the ACCC communities.

1.1.1 Structure of this Certificate Policy and relationship to the Certification Practice Statement

ACCC has created a set of specifications and requirements governing the implementation and operation of Certification Authorities, Registration Authorities, and other Public Key Infrastructure (PKI) components; and deals with:

- PKI Technical Standards;
- Certificate Policies (CP), including this CP;
- Requirements for Certification Practice Statements (CPS); and
- Any Subscriber or Relying Party Agreements, templates and other ACCC PKI guidelines.

This CP only applies to any certificates issued by, or under the authority of, ACCC or any of its entities directly or subsequently under the ACCC Root Certification Authority within the ACCC PKI.

The headings of this CP follow the framework set out in the Internet Engineering Task Force Request for Comment 3647 ("RFC 3647"). Additional sections or headings have been introduced where necessary for the purposes of this CP.

The provisions of this CP prevail over the provisions of the ACCC CPS to the extent of any direct inconsistency.

ACCC has engaged DigiCert as a Certificate Authority service provider. The provisions of the DigiCert Private PKI CP/CPS (https://www.digicert.com/legal-repository/) are provided for information, as they are part of the ACCC's arrangements with DigiCert.

Subscribers and Relying Parties agree to the terms of this CP, and accept that it governs the terms of their use of the ACCC PKI. Subscribers and Relying Parties are responsible for any costs or loss claimed by DigiCert from the ACCC in respect of Subscribers and Relying Parties use of and access to the ACCC PKI.

1.2 IDENTIFICATION

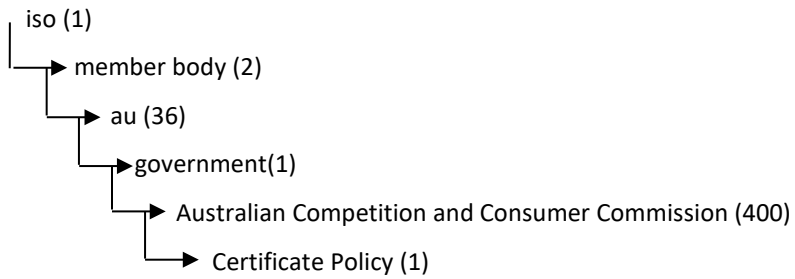
1.2.1 Certificate Policy Name

This document shall be named the **ACCC Certificate Policy**.

There are levels in this Certificate Policy, which are defined in subsequent sections. Each level has an assigned object identifier (OID) to be asserted in the Certificate Policies extension of certificates issued by CAs who comply with the applicable policy requirements.

1.2.2 Object Identification

Certificates issued in accordance with this CP shall be known by the Object Identifiers (OIDs) identified below. OIDs are registered by ACCC under the ACCC Arc as follows:



1.3 PKI PARTICIPANTS

1.3.1 Policy Management Authority (PMA)

The ACCC Policy Management Authority (PMA), manages the design, development, governance, implementation, and the overall operation of the ACCC PKI. The PMA is responsible for:

- Maintaining and publishing this CP;
- Reviewing and approving the CPS for compliance with this CP, for each CA that issues certificates under this CP;
- Reviewing periodic Compliance Audits to ensure that CAs are operating in compliance with their approved CPSs; and
- Ensuring continued conformance of each CA that issues certificates under this CP with applicable requirements as a condition for allowing continued participation.

The ACCC will perform the role of PMA in its capacity as the Consumer Data Right Accreditation Registrar.

1.3.2 Operational Authority (OA)

The ACCC PKI Operational Authority consists of the organisations that are responsible for the operation of the ACCC PKI, including issuing Certificates when directed by the ACCC PMA or any authorised ACCC Registration Authority (RA) operating under this CP, posting those Certificates and Certificate Revocation Lists (CRLs) into the repositories of the ACCC PKI, and ensuring the continued availability of these repositories to all users in accordance with section 2 of this document.

1.3.3 Root Certification Authority (RCA)

The ACCC PKI Root Certification Authority (RCA) is the Root CA (or Root CAs) of the ACCC PKI. Each ACCC PKI Root CA is a trust anchor for Relying Parties trying to establish the validity of a Certificate issued by an ACCC PKI Sub CA, whose chain of trust can be traced back to that specific Root CA.

The ACCC PKI Root CA(s) issue and revoke Certificates to ACCC PKI Sub CAs upon authorisation by the ACCC PMA. As operated by the Operational Authority, the ACCC PKI Root CAs are responsible for all aspects of the issuance and management of those Sub CA Certificates, as detailed in this CP, including:

- The certificate generation process;
- Publication of certificates;
- Revocation of certificates;
- Generation and destruction of CA signing keys; and
- Ensuring that all aspects of the CA services, operations, and infrastructure related to certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of this CP.

1.3.4 Subordinate Certification Authorities (SubCA)

The ACCC Subordinate CAs (SubCAs) are all of the ACCC PKI Intermediate and End-Entity Issuing CAs subordinate to an ACCC Root CA as defined below.

An Intermediate CA is a CA which is not a Root CA and whose primary function is to issue Certificates to other CAs. Intermediate CAs may or may not issue Certificates to End-Entities.

An Issuing CA is a CA whose primary function is to issue Certificates to End-Entities. An Issuing CA does not issue Certificates to other CAs.

As operated by the Operational Authority, an ACCC Sub CA is responsible for all aspects of the issuance and management of an end-entity Certificate, as detailed in this CP, including:

- The control over the registration process;
- The identification and authentication process;
- The Certificate manufacturing process;
- The publication of Certificates;
- The revocation of Certificates; and
- Ensuring that all aspects of the services, operations and infrastructure related to Certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of this CP.

1.3.5 Registration Authorities (RA)

The Registration Authority (RA) is the entity that collects and verifies each Subscriber's identity and information that is to be entered into the identity's public key certificate. The RA performs its function in accordance with a CPS approved by the PMA. The RA is responsible for:

- Control over the registration process; and
- The identification and authentication process.

An RA shall possess a certificate of assurance equal to or greater than that of the certificate being issued and protected as described in Sections 6.1.1 and 6.2.1.

1.3.6 Subscribers

A Subscriber is the entity whose name appears as the subject in a Certificate, who asserts that it uses its key and Certificate in accordance with the Certificate Policy asserted in the Certificate, and who does not itself issue Certificates. This entity has the duty to protect the Certificate that is provided to him/her/it as expressed in the General Terms and Conditions related to this CP. ACCC PKI Subscribers may include individuals, organisations, network or hardware Devices such as firewalls and routers, Servers, or aircraft and/or aircraft equipment. A Device Sponsor will assume the tasks and responsibilities of a "Subscriber" in this CP when the term "Subscriber" could be referenced or applied to a Device.

1.3.7 Device Sponsors

A Device Sponsor is an entity (eg, company or individual) who requests a certificate on behalf of a Subscriber that is a Device, Server or Appliance within the ACCC PKI ecosystem. The Device Sponsor asserts that the Device, Server or Appliance shall use the key and certificate in accordance with the certificate policy asserted in the certificate. A Device requires a representative to act on its behalf and vouch for the Device identity, this person is the Device Sponsor. The Device Sponsor is ultimately responsible to supply the CA with all identification data required for the certificate issuance.

1.3.8 Relying Party

A Relying Party is the entity that relies on the validity of the binding of the Subscriber's name to a Public Key. The Relying Party is responsible for deciding how to check the validity of the Certificate by checking the appropriate Certificate status information. The Relying Party can use the Certificate to verify the integrity of a digitally signed

message, to identify the creator of a message or document, or to establish confidential communications with the holder of the Certificate. A Relying Party may use information in the Certificate (such as Certificate Policy identifiers) to determine the suitability of the Certificate for a particular use.

The Relying Party must first select the Certificate appropriate for meeting the needs of that application. This will be determined by evaluating various risk factors including the value of the information, the threat environment, and the existing protection of the information environment. These determinations are made by the Relying Party and are not controlled by the ACCC PMA.

1.3.9 Certificate Status Authority (CSA)

A CSA is an authority that provides status of Certificates or certification paths. A CSA can be operated in conjunction with the CAs or independent of the CAs. Examples of a CSA are:

- Online Certificate Status Protocol (OCSP) Responders that provide revocation status of Certificates.
- Server-based Certificate Validation Protocol (SCVP) Servers that validate certifications paths and/or provide revocation status checking services.

OCSP Responders that are keyless and simply repeat responses signed by other Responders and SCVP Servers that do not provide Certificate validation services shall adhere to the same security requirements as repositories.

ACCC CAs that issue Certificates must provide an OCSP Responder.

An ACCC Root CA must not provide Certificate status via OCSP.

1.3.10 Time-Stamp Authority (TSA)

A TSA is an authority that issues and validates trusted timestamps. A TSA can be operated in conjunction with a ACCC CA or independent of the ACCC CA as approved by the ACCC PMA and in accordance to RFC 3161.

1.3.11 Other Participants

1.3.11.1 Related Authorities

The CAs and RAs operating under this CP may require the services of other security, community, and application authorities, such as compliance auditors and attribute authorities. The CPS shall identify the parties responsible for providing such services, and the mechanisms used to support these services.

1.3.11.2 Trusted Agent

A Trusted Agent is appointed by the PMA and may collect and verify Subscriber identity and information on behalf of an RA. Information shall be verified in accordance with section 3.2 and communicated to the RA in a secure manner.

A Trusted Agent shall not have direct access to the CA to enter or approve Subscriber information.

1.4 CERTIFICATE USAGE

1.4.1 Appropriate Certificate Uses

Appropriate certificate uses include, but are not limited to, the following:

- Certificates issued under this CP may be used for Digital Signature functions between or within businesses where a certain degree of identification as to company affiliation is required, such as systems access, and transaction validation. This may include communication of, and access to, non-sensitive client and company information. When used for Digital Signature purposes, the Relying Party may be reasonably assured as to the identity and corporate affiliation of the Subscriber.

- CAs may require Device Sponsors to use certificates issued under the same PKI for Authentication purposes when requesting Device certificates. Device Sponsor identity certificate requirements, if needed, shall be defined in the ACCC's CPS.

1.4.2 Prohibited Certificate Uses

Prohibited applications include the following:

- Any export, import, use or activity that contravenes any local or international laws or regulations;
- Any usage of certificates in conjunction with illegal activities;
- Any usage of certificates for personal use or purposes not related to the community's business;
- Any use of a certificate after it has been revoked;
- Any use of a certificate after it has expired;
- CA-certificates may not be used for any functions except CA functions. In addition, end-user Subscriber certificates shall not be used as CA-certificates.

1.5 POLICY ADMINISTRATION

1.5.1 Organization Administering the Document

ACCC PMA is responsible for all aspects of this CP.

1.5.2 Contact Person

Questions relating to this CP can be directed to:

ACCC PKI PMA
PMA Administrator
Email: CDRTechnicalOperations@accc.gov.au

1.5.3 Person Determining CPS Suitability for this CP

The ACCC PMA determines the suitability and applicability of this CP and the conformance of a CPS to this CP based on the results and recommendations received from PKI Auditors and/or Subject Matter Experts. The ACCC PMA is also responsible for evaluating and acting upon the results of compliance audits. Additionally, the auditor may not be the author of the CP or the CPS. The ACCC PMA shall determine the auditor's suitability.

1.5.4 CP Approval Procedures

The ACCC PMA approves the CP and any amendments. Amendments are made by either updating the entire CP or by publishing an addendum. The ACCC PMA determines whether an amendment to this CP requires notice or an OID change.

Updates supersede any designated or conflicting provisions of the referenced version of the CP.

1.6 DEFINITIONS AND ACRONYMS

1.6.1 Definitions

Accreditation	Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.
Activation Data	Secret data (eg, password, PIN code) that is used to perform cryptographic operations using a Private Key.
ACCC Directory	Repository accessible only to ACCC internal End-Entities and Relying Parties.

Authority Revocation List (ARL)	A list of revoked Certification Authority Certificates. Technically, an ARL is a CRL.
Authentication	The process whereby one party has presented an identity and claims to be that identity and the second party confirms that this assertion of identity is true.
Audit	An Independent review and examination of documentation, records and activities to access the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies or procedures.
Certificate	A Certificate is a data structure that is digitally signed by a Certification Authority, and that contains the following pieces of information: • The identity of the Certification Authority issuing it. • The identity of the certified End-Entity. • A Public Key that corresponds to a Private Key under the control of the certified End-Entity. • The Operational Period. • A serial number. The Certificate format is in accordance with ITU-T Recommendation X.509 version 3. (RFC 5280)
Certification Authority (CA)	A Certification Authority is an entity that is responsible for authorising and causing the issuance or revocation of a Certificate. By extension, the term "CA" can also be used to designate the infrastructure component that technically signs the Certificates and the revocation lists it issues. A Certification Authority can perform the functions of a Registration Authority (RA) and can delegate or outsource this function to separate entities. A Certification Authority performs three essential functions. First, it is responsible for identifying and authenticating the intended Authorised Subscriber to be named in a Certificate, and verifying that such Authorised Subscriber possesses the Private Key that corresponds to the Public Key that will be listed in the Certificate. Second, the Certification Authority actually creates and digitally signs the Authorised Subscriber's Certificate. The Certificate issued by the Certification Authority then represents that CA's statement as to the identity of the person named in the Certificate and the binding of that person to a particular public-private key pair. Third, the Certification Authority creates and digitally signs the Certificate Revocation Lists and/or Authority Revocation Lists.
Certificate Extension	A Certificate may include extension fields to convey additional information about the associated Public Key, the Subscriber, the Certificate Issuer, or elements of the certification process.
Certificate Manufacturing	The process of accepting a Public Key and identifying information from an authorised Subscriber, producing a digital Certificate containing that and other pertinent information, and digitally signing the Certificate.
Certificate Policy (CP)	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. Within this document, the term CP, when used without qualifier, refers to the ACCC CP, as defined in section 1.

Certification Practice Statement (CPS)	A statement of the practices, which a CA employs in issuing and revoking Certificates, and providing access to same. The CPS defines the equipment and procedures the CA uses to satisfy the requirements specified in the CP that are supported by it.
Certificate Request	A message sent from an applicant to a CA in order to apply for a digital certificate. The certificate request contains information identifying the applicant and the Public Key chosen by the applicant. The corresponding Private Key is not included in the request, but is used to digitally sign the entire request. If the request is successful, the CA will send back a certificate that has been digitally signed with the CA's Private Key.
Certificate Revocation List (CRL)	A list of revoked Certificates that is created, time stamped and signed by a CA. A Certificate is added to the list if revoked (eg, because of suspected key compromise, distinguished name (DN) change) and then removed from it when it reaches the end of the Certificate's validity period. In some cases, the CA may choose to split a CRL into a series of smaller CRLs. When an End-Entity chooses to accept a Certificate the Relying Party Agreement requires that this Relying Party check that the Certificate is not listed on the most recently issued CRL.
Certificate Status Authority (CSA)	A CSA is an authority that provides status of Certificates or certification paths.
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a person who has received a digitally signed message can determine: Whether the transformation was created using the private signing key that corresponds to the signer's public verification key. Whether the message has been altered since the transformation was made.
Distinguished Name	A string created during the certification process and included in the Certificate that uniquely identifies the End-Entity within the CA domain.
Encryption key pair	A public and private key pair issued for the purposes of encrypting and decrypting data.
Directory	A directory system that conforms to the ITU-T X.500 series of Recommendations.
End-Entity (EE)	A person, Device or application that is issued a certificate by a CA.
PKI Directory	Publicly-accessible Repository.
Entity	Any autonomous element within the PKI, including CAs, RAs and End-Entities.
Employee	An employee is any person employed in or by the ACCC.
Federal Information Processing Standards (FIPS)	Federal standards that prescribe specific performance requirements, practices, formats, communications protocols for hardware, software, data, telecommunications operation. U.S. Federal agencies are expected to apply these standards as specified unless a waiver has been granted in accordance with agency waiver procedures.
Hardware Token	A hardware Device that can hold Private Keys, digital Certificates, or other electronic information that can be used for authentication or authorisation. Smartcards and USB tokens are examples of hardware tokens.

Hardware Security Module (HSM)	An HSM is a hardware Device used to generate cryptographic key pairs, keep the Private Key secure and generate digital signatures. It is used to secure the CA keys, and in some cases the keys of some applications (End-Entities).
Incident	Misuse relating to a single credential regardless of the relying parties involved
Internet Engineering Task Force(IETF)	The Internet Engineering Task Force is a large open international community of network designers, operators, vendors, and researches concerned with the evolution of the Internet architecture and the smooth operation of the Internet.
Intermediate CA	A CA that is not a Root CA and whose primary function is to issue Certificates to other CAs. An Intermediate CA is a Subordinate CA.
Issuing CA	In the context of a particular Certificate, the issuing Certification Authority is the Certification Authority that signed and issued the End-Entity Certificate.
Key Generation	The process of creating a Private Key and Public Key pair.
key pair	Two mathematically related keys, having the properties that (i) one key can be used to encrypt data that can only be decrypted using the other key, and (ii) knowing one of the keys which is called the Public Key, it is computationally infeasible to discover the other key which is called the Private Key.
Local Registration Authority (LRA)	An entity that is responsible for identification and authentication of Certificate subjects, but that does not sign or issue Certificates (ie, an LRA is delegated certain tasks on behalf of a RA or CA).
OCSP	Protocol useful in determining the current status of a digital Certificate without requiring CRLs.
Object Identifier (OID)	An object identifier is a specially-formatted sequence of numbers that is registered with an internationally-recognised standards organisation.
Operational Authority (OA)	The Operational Authority is responsible to the Policy Management Authority for: Interpreting the *Certificate Policies* that were selected or defined by the Policy Management Authority. Developing a *Certification Practice Statement (CPS),* in accordance with the *Internet X.509 Public Key Infrastructure (PKIX) Certificate Policy and Certification Practice Framework (RFC 3647)*, to document the CA's compliance with the Certificate Policies and other requirements. Operating the Certification Authority in accordance with the CPS. Performing Registration Authority operations in accordance with the CPS.
Operational Period of a Certificate	The operational period of a Certificate is the period of its validity. It would typically begin on the date the Certificate is issued (or such later date as specified in the Certificate), and end on the date and time it expires as noted in the Certificate or earlier if revoked.
Organisation	Department, agency, partnership, trust, joint venture or other association.
Person	A human being (natural person), corporation, limited liability company, or other judicial entity, or a digital Device under the control of another person.
PIN	Personal Identification Number. See activation data for definition

PKI Disclosure Statement (PDS)	Defined by IETF's RFC 3647 as "An instrument that supplements a CP or CPS by disclosing critical information about the policies and practices of a CA/PKI. A PDS is a vehicle for disclosing and emphasizing information normally covered in detail by associated CP and/or CPS documents. Consequently, a PDS is not intended to replace a CP or CPS."
PKIX	IETF Working Group chartered to develop technical specifications for PKI components based on X.509 Version 3 Certificates.
Policy	This Certificate Policy.
Policy Management Authority (PMA)	The Policy Management Authority is responsible for: Dispute resolution. Selecting and/or defining *Certificate Policies*, in accordance with the *Internet X.509 Public Key Infrastructure (PKIX) Certificate Policy and Certification Practice Framework (RFC 3647)*, for use in the Certification Authority PKI or organisational enterprise. Approving of any interoperability agreements with external Certification Authorities. Approving practices, which the Certification Authority must follow by reviewing the *Certification Practice Statement* to ensure consistency with the *Certificate Policies.* Providing Policy direction to the CA and the Operational Authority.
Public Key Infrastructure (PKI)	A set of policies, processes, Server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke Public Key certificates.
Private Key	The Private Key of a key pair used to perform Public Key cryptography. This key must be kept secret.
Public Key	The Public Key of a key pair used to perform Public Key cryptography. The Public Key is made freely available to anyone who requires it. The Public Key is usually provided via a Certificate issued by a Certification Authority and is often obtained by accessing a repository.
Public/Private key pair	See key pair.
Registration	The process whereby a user applies to a Certification Authority for a digital Certificate.
Registration Authority (RA)	An Entity that is responsible for the identification and authentication of Certificate Subscribers before Certificate issuance, but does not actually sign or issue the Certificates (ie, an RA is delegated certain tasks on behalf of a CA).
Relying Party (RP)	A Relying Party is a recipient of a Certificate signed by an ACCC PKI CA who acts in reliance on those Certificates and/or digital signatures verified using that Certificate and who has agreed to be bound by the terms of this CP and the CPS. The term "Relying Party" designates the legal entity responsible for the recipient's actions.
Relying Party Agreement	An agreement, entered into by a Relying Party, that provides for the respective liabilities of ACCC or its Business Units and of the Relying Party. Such agreement is a prerequisite in order to be able to rely on the Certificate.
Repository	Publication service providing all information necessary to ensure the intended operation of issued digital Certificates (eg, CRLs, encryption Certificates, CA Certificates).

Revocation	To prematurely end the Operational Period of a Certificate from a specified time forward.
RFC3647	Document published by the IETF, which presents a framework to assist the writers of Certificate Policies or certification practice statements for participants within Public Key infrastructures, such as certification authorities, policy authorities, and communities of interest that wish to rely on Certificates. In particular, the framework provides a comprehensive list of topics that potentially (at the writer's discretion) need to be covered in a Certificate Policy or a certification practice statement.
Root CA	A CA that is the trust anchor for a set of relying parties.
SCVP	Protocol that allows a client to delegate Certificate path construction and Certificate path validation to a Server.
Signature key pair	A public and private key pair used for the purposes of digitally signing electronic documents and verifying digital signatures.
Signing (aka Issuing) CA	A CA whose primary function is to issue Certificates to End-Entities. A Signing CA is a Subordinate CA.
Software-based Certificate	A digital Certificate (and associated Private Keys) that are created and stored in software – either on a local workstation or on a Server.
Sponsoring Organisation	An organisation with which an Authorised Subscriber is affiliated (eg, as an employee, user of a service, business partner, customer).
Subordinate CA	A CA that is not a Root CA. It is subordinate to either a Root CA or other Subordinate CA.
Subscriber	An entity that is the subject of a Certificate and which is capable of using, and is authorised to use, the Private Key, that corresponds to the Public Key in the Certificate. Responsibilities and obligations of the Subscriber shall be as required by the *Certificate Policy* and *the General Terms and Conditions*.
General Terms and Conditions	An agreement, entered into by a Subscriber, that provides the responsibilities and obligations of the Subscribers when using Certificates. Such agreement is a prerequisite in order to be able to use the Private Key associated to the Certificate.
Token	A hardware security Device containing an End-Entity's Private Key(s) and Certificate. (see "Hardware Token")
Transaction	Any use of a single credential. Multiple transactions associated with misuse of a single credential constitute an incident.
Trusted Agent	An agent who a Registration Authority relies on to verify that an applicant fulfils part of or all of the necessary prerequisites to obtain a certificate for an End-Entity.
Trustworthy System	Computer hardware, software, and/or procedures that: (a) are reasonably secure from intrusion and misuse; (b) provide a reasonable level of availability, reliability, and correct operation; (c) are reasonably suited to performing their intended functions, and (d) adhere to generally accepted security procedures.

Valid Certificate	A Certificate that (1) a Certification Authority has issued, (2) the Subscriber listed in it has accepted, (3) has not expired, and (4) has not been revoked. Thus, a Certificate is not "valid" until it is both issued by a CA and has been accepted by the Subscriber.

1.6.2 Acronyms

ACCC	Australian Competition and Consumer Commission
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
C	Country
CA	Certification Authority
CBP	Commercial Best Practices (DEPRECATED)
CHUID	Cardholder Unique Identifier CMS
CMS	Card Management System
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSA	Certificate Status Authority
DC	Domain Component
DN	Distinguished Name
DNS	Domain Name Service
ECDH	Elliptic Curve Diffie Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EE	End-Entity
FASC-N	Federal Agency Smart Credential Number
FBCA	Federal Bridge Certification Authority
FIPS	(US) Federal Information Processing Standard
FIPS PUB	(US) Federal Information Processing Standard Publication
GUID	Globally Unique Identifier
HR	Human Resources
HTTP	Hypertext Transfer Protocol
ID	Identifier
IETF	Internet Engineering Task Force
ISO	International Organisation for Standardisation
KRP	Key Recovery Policy
KRPS	Key Recovery Practices Statement
LDAP	Lightweight Directory Access Protocol
MOA	Memorandum of Agreement
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
O	Organisation
OA	Operational Authority
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OU	Organisational Unit
PCA	Principal Certification Authority
PDS	PKI Disclosure Statement
PIN	Personal Identification Number
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification - Interoperable
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure

PKIX	Public Key Infrastructure X.509
PMA	Policy Management Authority
RA	Registration Authority
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SCEP	Simple Certificate Enrolment Protocol
SCVP	Server-based Certificate Validation Protocol
SHA	Secure Hash Algorithm
SSCD	Secure Signature-Creation Devices
SSL	Secure Sockets Layer
TDES	Triple Data Encryption Standard
TLS	Transport Layer Security
UPS	Uninterrupted Power Supply
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UUID	Universally Unique Identifier

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

All CAs that issue certificates under this CP must post all CA Certificates issued by or to the CA and Certificate Revocation Lists (CRLs) issued by the CA in a repository that is publicly accessible through all Uniform Resource Identifier (URI) references asserted in valid certificates issued by that CA.

2.1.1 Publication of CA Information

CAs issuing a certificate in accordance with this CP shall make the following items publicly available in their repositories:

- this CP and applicable Certification Practice Statements (CPS);
- the CRL; and
- all CA Certificates issued by the CA.

Signature and identity certificates need not be published in the PKI repository.

All publication by ACCC CAs shall be performed as soon as an internal event that may require publication (revocation, issuance or modification of certificate) is validated by the CA.

2.2 TIME OR FREQUENCY OF PUBLICATION

ACCC PKI CA shall publish CA Certificates and revocation data as soon as possible after issuance. ACCC PMA shall publish new or modified versions of this CP within seven days of their approval.

2.3 ACCESS CONTROLS ON REPOSITORIES

Read-only access to the repository is unrestricted. Logical and physical controls prevent unauthorized write access to repositories.

3. IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

All certificates shall have a clearly distinguishable and unique X.501 Distinguished Name (DN) in the certificate Subject name field and in accordance with RFC 5280.

Subject Alternative Name may be used, if marked non-critical; section 10 lists the accepted contents (email address, UPN, FQDN) and their specific formats.

3.1.2 Need for Names to be Meaningful

The certificates issued pursuant to this CP are meaningful only if the names that appear in the certificates can be understood and used by Relying Parties. Names used in the certificates must identify the person or object to which they are assigned.

Distinguished Names (DNs) shall be used where the common name represents the subscriber in a way that is easily understandable for humans.

- For Individuals, this will typically be a legal name.
- For End-Entity equipment, this may be a model name and serial number, an application process (eg, Organization X Mail List or Organization Y Multifunction Interpreter), or a fully qualified domain name (www.example.com), or network address (on the Internet, an IPv4 or IPv6 address in a recognizable standard form), or another kind of name that is meaningful in the domain of application.
- For organizations or corporations possessing an organizational medium-assurance hardware code-signing certificate, this must be the officially recognized legal name or registration number of the organization or corporation.
- All DNs shall satisfy asserted namespace constraints.
- Subject DNs shall accurately reflect the organization with which the Subject is affiliated.
- When User Principal Name (UPN) is used, it shall accurately reflect organizational structure.

3.1.3 Anonymity or Pseudonymity of Subscribers

ACCC may not accept any requests for anonymous or pseudonymous certificates.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting distinguished name forms are specified in X.501. Rules for interpreting e-mail addresses are specified in [RFC 2822].

3.1.5 Uniqueness of Names

Name uniqueness is required in each Certificate issued by each CA. The ACCC PMA shall be responsible for ensuring name uniqueness in certificates issued by the ACCC PKI CAs.

3.1.6 Recognition, Authentication, and Role of Trademarks

Subscribers may not request Certificates with any content that infringes the intellectual property rights of another entity. Unless otherwise specifically stated, this CP does not require an Issuer CA to verify an Applicant's right to use a trademark. Issuer CAs may reject any application or require revocation of any Certificate that is part of a trademark dispute.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Private Key

In all cases where the party named in a certificate generates its own keys, that party shall be required to prove possession of the private key, which corresponds to the public key in the certificate request. For signature keys, this may be done by the entity using its private key to sign a value and providing that value to the issuing CA. The CA shall then validate the signature using the party's public key.

3.2.2 Authentication of Organization Identity

Requests for Certificates in the name of an organization or corporation shall include all details listed in the ACCC CPS Section 3.2.2.

The ACCC RA shall verify the information, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the organization.

In all cases, the existence of an affiliated organization shall be verified prior to issuing end user Certificates on its behalf. The RA shall verify the authenticity of the requesting representative and the representative's authorization to act in the name of the organization. Moreover, requests for end user Certificates other than unaffiliated Subscribers shall include the name of the organization and shall be verified with the identified affiliated organization.

The ACCC RA approval process authenticates the identity of the organization named in the respective Digital Certificate Subscriber Agreement and per the reference documents in section 1.6.3 of the DigiCert Private PKI CP/CPS.

The RA authenticates the identity of the organization named in the Digital Certificate Subscriber Agreement by confirming that the organization name and address is accurate, documentation exists to confirm such identity and a trusted source has been used to verify the organization's identity as per Section 3.2.2 of the ACCC CPS.

Requests for cross-Certificates shall include the CA name, address, and documentation of the existence of the CA. Before issuing cross-Certificates, the issuing CA shall verify the information provided, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the CA.

3.2.3 Authentication of Subject Identity

3.2.3.1 Device Subjects

Where applicable, the ACCC RA authenticates the identity of the organization named in the respective Digital Certificate Subscriber Agreement and per the reference documents in section 1.6.3 of the DigiCert Private PKI CP/CPS.

Where individual vetting is required, the RA authenticates the individual identity of the:

- representative submitting the Digital Certificate Subscriber Agreement and Certificate Application, is a duly authorized representative of the organization as an employee, partner, member or agent and is authorized to act on behalf of the organization;
- corporate contact listed in the Digital Certificate Subscriber Agreement is an officer in the organization and can act on behalf of the organization; and
- administrator listed in the Digital Certificate Subscriber Agreement and Certificate Application, is a duly authorized representative of the organization as an employee, partner, member or agent and is authorized to act on behalf of the organization.

The CA or RA shall keep a record of the type and details of Authentication used. The registration information shall be verified.

3.2.4 Non-Verified Subscriber Information

Non-verifiable information may be included in a certificate, such as:

- Organization Unit (OU); and
- any other information designated as non-verified in the certificate and as permitted in the certificate profiles.

3.2.5 Validation of Authority

The RA's Certificate issuance process must confirm that the:

- Corporate Contact listed in the Digital Certificate Subscriber Agreement is an officer in the organization who can sign on behalf of the organization and bind the organization to the terms and conditions of the agreement;
- Representative submitting the Digital Certificate Subscriber Agreement and certificate application is authorized to act on behalf of the organization;
- Administrators listed on the Digital Certificate Subscriber Agreement and certificate application are authorized to act on behalf of the organization; and
- Contacts listed on the Digital Certificate Subscriber Agreement are authorized to act on behalf of the organization.

3.2.6 Criteria for Interoperation

Interoperating CAs shall adhere to the following requirements:

- Complete a policy mapping with the Subject CA's certificate policy with results satisfactory to both parties;
- Operate a PKI that has undergone a successful Compliance Audit pursuant to Section 8 of this CP and as set forth in the Subject CA certificate policy;
- Issue certificates compliant with the profiles described in this CP, and make certificate status information available in compliance with this CP; and
- Provide CA Certificate and certificate status information to the Relying Parties.

3.3 RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine Re-key

Subscribers may request re-key of a certificate prior to a certificate's expiration. After receiving a request for re-key, the RA may approve a new certificate with the same certificate contents except for a new Public Key and, optionally, an extended validity period. If the certificate has an extended validity period, the RA may perform some revalidation of the Applicant but may also rely on information previously provided or obtained.

CA and Subscriber certificate re-key follows the same procedures as initial certificate issuance in section 3.2.

Identity can be established through the use of the device's current valid signature key.

Rekey of Entity CA Certificates is not permitted.

3.3.2 Identification and Authentication for Re-key after Revocation

After a certificate has been revoked other than during a renewal or update action, the Subject is required to go through the initial registration process described in Section 3.2 to obtain a new certificate, unless he/she can be authenticated through the use of a valid public key certificate of equal or higher assurance, as specified in Section 3.3.1.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Requests to revoke a certificate may be signed using the certificate's associated private key, regardless of whether the private key has been compromised.

The CA or RA acting on its behalf shall authenticate a request for revocation of a Certificate. Authentication mechanisms shall balance the need to prevent unauthorized revocation requests against the need to quickly revoke Certificates. Revocation requests authenticated on the basis of the current key pair shall always be accepted as valid, even if this key pair is the one suspected of being compromised. Other revocation request authentication mechanisms may be used as well, such as challenge-response questions combined with a completed standard CA Revocation Request form that was sent to the Certificate holder at the time of the revocation request.

All revocation requests shall be ogged.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1 Who Can Submit a Certificate Application

4.1.1.1 Application for End-Entity Certificates by an individual

The Subscriber, or an RA acting on behalf of the Subscriber shall submit a Certificate application to the CA.

4.1.1.2 Application for End-Entity Certificates on behalf of a Device

The Device Sponsor, who needs to be a Subscriber, or an RA acting on behalf of the Subscriber shall submit a Certificate application to the CA.

4.1.1.3 Application for CA Certificates

For CA-Certificate applications to the ACCC Root or Intermediate CA, an authorized representative of the Subject CA shall submit the application to the ACCC PMA.

4.1.2 Enrollment Process and Responsibilities

Applicants for Public Key Certificates shall be responsible for providing accurate information in their applications for certification.

Information regarding attributes shall be verified via those offices or roles that have authority to assign the information or attribute. Relationships with these offices or roles shall be established prior to commencement of CA duties and shall be described in the applicable CPS.

For CA Certificates, the ACCC PMA shall verify all authorizations and other attribute information received from an applicant CA.

All Subscribers must agree to be bound by a relevant Subscriber Agreement that contains representations and warranties described in Section 9.9.

4.2 CERTIFICATE APPLICATION PROCESSING

It is the responsibility of the RA, or, in the case of a CA Certificate, the ACCC PMA, to verify that the information in a Certificate Application is accurate.

4.2.1 Performing Identification and Authentication Functions

The Certificate Application shall be subject to identification and Authentication checks as described in Section 3.2 and Section 3.3 of this CP.

Additionally, prior to certificate issuance, a Subscriber shall be required to accept a Subscriber Agreement stating that the Subscriber shall protect the private key and use the certificate and private key for authorized purposes only.

4.2.2 Approval or Rejection of Certificate Applications

The CA or the delegated RA must:

- verify the authority of the applicant that submits an application; and
- verify the integrity of the information in the certificate request.

The CA or the delegated RA may reject a Certificate Application.

A Certificate Application shall not be considered accepted until the CA or the delegated RA has accepted the application and decided to issue a certificate.

4.2.3 Time to Process Certificate Applications

All parties involved in certificate application processing shall use reasonable efforts to ensure that certificate applications are processed in a timely manner. Identity shall be established no more than 30 days before initial issuance of ACCC Certificates.

4.3 CERTIFICATE ISSUANCE

Upon receiving a request for a certificate, the CA or RA shall respond in accordance with the requirements set forth in this CP and in its CPS.

The certificate request may contain an already built ("to-be-signed") certificate. This certificate will not be signed until the process set forth in this CP and its CPS has been met.

While the Subscriber may do most of the data entry, it is still the responsibility of the CA and the RA to verify that the information is correct and accurate. This may be accomplished through a system approach linking trusted databases containing personnel information, through other equivalent authenticated mechanisms, or through personal contact with the Subscriber's sponsoring organization. If databases are used to confirm Subscriber information, then these databases must be protected from unauthorized modification to a level commensurate with the level of assurance of the certificate being sought.

4.3.1 CA Actions During Certificate Issuance

A Certificate is created and issued following the approval of a Certificate Application by the CA or following receipt of an RA's request to issue the Certificate. The CA creates and issues to a Certificate Applicant a Certificate based on the information in a Certificate Application following approval of such Certificate Application. The CA shall authenticate the source of a Certificate Request before issuance. Certificates shall be checked to ensure that all fields and extensions are properly populated. After generation, verification and acceptance the CA shall publish the Certificate to a repository in accordance with this CP and the applicable CPS. This shall be done in a timely manner as described in Section 4.9.5.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificates

CAs issuing Certificates to Subscribers shall, either directly or through an RA, notify Subscribers that they have created such Certificates, and provide Subscribers with access to the Certificates by notifying them that their Certificates are available and the methods for obtaining them. Such methods shall be described in the appropriate CPS.

The ACCC OA shall inform the ACCC PMA of any Certificate issuance to a CA by an ACCC Root or Intermediate CA. The ACCC PMA shall inform the authorized instance of the successful Certificate issuance

4.4 CERTIFICATE ACCEPTANCE

4.4.1 Conduct Constituting Certificate Acceptance

For the issuance of CA Certificates to ACCC PKI Sub CAs, the ACCC PMA shall set up an acceptance procedure indicating and documenting the acceptance of the issued CA Certificate.

4.4.2 Publication of the Certificate by the CA

As specified in Section 2.1, all CA Certificates shall be published in repositories.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

The ACCC PMA must be notified whenever a CA operating under this CP issues a CA Certificate.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

All Subscribers and Sponsors shall protect their Private Keys from unauthorized use or disclosure by third parties and shall use their Private Keys only for their intended purpose.

4.5.2 Relying Party Public Key and Certificate Usage

Reliance on a certificate must be reasonable under the circumstances. If the circumstances indicate a need for additional assurances, the Relying Party must obtain such assurances for such reliance to be deemed reasonable.

Before any act of reliance, Relying Parties shall independently assess the following:

- The appropriateness of the use of a certificate for any given purpose and determine that the certificate will, in fact, be used for an appropriate purpose that is not prohibited or otherwise restricted by Section 1.4.1 or 1.4.2. CAs and RAs are not responsible for assessing the appropriateness of the use of a certificate.
- The certificate is being used in accordance with the *keyUsage* and *extendedKeyUsage* extensions included in the certificate.
- The status of the Certificate and all Certificates in the chain of trust, including revocation status according to section 4.9.6.

Assuming that the use of the certificate is appropriate, Relying Parties shall utilize the appropriate software and/or hardware to perform digital signature verification or other cryptographic operations they wish to perform, as a condition of relying on certificates in connection with each such operation.

In circumstances where a Time Stamping service is used, applications verifying software packages signed with a code-signing Certificate used for Aircraft and Spacecraft Software Signature, shall check the timestamp, and shall reject any software package which either does not have a timestamp issued by a recognized Time Stamp Authority, or whose timestamp shows a time later than the time of the check, or whose timestamp shows a time before the 'Valid before' date of the Certificate signing the software package.

4.6 CERTIFICATE RENEWAL

Renewing a certificate means creating a new certificate with the same name, key and other information as the old one, but a new extended Validity Period and a new serial number is created. Certificates may be renewed in order to reduce the size of CRLs.

4.6.1 Circumstances for Certificate Renewal

A certificate may be renewed if the public key has not reached the end of its Validity Period, the associated private key has not been revoked or compromised and the Subscriber name and attributes are unchanged. In addition, the Validity Period of the certificate must not exceed the remaining lifetime of the private key, as specified in Section 6.3.2. The identity proofing requirement listed in Section 3.2 shall also be met.

The CA may automatically renew certificates during recovery from a key Compromise.

4.6.2 Who May Request Renewal

Only the certificate subject or an authorized representative of the certificate subject may request renewal of the Subscriber's certificates. The CA may renew a certificate without a corresponding request if the signing certificate is re-keyed.

The PMA may request renewal of a CA's Certificate.

4.6.3 Processing Certificate Renewal Requests

In all cases, Subscribers must provide proof of possession of the private key in order to renew the certificate. This can be achieved in the manner described in Section 3.2.1.

4.6.4 Notification of New Certificate Issuance to Device Sponsor

Notification shall be given to the Subscriber in accordance with Section 4.3.2.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

See Section 4.4.1.

4.6.6 Publication of the Renewal Certificate by the CA

Renewed certificates are published as described in Section 4.4.2.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.7 CERTIFICATE RE-KEY

The longer and more often a key is used, the more susceptible it is to loss or discovery. Therefore, it is important that a Subscriber periodically obtains new keys and reestablishes its identity. Re-keying a certificate means that a new certificate is created, having the same characteristics and level as the old one, except that the new certificate has a new, different, public key (corresponding to a new, different, private key) and a different serial number, and it may be assigned a different Validity Period. The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

Subscribers shall identify themselves for the purpose of re-keying as required in Section 3.3.

4.7.1 Circumstances for Certificate Re-key

A certificate may be re-keyed after revocation, for example, due to a compromised private key. A certificate may also be re-keyed before (to maintain continuity of certificate usage) or after expiration of the certificate and/or its key pair. It may also be re-keyed due to the issuance of a new hardware token.

4.7.2 Who May Request Certification of a New Public Key

A Subject may request the re-key of its Certificate.

A Device Sponsor may request re-key of a component Certificate.

4.7.3 Processing Certificate Re-keying Requests

Re-key requests are only accepted from the subject of the Certificate or the PKI sponsor. At a minimum, the Issuer CA shall comply with section 3.3.1 in identifying and authenticating the Subscriber or PKI sponsor prior to rekeying the Certificate.

4.7.4 Notification of New Certificate Issuance to Device Sponsors

Notification shall be given to the Subscriber in accordance with Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

See Section 4.4.1.

4.7.6 Publication of the Re-keyed Certificate by the CA

Re-keyed CA Certificates are published as described in Section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

No specific requirement.

4.8 CERTIFICATE MODIFICATION

4.8.1 Circumstances for Certificate Modification

An ACCC PKI Root CA may issue a new certificate to the Subject when some of the Subject information has changed (eg, change in subject attributes) and the Subject continues to be entitled to a certificate.

Certificate modification is only supported by this CP for CA Certificates. All other requests for Certificate modification shall be treated as new Certificate applications.

4.8.2 Who May Request Certificate Modification

The ACCC PMA may request modification to an ACCC PKI CA Certificate.

4.8.3 Processing Certificate Modification Requests

A certificate modification shall be achieved using one of the following processes:

- initial registration process as described in Section 3.2; or
- Identification & Authentication for Re-key as described in Section 3.3. In addition, the validation of the changed subject information shall be in accordance with the initial identity-proofing process as described in Section 3.2.

4.8.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

See Section 4.4.1.

4.8.6 Publication of the Modified Certificate by the CA

See Section 4.4.2.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

CAs operating under this CP shall issue CRLs covering all unexpired certificates issued under this CP except for OCSP responder certificates that include the id-pkix-ocsp-nocheck extension.

CAs operating under this CP shall make public a description of how to obtain revocation information for the certificates they publish, and an explanation of the consequences of using dated revocation information. This information shall be given to Device Sponsors during the certificate request or issuance, and shall be readily available to any potential Relying Party.

Revocation requests must be authenticated. Requests to revoke a certificate may be authenticated using that certificate's associated public key, regardless of whether the private key has been compromised. Revocation requests must be authenticated.

4.9.1 Circumstances for Revocation

Revocation shall occur on decision of the CA when reasonable and credible evidence exists to establish at least one of the following:

- the certificate has been delivered based upon wrong or falsified information;
- the identifying information or affiliation components of any names in the certificate become invalid;
- the confidentiality of a private key is no longer ensured or has been compromised;
- the media holding the private key is suspected or known to have been compromised;
- the certificate fees have not been paid according to the payment terms as indicated in the relevant agreement;
- the Subscriber can be shown to have violated one or more sections of this CP; or
- the Subscriber or the Subscriber's employer wishes to terminate their subscription to the CA.

If there is a risk of a private key disclosure during a maintenance cycle on a Device, then the certificate must be revoked, and measures must be taken to invalidate or securely erase the private key from the Device.

Whenever any of the above circumstances occur, the associated certificate shall be revoked and placed on the CRL. Revoked certificates shall be included on all new publications of the certificate status information until the certificates expire.

In addition, if it is determined subsequent to issuance of new Certificates that a private key used to sign requests for one or more additional Certificates may have been compromised at the time the requests for additional Certificates were made, all certificates authorized by directly or indirectly chaining back to that compromised key shall be revoked.

The CA shall revoke a Certificate if the binding between the subject and the subject's Public Key in the Certificate is no longer valid or if an associated Private Key is compromised. The Issuer CA will revoke a Subordinate CA Certificate within seven (7) days if one or more of the following occurs:

- the Subordinate CA requests revocation in writing;
- the Subordinate CA notifies the Issuer CA that the original certificate request was not authorized and does not retroactively grant authorization;
- the Issuer CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6,
- the Issuer CA obtains evidence that the CA Certificate was misused;
- the Issuer CA is made aware that the CA Certificate was not issued in accordance with or that Subordinate CA has not complied with this document or the applicable Certificate Policy or Certification Practice Statement;
- the Issuer CA determines that any of the information appearing in the CA Certificate is inaccurate or misleading;
- the Issuer CA or the Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the CA Certificate;
- revocation is required by the Issuer CA's Certificate Policy and/or Certification Practice Statement or if the Issuer CA's Certificate Policy and Certification Practice Statement are terminated; or

- the technical content or format of the CA Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties.

4.9.2 Who Can Request Revocation

The revocation of an individual or end-entity certificate may only be requested by one of the following:

- the Device Sponsor responsible for the Server, Device, or application;
- the Device Sponsor's employer organization;
- the personnel of the issuing CA; or
- the personnel of any RA associated with the issuing CA.

For CA certificates, authorized individuals representing the CA operations may request revocation of certificates. A written notice and brief explanation for the revocation shall subsequently be provided to the Device Sponsor.

4.9.3 Procedure for Revocation Request

A request to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (eg, digitally or manually signed).

The CA shall ensure that all procedures and requirements for revocation of a certificate of this type are documented in the CPS. Where a Subscriber's certificate is revoked, the revocation shall be published in the appropriate CRL.

For certificates whose operation involves the use of a cryptographic hardware token, a Sponsor ceasing its relationship with an organization that sponsored the certificate shall, prior to departure, surrender to the organization (through any accountable mechanism) all such hardware tokens that were issued by or on behalf of the sponsoring organization. The contents of the token, or the token itself, shall be destroyed in accordance with Section 6.2.10 promptly upon surrender and shall be protected from malicious use between surrender and such destruction of the key.

If an authorized administrator leaves an organization and the hardware tokens cannot be obtained from the Sponsor, then all Subscriber certificates associated with the un-retrieved tokens shall be immediately revoked for the reason of key Compromise.

4.9.4 Revocation Request Grace Period

There is no revocation grace period. Responsible parties must request revocation as soon as they identify the need for revocation.

4.9.5 Time Within Which CA Must Process the Revocation Request

The CA will revoke a CA Certificate within a reasonable time after receiving clear instructions from the ACCC PMA. Other certificates are revoked as quickly as practical after validating the revocation request.

4.9.6 Revocation Checking Requirement for Relying Parties

Use of revoked certificates could have damaging or catastrophic consequences in certain applications. The matter of how often new revocation data should be obtained is a determination to be made by the Relying Party and the system accreditor. If it is temporarily infeasible to obtain revocation information, then the Relying Party must either reject use of the certificate, or make an informed decision to accept the risk, responsibility and consequences for using a certificate whose authenticity cannot be guaranteed to the standards of this CP. Such use may occasionally be necessary to meet urgent operational requirements.

4.9.7 CRL Issuance Frequency

CRLs shall be issued periodically, even if there are no changes to be made, to ensure timeliness of information. Certificate status information may be issued more frequently than the issuance frequency described below. A CA

shall ensure that superseded certificate status information is removed from the PKI repository upon posting of the latest certificate status information.

Certificate status information shall be published no later than the next scheduled update. This will facilitate the local caching of certificate status information for offline or remote (laptop) operation. PKI Participants shall coordinate with the PKI repositories to which they post certificate status information to reduce latency between creation and availability.

The following table provides CRL issuance frequency requirements.

Table 1: CRL Issuance Frequency

Routine	At least once every 24 hours
Loss/Compromise of Private Key	Within 18 hours of notification
CA Compromise	Immediately, but no later than within 18 hours of notification

CRL issuance frequency requirements may be further constrained by applicable jurisdictional regulatory law.

The CAs that issue routine CRLs less frequently than the requirement for emergency CRL issuance (ie, CRL issuance for loss or Compromise of key or for Compromise of CA) shall meet the requirements specified above for issuing emergency CRLs.

Such CAs shall also be required to notify the other cross-certified PKI domains' Operational Authorities upon Emergency CRL issuance. This requirement shall be included in the respective MOA between ACCC and other respective PKI domains' responsible organisations.

4.9.8 Maximum Latency for CRLs

The maximum delay between the time a Subscriber certificate revocation request is received by a CA and the time that this revocation information is available to Relying Parties shall be no greater than twenty-four (24) hours.

4.9.9 Online Revocation/Status Checking Availability

In addition to CRLs, CAs and Relying Party client software may support online status checking with OCSP. Client software using online status checking need not obtain or process CRLs.

If online revocation/status checking is supported by a CA, the latency of certificate status information distributed online by the CA or its delegated status responders shall meet or exceed the requirements for CRL issuance stated in Section 4.9.7.

Since some Relying Parties might not be able to accommodate online communications, all CAs shall be required to support CRLs.

4.9.10 Online Revocation Checking Requirements

CAs shall support on-line status checking via OCSP using the CA-delegated trust model [RFC 2560]. For other types of Certificates, the CAs are not required to operate an OCSP Responder covering the Certificates they issue.

The ACCC PKI Repository shall contain and publish a list of all OCSP Responders operated by the CAs.

If OCSP is implemented, the service shall comply with the Internet Engineering Task Force (IETF) RFC 6960 to meet security and interoperability requirements.

4.9.11 Other Forms of Revocation Advertisements Available

Any alternate forms used to disseminate revocation information shall be implemented in a manner consistent with the security and latency requirements for the implementation of CRLs and online revocation and status checking.

4.9.12 Special Requirements Regarding Key Compromise

In the event of Compromise or suspected Compromise of the CA signing key, senior management of the CA Operator and the ACCC PMA shall be immediately notified. A CRL must be issued within eighteen (18) hours of notification. The requirements of Section 4.9.7 also apply.

4.9.13 Circumstances for Suspension

Certificate suspension is not supported by this CP.

4.9.14 Who Can Request Suspension

Certificate suspension is not supported by this CP.

4.9.15 Procedure for Suspension Request

Certificate suspension is not supported by this CP.

4.9.16 Limits on Suspension Period

Certificate suspension is not supported by this CP.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Certificate status can be ascertained by querying the CRL maintained and published in its repository by the CA, or by querying an OCSP responder operated by the CA, if present.

4.10.2 Service Availability

Relying Parties are bound to their obligations and the stipulations of this CP irrespective of the availability of the certificate status service.

The CRL shall be publicly available twenty-four (24) hours a day, seven (7) days a week. Care shall be taken by the CA to ensure that the public copy is replaced automatically when it is being updated.

4.10.3 Optional Features

No specific requirement.

4.11 End of Subscription

A Subscriber may terminate their subscription either by allowing the Subscriber certificate to expire without renewing or re-keying it, or by revoking the certificate before expiry without applying for a replacement.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

Under no circumstances shall any CA or end-entity signature key be escrowed by a third party.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

This CP neither requires nor prohibits the capability of recovering session keys. CAs that support session key encapsulation and recovery shall identify the document describing the practices in the applicable CPS.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

5.1.1 Site Location and Construction

All CA operations shall be conducted within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems. Such environments are based in part on the establishment of physical security tiers. A tier is a barrier such as a locked door or closed gate that provides mandatory Access Control for individuals and requires a positive response (eg, door unlocks or gate opens) for each individual to proceed to the next area. Each successive tier provides more restricted access and greater physical security against intrusion or unauthorized access. Moreover, each physical security tier encapsulates the next inner tier, such that an inner tier must be fully contained in an outside tier and cannot have a common outside wall with the outside tier, the outermost tier being the outside barrier of the building (eg, a perimeter fence or outside wall).

The location and construction of the facility housing the CA equipment, as well as sites housing remote workstations used to administer the CAs, shall be consistent with facilities used to house high-value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards, high security locks and intrusion sensors, shall provide robust multi-tier protection against unauthorized access to the CA equipment and records.

The workstation of remote administrators of the CA shall be located such that all accesses may be monitored, and that there are reasonable expectations that it would be impossible for a determined unauthorized individual to gain access to the workstation.

5.1.2 Physical Access

5.1.2.1 Physical Access for CA Equipment

CA, CSA and CMS equipment shall always be protected from unauthorized access. The physical Access Controls for CA equipment, as well as remote workstations used to administer the CAs, shall be auditable and:

- Ensure that no unauthorized access to the hardware is permitted;
- Ensure that all removable media and paper containing sensitive plain-text information is stored in secure containers;
- Be manually or electronically monitored for unauthorized intrusion at all times;
- Ensure an access log is maintained and inspected periodically;
- Provide at least three layers of increasing security such as perimeter, building, and CA bunker; and
- Require two-person physical Access Control to both the cryptographic module and computer systems.

Removable cryptographic modules shall be deactivated prior to storage. When not in use, removable cryptographic modules and the activation information used to access or enable cryptographic modules shall be placed in secure containers. Activation Data shall be either memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module or removable hardware associated with remote workstations used to administer the CA.

A security check of the facility housing the CA equipment or remote workstations used to administer the CAs shall occur if the facility is to be left unattended. At a minimum, the check shall verify the following:

- The equipment is in a state appropriate to the current mode of operation (eg, that cryptographic modules are in place when “open,” and secured when “closed,” and for the CA, that all equipment other than the repository is shut down);
- Any security containers are properly secured;
- Physical security systems (eg, door locks, vent covers) are functioning properly; and
- The area is secured against unauthorized access.

A person or group of persons shall be made explicitly responsible for making such checks. When a group of persons is responsible, a log identifying the person performing a check at each instance shall be maintained. If the facility is not continuously attended, the last person to depart shall initial a sign-out sheet that indicates the date and time and asserts that all necessary physical protection mechanisms are in place and activated.

5.1.2.2 Physical Access for RA Equipment

RA equipment shall be protected from unauthorized access while the RA cryptographic module is installed and activated. The RA shall implement physical Access Controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. These security mechanisms shall be commensurate with the level of threat in the RA equipment environment.

5.1.3 Power and Air Conditioning

The CA facilities shall be equipped with primary and backup power systems to ensure continuous, uninterrupted access to electric power. Also, these facilities shall be equipped with primary and backup heating/ventilation/air conditioning systems for temperature control.

The CA facilities shall have backup capability sufficient to lock out input, finish any pending actions, and record the state of the equipment automatically before lack of power or air conditioning causes a shutdown. The repositories (containing CA Certificates and CRLs) shall be provided with uninterrupted power sufficient for a minimum of six (6) hours of operation in the absence of commercial power, to maintain availability and avoid denial of service.

5.1.4 Water Exposures

CA equipment shall be installed such that it prevents damage from exposure to water.

Potential water damage from fire prevention and protection measures (eg, sprinkler systems) are excluded from this requirement.

5.1.5 Fire Prevention and Protection

CA facilities shall be equipped, and procedures shall be implemented, to prevent damaging exposure to flame or smoke. These measures shall meet all local applicable safety regulations.

5.1.6 Media Storage

CA media shall be stored so as to protect them from accidental damage (eg, water, fire, or electromagnetic) and unauthorized physical access. Media that contains audit, Archive, or backup information shall be duplicated and stored in a location separate from the CA location.

5.1.7 Waste Disposal

Sensitive media and documentation that are no longer needed for operations shall be destroyed in a secure manner. For example, sensitive paper documentation shall be shredded, burned, or otherwise rendered unrecoverable.

5.1.8 Off-Site Backup

Full system backups sufficient to recover from system failure shall be made on a periodic schedule, and described in a CA's CPS. Backups are to be performed and stored off-site not less than once per week, unless the CA is offline, in which case, it shall be backed up whenever it is activated or every seven (7) days, whichever is later. At least one full backup copy shall be stored at an off-site location (separate from CA equipment). Only the latest full backup need be retained. The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational CA.

Requirements for CA private key backup are specified in Section 6.2.4.

5.2 PROCEDURAL CONTROLS

5.2.1 Corporate Controls

The CA must maintain its status as a legal entity in accordance with the law stated in Section 9.15.2. The CA must maintain a system of quality assurance consistent with recognized standards for all of its certificate management operations. The CA management structure shall ensure that they are free from any commercial, financial, or other pressures which may impact the CA's status as an impartial and trustable entity.

5.2.2 Trusted Roles

The CA shall ensure a separation of duties into Trusted Roles for critical CA functions to prevent one CA staff member from maliciously using the CA system without detection. Each such Trusted Role's system access is to be limited to those actions which they are required to perform in fulfilling their responsibilities.

A Trusted Role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible, or the integrity of the CA will be weakened. The functions performed in these roles form the basis of trust for the entire PKI. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion.

The requirements of this policy are drawn in terms of four roles:

- PKI System Administrator – authorized to install, configure, and maintain the component; establish and maintain user accounts; configure profiles and audit parameters; and generate component keys.
- RA Officers – authorized to request or to approve Certificates or Certificate revocations.
- Internal Auditors – authorized to view and maintain audit logs.
- CA Operator – authorized to perform system backup and recovery.

The following sections define these and other trusted roles.

5.2.2.1 CA Administrator

The CA Administrator shall be responsible for:

- Installation, configuration, and maintenance of the CA and CSA (where applicable);
- Establishing and maintaining CA and CSA system accounts;
- Configuring certificate profiles or templates and audit parameters;
- Configuring CA, RA, and CSA audit parameters;
- Configuring CSA response profiles; and
- Generating and backing up CA and CSA keys.

CA System Administrators shall not issue certificates to Subscribers.

5.2.2.2 RA Officers

The RA Officer shall be responsible for:

- Registering new applicants and requesting the issuance of Certificates;
- Verifying the identity of applicants and accuracy of information included in Certificates;
- Entering Subscriber Information, and verifying correctness;
- Approving and executing the issuance of Certificates;
- Requesting, approving and executing the revocation of Certificates;
- Securely communicating requests to, and responses from, the CA; and
- Receiving and distributing Subscriber Certificates.

5.2.2.3 Internal Auditor

The Internal Auditor shall be responsible for:

- Reviewing, maintaining, and archiving audit logs;
- Performing or overseeing Compliance Audits to ensure that the CA, associated RA, and CSA (where applicable) is operating in accordance with the CPS; and
- Issuing attestation letter affirming the results of the audit.

5.2.2.4 CA Operator

The Operator shall be responsible for the routine operation of the CA equipment and operations such as system backups and recovery or changing recording media.

5.2.3 Additional Roles

5.2.3.1 Device Sponsor

A Device Sponsor fills the role of a Subscriber for non-human system components that are named as Public Key Certificate subjects. The Device Sponsor works with the RAs to register components (routers, firewalls) in accordance with Section 3.2.3 and is responsible for meeting the obligations of Subscribers as defined throughout this document.

A Device Sponsor need not be a Trusted role but shall have a credential that is equal to or higher Assurance Level than the credential that they are sponsoring.

5.2.3.2 Trusted Agent

A Trusted Agent is responsible for:

- Verifying identity, pursuant to Section 3.2; and
- Securely communicating Subscriber information to the RA.

A Trusted Agent is NOT a trusted role.

5.2.4 Number of Persons Required per Task

Multiparty control procedures are designed to ensure that at a minimum, the desired number of Trusted Persons are present to gain either physical or logical access to the CA.

Two or more persons are required for the following tasks:

- CA key generation;
- CA signing key activation; and
- CA private key backup.

Where multiparty control is required, at least one of the participants shall be an Administrator. All participants must serve in a Trusted Role as defined in Section 5.2.2. Multiparty control shall not be achieved using personnel that serve in the Audit Administrator Trusted Role.

5.2.5 Identification and Authentication for Each Role

An individual shall identify and Authenticate him/herself before being permitted to perform any actions set forth above for that role or identity.

5.2.6 Roles Requiring Separation of Duties

Individual CA personnel shall be specifically designated to the four roles defined in Section 5.2.2 above as applicable. Individuals shall not assume more than one role.

No individual in a Trusted Role shall be assigned more than one identity.

Role separation, when required as mentioned above, may be enforced by either the CA equipment, or procedurally, or by both means.

5.3 PERSONNEL CONTROLS

5.3.1 Qualifications, Experience, and Clearance Requirements

CAs shall require that personnel assigned to Trusted Roles have the requisite background, qualifications, and experience or be provided the training needed to perform their prospective job responsibilities competently and satisfactorily. The requirements governing the qualifications, selection and oversight of individuals who operate, manage, oversee, and audit the CA shall be set forth in the CPS.

All persons filling Trusted Roles shall be selected on the basis of loyalty, trustworthiness, and integrity, and shall be subject to a background investigation. Personnel appointed to Trusted Roles shall:

- Possess the expert knowledge, experience and qualifications necessary for the offered services and appropriate job function;
- Have successfully completed an appropriate training program;
- Have demonstrated the ability to perform their duties;
- Be trustworthy;
- Have no other duties that would interfere or conflict with their duties for the Trusted Role;
- Have not been previously relieved of duties for reasons of negligence or non-performance of duties;
- Have not been convicted of a serious crime or other offense which affects his/her suitability for the position; and
- Have been appointed in writing by the CA management.

For RAs and Trusted Persons, in addition to the above, the person may be a citizen of the country where the PKI is located.

5.3.2 Background Check Procedures

All persons filling Trusted Roles (including CA Trusted Roles and RA role) shall, at a minimum, pass a background investigation covering the following areas:

- Confirmation of previous employment;
- Confirmation of the highest or most relevant educational degree;
- Place of residence;
- Search of criminal records;
- Check of references; and
- Check of credit/financial records.

The period of investigation must cover at least the last five (5) years for each area, except the residence check which must cover at least the last three (3) years. Regardless of the date of award, the highest educational degree shall be verified.

Factors revealed in a background check that may be considered grounds for rejecting candidates for Trusted Roles or for taking action against an existing Trusted Person may include but is not limited to the following:

- Misrepresentations made by the candidate or Trusted Person;
- Highly unfavorable or unreliable personal references;
- Certain criminal convictions; and
- Indications of a lack of financial responsibility.

5.3.3 Training Requirements

All personnel performing duties with respect to the operation of the CA or RA shall receive comprehensive training. Training shall be conducted in the following areas:

- CA or RA security principles and mechanisms;
- All PKI software versions in use on the CA or RA system;
- All PKI duties they are expected to perform;
- Disaster recovery and business continuity procedures; and
- Stipulations of this CP.

5.3.4 Retraining Frequency and Requirements

All individuals responsible for PKI Trusted Roles shall be made aware of changes in the CA or RA operation. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented. Examples of such changes are CA software or hardware upgrade, changes in automated security systems, and relocation of equipment.

Documentation shall be maintained identifying all personnel who received training and the level of training completed.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

The CA shall take appropriate administrative and disciplinary actions against personnel who have performed actions involving the CA or its RA that are not authorized in this CP, CPSs, or other published procedures.

5.3.7 Independent Contractor Requirements

Contractors fulfilling Trusted Roles are subject to all personnel requirements stipulated in this CP.

PKI vendors who provide any services shall establish procedures to ensure that any subcontractors perform in accordance with this CP and the CPS.

5.3.8 Documentation Supplied to Personnel

The CA shall make available to its personnel the certificate policy they support, the CPS, and any relevant statutes, policies, or contracts. Other technical, operations, and administrative documents (eg, Administrator Manual, User Manual) shall be provided in order for the Trusted Persons to perform their duties.

5.4 AUDIT LOGGING PROCEDURES

Audit log files shall be generated for all events relating to the security of the CAs and RAs. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during Compliance Audits.

5.4.1 Types of Events Recorded

All security auditing capabilities of the CA and RA operating system and the CA and RA applications required by this CP shall be enabled during installation. At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

- The type of event;
- The date and time the event occurred;
- A success or failure indicator when executing the CA's signing process;
- A success or failure indicator when performing certificate revocation; and
- The identity of the entity and/or Operator that caused the event.
- A message from any source requesting an action by the CA is an auditable event; the corresponding audit record must also include message date and time, source, destination, and contents.

The CA, CSA, and RA shall record the events identified in the list below. Where these events cannot be electronically logged, the CA, CSA, and RA shall supplement electronic audit logs with physical logs as necessary.

Table 2: Auditing Events

Auditable Event	CA	CSA	RA
SECURITY AUDIT			
Any changes to the audit parameters, eg, audit frequency, type of event audited	X	X	X
Any attempt to delete or modify the audit logs	X	X	X
IDENTIFICATION AND AUTHENTICATION			
Successful and unsuccessful attempts to assume a role	X	X	X
The value of *maximum Authentication attempts* is changed	X	X	X
The number of unsuccessful Authentication attempts exceeds the *maximum Authentication attempts* during user login	X	X	X
An Administrator unlocks an account that has been locked as a result of unsuccessful Authentication attempts	X	X	X
An Administrator changes the type of Authentication, eg, from a password to biometric	X	X	X
LOCAL DATA ENTRY			
All security-relevant data that is entered in the system	X	X	X
REMOTE DATA ENTRY			
All security-relevant messages that are received by the system	X	X	X
DATA EXPORT AND OUTPUT			
All successful and unsuccessful requests for confidential and security-relevant information	X	X	X

Auditable Event	CA	CSA	RA
KEY GENERATION			
Whenever the Component generates a key. (Not mandatory for single session or one-time use symmetric keys)	X	X	X
PRIVATE KEY LOAD AND STORAGE			
The loading of Component private keys	X	X	X
All access to certificate Subject private keys retained within the CA for key recovery purposes	X	N/A	N/A
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE			
All changes to the trusted public keys, including additions and deletions	X	X	X
SECRET KEY STORAGE			
The manual entry of secret keys used for Authentication	X	X	X
PRIVATE AND SECRET KEY EXPORT			
The export of private and secret keys (keys used for a single session or message are excluded)	X	X	X
CERTIFICATE REGISTRATION			
All certificate requests	X	N/A	X
CERTIFICATE REVOCATION			
All certificate revocation requests	X	N/A	X
CERTIFICATE STATUS CHANGE APPROVAL			
The approval or rejection of a certificate status change request	X	N/A	N/A
CA CONFIGURATION			
Any security-relevant changes to the configuration of the component	X	X	X
ACCOUNT ADMINISTRATION			
Roles and users are added or deleted	X	-	-
The Access Control privileges of a user account or a role are modified	X	-	-
CERTIFICATE PROFILE MANAGEMENT			
All changes to the certificate profile	X	N/A	N/A

Auditable Event	CA	CSA	RA
CERTIFICATE STATUS AUTHORITY MANAGEMENT			
All Changes to the CSA profile (eg, OCSP Profile)	N/A	X	N/A
REVOCATION PROFILE MANAGEMENT			
All changes to the revocation profile	X	N/A	N/A
CRL PROFILE MANAGEMENT			
All changes to the CRL profile	X	N/A	N/A
MISCELLANEOUS			
Appointment of an individual to a Trusted Role	X	X	X
Designation of personnel for multiparty control	X	-	N/A
Installation of the operating system	X	X	X
Installation of the PKI application	X	X	X
Installing hardware cryptographic modules	X	X	X
Removing hardware cryptographic modules	X	X	X
Destruction of cryptographic modules	X	X	X
System startup	X	X	X
Logon attempts to PKI applications	X	X	X
Receipt of hardware / software	X	X	X
Attempts to set passwords	X	X	X
Attempts to modify passwords	X	X	X
Backing up CA internal database	X	-	-
Restoration from backup of the internal CA database	X	-	-
File manipulation (eg, creation, renaming, moving)	X	-	-
Posting of any material to a PKI repository	X	-	-
Access to CA internal database	X	X	-
All certificate Compromise notification requests	X	N/A	X
Re-key of the component	X	X	X

Auditable Event	CA	CSA	RA
CONFIGURATION CHANGES			
Hardware	X	X	-
Software	X	X	X
Operating system	X	X	X
Patches	X	X	-
Security profiles	X	X	X
PHYSICAL ACCESS / SITE SECURITY			
Personnel access to room housing component	X	-	-
Access to the component	X	X	-
Known or suspected violations of physical security	X	X	X
ANOMALIES			
Software error conditions	X	X	X
Software check integrity failures	X	X	X
Receipt of improper messages	X	X	X
Misrouted messages	X	X	X
Network attacks (suspected or confirmed)	X	X	X
Equipment failure	X	-	-
Electrical power outages	X	-	-
Uninterruptible Power Supply (UPS) failure	X	-	-
Obvious and significant network service or access failure	X	-	-
Violations of CP	X	X	X
Violations of CPS	X	X	X
Resetting Operating System Clock	X	X	X

5.4.2 Frequency of Processing Log

Audit logs shall be reviewed at least once every thirty (30) days, unless the CA is offline, in which case the audit logs shall be reviewed when the system is activated or every thirty (30) days, whichever is later. Statistically significant

samples of security audit data generated by the CA, CSA, or RA since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for evidence of malicious activity. The Audit Administrator shall explain all significant events in an audit log summary. Actions taken as a result of these reviews shall be documented.

Such reviews involve verifying that the log has not been tampered with, there is no discontinuity or other loss of audit data, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs.

5.4.3 Retention Period for Audit Log

Audit logs shall be retained onsite for at least sixty (60) days and must be retained in the manner described below. For the CA and CSA, the Audit Administrator shall be the only person managing the audit log (eg, review, backup, rotate, delete). For the RA, a system administrator other than the RA shall be responsible for managing the audit log.

5.4.4 Protection of Audit Logs

System configuration and operational procedures shall be implemented together to ensure that:

- Only authorized people have read access to the logs;
- Only authorized people may Archive audit logs; and
- Audit logs are not modified.

The person performing audit log Archive need not have modify access, but procedures must be implemented to protect archived data from destruction prior to the end of the audit log retention period (note that deletion requires modification access). Audit logs shall be moved to a safe, secure storage location separate from the CA equipment.

It is acceptable for the system to over-write audit logs after they have been backed up and archived.

5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries shall be backed up at least monthly, unless the CA is offline, in which case audit logs and audit summaries shall be backed up when the system is activated or every thirty (30) days, whichever is later. A copy of the audit log shall be sent off-site in accordance with the CPS following review.

5.4.6 Audit Collection System (Internal vs External)

The audit log collection system may or may not be external to the CA, CSA, or RA system. Automated audit processes shall be invoked at system or application startup, and cease only at system or application shutdown. Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, then the CA shall determine whether to suspend CA operation until the problem is remedied.

5.4.7 Notification to Event-Causing Subject

There is no requirement to notify a Subject that an event was audited. Real-time alerts are neither required nor prohibited by this CP.

5.4.8 Vulnerability Assessments

No stipulation beyond Section 5.4.2.

5.5 RECORDS ARCHIVAL

5.5.1 Types of Events Archived

CA, CSA, and RA Archive records shall be sufficiently detailed to determine the proper operation of the PKI and the validity of any certificate (including those revoked or expired) issued by the CA. At a minimum, the following data shall be recorded for Archive:

Table 3: Archiving Events

Data To Be Archived	CA	CSA	RA
Certificate Policy	X	X	X
Certification Practice Statement	X	X	X
Contractual obligations	X	X	X
System and equipment configuration	X	X	-
Modifications and updates to system or configuration	X	X	-
Certificate requests	X	-	-
All certificates issued and/or published	X	N/A	N/A
Record of component re-key	X	X	X
Revocation requests	X	-	-
Subscriber identity Authentication data as per Section 3.2.3	X	N/A	X
Documentation of receipt and acceptance of certificates	X	N/A	X
Subscriber Agreements	X	N/A	X
Documentation of receipt of tokens	X	N/A	X
All CRLs issued and/or published	X	N/A	N/A
All audit logs	X	X	X
Other data or applications to verify Archive contents	X	X	X
Compliance auditor reports	X	X	X

5.5.2 Retention Period for Archive

Archive records must be kept for a minimum of ten (10) years and six (6) months, or as further required by applicable law or industry regulation.

If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the Archive site. Alternatively, an entity may retain data using whatever procedures have been approved by the Australian and/or U.S. National Archives and Records Administration for that

category of documents. Applications required to process the Archive data shall also be maintained for the minimum retention period specified above.

5.5.3 Protection of Archive

The Archive must be protected as specified by the privacy laws of the country where the Device information was collected.

No unauthorized user shall be permitted to write to, modify, or delete the Archive. For the CA and CSA, the authorized individuals are Audit Administrators. For the RA, the authorized individuals must be someone other than the RA (eg, Information Assurance Officer or IAO). The contents of the Archive shall not be released except as determined by the CA, or as required by law. Records of individual transactions may be released upon request of any Subscriber involved in the transaction or their legally recognized agents. Archive media shall be stored in a safe, secure storage facility separate from the PKI components (CA, CSA, or RA) with physical and procedural security controls equivalent or better than those for the PKI.

5.5.4 Archive Backup Procedures

The CPS or a referenced document shall describe how Archive records are backed up, and how the Archive backups are managed.

5.5.5 Requirements for Timestamping of Records

CA Archive records shall be automatically timestamped as they are created. The CPS shall describe how system clocks used for time-stamping are maintained in synchrony with an authoritative time standard.

5.5.6 Procedures to Obtain and Verify Archive Information

Procedures, detailing how to create, verify, package, transmit, and store Archive information, shall be described in the applicable CPS.

5.6 KEY CHANGEOVER

To minimize the risk from Compromise of a CA's private signing key, that key may be changed often; from that time on, only the new key shall be used for certificate signing purposes. The older, but still valid, certificate will be available to verify old signatures until all the certificates signed using the associated private key have also expired. If the old private key is used to sign CRLs, then the old key shall be retained and protected.

Refer to Section 6.3.2 for certificate operational periods and key pair usage periods.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

If a CA or CSA detects a potential hacking attempt or other form of Compromise, it shall perform an investigation in order to determine the nature and the degree of damage. If the CA or CSA key is suspected of Compromise, the procedures outlined in Section 5.7.3 shall be followed.

The ACCC PMA shall be notified if any CAs operating under this CP experience the following:

- suspected or detected Compromise of the CA systems;
- physical or electronic penetration of CA systems;
- successful denial of service attacks on CA components; or
- any incident preventing the CA from issuing a CRL within forty-eight (48) hours of the issuance of the previous CRL.

The ACCC PMA shall take appropriate steps to protect the integrity of the PKI.

The CA shall reestablish operational capabilities as quickly as possible in accordance with procedures set forth in the CA's CPS.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

When computing resources, software, and/or data are corrupted, CAs operating under this CP shall respond as follows:

- Before returning to operation, ensure that the system's integrity has been restored.
- If the CA signature keys are not destroyed, CA operation shall be reestablished, giving priority to the ability to generate certificate status information within the CRL issuance schedule specified in Section 4.9.7.
- If the CA signature keys are destroyed, CA operation shall be reestablished as quickly as possible, giving priority to the generation of a new CA key pair.
- If a CA cannot issue a CRL prior to the time specified in the next update field of its currently valid CRL, then all CAs that have been issued certificates by the CA shall be securely notified immediately. This will allow other CAs to protect their Subscriber's interests as Relying Parties.
- If the ability to revoke certificates is inoperative or damaged, the CA shall reestablish revocation capabilities as quickly as possible in accordance with procedures set forth in the respective CPS. If the CA's revocation capability cannot be established in a reasonable time-frame, the CA shall determine whether to request revocation of its certificate(s). If the CA is a Root CA, the CA shall determine whether to notify all Subscribers who use the CA as a trust anchor to delete the trust anchor.

5.7.3 Private Key Compromise Procedures

The Subscriber shall report any suspected or real compromise of their Private Key to their issuing CA or RA, and the CA shall follow the requirements listed in Section 4.9.

If a CA's signature keys are compromised, lost, or suspected to be compromised:

- All cross certified CAs shall be securely notified at the earliest feasible time (so that entities may issue CRLs revoking any cross-Certificates issued to the CA);
- A new CA key pair shall be generated by the CA in accordance with procedures set forth in the applicable CPS;
- New CA Certificates shall be requested in accordance with the initial registration process set elsewhere in this CP;
- The CA shall request all Subscribers to re-key using the procedures outlined in section 3.3.2; and
- If the CA is a Root CA, it shall provide the Subscribers the new trust anchor using secure means.

The ACCC PMA shall also investigate what caused the compromise or loss, and what measures must be taken to preclude recurrence.

If a CSA key is compromised, all Certificates issued to the CSA shall be revoked, if applicable. The CSA shall generate a new key pair and request new Certificate(s), if applicable. As a CSA operated by the ACCC PKI may not be a trust anchor, there are no specific requirements regarding trust anchor propagation.

If a CMS key is compromised, all Certificates issued to the CMS shall be revoked. The CMS shall generate a new key pair and request new Certificate(s).

If RA signature keys are compromised, lost, or suspected to be compromised:

- The RA Certificate shall be immediately revoked;
- A new RA certificate shall be requested in accordance with the initial registration process described elsewhere in this CP; and
- All certificate registration requests approved by the RA since the date of the suspected Compromise shall be reviewed to determine which are legitimate.

For those certificate requests or approval whose legitimacy cannot be ascertained, the resultant certificates shall be revoked and their Subjects (ie, Subscribers) shall be notified of revocation.

5.7.4 Business Continuity Capabilities after a Disaster

The CA Operator shall provide an alternate secure facility that conforms to all the provisions of the present document for resumption of the CA following any CA service interruption.

5.8 CA, CSA, OR RA TERMINATION

Prior to CA termination, the RA shall provide archived data to an Archive facility as specified in the CPS. As soon as possible, the CA will advise all other organizations to which it has issued certificates of its termination, using an agreed-upon method of communication specified in the CPS.

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

All Subscribers shall generate their own Digital Signature keys using an approved algorithm as detailed in Section 6.1.5.

The following table provides the requirements for key pair generation for the various entities:

Table 4: key pair Generation

Entity	FIPS 140-2 Level	Hardware Or Software	Key Storage Restricted To the Module on Which the Key Was Generated
CA	3	Hardware	Yes
RA	1	Software	No requirement
CSA	2	Hardware	Yes
Code Signing	2	Hardware	Yes
End-Entity	No requirement	Software/Hardware	No requirement

6.1.1.1 CA Key Pair Generation

CA keys shall be generated in a Key Generation Ceremony using multi-person control for CA key pair generation, as specified in Section 6.2.2.

CA key pair generation must create a verifiable audit trail showing that the security requirements for procedures were followed. The documentation of the procedure must be detailed enough to show that appropriate role separation was used.

6.1.1.2 Subscriber Key Pair Generationn

Subscriber key pair generation may be performed by the Subscriber, Sponsor CA, or RA. If the CA or RA generates Subscriber key pairs, the requirements for key pair delivery specified in Section 6.1.2 must also be met.

6.1.2 Private Key Delivery to the Subscriber or Sponsors

A CA shall generate its own key pair and therefore does not need private key delivery.

If Subscribers generate their own key pairs, then there is no need to deliver Private Keys, and this section does not apply.

When a CA or RA generates key pairs on behalf of a Subscriber, the private keys must be delivered securely to the Subscriber and the following requirements must be met:

- Anyone who generates a private signing key for a Subscriber shall not retain any copy of the key after delivery of the Private Key to the Subscriber;
- The Private Key shall be protected from activation, compromise, or modification during the delivery process;
- The Subscriber shall acknowledge receipt of the Private Key(s); and

- Delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers:
    - For hardware modules, accountability for the location and state of the module shall be maintained until the Subscriber accepts possession of it; and
    - For electronic delivery of Private Keys, the key material shall be encrypted using a cryptographic algorithm and key size at least as strong as the Private Key. Activation data shall be delivered using a separate secure channel. The CA or the RA shall maintain a record of the Device Sponsor acknowledgement of receipt of the token.

The CA or the RA shall maintain a record of the Subscriber acknowledgement of receipt of the token.

6.1.3 Public Key Delivery to Certificate Issuer

Where key pairs are generated by the Subscriber or RA, the public key and the Subscriber's identity shall be delivered securely to the CA for certificate issuance. The delivery mechanism shall bind the Subscriber's verified identity to the public key. If cryptography is used to achieve this binding, it shall be at least as strong as the CA keys used to sign the certificate.

6.1.4 CA Public Key Delivery to Relying Parties

The public key of a trust anchor shall be provided to the Relying Parties or Subscribers acting as Relying Parties in a secure manner so that the trust anchor is not vulnerable to modification or substitution.

6.1.5 Key Sizes

Key pairs shall be of sufficient length to prevent others from determining the key pair's private key using cryptanalysis during the period of expected utilization of such key pairs.

ACCC Certificates shall meet the following requirements for algorithm type and key size:

Table 5: Algorithm Type and Key Size

	Root CA	Sub-CA	Subscriber Cert
Supported Digest Algorithm	SHA-256 or 512	SHA-256 or 512	SHA-256 or 512
Supported Elliptic Curve Cryptography	P-256 or 384	P-256 or 384	P-256
Supported RSA	4096	2048 or 4096	2048 or 4096

6.1.6 Public Key Parameters Generation and Quality Checking

RSA keys shall be generated and have their prime numbers validated for primality in accordance with FIPS 186-3 except keys meant for use for the low assurance levels.

Elliptic Curve Cryptography (ECC) keys shall be generated in accordance with FIPS 186-4, and curves from FIPS 186-4 shall be used.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

The use of a specific key is determined by the key usage extension in the X.509 Certificate. The Certificate Profiles in section 10 specify the allowable values for this extension for different types of Certificates issued by the ACCC PKI CAs.

CA Certificates shall set the cRLSign and certSign bits.

Public keys that are bound into Certificates shall be certified for use in signing or encrypting, but not both. This restriction is not intended to prohibit use of protocols (like the Transport Layer Security) that provide authenticated connections using key management Certificates and require setting both digitalSignature and keyEncipherment bits to be set.

For End Entity certificates, the Extended Key Usage extension shall always be present and shall not contain anyExtendedKeyUsage OID.

The extended key usage shall meet the requirements stated in section 10.9. Extended Key Usage OIDs shall be consistent with key usage bits asserted.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards and Controls

The relevant standards for cryptographic modules are FIPS PUB 140-2, Security Requirements for Cryptographic Modules. The ACCC PMA may determine that other comparable validation, certification, or verification standards are sufficient. These standards shall be published by the ACCC PMA. Cryptographic modules shall be validated to the FIPS 140-2 level identified in section 6.1, or validated, certified, or verified to requirements published by the ACCC PMA.

The table in Section 6.1.1 summarizes the minimum requirements for cryptographic modules; higher levels may be used. In addition, private keys shall not exist outside the cryptographic module in *plaintext* form.

6.2.2 Private Key (n out of m) Multi-Person Control

A single person shall not be permitted to activate or access any cryptographic module that contains the complete CA private signing key. CA signature keys may be backed up only under two-person control. Access to CA signing keys backed up for disaster recovery shall be under at least two-person control. The names of the parties used for two-person control shall be maintained on a list that shall be made available for inspection during Compliance Audits.

6.2.3 Private Key Escrow

Digital Signature Private Keys may not be escrowed.

End-Entity Private Keys used solely for decryption shall be escrowed prior to the generation of the corresponding Certificates, with the exception of decryption Private Keys associated with aircraft and/or aircraft equipment encryption Certificates which do not need to be escrowed. Furthermore, if the data protected by these decryption keys will require recovery, such keys do not need to be escrowed.

If the CA retains the Subscriber private encryption keys for business continuity purposes, the CA shall escrow such keys to protect them from unauthorized modification or disclosure through physical and cryptographic means.

6.2.4 Private Key Backup

6.2.4.1 Backup of CA Private Signature Key

The CA private signature keys shall be backed up under the same multi-person control as used to generate and protect the original signature key. A single backup copy of the signature key shall be stored at or near the CA location.

A second backup copy shall be kept at the CA backup location.

Procedures for CA private signature key backup shall be included in the appropriate CPS and shall meet the multiparty control requirement of section 5.2.4.

6.2.4.2 Backup of Subscriber Private Signature Key

Subscriber private signature keys whose corresponding Public Key is contained in a Certificate asserting the basic-software or medium-software may be backed up or copied, but must be held in the Subscriber's control. Storage must ensure security controls consistent with the protection provided by the subscriber's Cryptographic Module.

Subscriber private signature keys whose corresponding Public Key is contained in a Certificate asserting an Assurance Level other than those listed above shall not be backed up or copied.

6.2.4.3 CSA Private Signature Key

If backed up, the CSA private signature keys shall be backed up under the same single or multi-person control as used to generate the CSA private signature key, and shall be accounted for and protected in the same manner as the original. A single backup copy of the CSA private signature key may be stored at or near the CSA location. A second backup copy may be kept at the CSA backup location. Procedures for CSA private signature key backup shall be included in the appropriate CPS.

6.2.5 Private Key Archival

Private signature keys shall not be archived.

6.2.6 Private Key Transfer into or from a Cryptographic Module

CA private keys may be exported from the cryptographic module only to perform CA key backup procedures as described in Section 6.2.4. At no time shall the CA private key exist in *plaintext* outside the cryptographic module.

All other keys shall be generated by and in a cryptographic module. In the event that a private key is to be transported from one cryptographic module to another, the private key must be encrypted during transport; private keys must never exist in *plaintext* form outside the cryptographic module boundary.

Private or symmetric keys used to encrypt other private keys for transport must be protected from disclosure.

Entry of a private key into a cryptographic module shall use mechanisms to prevent loss, theft, modification, unauthorized disclosure, or unauthorized use of such private key.

6.2.7 Private Key Storage on Cryptographic Module

The cryptographic module may store Private Keys in any form as long as the keys are not accessible without an authentication mechanism that is in compliance with the appropriate FIPS 140-2 level, as described in Section 6.1.1.

6.2.8 Method of Activating Private Key

The Subscriber must be authenticated to the cryptographic module before the activation of any Private Key(s). Acceptable means of authentication include but are not limited to passphrases, PINs, or biometrics. Entry of activation data shall be protected from disclosure (ie, the data should not be displayed while it is entered).

6.2.9 Method of Deactivating Private Key

Cryptographic modules that have been activated shall not be available to unauthorized access. After use, the cryptographic module shall be deactivated (eg, via a manual logout procedure or automatically after a period of inactivity). CA cryptographic modules shall be stored securely when not in use.

When an online CA is taken offline, the CA shall remove the token containing the private key from the reader in order to deactivate it.

With respect to the private keys of offline CAs, after the completion of a Key Generation Ceremony, in which such private keys are used for private key operations, the CA shall remove the token containing the private keys from the reader in order to deactivate them. Once removed from the reader, tokens shall be securely stored.

When deactivated, private keys shall be kept in encrypted form only. They shall be cleared from memory before the memory is de-allocated. Any disk space where private keys were stored shall be overwritten before the space is released to the operating system.

6.2.10 Method of Destroying Private Key

Private key destruction procedures shall be described in the CPS and must be sufficient to ensure that it is impossible to recover any part of the private key from any cryptographic module, memory or disk space.

If proper destruction of the private key cannot be guaranteed, then the key must be treated as compromised and the certificate revoked.

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The public key is archived as part of the certificate archival. The issuing CA shall retain all verification public keys for a minimum of twenty (20) years or as further required by applicable law or industry regulation.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

To minimize risk from compromise of a CA's private signing key, that key may be changed often; from that time on, only the new key shall be used for Certificate signing purposes. The older, but still valid, Certificate will be available to verify old signatures until all of the Certificates signed using the associated Private Key have also expired. If the old Private Key is used to sign CRLs, then the old key shall be retained and protected.

The following table provides the lifetimes for Certificates and associated Private Keys.

Table 6: Key Operational & Usage Period

Key	RSA 2048 Bit ECC P-256		RSA 4096 Bit ECC P-384	
	Private Key	Certificate	Private Key	Certificate
Root CAs	20 years	20 years	20 years	20 years
Sub CAs	15 years	15 years	15 years	15 years
Subscriber Identity or Signature	3 years	3 years	5 years	5 years
Subscriber Encryption	N/A	3 years	N/A	3 years
Role Identity or Signature	3 years	3 years	3 years	3 years
Role Encryption	N/A	3 years	N/A	3 years
Code Signer	10 years	10 years	10 years	10 years
PIV-AV Content Signer	3 years	9 years	3 years	3 years
Server or Device Identity or Signature	3 years	3 years	3 years	3 years
Server or Device Encryption	N/A	3 years	N/A	3 years

Key	RSA 2048 Bit ECC P-256		RSA 4096 Bit ECC P-384	
	Private Key	Certificate	Private Key	Certificate
OCSP Responders	10 years	10 years	15 years	15 years
Time-stamp Authority	10 year	10 years	10 year	10 years

A CA shall not generate a Certificate for a Subscriber whose validity period would be longer than the CA Certificate validity period. As a consequence, the CA key pair shall be changed at the latest at the time of CA Certificate expiration minus Subscriber Certificate validity duration.

Notwithstanding the above table, in all cases the CA private key may be used to sign OCSP Certificates and CRLs until the CA Certificate expires.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

The activation data used to unlock private keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected and shall meet the applicable security policy requirements of the cryptographic module used to store the keys.

Subscriber activation data may be user selected. For CAs, it shall either entail the use of biometric data or satisfy the policy-enforced at/by the cryptographic module. If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

When a CA uses passwords as activation data for the CA signing key, at a minimum the activation data shall be changed upon CA re-key.

To the extent passwords are used as Activation Data, the CA's activation participants shall generate passwords that cannot easily be guessed or cracked by dictionary attacks. Participants may not need to generate Activation Data, for example if they use biometric access Devices. These passwords shall be changed upon CA re-key.

6.4.2 Activation Data Protection

Data used to unlock private keys shall be protected from disclosure by a combination of cryptographic and physical Access Control mechanisms. Activation Data should be either biometric in nature or memorized. If written down, it shall be secured at the level of the data that the associated cryptographic module is used to protect, and shall not be stored with the cryptographic module. In all cases, the protection mechanism shall include a facility to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts as set forth in the respective certificate policy or CPS.

6.4.3 Other Aspects of Activation Data

CAs, CSAs, and RAs shall change the Activation Data whenever the token is re-keyed or returned for maintenance.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

The following computer security functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The CA, CSA, CMS and RA shall include the following functionality:

- Require authenticated logins;
- Provide discretionary Access Control, including managing privileges of users to limit users to their assigned roles;
- Provide a security audit capability (See Section 5.4);
- Prohibit object re-use;
- Require use of cryptography for session communication and database security;
- Require a trusted path for identification and Authentication;
- Provide domain isolation for processes;
- Provide self-protection for the operating system;
- Require self-test security related CA services (eg, check the integrity of the audit logs); and
- Support recovery from key or system failure.

The computer system shall be configured with the minimum of the required accounts and network services, and shall not permit remote login.

The computer system hosting the CA must have been hardened against all known threats.

6.5.2 Computer Security Rating

No stipulation.

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

The system development controls for the CA, CSA, CMS and CSA are as follows:

- Use software that has been designed and developed under a formal, documented development methodology;
- Procured hardware and software shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with (eg, by ensuring the equipment was randomly selected at time of purchase);
- Specially-developed hardware and software shall be developed in a controlled environment, and the development process shall be defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software;
- All hardware must be shipped or delivered via controlled methods that provide a continuous chain of accountability from the purchase location to the operations location;
- The hardware and software shall be dedicated to performing PKI activities. There shall be no other applications, hardware Devices, network connections, or component software installed which is not part of the PKI operation;
- Proper care shall be taken to prevent malicious software from being loaded onto the equipment. Applications required to perform PKI operations shall be obtained from sources authorized by local policy. CA, CSA, CMS and CSA hardware and software shall be scanned for malicious code on first use and periodically thereafter; and
- Hardware and software updates shall be purchased or developed in the same manner as original equipment, and shall be installed by trusted and trained personnel in a defined manner.

6.6.2 Security Management Controls

The configuration of the CA, CMS and CSA system, in addition to any modifications and upgrades, shall be documented and controlled. The CA, CMS and CSA software, when first loaded, shall be verified as being that supplied from the vendor, with no modifications, and be the version intended for use. The CA, CMS and CSA system shall provide a mechanism to periodically verify the integrity of the software as specified in the CPS.

The CA shall also have mechanisms and policies in place to control and monitor the configuration of the CA and CMS system.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 NETWORK SECURITY CONTROLS

CAs, CSAs, CMS and RAs shall employ appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Such measures shall include the use of guards, firewalls and filtering routers. Unused network ports and services shall be turned off. Any network software present shall be necessary to the functioning of the component.

Any boundary control Devices used to protect the network on which the PKI equipment is hosted shall deny all but the necessary services to the PKI equipment even if those services are enabled for other Devices on the network.

6.8 TIME-STAMPING

All CA, CMS and CSA components shall regularly synchronize with a time service such as National Institute of Standards and Technology (NIST) Atomic Clock or NIST Network Time Protocol Service. Time derived from the time service shall be used for establishing the time of:

- Initial validity type of a Device's certificate;
- Revocation of a Device's certificate;
- Posting of CRL updates; and
- OCSP or other CSA responses.

Certificates, CRLs, and other revocation database entries shall contain time and date information. Asserted times shall be accurate to within three (3) minutes. Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events (see Section 5.4.1).

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

ACCC Certificates shall contain the identity and attribute data of a subject using the base certificate with applicable extensions. The base certificate shall contain the version number of the certificate, the certificate's identifying serial number, the signature algorithm used to sign the certificate, the issuer's distinguished name, the Validity Period of the certificate, the subject's distinguished name, information about the subject's public key, and extensions (See Table 7 below).

Table 7: Certificate Profile Basic Fields

Field	[RFC5280] Section	Requirement or Recommendation
tbsCertificate	4.1.1.1	Follows [RFC 5280] guidance
version	4.1.2.1	See CP Section 7.1.1.
serialNumber	4.1.2.2	Shall be a unique positive integer assigned by the CA and shall not be longer than 20 octets.
signature	4.1.2.3	See CP Section 7.1.3.
issuer	4.1.2.4	See CP Section 7.1.4.
validity	4.1.2.5	See CP Section 6.3.2.
subject	4.1.2.6	See CP Section 7.1.4.
subjectPublicKeyInfo	4.1.2.7	See CP Section 7.1.3.
extensions	4.1.2.9	See CP Section 7.1.2.
signatureAlgorithm	4.1.1.2	Follows [RFC 5280] guidance
algorithmIdentifier	4.1.1.2	See CP Section 7.1.3.
algorithm	4.1.1.2	See CP Section 7.1.3.
parameters	4.1.1.2	See CP Section 7.1.3.
signatureValue	4.1.1.3	Follows [RFC 5280] guidance

7.1.1 Certificate Version Number(s)

ACCC Certificates shall be X.509 v3 certificates. The certificate version number shall be set to the integer value of "2" for Version 3 certificates.

7.1.2 Certificate Extensions

ACCC Certificate extensions provide methods for associating additional attributes with public keys and for managing relationships between CAs. ACCC Certificates shall follow the guidance in [RFC 5280/6818] and shall contain the standard extensions shown in Section 10, unless they are denoted as optional.

7.1.3 Algorithm Object Identifiers (OIDs)

Certificates issued under this CP shall use the following OIDs for signatures;

Table 8: Algorithm OIDs

Algorithm	OID
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1 (1) 11}
Sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1 (1) 12}
Sha512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1 (1) 13}
Ecdsa-with-Sha256	{iso(1) member-body(2) us(840) ansi-X9-62 (10045) signature (4) specified (3) sha256 (2)}
Ecdsa-with-Sha384	{iso(1) member-body(2) us(840) ansi-X9-62 (10045) signature (4) specified (3) sha384 (3)}

7.1.4 Name Forms

The Subject and Issuer fields of the Certificate shall be populated with a unique Distinguished Name (DN) in accordance with one or more of the X.500 series standards, with the attribute type as further constrained by RFC 5280. Subject and Issuer fields shall include attributes as detailed in Table 9 below.

Table 9: CA Certificates Subject Name Fields

Name	Field	Value	Requirement
countryName	(C=)	<Country Code>	Shall be the two-letter ISO 3166-1 country code for the country in which the Root CA's service provider's place of business is located.
organizationName	(O=)	<Organization>	Shall contain the issuer organization name.
organizationalUnitName	(OU=)	<Addition Information>	May contain one or more OUs containing additional identifying information.
commonName	(CN=)	<Name> CA	Shall contain the common name that identifies the CA (eg, ACCC Root CA and ACCC Issuing CA).

Subscriber Certificates

The following naming attributes shall be used to populate the Subject in Subscriber certificates issued under this CP:

Table 10: Subscriber Certificate Subject Fields

Name	Field	Value	Requirement
countryName	(C=)	<Country Name>	Shall be the two-letter ISO 3166-1 country code for the country in which the Subscriber's place of business is located.
organizationName	(O=)	<Organization>	Shall contain the Subscriber's organization name (or abbreviation thereof), trademark, or other meaningful identifier.
organizationalUnitName	[OU=]	<Addition Information>	[Optional] May contain one or more OUs containing additional identifying information.
See content description in Section 10	[CN=]	<Subscriber Identifier's>	Additional naming attributes for uniquely identifying the subject including common name, serialNumber, email.

7.1.5 Name Constraints

The CAs may assert critical or non-critical name constraints beyond those specified in the Certificate Formats in section 10 subject to the requirements above.

In the case where an ACCC PKI CA certifies another CA within the ACCC PKI, the certifying ACCC PKI CA shall impose restrictions on the name space authorised in the subordinate ACCC PKI CA, which are at least as restrictive as its own name constraints.

The ACCC PKI CAs shall not obscure a Subscriber Subject name. Issuer names shall not be obscured. ACCC PKI CAs may assert critical or non-critical name constraints beyond those specified in the Certificate Formats.

7.1.6 Certificate Policy Object Identifier

CA and Subscriber certificates issued under this CP shall assert the policy OID listed in Section 1.2.2 of this CP.

Table 14 and Table 15 show the *certificatePolicies* extension settings for ACCC Subscriber Certificates and specifies that all ACCC Subscriber Certificates:

- May include the *certificatePolicies* extension; and
- If included, shall set the criticality of the *certificatePolicies* extension to FALSE.

7.1.7 Usage of Policy Constraints Extension

The CAs shall not assert policy constraints in CA Certificates.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued under this CP may contain policy qualifiers such as user notice, policy name, and CP and/or CPS pointers.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Processing semantics for the critical certificate policy extension shall conform to RFC 5280 certification path processing rules.

7.2 CRL PROFILE

CRLs shall conform to [RFC 5280] and contain the basic fields and contents specified in Table 11 below:

Table 11: CRL Profile Basic Fields

Field	Referenced Standard	Section	Requirement or Recommendation
version	[RFC 5280]	5.1.2.1	See Section 7.2.1.
signature	[RFC 5280]	5.1.2.2	Algorithm used to sign the CRL as per Section 7.1.3.
issuer	[RFC 5280]	5.1.2.3	Entity that has signed and issued the CRL as per Section 7.1.4.
thisUpdate	[RFC 5280]	5.1.2.4	Indicates the issue date of the CRL. CRLs are effective upon issuance.
nextUpdate	[RFC 5280]	5.1.2.5	Indicates the date by which the next CRL will be issued.
revokedCertificates	[RFC 5280]	5.1.2.6	Listing of revoked certificates, including the Serial Number of the revoked certificate and the Revocation Date.
authorityKeyIdentifier	[RFC 5280]	5.2.1	Follows the guidance in RFC 5280. Criticality is FALSE.
cRLNumber	[RFC 5280]	5.2.3	A monotonically increasing sequence number for a given CRL scope and issuer. Criticality is FALSE.
signatureAlgorithm	[RFC 5280]	5.1.1.2	Follows the guidance in RFC 5280 as per Section 7.1.3.
signatureValue	[RFC 5280]	5.1.1.3	Follows the guidance in RFC 5280.

7.2.1 CRL Version Number(s)

The CAs shall support the issuance of X.509 Version 2 CRLs. The CRL version number shall be set to the integer value of "1" for Version 2 [RFC 5280, Section 5.1.2.1].

7.2.2 CRL and CRL Entry Extensions

Critical CRL extensions shall not be used. Section 10 contains the CRL formats.

7.3 OCSP PROFILE

OCSP requests and responses shall be in accordance with RFC 2560. Section 10 contains the OCSP request and response formats.

7.3.1 OCSP Version Number(s)

OCSP responses shall support use of OCSP version 1 as defined by [RFC 6960] and [RFC 5019].

7.3.2 OCSP Extensions

Responses shall support the nonce extension.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

ACCC may take reasonable steps to implement Compliance Audit mechanisms to ensure that the requirements of their certificate policy/CPS are being implemented and enforced.

This specification does not impose a requirement for any particular assessment methodology.

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

All CAs, RAs, CMS and CSAs operating under this CP may be subject to a periodic Compliance Audit.

8.2 IDENTITY AND QUALIFICATIONS OF ASSESSOR

The compliance auditor shall demonstrate competence in the field of Compliance Audits, and shall be thoroughly familiar with requirements of the applicable certificate policy. The compliance auditor must perform such Compliance Audits as a primary responsibility.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The compliance auditor shall either represent a firm, which is independent from the entities (CA or RA) being audited, or it shall be sufficiently organizationally separated from that entity to provide an unbiased, independent evaluation. An example of the latter situation may be an organizational audit department provided it can demonstrate organizational separation and independence. To further insure independence and objectivity, the compliance auditor may not have served the entity in developing or maintaining the entity's PKI facility, associated IT and network systems, or CPS. The ACCC PMA shall determine whether a compliance auditor meets this requirement.

In the event an entity chooses to engage compliance auditor services internal to its parent organization, it shall undergo an audit from an external third party audit firm every third year, at a minimum.

8.4 TOPICS COVERED BY ASSESSMENT

The purpose of a Compliance Audit shall be to verify that a component operates in accordance with the applicable certificate policy, CPS, the agreement between the PKI service provider and the ACCC PMA, and any additional MOAs between the PKI and other entities.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

When the compliance auditor finds a discrepancy between the requirements of this CP or the stipulations in the CPS and the design, operation, or maintenance of the PKI authorities, the following actions shall be performed:

- The compliance auditor shall note the discrepancy;
- The compliance auditor shall notify the responsible party promptly; and
- The party responsible for correcting the discrepancy shall determine what further notifications or actions are necessary pursuant to the requirements of the applicable certificate policy and agreement, and then proceed to make such notifications and take such actions without delay.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the ACCC PMA may decide to temporarily halt operation of the CA or RA, to revoke a certificate issued to the CA or RA, or take other actions it deems appropriate. The ACCC PMA will develop procedures for making and implementing such determinations. In accordance with Section 8.1, a Compliance Audit may be required to confirm the implementation and effectiveness of the remedy.

8.5.1 Factors Considered

The decision regarding what actions to take will be based on previous responses to problems, the severity of the deficiency, the risks a prohibition may impose and the disruption to the Community, and the recommendations of the Auditor.

8.6 COMMUNICATION OF RESULTS

A Compliance Audit report package, including identification of corrective measures taken or being taken by the PKI, shall be provided to the ACCC PMA as set forth in Section 8.1.

The report shall identify the versions of the CP and CPS used in the assessment. Additionally, where necessary, the results shall be communicated as set forth in 8.5 above.

8.6.1 Retention of Audit Reports

Results of all Audits, as well as the data used to generate these results must be kept for a minimum of ten (10) years or as further required by applicable law or industry regulation.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

ACCC, in its sole discretion, may determine whether to charge fees, and in what amount, for the issuance of certificates provided by the ACCC PKI.

9.2 CERTIFICATE ISSUANCE, MANAGEMENT AND RENEWAL FEES

ACCC is entitled to charge end-user Subscribers for the issuance, management, and renewal of certificates provided by the ACCC PKI.

9.3 CERTIFICATE ACCESS FEES AND OTHER SERVICES

ACCC, in its sole discretion, may determine whether to charge fees, and in what amount, for ACCC PKI services.

There shall be no fee associated with Relying Party access to Certificates in the ACCC PKI Directory.

9.4 REVOCATION OR STATUS INFORMATION ACCESS FEES

There shall be no fee associated with Relying Party access to certificate revocation or certificate status information.

9.5 FINANCIAL RESPONSIBILITY

9.5.1 Insurance Coverage

No stipulation.

9.6 CONFIDENTIALITY OF BUSINESS INFORMATION

Subscribers acknowledge that any information made public in a Certificate is deemed not private. In that respect, Certificates, OCSP responses, CRLs and personal or corporate information appearing in them and in public directories are not considered as private or confidential.

Personal and corporate information, which does not appear in certificates and in public directories, held by a CA or an RA is considered confidential and shall not be disclosed by the CA or RA. Unless required by law or court order, any disclosure of such information requires Subscriber's written prior consent.

The treatment of confidential business information provided to external PKIs in the context of submitting an application for cross certification will be in accordance with the terms of the agreements entered into between the applicable entity and ACCC.

Each CA shall maintain the confidentiality of confidential business information that is clearly marked or labelled as confidential or by its nature should reasonably be understood to be confidential, and shall treat such information with the same degree of care and security as the CA treats its own most confidential information.

9.7 PRIVACY OF PERSONAL INFORMATION

For the purposes of PKI related services, the ACCC PKI collects, stores, processes and discloses personally identifiable information in accordance with the terms of the ACCC Certificate Subscriber Agreement and applicable laws and regulations.

Details and requests to access the information collected by the ACCC PKI may be found at https://www.accc.gov.au/publications/accc-aer-privacy-policy

9.8 INTELLECTUAL PROPERTY RIGHTS

ACCC PKI CAs retain all intellectual property rights in and to the Certificates and revocation information that they issue. ACCC grants permission to reproduce and distribute its Certificates on a non-exclusive royalty-free basis, provided that they are reproduced in full and that use of Certificates is subject to a Relying Party Agreement with the relevant CA. The subscriber, who has a Certificate delivered by the ACCC PKI, retains all intellectual rights to the information it has provided and contained in the certificate delivered by ACCC PKI CA. An external CA, which cross-certifies with the ACCC PKI, retains all intellectual rights it owns in the information contained in the CA certificate delivered by ACCC PKI PCAs.

Except as ACCC may expressly authorize in writing, no party may:

- Reverse engineer, translate, disassemble, decompile the whole or any part of any software or system or any part therefore or otherwise attempt to access any software source code embedded in or operating using any system;
- Assign, transfer, sell, license, sub-license, lease, rent, charge or otherwise deal in or encumber, any software or system or any part thereof or use same on behalf of or for the benefit of any third party, or make available the same in any way whatsoever to any third party without the ACCC prior written consent;
- Remove or alter any trademark or any copyright or other proprietary notice on any software, system or any other materials;
- Distribute, create derivative works of or modify any materials, software or systems or any part thereof in anyway, or use, copy, duplicate or display same on a commercial or development basis; and
- Provide any service using a certificate provided by ACCC except as authorized and provided in this CP.

These restrictions shall not be construed in a manner that would violate any applicable law.

9.9 REPRESENTATION AND WARRANTIES

9.9.1 ACCC Representation

ACCC represents that, to its knowledge, Certificates issued subject to the mechanisms set out in this CP meet the material requirements of this CP.

9.9.2 Subscriber Representations

Prior to being issued a Certificate by a ACCC PKI CA Subscribers shall agree in a separate writing on the protection of the Private Key issued, specifically they agree to:

- Represent only themselves in all communications with the PKI authorities;
- Protect their Private Key (s) at all times and prevent them from unauthorized access in accordance with this CP;
- Promptly notify the appropriate ACCC CA or other CA for cross-certifications upon suspicion of loss or compromise of their Private Keys;
- Abide by all the terms, conditions, and restrictions levied on the use of their Private Key(s) and Certificates, as set forth in this CP;
- Use Certificates provided by the ACCC PKI CAs only for legal purposes and in accordance with this CP; and
- Cease to use ACCC certificates if they become invalid and remove them from any applications and/or devices they have been installed on.

9.9.3 Relying Party Representations

Parties who rely upon the Certificates issued under a policy defined in this document shall:

- Use the Certificate for the purpose for which it was issued, as indicated in the Certificate information (eg, the key usage extension);
- Check each Certificate for validity, using procedures described in the X.509 standard [ISO 9594-8], prior to reliance;

- Establish trust in the CA who issued a Certificate by verifying the Certificate path in accordance with the guidelines set by the X.509 Version 3 Amendment; and
- Preserve original signed data, the applications necessary to read and process that data, and the cryptographic applications needed to verify the digital signatures on that data for as long as it may be necessary to verify the signature on that data.

9.10 DISCLAIMER OF WARRANTY

To the extent permitted by applicable law, cross-certificates agreements and any other related agreements that may contain disclaimers of all warranties:

EXCEPT FOR THE EXPLICIT REPRESENTATIONS, WARRANTIES, AND CONDITIONS PROVIDED IN THIS CP OR THOSE BETWEEN THE AUSTRALIAN COMPETITION AND CONSUMER COMMISSION AND ITS CUSTOMERS UNDER SEPARATE AGREEMENTS AND TO THE EXTENT PERMITTED BY APPLICABLE LAW, (A) CERTIFICATES ISSUED BY AUSTRALIAN COMPETITION AND CONSUMER COMMISSION AND THE AUSTRALIAN COMPETITION AND CONSUMER COMMISSION PKI ARE PROVIDED "AS IS", AND AUSTRALIAN COMPETITION AND CONSUMER COMMISSION, ITS EMPLOYEES, OFFICERS, AGENTS, REPRESENTATIVES, AND DIRECTORS DISCLAIM ALL OTHER WARRANTIES, REPRESENTATIONS, TERMS, CONDITIONS AND OBLIGATIONS OF EVERY TYPE, WHETHER EXPRESSED, IMPLIED OR STATUTORY (INCLUDING, WITHOUT LIMITATION, ANY REPRESENTATIONS AND WARRANTIES OF SUITABILITY, SATISFACTORY QUALITY OR FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, TITLE, SECURITY, OR ACCURACY OF INFORMATION PROVIDED), AND FURTHER DISCLAIM ANY AND ALL LIABILITY FOR NEGLIGENCE, FAILURE TO WARN and/OR LACK OF REASONABLE CARE AND (B) THE ENTIRE RISK OF THE USE OF ANY AUSTRALIAN COMPETITION AND CONSUMER COMMISSION CERTIFICATES, ANY SERVICES PROVIDED BY AUSTRALIAN COMPETITION AND CONSUMER COMMISSION, OR THE VALIDATION OF ANY DIGITAL SIGNATURES LIES WITH THE APPLICABLE PARTICIPANT.

THIS CLAUSE IS SUBJECT ALWAYS TO SECTION 9.11 (LIMITATIONS OF LIABILITY).

9.11 LIMITATIONS OF LIABILITY

The liability of Subscribers shall be as set forth in the applicable terms accepted by Subscriber prior issuance of a Certificate. and Conditions, subject to the applicable law governing the relationship between the parties.

The liability (and/or limitation thereof) of Relying Parties shall be as set forth in the applicable Relying Party Agreements between the applicable ACCC CA and the Relying Party.

OTHER THAN THE ABOVE DESCRIBED LIMITATIONS OF LIABILITY, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL AUSTRALIAN COMPETITION AND CONSUMER COMMISSION BE LIABLE FOR ANY INDIRECT DAMAGES OF ANY KIND, INCLUDING CONSEQUENTIAL, INCIDENTAL, SPECIAL, PUNITIVE, ANY COSTS, EXPENSES, OR LOSS OF PROFITS, OR OTHER DAMAGES WHATSOEVER ARISING OUT OF OR RELATED TO THIS CP, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO EVENT SHALL AUSTRALIAN COMPETITION AND CONSUMER COMMISSION BE LIABLE FOR ANY USAGE OF A CERTIFICATE THAT EXCEEDS THE LIMITATIONS OF USAGE STATED IN THIS CP OR THAT IS NOT IN COMPLIANCE WITH THIS CP.

AUSTRALIAN COMPETITION AND CONSUMER COMMISSION SHALL NOT BE LIABLE FOR ANY DAMAGE ARISING FROM THE COMPROMISE OF A SUBSCRIBER'S CERTIFICATE, LOSS OF ANY DATA OR ANY OTHER LIABILITY WHATSOEVER IN CONNECTION WITH A CERTIFICATE.

SAVE FOR LIABILITY WHICH IS NOT PERMISSIBLE AT LAW TO BE CAPPED, THE TOTAL, AGGREGATE LIABILITY OF EACH AUSTRALIAN COMPETITION AND CONSUMER COMMISSION CA ARISING OUT OF OR RELATED TO IMPROPER ACTIONS BY THE AUSTRALIAN COMPETITION AND CONSUMER COMMISSION CA SHALL BE LIMITED TO ONE THOUSAND DOLLARS ($1,000 USD).

9.12 INDEMNITIES

9.12.1 Indemnification by Relying Parties

To the extent permitted by applicable law, and any applicable contractual agreements, Relying Party agrees to indemnify and hold ACCC harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind including reasonable attorneys' fees that ACCC may incur as a result of:

- The Relying Party's failure to perform the obligations of a Relying Party;
- The Relying Party's reliance on a Certificate; or
- The Relying Party's failure to check the status of such Certificate to determine if the Certificate is expired or revoked.

Any applicable contractual agreement with ACCC may include additional indemnity obligations.

9.12.2 Indemnification by Subscribers

To the extent permitted by applicable law, Subscriber agrees to indemnify and hold ACCC harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind including reasonable attorneys' fees that ACCC may incur as a result of:

- Falsehood or misrepresentation of fact by the Subscriber on the Subscriber's Certificate Application;
- Fraudulent or negligent use of certificates by the Subscriber;
- Unauthorized use of the certificates by Subscribers including use of certificates beyond the prescribed use defined by this CP;
- Failure by the Subscriber to disclose a material fact on the Certificate Application;
- The Subscriber's failure to protect the Subscriber's Private Key, to use a Trustworthy System, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's Private Key; or
- The Subscriber's use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the Intellectual Property Rights of a third party.

The applicable terms may include additional indemnity obligations.

9.13 TERM AND TERMINATION

9.13.1 Term

This CP becomes effective upon its adoption by the ACCC PMA and publication in the appropriate directory. Amendments to this CP shall become effective upon execution by the ACCC PMA and publication in the appropriate Repository.

9.13.2 Termination

While this CP may be amended from time to time, it shall remain in force until replaced by a newer version.

ACCC may decide to terminate this CP as a right, at any time, for convenience. If the ACCC terminates this CP in accordance with this Section 9.13.2, the ACCC reserves the right to revoke any Certificate. All Entities shall be notified 6 (six) months prior to the effective termination of this CP.

9.13.3 Effect of Termination and Survival

Upon termination of this CP, CAs cross-certified with or subordinate to ACCC PKI CAs are nevertheless bound by its terms for all Certificates issued for the remainder of the validity periods of such Certificates. Termination or expiration shall not affect any provision of this CP which is expressly or by implication intended to come into or remain in effect on or after termination or expiration, including the following sections of this CP: 2.1, 2.2, 5.4, 5.5, 6.2-6.4, 6.8, 9.2-9.4, 9.7-9.10, 9.13-9.15.7.

9.14 AMENDMENTS

9.14.1 Procedure for Amendment

The ACCC PMA shall review this CP at least once every year.

If the ACCC PMA wishes to recommend amendments or corrections to this CP such modifications shall be circulated to appropriate parties identified by the ACCC PMA. Comments from such parties will be collected and considered by the ACCC PMA. Following approval by the ACCC PMA, public notification of amendments shall be made.

Notwithstanding the foregoing, if the ACCC PMA believes that material amendments to the CP are necessary immediately to stop or prevent a breach of the security of ACCC, the ACCC PMA shall be entitled to make such amendments effective immediately upon publication in the Repository without having to circulate the amendments prior to their adoption.

9.14.2 Notification Mechanism and Period

This CP and any subsequent changes shall be made publicly available within seven (7) days of approval by the ACCC PMA. The Subscriber shall be bound by the most up to date version of the CP from its date of publication.

The most up to date copy of this CP can be found at https://www.cdr.gov.au/.

9.14.3 Circumstances Under Which OID Must be Changed

Certificate policy OIDs shall be changed if the ACCC PMA determines that a change in this Certificate Policy reduces the level of assurance provided.

9.15 MISCELLANEOUS PROVISIONS

9.15.1 Dispute Resolution Provisions

The ACCC PMA shall facilitate the resolution between entities when conflicts arise as a result of the use of certificates issued under this CP.

9.15.2 Governing Law

This CP will be governed by the laws of the Australian Capital Territory, without regard to conflicts of law principles. Application of the Uniform Computer Information Transactions Act and United Nations Convention on Contracts for the International Sale of Goods, 1980, and any successor law to either is specifically excluded. Courts with jurisdiction in the Australian Capital Territory will have exclusive jurisdiction to adjudicate any dispute arising out of or related to this CP and the parties hereby submit to the jurisdiction of such courts.

9.15.3 Compliance with Applicable Law

Each party will comply with all applicable international, national and U.S. federal, state and local laws, regulations and ordinances in performance or reliance on this CP.

9.15.4 Assignment

ACCC may assign any rights or obligations it may have under this CP without the advance written consent of the other party, other parties may not assign any rights or obligations without ACCC`s consent, not to be unreasonably withheld.

9.15.5 Severability

If any provision or portion of a provision of this CP is determined to be illegal, invalid, or unenforceable, the validity of the remaining provisions will not be affected. The parties may agree to replace the stricken provision with a valid and enforceable provision as set out in this CP.

9.15.6 Waiver

The failure of either party to enforce at any time any provision of this CP will not be construed to be a continuing waiver of those provisions.

9.15.7 Force Majeure

Neither party will be liable to the other for any failure to meet its obligations due to any Force Majeure event. Force Majeure is an event beyond the reasonable control of the non-performing party and may include but is not limited to: (a) delays or refusals to grant an export license or the suspension or revocation thereof, (b) any other acts of any government that would limit a party's ability to perform under this Agreement, (c) fires, earthquakes, floods, tropical storms, hurricanes, tornadoes, severe weather conditions, or any other acts of God, (d) quarantines or regional medical crises, (e) shortages or inability to obtain materials or components, (f) labor strikes or lockouts, and (g) riots, strife, insurrection, civil disobedience, landowner disturbances, armed conflict, terrorism or war, declared or not (or impending threat of any of the foregoing, if such threat might reasonably be expected to cause injury to people or property) (h) failure of equipment, failure of telecommunications lines, lack of internet access, sabotage. If a force majeure event causes a delay, then the date of performance will be extended by the period of time that the non-performing party is actually delayed, or for any other period as the parties may agree in writing.

THE AUSTRALIAN COMPETITION AND CONSUMER COMMISSION HAS NO LIABILITY FOR ANY DELAYS, NON-DELIVERIES, NON-PAYMENTS, MIS-DELIVERIES OR SERVICE INTERRUPTIONS CAUSED BY ANY THIRD PARTY ACTS OR THE INTERNET INFRASTRUCTURE OR ANY NETWORK EXTERNAL TO THE AUSTRALIAN COMPETITION AND CONSUMER COMMISSION.

10. CERTIFICATE, CRL AND OCSP FORMATS

This section contains the formats for the various PKI objects such as Certificates, CRLs, and OCSP requests and responses.
Certificates and CRLs issued under a policy OID of this CP shall not contain any critical extensions not listed in the profiles in this section or in Section 7.1.2. Certificates and CRLs issued under a policy OID of this CP may contain non-critical extensions not listed in the profiles in this section provided interoperability is not affected.

When multiple entries are asserted in the caIssuers field of the AIA extension and CRL Distribution Point, the first shall point to a resource that is publicly available and when both LDAP and HTTP URIs are given, the HTTP URI shall be listed first.

CAs may issue partitioned CRLs according to the following criteria:

- The CRLs are not indirect CRLs;
- The CRLs are not partitioned by reason code; and
- CRL Distribution Point and Issuing Distribution Point do not assert a name relative to the Issuer.

If the CA provides OCSP services, the CA must also issue a full and complete CRL (ie, a CRL without an Issuing Distribution Point extension) for use by the OCSP responder.

10.1 SELF-SIGNED ROOT CERTIFICATE (TRUST ANCHOR)

Table 12: Self-Signed Root Certificate

Field	Minimum Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11} or ecdsa-with-Sha256 {1 2 840 10045 4 3 2}
Issuer Distinguished Name	Unique X.500 CA DN as specified in Section 7.1.4 of this CP
Validity Period	As per Section 6.3.2
Subject Distinguished Name	Unique X.500 CA DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	for RSA: 4096-bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1} for ECC: 384 bit prime, id-ecPublicKey {1 2 840 10045 2 1}
Issuer's Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11} or ecdsa-with-sha256 WithRSAEncryption {1 2 840 10045 4 3 2}

Extension	Minimum Value
Subject Key Identifier	c=no; Octet String (Method 1)
Key Usage	c=yes; digitalSignature, keyCertSign, cRLSign, Off-line cRLSigning
Basic Constraints	c=yes; cA=True; path length constraint absent

10.2 SUBORDINATE CA CERTIFICATE (INTERMEDIATE & ISSUING CAS)

Table 13: SubCA Certificates

Field	Minimum Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11} or ecdsa-with-Sha256 {1 2 840 10045 4 3 2}
Issuer Distinguished Name	Unique X.500 CA DN as specified in Section 7.1.4 of this CP
Validity Period	As per Section 6.3.2
Subject Distinguished Name	Unique X.500 CA DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	for RSA: 2048-bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1} for ECC: 256 bit prime, id-ecPublicKey {1 2 840 10045 2 1}
Issuer's Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11} or ecdsa-with-sha256 WithRSAEncryption {1 2 840 10045 4 3 2}

Extension	Minimum Value
Authority Key Identifier	c=no; Octet String (Method 1 Key ID)
Subject Key Identifier	c=no; Octet String (Method 1)
Key Usage	c=yes; digitalSignature, keyCertSign, cRLSign, Off-line cRLSigning
Basic Constraints	c=yes; cA=True; path length constraint per Issuer PKI.
Certificate Policies	c=no; {Issuer's CP OID n} ... as per Section 1.2.2 and Section 7.1.6
CRL Distribution Points	c=no; distributionPoint shall be the only field populated, and it shall contain an LDAP and/or HTTP URI. The reason and crlIssuer fields shall not be populated. The CRL shall point to a full and complete CRL or a Distribution Point based partitioned CRL. The Distribution Point field shall contain a full name (ie, the Distribution Point field shall not contain nameRelativetoCRLIssuer)

10.3 Device Authentication Certificate

Table 14: Device Authentication Certificates

Field	Minimum Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11} or ecdsa-with-Sha256 {1 2 840 10045 4 3 2}
Issuer Distinguished Name	Unique X.500 CA DN as specified in Section 7.1.4 of this CP
Validity Period	As per Section 6.3.2
Subject Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP cn={ Host URL | Host IP Address | Host Name }
Subject Public Key Information	for RSA: 2048-bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1} for ECC: 256 bit prime, id-ecPublicKey {1 2 840 10045 2 1}
Issuer's Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11} or ecdsa-with-sha256 WithRSAEncryption {1 2 840 10045 4 3 2}

Extension	Minimum Value
Authority Key Identifier	c=no; Octet String (Method 1 Key ID)
Subject Key Identifier	c=no; Octet String (Method 1)
Key Usage	c=yes; digitalSignature. keyEncipherment (optional)
Extended Key Usage	c=no; As per Section 10.9
Basic Constraints	c=yes; EE=True; path length None.
Certificate Policies	c=no; {Issuer's CP OID n} ... as per Section 1.2.2 and Section 7.1.6
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing certificates issued to Issuing CA or LDAP URL pointer to the cACertificate attribute of the Issuing CA; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points	c=no; distributionPoint shall be the only field populated, and it shall contain an LDAP and/or HTTP URI. The reason and crlIssuer fields shall not be populated. The CRL shall point to a full and complete CRL or a Distribution Point based partitioned CRL. The Distribution Point field shall contain a full name (ie, the Distribution Point field shall not contain nameRelativetoCRLIssuer)
Subject Alternative Name	C=no, always present, Host URL | IP Address | Host Name

10.4 Subscriber Identity Certificate

Table 15: Subscriber Identity Certificates

Field	Minimum Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11} or ecdsa-with-Sha256 {1 2 840 10045 4 3 2}
Issuer Distinguished Name	Unique X.500 CA DN as specified in Section 7.1.4 of this CP
Validity Period	As per Section 6.3.2
Subject Distinguished Name	Unique X.500 subject DN conforming to section 7.1.4 of this CP
Subject Public Key Information	for RSA: 2048-bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1} for ECC: 256 bit prime, id-ecPublicKey {1 2 840 10045 2 1}
Issuer's Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11} or ecdsa-with-sha256 WithRSAEncryption {1 2 840 10045 4 3 2}

Extension	Minimum Value
Authority Key Identifier	c=no; Octet String (Method 1 Key ID)
Subject Key Identifier	c=no; Octet String (Method 1)
Key Usage	c=yes; digitalSignature
Extended Key Usage	c=no; As per Section 10.9
Basic Constraints	c=yes; EE=True; path length None.
Certificate Policies	c=no; {Issuer's CP OID n} ... as per Section 1.2.2 and Section 7.1.6
Subject Alternative Name	c=no; URI (mandatory for PIV-AV-hardware, otherwise optional); others optional
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing certificates issued to Issuing CA or LDAP URL pointer to the cACertificate attribute of the Issuing CA; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points	c=no; distributionPoint shall be the only field populated, and it shall contain an LDAP and/or HTTP URI. The reason and crlIssuer fields shall not be populated. The CRL shall point to a full and complete CRL or a Distribution Point based partitioned CRL. The Distribution Point field shall contain a full name (ie, the Distribution Point field shall not contain nameRelativetoCRLIssuer)

10.5 OCSP RESPONDER CERTIFICATE

Table 16: OCSP Responder Certificates

Field	Minimum Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11} or ecdsa-with-Sha256 {1 2 840 10045 4 3 2}
Issuer Distinguished Name	Unique X.500 CA DN as specified in Section 7.1.4 of this CP
Validity Period	As per Section 6.3.2
Subject Distinguished Name	Unique X.500 OCSP Responder (subject) DN conforming to section 7.1.4 of this CP
Subject Public Key Information	for RSA: 2048-bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1} for ECC: 256 bit prime, id-ecPublicKey {1 2 840 10045 2 1}
Issuer's Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11} or ecdsa-with-sha256 WithRSAEncryption {1 2 840 10045 4 3 2}

Extension	Minimum Value
Authority Key Identifier	c=no; Octet String (Method 1 Key ID)
Subject Key Identifier	c=no; Octet String (Method 1)
Key Usage	c=yes; digitalSignature, nonRepudiation
Extended Key Usage	c=yes; id-kp-OCSPSigning {1 3 6 1 5 5 7 3 9}
Basic Constraints	c=yes; EE=True; path length None.
Certificate Policies	c=no; {Issuer's CP OID n} ... as per Section 1.2.2 and Section 7.1.6
Subject Alternative Name	c=no; HTTP URL for the OCSP Responder
No Check id-pkix-ocsp-nocheck; {1 3 6 1 5 5 7 48 1 5}	c=no; Null
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing certificates issued to Issuing CA or LDAP URL pointer to the cACertificate attribute of the Issuing CA; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder

10.6 CRL FORMAT

Table 17: CRL Format

Field	Minimum Value
Version	V2 (1)
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11} or ecdsa-with-Sha256 {1 2 840 10045 4 3 2}
Issuer Distinguished Name	Unique X.500 CA DN as specified in Section 7.1.4 of this CP
thisUpdate	expressed in UTCTime until 2049
nextUpdate	expressed in UTCTime until 2049 (>= thisUpdate + CRL issuance frequency)
Revoked certificates list	0 or more 2-tuple of certificate serial number and revocation date (in Generaliized Time)
Issuer's Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11} or ecdsa-with-sha256 WithRSAEncryption {1 2 840 10045 4 3 2}

Extension	Minimum Value
CRL Number	c=no; monotonically increasing integer (never repeated)
Authority Key Identifier	c=no; Octet String (same as in Authority Key Identifier field in certificates

CRL Entry Extension	Minimum Value
Reason Code	c=no; optional, must be included when reason code = key compromise or CA compromise

10.7 OCSP Request Format

Table 18: OCSP Request Format

Field	Minimum Value
Version	V1 (0)
Requestor Name	DN of the requestor (required)
Request List	List of certificates as specified in RFC 2560

Request Extension	Minimum Value
None	None

Request Entry Extension	Minimum Value
None	None

10.8 OCSP Response Format

Table 19: OCSP Response Format

Field	Minimum Value
Response Status	As specified in RFC 2560
Response Type	id-pkix-ocsp-basic {1 3 6 1 5 5 7 48 1 1}
Version	V1 (0)
Responder ID	Octet String (same as subject key identifier in Responder certificate)
Produced At	Produced At Generalized Time
List of Responses	Each response will contain certificate id; certificate status (including revocation time and revocation reason, if applicable), thisUpdate (from CA CRL), and nextUpdate (from CA CRL).
Responder Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11} or ecdsa-with-Sha256 {1 2 840 10045 4 3 2}
Certificates	Applicable certificates issued to the OCSP Responder

Response Extension	Minimum Value
Nonce	c=no; Value in the nonce field of request (required, if present in request)

Response Entry Extension	Minimum Value
None	None

10.9 Extended Key Usage (EKU)

Table 20: Extended Key Usage

Certificate Type	Required EKU	Optional EKU	Prohibited EKU
CA	None	None	All
OCSP Responder	id-kp-OCSPSigning {1 3 6 1 5 5 7 3 9}	None	All Others
Subscriber, Group, Role: Authentication	id-kp-clientAuth {1.3.6.1.5.5.7.3.2}; smartCardLogon {1.3.6.1.4.1.311.20.2.2}; id-pkinit-KPClientAuth {1 3 6 1 5 2 3 4}	None	All Others
Subscriber, Group, Role, and Organisation Subscriber: Signature	id-kp-emailProtection {1.3.6.1.5.5.7.3.4}; Adobe Certified Document Signing {1.2.840.113583.1.1.5}	None	All Others
Subscriber, Group, Role: Encryption	id-kp-emailProtection {1.3.6.1.5.5.7.3.4};	Any EKU that is consistent with Key Usage, eg, Encrypting File System {1.3.6.1.4.1.311.10.3.4}	Any EKU that is not consistent with Key Usage anyExtendedKeyUsage {2.5.29.37.0}
Device Authentication, Web Server	id-kp-ServerAuth {1 3 6 1 5 5 7 3 1} id-kp-clientAuth {1.3.6.1.5.5.7.3.2}	None	All Others
Device Signature	None	None	All
Device Encryption	None	None	All

Certificate Type	Required EKU	Optional EKU	Prohibited EKU
Certificate Type	**Required EKU**	**Optional EKU**	**Prohibited EKU**
Device Encryption used for Database Encryption	id-kp-databaseEncryption {1 3 6 1 4 1 11243 20 1 3}	None	All Others
Domain Controller	id-kp-ServerAuth {1 3 6 1 5 5 7 3 1}; id-kp-clientAuth {1.3.6.1.5.5.7.3.2}; id-pkinit-KPKdc {1 3 6 1 5 2 3 5}; smartCardLogon {1.3.6.1.4.1.311.20.2.2}	None	All Others
Subscriber or Role Authentication, or Device Authentication Certificate used for VPN Client	id-kp-clientAuth {1 3 6 1 5 5 7 3 2}; iKEIntermediate {1 3 6 1 5 5 8 2 2}; id-kp-ipsecIKE {1 3 6 1 5 5 7 3 17}	None	All Others
Device Authentication Certificate used for VPN Server	id-kp-serverAuth {1 3 6 1 5 5 7 3 1}; id-kp-clientAuth {1 3 6 1 5 5 7417 3 2}; iKEIntermediate {1 3 6 1 5 5 8 2 2}; id-kp-ipsecIKE {1 3 6 1 5 5 7 3 17}	None	All Others
Subscriber or Role Authentication, or Device Authentication Certificate used for Web Client	id-kp-clientAuth {1 3 6 1 5 5 7 3 2}	None	All Others

11. References

NS4009 NSTISSI 4009, National Information Systems Security Glossary, April 6, 2015.

RFC 2119 Key words for use in RFCs to Indicate Requirement Levels (Bradner), March 1997
https://www.ietf.org/rfc/rfc2119.txt

RFC 2822 Internet Message Format, IETF (Resnick), April 2001.
https://www.ietf.org/rfc/rfc2822.txt

RFC 3647 Internet X.509 PKI Certificate Policy and Certification Practices Framework, IETF (Chokhani, Ford, Sabett, Merrill, and Wu), November 2003.
https://www.ietf.org/rfc/rfc3647.txt

RFC 4210 Internet X.509 PKI Certificate Management Protocol (CMP), IETF (Adams, Farrell, Kause, and Mononen), September 2005.
https://www.ietf.org/rfc/rfc4210.txt

RFC 5019 The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments, IETF (Deacon, and Hurst), September 2007.
https://www.ietf.org/rfc/rfc5019.txt

RFC 5280 Internet X.509 PKI Certificate and Certification Revocation List (CRL) Profile, IETF (Cooper, Santesson, Farrell, Boeyen, Housley, and Polk), May 2008.
https://www.ietf.org/rfc/rfc5280.txt

RFC 6818 Updates to the Internet X.509 PKI Certificate and Certification Revocation List (CRL) Profile, IETF (Lee), January 2013.
https://www.ietf.org/rfc/rfc6818.txt

RFC 6960 X.509 Internet PKI Online Certificate Status Protocol – OCSP, IETF (Santesson, Myers, Ankney, Malpani, Galperin, and Adams), June 2013.
https://www.ietf.org/rfc/rfc6960.txt

FIPS 140-2 Security Requirements for Cryptographic Modules, FIPS 140-2, May 25, 2001; (Change Notice 2, 12/3/2002), is available at: https://doi.org/10.6028/NIST.FIPS.140-2
http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

FIPS 186-4 Digital Signature Standards (DSS), FIPS 186-4, July 2013.
http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf