Australian Competition and Consumer Commission
Certification Practice Statement
(ACCC CPS)

Version: 1.0

Date of Publication: 14 May 2020

TABLE OF CONTENTS

TABLE OF TABLES

Nil

Revision History

Date	Document Number	Revision Number	Updates
14 May 2020	1	1.0	Initial release

1. INTRODUCTION

1.1. OVERVIEW

This Certification Practice Statement (CPS) defines the procedural and operational practices that ACCC requires entities to adhere to when issuing and managing digital certificates within the ACCC Public Key Infrastructure (PKI). ACCC Certificates are controlled by the ACCC Policy Management Authority (PMA) that governs Certification Authorities (CAs), Registration Authorities (RAs), Certificate Status Authority (CSA), Subscribers, Relying Parties and other PKI entities that interoperate with or within the ACCC PKI.

The ACCC PKI will provide the following security management services:

- Key generation and storage;
- Certificate generation, modification, re-key, and distribution;
- Certificate Revocation List (CRL) generation and distribution;
- Directory management of certificate related items;
- Certificate token initialization, programming, and management; and
- System management functions to include security audit, configuration management, and Archive.

This CPS and the DigiCert Private PKI Certificate Policy (CP)/Certification Practices Statement (CPS), define the practices that the RA uses to fulfill its obligations under the program's PKI requirements. Certificates issued are the basis for a number of security services including authentication, confidentiality, integrity, and non-repudiation. In order for a certificate to be in compliance with appropriate specifications, it shall comply with the reference documents in section 1.6.3 of the DigiCert Private PKI CP/CPS.

Note: all subsequent references to DigiCert CP/CPS in this document refer to the DigiCert Private PKI CP/CPS available publicly here: https://www.digicert.com/legal-repository/**.**

Other important documents in the ACCC PKI include the Certificate Policy (CP), Subscriber Agreements, Relying Party Agreement (RPA).

This CPS is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Statement Framework.

1.2. DOCUMENT NAME AND IDENTIFICATION

This document is the **ACCC Certification Practices Statement**.

1.3. PKI PARTICIPANTS

1.3.1 ACCC Policy Management Authority (PMA)

Refer to the ACCC CP Section 1.3.1.

1.3.2 Operational Authority (OA)

Refer to the ACCC CP Section 1.3.2.

1.3.3 Root Certification Authority (RCA)

Refer to the ACCC CP Section 1.3.3.

1.3.4 Subordinate Certification Authorities (SubCA)

Refer to the ACCC CP Section 1.3.4.

1.3.5 Registration Authorities (RA)

Refer to the ACCC CP Section 1.3.5.

1.3.6 Subscribers

Refer to the ACCC CP Section 1.3.6.

1.3.7 Device Sponsors

Refer to the ACCC CP Section 1.3.7.

1.3.8 Relying Party

Refer to the ACCC CP Section 1.3.8.

1.3.9 Certificate Status Authority (CSA)

Refer to the ACCC CP Section 1.3.9.

1.3.10 Time-Stamp Authority (TSA)

Refer to the ACCC CP Section 1.3.10.

1.3.11 Other Participants

1.3.11.1 Related Authorities

Refer to the ACCC CP Section 1.3.11.1

1.3.11.2 Trusted Agent

Refer to the ACCC CP Section 1.3.11.2

1.4. CERTIFICATE USAGE

1.4.1 Appropriate Certificate Uses

Refer to the ACCC CP Section 1.4.1 and ACCC Subscriber Agreement.

1.4.2 Prohibited Certificate Uses

Refer to the ACCC CP Section 1.4.2 and ACCC Subscriber Agreement.

1.5. POLICY ADMINISTRATION

1.5.1 Organization Administering the Document

This CPS is administered by the ACCC Policy Management Authority (PMA).

1.5.2 Contact Person

Comments concerning this CPS may be submitted to the following:

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

1.5.3 Person Determining CPS Suitability for the Policy

This CPS may be approved as sufficient for fulfilling the obligations under the CP when the CPS has been reviewed by an auditor or compliance analyst competent in the operations of a PKI, and when said person determines that this CPS is in fact in compliance with all aspects of the CP. Additionally, the auditor may not be the author of the CP or this CPS. The ACCC PMA shall determine the auditor's suitability.

1.5.4 CPS Approval Procedures

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

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

1.6. DEFINITIONS AND ACRONYMS

Refer to the ACCC CP Section 1.6.1 and 1.6.2

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

All CAs that issue certificates under the CP and this CPS must post all CA Certificates issued by or to the CA and 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. To promote consistent access to certificates and CRLs, the repository implements Access Controls and communication mechanisms to prevent unauthorized modification or deletion of information.

The PKI repository for the services set forth in this CPS is located at https://www.cdr.gov.au/.

2.1.1 Publication of certification information

The ACCC PKI repositories are accessible through several means of communication:

1. On the web: https://www.cdr.gov.au/.
2. By email to CDRTechnicalOperations@accc.gov.au
3. By mail addressed to: N/A
4. By telephone Tel: N/A

2.2 INTEROPERABILITY

Where Certificates and CRLs are published in the ACCC Directory or the ACCC Enterprise PKI Directory, standards-based schemas for directory objects and attributes shall be implemented. ACCC Repositories as defined above shall be interoperable as required with all repositories operated by CAs with which the ACCC PKI is cross-certified.

The following interoperability profile is defined:

- **Protocol**: access to Certificates and CRLs stored in the ACCC Directory and ACCC PKI Directory shall be provided using the following protocols: LDAP and HTTP.
- **Naming**: CA Certificates shall be stored in the ACCC Directory and ACCC PKI Directory in the entry that appears in the Certificate subject name. The issued By element shall contain the Certificate(s) issued by a CA whose name the entry represents. CRLs shall be stored in the ACCC PKI Directory in the entry that appears in the CRL issuer name.
- **Authentication**: for read access to the information in the Internet, "none" authentication shall be sufficient. Any write, update, add entry, delete entry, add attribute, delete attribute, change schema etc., shall require password over SSL or stronger authentication mechanism.

2.3 TIME OR FREQUENCY OF PUBLICATION

CA Certificates are published in a repository as soon as possible after issuance. CRLs for end-user Certificates are issued at least once per day. CRLs for CA Certificates are issued at least every 12 months, and also within 18 hours if a CA Certificate is revoked. Under special circumstances, the CA may publish new CRLs prior to the scheduled issuance of the next CRL. (See Section 4.9 for additional details.)

New or modified versions of the CP, this CPS, Subscriber Agreements, or Relying Party Agreement are typically published within seven days after their approval.

2.4 ACCESS CONTROLS ON REPOSITORIES

Information published in the ACCC repository is public information. ACCC PKI shall provide unrestricted read access to its repositories and shall implement logical and physical controls to prevent unauthorized write access to such repositories.

3. IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

All certificates (CAs, RAs, CSAs, and Subscribers) have a clearly distinguishable and unique X.501 Distinguished Name (DN) in the certificate Subject name field and in accordance with the ACCC CP, RFC 5280 & 6818.

3.1.2 Need for Names to be Meaningful

The certificates issued pursuant to this CPS 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.

Refer to the ACCC CP Section 3.1.2 for further Naming details.

3.1.3 Anonymity or Pseudonymity of Subscribers

CA Certificates do not contain anonymous or pseudonymous identities.

DNs in certificates issued to Subscribers may contain a pseudonym to meet local privacy regulations as long as name space uniqueness requirements are met and as long as such name is unique and traceable to the actual entity.

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 across the ACCC domains are enforced. CAs and RAs enforce name uniqueness within the X.500 name space, for which they have been authorized. Uniqueness in the Subject DN field is checked by the RA in all issued certificates for end entity Certificates.

The ACCC PMA is responsible for ensuring name uniqueness in certificates issued by the ACCC CAs.

3.1.6 Recognition, Authentication, and Role of Trademarks

The CA reserves the right to make all decisions regarding Subscriber names in all assigned certificates. Subscribers do not use names in their Certificate Applications that knowingly infringe upon the Intellectual Property Rights of others. Unless otherwise specifically stated in this CPS, ACCC does not verify or determine whether a Subscriber has Intellectual Property Rights in the name appearing in a DN or to arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark. ACCC operating under this CPS is entitled, without liability to any Subscriber, to reject or suspend any certificate because of such dispute. If the CA rejects a Certificate Application because the Subscriber name is not sufficiently unique, then the Subscriber either proposes a new unique name or requests the ACCC PMA to make a determination on the uniqueness of the proposed Subscriber name. The ACCC PMA is entitled, without any liability to any Subscriber, to approve or reject proposed Subscriber names pursuant to Section 3.1.5

3.2 INITIAL IDENTITY VALIDATION

The CA or RA may use any legal means of communication or investigation to ascertain the identity of an organizational or individual Applicant. The CA may refuse to issue a Certificate in its sole discretion.

3.2.1 Method to Prove Possession of Private Key

The ACCC RAs establish that the Applicant holds or controls the Private Key corresponding to the Public Key by performing signature verification or decryption on data purported to have been digitally signed or encrypted with the Private Key by using the Public Key associated with the certificate request.

The ACCC RA verifies proof of private key possession by verifying the Subscriber's digital signature on the PKCS #10 Certificate Signing Request (CSR) with the public key in the CSR. If the RA generates the key pair on behalf of the Subscriber, proof of possession by the subscriber is not required.

3.2.2 Authentication of Organization Identity

Requests for Certificates in the name of an organization or corporation shall include the following:

- Full organization name;
- Address of its head office;
- Documentation of the existence of the organization (such as articles of incorporation or corporation number);
- Its Dun and Bradstreet (DUNS) identifier if doing business within Australian, the United States of America or elsewhere where this identifier is commonly used. If a DUNS identifier is not able to be provided, the Entity CA shall verify with another third party (eg, tax authority, country, state or province corporate registry) the existence of the company, and record that identifier; and
- A letter from its authorized representative officially requesting said Certificate.

3.2.3 Authentication of Subject Identity

3.2.3.1 Device Subjects

For purposes of accountability and responsibility, an application for a Certificate of this type for a server, network device, application, or other non-human Subscriber (including sub-components and systems) shall be made by a human Device Sponsor and the Certificates issued to such a device shall be attributable to that Device Sponsor.

The Device Sponsor shall provide the following registration information corresponding to the server, application, or device:

- Equipment identification (eg, serial number, aircraft registration number, aircraft part number) or service name (eg, DNS Fully Qualified Domain Name, IP address, Entity identifier per [Section 7], or other network address) sufficient to uniquely identify the Subject;
- Equipment Public Keys;
- Equipment authorizations and attributes (if any are to be included in the Certificate); and
- Contact information to enable the CA or RA to communicate with the Device Sponsor when required.

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

- Verification of digitally signed messages sent from the Device Sponsor requesting the device Certificate (using Certificates of equivalent or greater assurance than that being requested); or
- In-person registration of the Device Sponsor requesting the device Certificate, with the identity of the Device Sponsor confirmed in accordance with the requirements of [Section 3.2.3.2] Individual Subjects

All Device Sponsors (including when a Device's Sponsor changes) shall be accountable for all device certificates under his/her sponsorship to ensure the devices are authorized to be issued Certificates or to continue to possess Certificates issued by the Entity CA.

Refer to the Section 3.2.3.1 of the ACCC CP for full details.

3.2.3.2 Individual Subjects

An RA shall ensure that the Applicant's identity information is verified and checked in accordance with the applicable CP and CPS. The CA or an RA shall ensure that the Applicant's identity information and public key are properly bound. Additionally, the CA or the RA shall record the process that was followed for issuance of each Certificate. Process information shall depend upon the Certificate level of assurance and shall be addressed in the applicable CPS. The process documentation and authentication requirements shall include the following:

Note: Personally identifiable information may be collected and stored to the extent permitted by applicable law. CAs and RAs are responsible for ensuring that they are compliant with all applicable laws when collecting such information.

- The identity of the person performing the identity verification;
- A signed declaration by that person that he or she verified the identity of the Applicant as required by the applicable CPS which may be met by establishing how the Applicant is known to the verifier as required by this CP; and
- The date and time of the verification.

3.2.4 Non-verified Device Sponsor Information

Refer to the ACCC CP Section 3.2.4.

3.2.5 Validation of Authority

Refer to the ACCC CP Section 3.2.5.

3.2.6 Criteria for Interoperation

Refer to the ACCC CP Section 3.2.6.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine Re-key

A request for re-key may only be made by the Device Sponsor in whose name the Device keys have been issued. All requests for re-key shall be authenticated by the CA, and the subsequent response shall be authenticated by the Device Sponsor. This may be done by an online method in accordance with RFC 4210.

Alternatively, a Device Sponsor requesting re-key may Authenticate the request using its valid digital signature key pair. Where the key has expired, the request for re-key shall be authenticated by the CA in the same manner as the initial registration.

When the current signing key is used for identification and Authentication purposes, the life of the new certificate shall not exceed the initial identity-proofing times specified in the paragraph above.

3.3.2 Identification and Authentication for Re-key After Revocation

Refer to the ACCC CP Section 3.3.2.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

The RA authenticates all revocation requests received before requesting revocation from the CA. The RA may authenticate revocation requests by referencing the use of the Private Key corresponding to the Certificate's Public Key, regardless of whether the associated Private Key is compromised.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

The Certificate Application process must provide sufficient information to:

- Establish the Applicant's authorization (by the employing or sponsoring agency) to obtain a certificate (per Section 3.2.2 and 3.2.3);
- Establish and record identity of the Subscriber (per Section 3.2.2 and 3.2.3);
- Obtain the Applicant's public key and verify the Applicant's possession of the private key for each certificate requested (per Section 3.2.1); and
- Verify authorization information requested for inclusion in the certificate.

These steps may be performed in any order that is convenient for the PKI authorities and Applicants that does not defeat security, but all must be completed before certificate issuance.

4.1.1 Who Can Submit a Certificate Application

An individual authorized to request Certificates on behalf of the Applicant may submit certificate requests. Applicants are responsible for any data that the Applicant or an agent of the Applicant supplies to the CA or RA.

A Certificate Application may be submitted by any of the following:

- Any individual who will be the subject of an individual certificate, or who owns or operates a Device, or application that will be the subject of an end-entity certificate;
- Any authorized representative of an organization or entity;
- Any authorized representative of a CA; or
- Any authorized representative of a RA.

The Certificate Application is a package consisting of the following:

- The Digital Certificate Subscriber Agreement.
- The Subscriber profile containing contact information; and
- The Naming Document, which specifies the content to be bound in the certificate.

4.1.2 Enrollment Process and Responsibilities

All Subscribers must agree to be bound by a relevant Subscriber Agreement that contains representations and warranties described in Section 9.6 and to undergo an enrollment process consisting of the following:

- Completing a Certificate Application and providing true and correct information;
- Generating, or arranging to have generated by a Trusted Person, or trusted authority, a key pair, in accordance with Section 6.1.1 of this CPS;
- Delivering his, her, or its public key, directly or through an RA, to the CA's facility; and
- Demonstrating possession of the private key corresponding to the public key as described in Section 3.2.1.

All communications among PKI authorities supporting the Certificate Application and issuance process is authenticated and protected from modification; any electronic transmission of shared secrets is protected. Communications may be electronic or out-of-band. Where electronic communications are used, cryptographic mechanisms commensurate with the strength of the public/private key pair is used. Out-of-band communications protect the confidentiality and integrity of the data.

4.1.2.1 End-Entity Certificates

The applicant and the RA must perform the following steps when an applicant applies for a Certificate:

- establish and record identity of Subscriber (per [Section 3.2]);
- obtain a public/private key pair for each Certificate required;

- establish that the Public Key forms a functioning key pair with the Private Key held by the Subscriber (per [Section 3.2.1]);
- provide a point of contact for verification of any roles or authorizations requested; and
- verify the authority of the applicant.

These steps may be performed in any order that is convenient for the RA and Subscribers, and that do not defeat security; but all must be completed prior to Certificate issuance.

Any electronic transmission of shared secrets shall be protected (eg, encrypted, or using a split secret scheme where the parts of the shared secret are sent using multiple, separate channels) using means commensurate with the requirements of the data to be protected by the Certificates being issued.

4.1.2.2 CA Certificates

The ACCC PMA shall make the procedures and application form available to entities requesting issuance of a CA Certificate from an ACCC Root or Intermediate CA.

An ACCC Root CA shall certify ACCC Sub CAs implementing this CPS only as authorized by the ACCC PMA.

The ACCC PMA shall evaluate the submitted application in accordance with procedures that it shall develop and publish, and make a determination regarding whether to issue the requested Certificate(s), and what policy mapping to express in the Certificate(s), if applicable.

The ACCC PMA may commission a CPS compliance analysis prior to authorizing the OA to issue and manage CA Certificates operating within the ACCC PKI Domain.

ACCC CAs shall only issue Certificates asserting the OIDs outlined in the ACCC CP upon receipt of written authorization from the ACCC PMA, and then may only do so within the constraints imposed by the ACCC PMA or its designated representatives.

4.2 CERTIFICATE APPLICATION PROCESSING

Information in Certificate Applications must be verified as accurate before certificates are issued. PKI authorities specify procedures to verify information in Certificate Applications.

4.2.1 Performing Identification and Authentication Functions

After receiving a certificate application, the RA verifies the application information and other information in accordance with Section 3.2. Additionally, prior to certificate issuance, a Subscriber is required to read and accept a Subscriber Agreement stating that the Subscriber protects the private key and use the certificate and private key for authorized purposes only.

The RA must create and maintain records sufficient to establish that it has performed its required verification tasks and communicate the completion of such performance to the CA. After verification is complete, the CA evaluates the corpus of information and decides whether or not to issue the Certificate. If some or all of the documentation used to support an application is in a language other than English, a CA or RA employee, or an agent skilled in the language performs the final cross-correlation and due diligence.

4.2.2 Approval or Rejection of Certificate Applications

A Certificate Application is approved by the CA or RA if all of the following conditions are met:

- Successful identification and Authentication of all required Device information as described in Section 3.2; and
- Payment (if applicable) has been received.

A Certificate Application is rejected by the CA or RA if any one or more of the following conditions arises:

- Identification and Authentication of all required Subscriber information as described in Section 3.2 cannot be completed;
- The Subscriber fails to furnish supporting documentation upon request;
- The Subscriber fails to respond to notices within a specified time;
- Payment (if applicable) has not been received; or
- The RA or CA believes that issuing a certificate to the Subscriber may bring the CA into disrepute.

If the certificate application is not rejected and is successfully validated in accordance with this CPS, the CA or RA will approve the certificate application and the CA will issue the Certificate. CAs and RAs are not liable for any rejected Certificate and are not obligated to disclose the reasons for a rejection. Rejected Applicants may re-apply. Subscribers are required to check the Certificate's contents for accuracy prior to using the certificate.

4.2.3 Time to Process Certificate Applications

Under normal circumstances, ACCC verifies an Applicant's information and issues a digital Certificate within a reasonable time frame. Issuance time frames are greatly dependent on when the Applicant provides the details and documentation necessary to complete validation. ACCC will usually complete the validation process and issue or reject a certificate application in less than thirty days after receiving all of the necessary details and documentation from the Applicant, although events outside of the control of ACCC can delay the issuance process.

4.3 CERTIFICATE ISSUANCE

4.3.1 CA Actions during Certificate Issuance

A certificate is created and issued following the approval of a Certificate Application by a CA or following receipt of a RA's request to issue the certificate. Upon receiving the request, the CAs/RAs:

- Verify the identity and authority of the requester;
- Check to ensure that all fields and extensions are properly populated;
- Build and sign a certificate if all certificate requirements have been met (in the case of a RA, have the CA sign the certificate); and
- Make the certificate available to the Device after confirming that the Device Sponsor has formally acknowledged their obligations as described in Section 9.6.

The CA confirms the source of a certificate request before issuance. The CA does not issue end entity Certificates directly from its root Certificates. Databases and CA processes occurring during certificate issuance are protected from unauthorized modification. After issuance is complete, the Certificate is stored in a database and sent to the Subscriber.

The CA shall verify the source of a certificate request before issuance. The CA and any RA shall protect databases under their control and that are used to confirm Subscriber identity information from unauthorized modification or use. The CA shall perform its actions during the certificate issuance process in a secure manner.

Certificate issuance by the Root CA requires an individual authorized by the CA (ie,. the CA Key Manager or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

The ACCC PKI may deliver Certificates in any secure manner within a reasonable time after issuance. Generally, the ACCC PKI delivers Certificates via email to the email address designated by the Subscriber during the application process or by providing the Subscriber a hypertext link to a User ID/Password protected location where the Subscriber may log in and download the certificate.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 Conduct Constituting Certificate Acceptance

An issued certificate will be deemed to have been accepted when it has been downloaded, installed, or used by the Subscriber or Sponsor, and the Subscriber or Sponsor has not objected to the certificate or its contents.

4.4.2 Publication of the Certificate by the CA

The ACCC PKI publishes all CA Certificates in its repository. The ACCC PKI publishes end-entity Certificates by delivering them to the Subscriber or Sponsor.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities.

The ACCC PMA will be notified at least two weeks prior to the issuance of a new CA certificate. In addition, all new artifacts (CA certificates, CRL DP, AIA URLs, etc.) produced as a result of the CA certificate issuance shall be provided to the ACCC PMA within 24 hours following issuance.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

Use of the private key corresponding to the public key in the certificate shall only be permitted once the Subscriber or Sponsor has agreed to the Subscriber Agreement and accepted the certificate. The certificate shall be used lawfully in accordance with the Subscriber Agreement and the terms of this CP. Certificate use must be consistent with the *keyUsage* and *extendedKeyUsage* extensions, in the associated certificate.

Subscribers and Sponsors shall protect their private keys from unauthorized use and shall discontinue use of the private key following expiration or revocation of the certificate and use Certificates in accordance with their intended purpose.

4.5.2 Relying Party Public Key and Certificate Usage

Relying Parties may only use software that is compliant with X.509, IETF RFCs, and other applicable standards. ACCC does not warrant that any third-party software will support or enforce the controls and requirements found herein.

A Relying Party should use discretion when relying on a Certificate and should consider the totality of the circumstances and risk of loss prior to relying on a Certificate. If the circumstances indicate that additional assurances are required, the Relying Party must obtain such assurances before using the Certificate. Any warranties provided by ACCC are only valid if a Relying Party's reliance was reasonable and if the Relying Party adhered to the Relying Party Agreement set forth in the ACCC repository.

A Relying Party should rely on a digital signature or SSL/TLS handshake only if:

1. the digital signature or SSL/TLS session was created during the operational period of a valid Certificate and can be verified by referencing a valid Certificate,
2. the Certificate is not revoked, and the Relying Party checked the revocation status of the Certificate prior to the Certificate's use by referring to the relevant CRLs or OCSP responses, and
3. the Certificate is being used for its intended purpose and in accordance with this CPS.

Before relying on a time-stamp token, a Relying Party must:

1. Verify that the time-stamp token has been correctly signed and that the Private Key used to sign the time-stamp token has not been compromised prior to the time of the verification,
2. Consider any limitations on the usage of the time-stamp token indicated by the time-stamp policy, and
3. Consider any other precautions prescribed in this CPS or elsewhere.

4.6 CERTIFICATE RENEWAL

4.6.1 Circumstance for Certificate Renewal

The Issuing CA may renew a Certificate if:

1. the associated Public Key has not reached the end of its validity period,
2. the associated Private Key has not been compromised,
3. the Subscriber and attributes remain consistent, and
4. re-verification of subscriber identity is required by Section 0.

The Issuing CA may also renew a Certificate if a CA Certificate is re-keyed or as otherwise necessary to provide services. After renewing a Subscriber Certificate, the Issuing CA may not re-key, renew, or modify the old Certificate.

4.6.2 Who May Request Renewal

Refer to the ACCC CP Section 4.6.2.

4.6.3 Processing Certificate Renewal Requests

Renewal application requirements and procedures are the same as those used during the Certificate's original issuance. The CA or RA may refuse to renew a Certificate if it cannot verify any rechecked information. If a Subject or Subject Device Sponsor is renewing a Subscriber Certificate and the relevant information has not changed, then the CA or RA does not require any additional identity vetting.

4.6.4 Notification of New Certificate Issuance to Subscriber

Notification is 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

ACCC publishes a renewed Certificate by delivering it to the Subscriber as per Section 4.4.2.

All renewed CA Certificates are published in ACCC's repository.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.7 CERTIFICATE RE-KEY

4.7.1 Circumstance for Certificate Rekey

Refer to the ACCC CP Section 4.7.1.

4.7.2 Who May Request Certificate Rekey

Refer to the ACCC CP Section 4.7.2.

4.7.3 Processing Certificate Rekey Requests

A Certificate re-key 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 3.2.

4.7.4 Notification of Certificate Rekey to Subscriber

Notification is given to the Subscriber in accordance with Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Rekeyed Certificate

See Section 4.4.1.

4.7.6 Publication of the Issued 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 Stipulation.

4.8 CERTIFICATE MODIFICATION

4.8.1 Circumstances for Certificate Modification

Refer to the ACCC CP Section 4.8.1.

4.8.2 Who May Request Certificate Modification

Refer to the ACCC CP Section 4.8.2.

4.8.3 Processing Certificate Modification Requests

After receiving a request for modification, ACCC PMA verifies any information that will change in the modified CA Certificate. ACCC will only issue the modified CA Certificate after completing the verification process on all modified information. ACCC will not issue a modified CA Certificate that has a validity period that exceeds the applicable time limits found in section 3.3.1 or 6.3.2.

4.8.4 Notification of Certificate Modification to Subscriber

See Section 4.3.2.

4.8.5 Conduct Constituting Acceptance of a 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 Modification by the CA to Other Entities

See Section 4.4.3.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

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

CAs operating under the CP and this CPS 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 is given to Device Sponsors during the certificate request or issuance, and are 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.

4.9.1 Circumstances for Revocation

Refer to the ACCC CP Section 4.9.1.

4.9.2 Who Can Request Revocation

Refer to the ACCC CP Section 4.9.2.

4.9.3 Procedure for Revocation Request

ACCC processes a revocation request as follows:

1. ACCC logs the identity of entity making the request or problem report and the reason for requesting revocation. ACCC may also include its own reasons for revocation in the log.
2. ACCC may request confirmation of the revocation from a known administrator, where applicable, via out-of-band communication (eg, telephone, fax, etc.).
3. If the request is authenticated as originating from the Subscriber, ACCC revokes the Certificate.
4. For requests from third parties, ACCC personnel begin investigating the request within 24 hours after receipt and decide whether revocation is appropriate based on the following criteria:
    a. the nature of the alleged problem,
    b. the number of reports received about a particular Certificate or website,
    c. the identity of the complainants (for example, complaints from a law enforcement official that a web site is engaged in illegal activities have more weight than a complaint from a consumer alleging they never received the goods they ordered), and
    d. relevant legislation.
5. If ACCC determines that revocation is appropriate, ACCC personnel revoke the Certificate and update the CRL.

The ACCC PMA shall be notified at least two weeks prior to the revocation of a CA certificate, whenever possible.

For emergency revocation, CAs shall follow the notification procedures in Section 5.7.

ACCC maintains a continuous 24/7 ability to internally respond to any high priority revocation requests. If appropriate, ACCC forwards complaints to relevant law enforcement authorities.

4.9.4 Revocation Request Grace Period

Refer to the ACCC CP Section 4.9.4.

4.9.5 Time within which CA Must Process the Revocation Request

The CA begins the investigation of a certificate revocation request promptly after receipt. RAs that accept revocation requests should promptly provide the request to the CA via their system or through email. There is no stipulation about when certificate revocation requests are completed. Such timing depends largely on the availability of information supporting authorization of the certificate revocation request and the expected impact of revocation.

4.9.6 Revocation Checking Requirement for Relying Parties

Prior to relying on information listed in a Certificate, a Relying Party must confirm the validity of each Certificate in the certificate path in accordance with IETF PKIX standards, including checking for certificate validity, issuer-to-subject name chaining, policy and key use constraints, and revocation status through CRLs or OCSP responders identified in each Certificate in the chain.

4.9.7 CRL Issuance Frequency

Refer to ACCC CP Section 4.9.7.

4.9.8 Maximum Latency for CRLs

CRLs for Certificates issued to end entity subscribers are posted automatically to the online repository within a commercially reasonable time after generation, usually within minutes of generation. 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 is no greater than twenty-four (24) hours.

4.9.9 On-line Revocation/Status Checking Availability

ACCC makes certificate status information available via OCSP for all Subscriber Certificates. OCSP responses are provided within a commercially reasonable time and no later than six seconds after the request is received, subject to transmission latencies over the Internet.

OCSP responses conform to RFC 5019 and/or RFC 6960. OCSP responses either:

1. Are signed by the CA that issued the Certificates whose revocation status is being checked, or
2. Are signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked.

In the latter case, the OCSP signing Certificate contains an extension of type id-pkix-ocsp-nocheck, as defined by RFC 6960.

4.9.10 On-line Revocation Checking Requirements

A relying party must confirm the validity of a Certificate in accordance with section 4.9.6 prior to relying on the Certificate.

ACCC supports an OCSP capability using the GET method for Certificates issued in accordance with the ACCC CP. OCSP Responders under ACCC direct control will not respond with a "good" status for a certificate that has not been issued.

4.9.11 Other Forms of Revocation Advertisements Available

Any alternate forms used to disseminate revocation information are 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 Related to Key Compromise

ACCC uses commercially reasonable efforts to notify potential Relying Parties if it discovers or suspects the compromise of a Private Key. ACCC will transition any revocation reason code in a CRL to “key compromise” upon discovery of such reason or as required by an applicable CP. If a Certificate is revoked because of compromise, ACCC will issue a new CRL within 18 hours after receiving notice of the compromise.

4.9.13 Circumstances for Suspension

Certificate suspension is not supported by this CPS.

4.9.14 Who Can Request Suspension

Certificate suspension is not supported by this CPS.

4.9.15 Procedure for Suspension Request

Certificate suspension is not supported by this CPS.

4.9.16 Limits on Suspension Period

Certificate suspension is not supported by this CPS.

4.10 CERTIFICATE STATUS SERVICES

4.10.1 Operational Characteristics

Certificate status information is available via CRL and OCSP responder. The serial number of a revoked Certificate remains on the CRL until one additional CRL is published after the end of the Certificate's validity period. OCSP information for subscriber Certificates is updated at least every four days. OCSP information for subordinate CA Certificates is updated at least every 12 months and within 24 hours after revoking the Certificate.

4.10.2 Service Availability

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

Certificate status services are available 24x7 without interruption. This includes the online repository that application software can use to automatically check the current status of all unexpired Certificates issued by the CA. Care is taken by the CA to ensure that the public copy of the CRL is replaced automatically when it is being updated.

4.10.3 Optional Features

No stipulation.

4.11 END OF SUBSCRIPTION

Refer to the ACCC CP Section 4.11.

4.12 KEY ESCROW AND RECOVERY

4.12.1 Key Escrow and Recovery Policy Practices

Refer to the ACCC CP Section 4.12.1.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Refer to the ACCC CP Section 4.12.2.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

All entities performing CA functions under this CPS implement and enforce the following physical, procedural, logical, and personnel security controls for a CA.

5.1 PHYSICAL CONTROLS

CA equipment is protected from unauthorized access while the cryptographic module is installed and activated. The CA implements physical Access Controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. CA cryptographic modules are protected against theft, loss, and unauthorized use.

All the physical control requirements specified below apply equally to the Root and Sub-CAs, and any remote workstations used to administer the CAs, except where specifically noted.

5.1.1 Site Location and Construction

ACCC CA operations are performed from secure and geographically diverse commercial data centers. The data centers are equipped with logical and physical controls that make ACCC PKI CA operations inaccessible to non-trusted personnel. ACCC PKI operates under a security policy designed to detect, deter, and prevent unauthorized access to ACCC operations.

Remote access and remote administration of the CA are monitored. Workstations are located such 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 Data Centers

ACCC PKI has implemented equipment protection from unauthorized access and physical controls to reduce the risk of equipment tampering. The data centers where the ACCC CA systems operate have security personnel on duty full time (24 hours per day, 365 days per year). Access to the data centers housing the CA platforms includes at least three layers of increasing security (eg perimeter, building, rooms, cages, cabinets, etc.) and requires two-factor authentication—the individual must have an authorized access card and pass biometric access control authenticators. These biometric authentication access systems log each use of the access card, which is reviewed periodically. The ACCC CA deactivates and securely stores its CA equipment when not in use. Activation data must either be memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module. Activation data is never stored with the cryptographic module or removable hardware associated with equipment used to administer the ACCC CA Private Keys. Removable cryptographic modules are deactivated prior to storage. When not in use, removable cryptographic modules and the activation information used to access or enable cryptographic modules are placed in ER (TL-15) UL 687, UL768, UL140 rated safes. Cryptographic hardware includes a mechanism to lock the hardware after a certain number of failed login attempts.

The ACCC CA data centers are continuously attended. However, if ACCC CA ever becomes aware that a data center is to be left unattended or has been left unattended for an extended period of time, ACCC CA personnel will perform a security check of the data center to verify that:

1. The CA equipment is in a state appropriate to the current mode of operation,
2. Any security containers are properly secured,
3. Physical security systems (eg, door locks) are functioning properly, and
4. The area is secured against unauthorized access.

The ACCC CA administrators are responsible for making these checks and must sign off that all necessary physical protection mechanisms are in place and activated. The identity of the individual making the check is logged.

5.1.2.2 RA Operations Areas

RA operations are protected using physical access controls making them accessible only to appropriately authorized individuals. Access to secure areas of buildings requires the use of an "access" or "pass" card. Access card use is logged by the building security system. The exterior and internal passageways of buildings are equipped with motion detecting sensors and video cameras. Access card logs and video records are reviewed on a regular basis. RAs securely store all removable media and paper containing sensitive plain-text information related to RA operations in secure containers. Refer to Section 5.4 for retention periods.

5.1.2.3 CA Key Generation and Storage

The ACCC CA securely stores the cryptomodules used to generate and store CA Private Keys. Access to the rooms used for key storage and key generation activities is controlled and logged by the building access card system. When not in use during a key ceremony, CA cryptomodules are locked in a safe that provides two-person physical access control. Access to the safe is manually logged. Access card logs and the manual logs of access to the safe are reviewed on a regular basis.

5.1.3 Power and Air Conditioning

Data centers have primary and secondary power supplies that ensure continuous and uninterrupted access to electric power. Uninterrupted power supplies (UPS) and diesel generators provide redundant backup power. ACCC CA monitors capacity demands and makes projections about future capacity requirements to ensure that adequate processing power and storage are available.

The CA facilities 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 and associated network communication systems (containing CA Certificates and CRLs) are 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.

The ACCC CA data center facilities use multiple load-balanced HVAC systems for heating, cooling, and air ventilation through perforated-tile raised flooring to prevent overheating and to maintain a suitable humidity level for sensitive computer systems.

5.1.4 Water Exposures

The cabinets housing the ACCC CA systems are located on raised flooring, and the data centers are equipped with monitoring systems to detect excess moisture.

5.1.5 Fire Prevention and Protection

The data centers are equipped with fire suppression mechanisms. They are equipped and procedures are implemented, to prevent damaging exposure to flame or smoke. These measures meet all local applicable safety regulations.

5.1.6 Media Storage

The ACCC CA protects its media from accidental damage (water, fire, electromagnetic). Backup files are created on a daily basis. ACCC CA backup files are maintained at locations separate from ACCC CA primary data operations facility.

5.1.7 Waste Disposal

All unnecessary copies of printed sensitive information are shredded on-site before disposal. All electronic media are physically destroyed or are overwritten multiple times to prevent the recovery of the data.

5.1.8 Off-site Backup

The ACCC CA maintains at least one full backup and makes regular backup copies of any information necessary to recover from a system failure at least once every six months. For disaster recovery purposes, backup copies of CA

Private Keys and activation data are stored off-site in safe deposit boxes located inside insured financial institutions and are accessible only by trusted personnel. Backups are to be performed and stored off-site not less than once per week, unless the CA is offline, in which case, it is backed up whenever it is activated or every seven (7) days, whichever is later.

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

5.2 PROCEDURAL CONTROLS

5.2.1 Corporate Controls

ACCC maintains its status as a legal entity in accordance with the national law stated in Section 9.15. It maintains a system of quality assurance consistent with recognized standards for all of its certificate management operations. The CA management structure ensures that it is 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

Personnel acting in trusted roles include CA and RA system administration personnel, and personnel involved with identity vetting and the issuance and revocation of Certificates. The functions and duties performed by persons in trusted roles are distributed so that one person alone cannot circumvent security measures or subvert the security and trustworthiness of the PKI operations. A list of personnel appointed to trusted roles is maintained and reviewed annually.

The roles are defined as:

1. CA Administrator,
2. RA Officer,
3. Internal Auditor, and
4. CA Operator.

5.2.2.1 CA Administrator

Refer to the ACCC CP Section 5.2.2.1.

5.2.2.2 RA Officers

Refer to the ACCC CP Section 5.2.2.2.

5.2.2.3 Internal Auditors

Refer to the ACCC CP Section 5.2.2.3.

5.2.2.4 CA Operator

The Operator is 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 Operational Authority

The ACCC PKI Operational Authority consists of the organizations that are responsible for the operation of the ACCC PKI CAs, including issuing Certificates when directed by the ACCC PMA or any authorised ACCC Registration Authority (RA) operating under this CPS, 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.

5.2.3.2 Device Sponsor

Refer to the ACCC CP Section 5.2.3.2.

5.2.3.3 Trusted Agent

Refer to the ACCC CP Section 5.2.3.3.

5.2.4 Number of Persons Required per Task

ACCC requires that at least two people acting in a trusted role (except for the Internal Auditor) and including a "CA Administrator" take action requiring a trusted role, such as activating ACCC Private CA Keys, generating a CA key pair, or backing up a ACCC CA Private Key.

Access to CA cryptographic modules is strictly enforced by multiple Trusted Persons throughout module lifecycles, from incoming receipt and inspection to final logical and/or physical destruction. Once a CA is activated with operational keys, further Access Controls are invoked to maintain split control over both physical and logical access to the CA. No single person alone has physical access to a CA module and no single person alone holds all credentials necessary to activate the CA.

5.2.5 Identification and Authentication for each Role

All personnel are required to authenticate themselves to CA and RA systems before they are allowed access to systems necessary to perform their trusted roles.

5.2.6 Roles Requiring Separation of Duties

Roles requiring a separation of duties include:

1. Those performing authorization functions such as the verification of information in certificate applications and approvals of certificate applications and revocation requests;
2. Those performing backups, recording, and record keeping functions;
3. Those performing audit, review, oversight, or reconciliation functions; and
4. Those performing duties related to CA key management or CA administration.

To accomplish this separation of duties, ACCC or Operational Authority specifically designates individuals to one of the trusted roles defined in Section 5.2.2 above. ACCC or the Operational Authorities appoint individuals to only one of the RA Officer, PKI System Administrator, CA Operator, or Internal Auditor roles. Individuals who assume one of the four trusted roles may not assume any other role, and under no circumstances shall any of the four other roles perform its own Compliance Audit. ACCC PKI systems identify and authenticate individuals acting in trusted roles, restrict an individual from assuming multiple roles, and prevent any individual from having more than one identity.

5.3 PERSONNEL CONTROLS

5.3.1 Qualifications, Experience, and Clearance Requirements

Refer to the ACCC CP Section 5.3.1.

5.3.2 Background Check Procedures

ACCC and Operational Authorities verify the identity of each employee appointed to a trusted role and performs a background check prior to allowing such person to act in a trusted role. ACCC requires each individual to appear in-person before a human resources employee whose responsibility it is to verify identity. The human resources employee verifies the individual's identity using government-issued photo identification (eg, passports and/or driver's licenses reviewed, Employment Eligibility Verification, or comparable procedure for the jurisdiction in which the individual's identity is being verified).

Background checks include employment history, education, character references, credit history, social security number, previous residences, and criminal background. Checks of previous residences are over the past three years. All other checks are for the previous five years. The highest education degree obtained is verified regardless of the date awarded. Based upon the information obtained during the background check, the human resources department makes an adjudication decision, with the assistance of legal counsel when necessary, as to whether the individual is suitable for the position to which they will be assigned. Background checks are refreshed and re-adjudication occurs at least every ten years.

5.3.3 Training Requirements

Training is provided via a mentoring process involving senior members of the team to which the employee belongs.

ACCC and Operational Authorities maintain records of who received training and what level of training was completed. Officers and Registration Authorities must have the minimum skills necessary to satisfactorily perform validation duties before being granted validation privileges. Where competence is demonstrated in lieu of training, ACCC or the Operational Authority maintains supporting documentation.

5.3.4 Retraining Frequency and Requirements

Employees must maintain skill levels that are consistent with industry-relevant training and performance programs in order to continue acting in trusted roles. The CA or RA shall make all employees acting in trusted roles aware of any changes to CA or RA operations, and if such operations change, the CA or RA shall provide documented training, in accordance with an executed training plan, to all employees acting in trusted roles.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

An employee or agent failing to comply with the CP, this CPS, and any other published procedure, whether through negligence or malicious intent, is subject to administrative or disciplinary action, including termination of employment or agency and criminal sanctions. If a person in a trusted role is cited by management for unauthorized or inappropriate actions, the person will be immediately removed from the trusted role pending management review. After management has reviewed and discussed the incident with the employee involved, management may reassign that employee to a non-trusted role or dismiss the individual from employment as appropriate.

5.3.7 Independent Contractor Requirements

Independent contractors who are assigned to perform trusted roles are subject to the duties and requirements specified for such roles in this Section 5.3 and are subject to sanctions stated above in Section 5.3.6. They establish procedures to ensure that any subcontractors perform in accordance with the CP and this CPS.

5.3.8 Documentation Supplied to Personnel

Personnel in trusted roles are provided with the documentation necessary to perform their duties, including a copy of the CP, this CPS, and other technical and operational documentation needed to maintain the integrity of CA and RA operations. Personnel are also given access to information on internal systems and security documentation, identity vetting policies and procedures, discipline-specific books, treatises and periodicals, and other information.

5.4 AUDIT LOGGING PROCEDURES

The security audit logs for each auditable event defined in this section are maintained in accordance with Section 5.5.2.

5.4.1 Types of Events Recorded

ACCC PKI systems require identification and authentication at system logon with a unique user name and password. Important system actions are logged to establish the accountability of the operators who initiate such actions.

ACCC PKI enables all essential event auditing capabilities of its CA applications in order to record the events listed below. If ACCC PKI applications cannot automatically record an event, ACCC or the Operational Authority implements manual procedures to satisfy the requirements. For each event, ACCC or the Operational Authority records the relevant (i) date and time, (ii) type of event, (iii) success or failure, and (iv) user or system that caused the event or initiated the action. ACCC or the Operational Authority records the precise time of any significant events. All event records are available to auditors as proof of ACCC PKI practices.

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

Refer to the ACCC CP Section 5.4.1 for Auditing Events Table.

5.4.2 Frequency of Processing Log

At least once a month, an ACCC or Operational Authority administrator reviews the logs generated by ACCC PKI systems. The administrator may perform the checks using automated tools. During these checks, the administrator:

(1) checks whether anyone has tampered with the log,

(2) scans for anomalies or specific conditions, including any evidence of malicious activity, and

(3) prepares a written summary of the review.

Any anomalies or irregularities found in the logs are investigated. The summaries include recommendations to ACCC PKI operations management and are made available to ACCC PKI auditors upon request. ACCC or the Operational Authorities document any actions taken as a result of a review.

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

Refer to the ACCC CP Section 5.4.3.

5.4.4 Protection of Audit Log

CA audit log information is retained on equipment until after it is copied by a system administrator. The ACCC CA systems are configured to ensure that:

(i) only authorized people have read access to logs,

(ii) only authorized people may archive audit logs, and

(iii) audit logs are not modified. Audit logs are protected from destruction prior to the end of the audit log retention period and are retained securely on-site until transferred to a backup site. It is acceptable for the system to over-write audit logs after they have been backed up and archived. ACCC off-site storage location is a safe and secure location that is separate from the location where the data was generated. Refer to Section 5.1.8.

Audit logs are made available to auditors upon request.

5.4.5 Audit Log Backup Procedures

ACCC or the Operational Authorities make regular backup copies of audit logs and audit log summaries and saves a copy of the audit log to a secure, off-site location on at least a monthly basis.

5.4.6 Audit Collection System (internal vs. external)

Automatic audit processes begin on system startup and end at system shutdown. If an automated audit system fails and the integrity of the system or confidentiality of the information protected by the system is at risk, ACCC and Operational Authority Administrators are notified and the ACCC PMA will consider suspending the CA's or RA's operations until the problem is remedied.

5.4.7 Notification to Event-causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

No stipulation beyond Section 5.4.2.

5.5 RECORDS ARCHIVAL

ACCC and Operational Authorities comply with all record retention policies that apply by law. ACCC and Operational Authorities include sufficient detail in all archived records to show that a Certificate or time-stamp token was issued in accordance with this CPS.

5.5.1 Types of Records Archived

CA, CSA, and RA Archive records are 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. ACCC or the Operational Authorities retain information in its archives (as such information pertains to ACCC CA operations).

Refer to the ACCC CP Section 5.5.1 for the Archived Records Table.

5.5.2 Retention Period for Archive

ACCC or the Operational Authorities retain archived data associated with Certificates for at least 10.5 years.

5.5.3 Protection of Archive

Archive records are stored at a secure off-site location and are maintained in a manner that prevents unauthorized modification, substitution, or destruction. The Archive is protected as specified by the privacy laws of the country where the Subscriber information was collected. Archives are not released except as allowed by legal counsel or as required by law. ACCC or the Operational Authorities maintain any software application required to process the archive data until the data is either destroyed or transferred to a newer medium.

If there is a need to transfer any media to a different archive site or equipment, ACCC or the Operational Authority will maintain both archived locations and/or pieces of equipment until the transfer are complete. All transfers to new archives will occur in a secure manner. Records of individual transactions may be released upon request of any Subscriber involved in the transaction or their legally recognized agents. Archive media is 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

On at least an annual basis, ACCC or the Operational Authority creates an archive disk of the data listed in Section 5.5.1 by grouping the data types together by source into separate, compressed archive files. ACCC or the Operational Authority stores the archive disk in a secure off-site location for the duration of the set retention period. RAs create and store archived records in accordance with the applicable documentation retention policy.

5.5.5 Requirements for Timestamping of Records

ACCC PKI automatically timestamps archived records with system time (non-cryptographic method) as they are created. ACCC PKI synchronizes its system time at least every eight hours using a real time value distributed by a recognized UTC(k) laboratory or National Measurement Institute. Refer to Section 6.8.

5.5.6 Procedures to Obtain and Verify Archive Information

Details concerning the creation and storage of archive information are found in Section 5.5.4. After receiving a request made for a proper purpose by a customer, its agent, or a party involved in a dispute over a transaction involving the PKI, ACCC may elect to retrieve the information from archival. ACCC may elect to transmit the relevant

information via a secure electronic method or courier, or it may also refuse to provide the information in its discretion and may require prior payment of all costs associated with the data.

5.6 KEY CHANGEOVER

Key changeover procedures enable the smooth transition from expiring CA Certificates to new CA Certificates. Towards the end of a CA Private Key's lifetime, ACCC ceases using the expiring CA Private Key to sign Certificates and uses the old Private Key only to sign CRLs and OCSP responder Certificates. A new CA signing key pair is commissioned and all subsequently issued Certificates and CRLs are signed with the new private signing key. Both the old and the new key pairs may be concurrently active. This key changeover process helps minimize any adverse effects from CA certificate expiration. The corresponding new CA Public Key Certificate is provided to subscribers and relying parties through the delivery methods detailed in Section 6.1.4. Where ACCC has cross-certified another CA that is in the process of a key rollover, ACCC obtains a new CA Public Key (PKCS#10) or new CA Certificate from the other CA and distributes a new CA cross Certificate following the procedures described above.

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

The Validity Periods of ACCC issued certificates are Nested such that the Validity Periods of issued certificates is contained within the Validity Period of the issuing CA. In other words, ACCC CAs will not issue certificates that extend beyond the expiration date of their own certificates and public keys (thus this is a Nested PKI).

PKI Participants must cease all use of their private key pairs after their Validity Period has expired.

For additional constraints on certificate life and key sizes, see Section 6.1.5.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

ACCC and Operational Authorities maintain incident response procedures to guide personnel in response to security incidents, natural disasters, and similar events that may give rise to system compromise. ACCC reviews, tests, and updates its incident response plans and procedures on at least an annual basis.

If a CA or CSA detects a potential hacking attempt or other form of Compromise, it will 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 are followed.

The ACCC PMA will be notified if any CAs operating under this CPS experiences 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 will take appropriate steps to protect the integrity of the PKI.

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

ACCC or the Operational Authorities will make regular system backups on at least a weekly basis and maintains backup copies of its Private Keys, which are stored in a secure, off-site location. If ACCC or the Operational Authorities discover that any of its computing resources, software, or data operations have been compromised, ACCC assesses the threats and risks that the compromise presents to the integrity or security of its operations or those of affected parties. If ACCC determines that a continued operation could pose a significant risk to Relying Parties or Subscribers, ACCC suspends such operation until it determines that the risk is mitigated.

When computing resources, software, and/or data are corrupted, CAs operating under the CP and this CPS will 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 will be reestablished, giving priority to the ability to generate certificate status information within the CRL issuance schedule specified in Section 4.9.
- If the CA signature keys are destroyed, CA operation will 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 is securely notified immediately. This will allow other CAs to protect their Device Sponsors' interests as Relying Parties.
- If the ability to revoke certificates is inoperative or damaged, the CA will reestablish revocation capabilities as quickly as possible in accordance with procedures set forth in each respective CPS. If the CA's revocation capability cannot be established in a reasonable time-frame, the CA will determine whether to request revocation of its certificate(s). If the CA is a Root CA, the CA will determine whether to notify all Subscribers who use the CA as a trust anchor to delete the trust anchor.

5.7.3 Entity Private Key Compromise Procedures

If ACCC suspects that one of its Private Keys has been comprised or lost then an emergency response team organized by the ACCC PMA will convene and assess the situation to determine the degree and scope of the incident and take appropriate action, specifically:

1. Collect information related to the incident;
2. Begin investigating the incident and determine the degree and scope of the compromise;
3. Have its incident response team determine and report on the course of action or strategy that should be taken to correct the problem and prevent reoccurrence;
4. If appropriate, contact government agencies, law enforcement, and other interested parties and activate any other appropriate additional security measures;
5. If the compromise involves a Private Key used to sign time-stamp tokens, provide a description of the compromise to Subscribers and Relying Parties;
6. Notify any cross-certified entities of the compromise so that they can revoke their cross-Certificates;
7. Make information available that can be used to identify which Certificates and time-stamp tokens are affected, unless doing so would breach the privacy of an ACCC user or the security of ACCC PKI services;
8. Monitor its system, continue its investigation, ensure that data is still being recorded as evidence, and make a forensic copy of data collected;
9. Isolate, contain, and stabilize its systems, applying any short-term fixes needed to return the system to a normal operating state;
10. Prepare and circulate an incident report that analyzes the cause of the incident and documents the lessons learned; and
11. Incorporate lessons learned into the implementation of long term solutions and the Incident Response Plan.

ACCC may generate a new key pair and sign a new Certificate. If a disaster physically damages ACCC PKI equipment and destroys all copies of ACCC signature keys then ACCC will provide notice to affected parties at the earliest feasible time.

The ACCC PMA will 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 will be revoked, if applicable. The CSA will generate a new key pair and request new certificate(s), if applicable. If the CSA is a trust anchor, the Relying Parties will be provided the new trust anchor in a secure manner (so that the trust anchor integrity is maintained) to replace the compromised trust anchor.

5.7.4 Business Continuity Capabilities after a Disaster

To maintain the integrity of its services, ACCC and/or Operational Authorities implement data backup and recovery procedures as part of its Business Continuity Management Plan (BCMP). Stated goals of the BCMP are to ensure that certificate status services be only minimally affected by any disaster involving ACCC PKI's primary facility and that ACCC and/or Operational Authorities be capable of maintaining other services or resuming them as quickly as possible following a disaster. ACCC and/or Operational Authorities review, tests, and updates the BCMP and

supporting procedures at least annually. The CA Operator will 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.

ACCC PKI systems are redundantly configured at its primary facility and are mirrored at a separate, geographically diverse location for failover in the event of a disaster. If a disaster causes ACCC PKI primary CA operations to become inoperative, ACCC will re-initiate its operations at its secondary location giving priority to the provision of certificate status information capabilities, if affected.

5.8 CA, RA OR CSA TERMINATION

Before terminating its CA activities, ACCC will:

1. Provide notice and information about the termination by sending notice by email to its customers, Application Software Vendors, and cross-certifying entities and by posting such information on ACCC web site; and
2. Transfer all responsibilities to a qualified successor entity.

If a qualified successor entity does not exist, ACCC will:

1. transfer those functions capable of being transferred to a reliable third party and arrange to preserve all relevant records with a reliable third party or a government, regulatory, or legal body with appropriate authority;
2. revoke all Certificates that are still un-revoked or un-expired on a date as specified in the notice and publish final CRLs;
3. destroy all Private Keys; and
4. make other necessary arrangements that are in accordance with this CPS.

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 key pair Generation

All keys must be generated using a FIPS-approved method or equivalent international standard. Key pair generation will be performed using FIPS 140-2 rated cryptographic modules and processes that provide the required cryptographic strength of the generated keys and prevent the loss, disclosure, modification, or unauthorized use of private keys.

ACCC CA key pairs are generated by multiple trusted individuals acting in trusted roles and using a cryptographic hardware device as part of scripted key generation ceremony. Activation of the hardware requires the use of two-factor authentication tokens. ACCC or the Operational Authorities create auditable evidence during the key generation process to prove that the CPS was followed and role separation was enforced during the key generation process.

Subscribers must generate their keys in a manner that is appropriate for the certificate type.

Refer to the ACCC CP Section 6.1.1 for the Key Generation Table.

When private keys are not generated on the token to be used, originally generated private keys will be destroyed after they have been transferred to the token. This does not prohibit the key generating modules to act as the key escrow module as well.

6.1.1.1 CA key pair Generation

All keys must be generated using a FIPS-approved method or equivalent international standard. The ACCC CA key pairs are generated by multiple trusted individuals acting in trusted roles and using a cryptographic hardware device as part of scripted key generation ceremony. The cryptographic hardware is evaluated to FIPS 140-1 Level 3 and EAL 4+. Activation of the hardware requires the use of two-factor authentication tokens. Auditable evidence during the key generation process to prove that the CPS was followed, and role separation was enforced during the key generation process.

6.1.1.2 Subscriber key pair Generation

Subscriber key pair generation may be performed by the Subscriber or Device 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.

If Devices are capable of generating their own keys and Certificate Signing Requests (CSRs), the CSR can only include the intended Subject name if the Device has the means of knowing the unique identity on which it is installed. If this is not the case, the CSR contains a placeholder name, and a process will need to be determined with the CA for the Device Sponsor and Trusted Person to provide the intended name to the CA as part of the identity-proofing and enrollment process. This process is described in Section 3.2.

6.1.2 Private Key Delivery to Subscriber

If ACCC, CMS, RA or Sponsor generates a key for a Subscriber, then it must deliver the Private Key securely to the Subscriber. Keys may be delivered electronically (such as through secure email or stored in a cloud-based system) or on a hardware cryptographic module. In all cases:

1. Except where escrow/backup services are authorized and permitted, the key generator must not retain access to the Subscriber's Private Key after delivery;
2. The key generator must protect the Private Key from activation, compromise, or modification during the delivery process;
3. The Subscriber must acknowledge receipt of the Private Key(s), typically by having the Subscriber use the related Certificate; and

4. The key generator must deliver the Private Key in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers, including:

    a. For hardware modules, the key generator maintaining accountability for the location and state of the module until the Subscriber accepts possession of it, and

    b. For electronic delivery of Private Keys, the key generator encrypting key material using a cryptographic algorithm and key size at least as strong as the Private Key. The key generator shall deliver activation data using a separate secure channel.

The entity assisting the Subscriber with key generation shall maintain a record of the Subscriber's acknowledgement of receipt of the device containing the Subscriber's key pair. A CMS, RA or Sponsor providing key delivery services is required to provide a copy of this record to ACCC.

The CA or the RA maintains a record of the Subscriber or Sponsor acknowledgement of receipt of the token.

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

Subscriber key pair generation may be performed by the Subscriber. In this case, the private key delivery to a Subscriber or Sponsor is unnecessary.

6.1.3 Public Key Delivery to Certificate Issuer

Refer to the ACCC CP Section 6.1.3.

6.1.4 CA Public Key Delivery to Relying Parties

ACCC CA trust anchor public keys will be provided to the Relying Parties or Subscriber acting as Relying Parties in a secure manner so that the trust anchor is not vulnerable to modification or substitution. Acceptable methods for delivery of a trust anchor include but are not limited to:

1. Loading a trust anchor onto tokens delivered to Relying Parties via secure mechanisms;
2. Secure distribution of trust anchor through secure out-of-band mechanisms;
3. Comparison of certificate hash (fingerprint) against the trust anchor hash made available via authenticated out-of-band sources (note that fingerprints or hashes posted in-band along with the certificate are not acceptable as an Authentication mechanism); and
4. Downloading a trust anchor from trusted web sites (eg, CA web site) secured with a currently valid certificate of equal or greater assurance level than the certificate being downloaded, and the trust anchor is not in the Certificate Chain for the web site certificate.

Systems using cryptographic hardware tokens store trusted certificates such that unauthorized alteration or replacement is readily detectable.

6.1.5 Key Sizes

Refer to the ACCC CP Section 6.1.5.

6.1.6 Public Key Parameters Generation and Quality Checking

The ACCC CA uses a cryptomodule that conforms to FIPS 186-2 and provides random number generation and onboard generation of up to 4096-bit RSA Public Keys and conforms to FIPS 186-4 random number generation for Elliptic Curve Cryptography (ECC) Keys up to 521-bit. The value of the public exponent equates to an odd number equal to three or more.

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

ACCC PKI Certificates include key usage extension fields that specify the intended use of the Certificate and technically limit the Certificate's functionality in X.509v3-compliant software.

The use of a specific key is determined by the key usage extension in the X.509 Certificate.

Private Keys corresponding to Root CA Certificates are not used to sign Certificates except in the following cases:

1. Self-signed Certificates to represent the Root CA itself;
2. Certificates for Subordinate CAs and Cross Certificates;
3. Certificates for infrastructure purposes (eg administrative role certificates, internal CA operational device certificates; and
4. Certificates for OCSP Response verification.

Subscriber Certificates assert key usages based on the intended application of the key pair. In particular, Certificates to be used for digital signatures (including authentication) set the digitalSignature and/or nonRepudiation bits. Certificates to be used for key or data encryption shall set the keyEncipherment and/or dataEncipherment bits. Certificates to be used for key agreement shall set the keyAgreement bit.

Key usage bits and extended key usages are specified in the certificate profile for each type of Certificate ACCC CA Certificates have at least two key usage bits set: keyCertSign and cRLSign, and for signing OCSP responses, the digitalSignature bit is also set.

Refer to Section 10 for a full list of allowable certificate extensions and extension values for all certificate types issued from ACCC PKI.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

Private keys hosted within the ACCC PKI are protected using Trustworthy Systems. Private key holders will take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of such private keys in accordance with the CP, this CPS, and contractual obligations specified in the appropriate agreement.

The relevant standard for cryptographic modules is Security Requirements for Cryptographic Modules [FIPS 140-2].

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

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

ACCC PKI authentication mechanisms are protected securely when not in use and may only be accessed by actions of multiple trusted persons. A single person is not permitted to activate or access any cryptographic module that contains the complete CA private signing key.

Backups of CA Private Keys are securely stored off-site and require two-person access. Re-activation of a backed-up CA Private Key (unwrapping) requires the same security and multi-person control as when performing other sensitive CA Private Key operations. The names of the parties used for two-person control are maintained on a list that is made available for inspection during Compliance Audits.

6.2.3 Private Key Escrow

ACCC does not escrow its signature keys. Subscribers may not escrow their private signature keys.

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

6.2.4 Private Key Backup

ACCC Private Keys are generated and stored inside the ACCC CA PKI cryptographic modules, which have been evaluated to at least FIPS 140-2 Level 3 and EAL 4+. When keys are transferred to other media for backup and disaster recovery purposes, the keys are transferred and stored in an encrypted form. ACCC CA key pairs are backed up by multiple trusted individuals using a cryptographic hardware device as part of scripted key backup process. Backed up keys are never stored in a plain text form outside of the cryptographic module.

Subscriber private keys may be backed up or copied but must be held under the control of the Subscriber, Sponsor or other authorized administrator. Backed up Subscriber private keys are not to be stored in *plaintext* format outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the Subscriber's cryptographic module.

6.2.5 Private Key Archival

ACCC PKI does not archive Private Signature Keys.

6.2.6 Private Key Transfer into or from a Cryptographic Module

All keys must be generated by and in a cryptographic module. Private Keys are exported from the cryptographic module into backup tokens only for HSM transfer, offline storage, and backup purposes. The Private Keys are encrypted when transferred out of the module and never exist in plaintext form. When transported between cryptographic modules, ACCC encrypts the Private Key and protects the keys used for encryption from disclosure; private keys must never exist in plaintext form outside the cryptographic module boundary. Private Keys used to encrypt backups are securely stored and require two-person access. 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 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

ACCC PKI Private Keys are generated and stored inside cryptographic modules which have been evaluated to at least FIPS 140-2. As per Section 6.1.1.

6.2.8 Method of Activating Private Keys

ACCC PKI Private Keys are activated according to the specifications of the cryptographic module manufacturer. Activation data entry is protected from loss, theft, modification, disclosure, or unauthorized use.

6.2.8.1 CA Administrator Activation

Method of activating the CA system by a CA Administrator require:

1. Use a smart card, biometric access Device, password in accordance with Section 6.4.1, or security of equivalent strength to Authenticate the Administrator before the activation of the private key, which includes, for instance, a password to operate the private key, a Windows logon or screen saver password, or a network logon password; and
2. Take commercially reasonable measures for the physical protection of the Administrator's workstation to prevent use of the workstation and its associated private key without the Administrator's authorization.

6.2.8.2 Offline CAs Private Key

Once the CA system has been activated, a threshold number of shareholders is required to supply their Activation Data in order to activate an offline CA's private key, as defined in Section 6.2.2. Once the private key is activated, it will be active until termination of the session.

6.2.8.3 Online CAs Private Keys

An online CA's private key is activated by a threshold number of shareholders, as defined in Section 6.2.2, supplying their Activation Data (stored on secure media). Once the private key is activated, the private key may be active for an indefinite period until it is deactivated when the CA goes offline.

6.2.8.4 Device Private Keys

A Device may be configured to activate its private key, provided that appropriate physical and logical Access Controls are implemented for the Device. The strength of the security controls are commensurate with the level of threat in the Device's environment, and will protect the Device's hardware, software, private keys and its Activation Data

from Compromise. If the private key is stored in a protected form using password-based encryption, then the password or pass-phrase Activation Data must be entered each time the Device and the security application are initialized in order to unlock the private key for operational use.

6.2.9 Method of Deactivating Private Keys

The ACCC CA Private Keys are deactivated via logout procedures on the applicable HSM device when not in use. ACCC never leaves its HSM devices in an active unlocked or unattended state.

When an online CA is taken offline, the CA removes 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 removes the token containing the private keys from the reader in order to deactivate them. Once removed from the reader, tokens will be securely stored.

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

Subscribers should deactivate their Private Keys via logout and removal procedures when not in use.

6.2.10 Method of Destroying Private Keys

ACCC and Operational Authority personnel, acting in trusted roles, destroy CA, RA, and status server Private Keys when no longer needed. Subscribers must destroy their Private Keys when the corresponding Certificate is revoked or expired or if the Private Key is no longer needed. If proper destruction of the private key cannot be guaranteed, then the key must be treated as compromised and the certificate revoked.

ACCC may destroy a Private Key by deleting it from all known storage partitions. ACCC or Operational Authorities also zeroizes the HSM device and associated backup tokens according to the specifications of the hardware manufacturer. This reinitializes the device and overwrites the data with random data or binary zeros. If the zeroization or re-initialization procedure fails, ACCC or the Operational Authority will crush, shred, and/or incinerate the device in a manner that destroys the ability to extract any Private Key.

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

Refer to the ACCC CP Section 6.3.1.

6.3.2 Certificate Operational Periods and key pair Usage Periods

Refer to the ACCC CP Section 6.3.2 for the Key Operational & Usage Period.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

ACCC or Operational Authorities activate the cryptographic module containing its CA Private Keys according to the specifications of the hardware manufacturer. This method has been evaluated as meeting or exceeding the requirements of Level 2 in FIPS 140-2 with the cryptographic hardware is held under two-person control. ACCC and/or Operational Authorities will only transmit activation data via an appropriately protected channel and at a time and place that is distinct from the delivery of the associated cryptographic module.

All ACCC PKI personnel and Subscribers are instructed to use strong passwords and to protect PINs and passwords. ACCC and Operational Authority employees are required to create non-dictionary, alphanumeric passwords with a minimum length and to change their passwords on a regular basis as per ACCC and Operational Authorities Security Policy. If ACCC or Operational Authorities uses passwords as activation data for a signing key, ACCC or the Operational Authority will change the activation data change upon rekey of the CA Certificate.

6.4.2 Activation Data Protection

ACCC PKI protects data used to unlock Private Keys from disclosure using a combination of cryptographic and physical access control mechanisms. Protection mechanisms include keeping activation mechanisms secure using role-based physical control. All ACCC and Operational Authority personnel are instructed to memorize and not to write down their password or share it with another individual. If written down, it will be secured at the level of the data that the associated cryptographic module is used to protect and will not be stored with the cryptographic module. ACCC and the Operational Authority locks accounts used to access secure CA processes if a certain number of failed password attempts occur in accordance with ACCC and Operational Authorities' Security Policy.

6.4.3 Other Aspects of Activation Data

Refer to the ACCC CP Section 6.4.3.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

ACCC and the Operational Authorities secure the ACCC PKI CA systems and authenticates and protects communications between its systems and trusted roles. ACCC PKI CA servers and support-and-vetting workstations run on trustworthy systems that are configured and hardened using industry best practices. The computer system hosting the CA is hardened against all known threats. All CA systems are scanned for malicious code and protected against spyware and viruses.

ACCC PKI CA systems, including any remote workstations, are configured to:

1. authenticate the identity of users before permitting access to the system or applications,
2. manage the privileges of users and limit users to their assigned roles,
3. generate and archive audit records for all transactions,
4. enforce domain integrity boundaries for security critical processes, and
5. support recovery from key or system failure.

All Certificate Status Servers:

1. authenticate the identity of users before permitting access to the system or applications,
2. manage privileges to limit users to their assigned roles,
3. enforce domain integrity boundaries for security critical processes, and
4. support recovery from key or system failure.

The ACCC CA enforces multi-factor authentication on any account capable of directly causing Certificate issuance.

The computer system is configured with the minimum of the required accounts and network services and will not permit remote login.

6.5.2 Computer Security Rating

No stipulation.

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

ACCC and Operational Authorities have mechanisms in place to control and monitor the acquisition and development of its CA systems. Change requests require the approval of at least one administrator who is different from the person submitting the request. ACCC and Operational Authorities only install software on ACCC PKI CA systems if the software is part of the CA's operation. CA hardware and software are dedicated to performing operations of the CA.

Vendors are selected based on their reputation in the market, ability to deliver quality product, and likelihood of remaining viable in the future. Management is involved in the vendor selection and purchase decision process. Non-PKI hardware and software is purchased without identifying the purpose for which the component will be used. All hardware and software are shipped under standard conditions to ensure delivery of the component directly to a trusted employee who ensures that the equipment is installed without opportunity for tampering.

Some of the PKI software components used by ACCC and Operational Authorities are developed in-house or by consultants using standard software development methodologies. All such software is designed and developed in a controlled environment and subjected to quality assurance review. Other software is purchased commercial off-the shelf (COTS). Quality assurance is maintained throughout the process through testing and documentation or by purchasing from trusted vendors as discussed above.

Updates of equipment and software are purchased or developed in the same manner as the original equipment or software and are installed and tested by trusted and trained personnel. All hardware and software essential to ACCC PKI operations is scanned for malicious code on first use and periodically thereafter.

Procured hardware and software is 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). All specially developed hardware and software is developed in a controlled environment, and the development process is defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software.

All hardware is 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 is dedicated to performing PKI activities. There will be no other applications, hardware Devices, network connections, or component software installed which is not part of the PKI operation.

Proper care is taken to prevent malicious software from being loaded onto the equipment. Applications required to perform PKI operations will be obtained from sources authorized by local policy. CA and CSA hardware and software will be scanned for malicious code on first use and periodically thereafter and Hardware and software updates will be purchased or developed in the same manner as original equipment and will be installed by trusted and trained personnel in a defined manner.

6.6.2 Security Management Controls

The ACCC CA has mechanisms in place to control and monitor the security-related configurations of its CA systems. When loading software onto a CA system, ACCC and/or the Operational Authorities verify that the software is the correct version and is supplied by the vendor free of any modifications. ACCC and/or the Operational Authorities verify the integrity of software used with its CA processes at least once a week. The configuration of the CA and CSA system, in addition to any modifications and upgrades, will be documented and controlled.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 NETWORK SECURITY CONTROLS

ACCC and/or the Operational Authorities document and control the configuration of its systems, including any upgrades or modifications made. CAs, CSAs, and RAs employ appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. The ACCC PKI CA system is connected to one internal network

and is protected by firewalls and Network Address Translation for all internal IP addresses (eg, 192.168.x.x). Root Keys are kept offline and brought online only when necessary to sign Certificate-issuing subordinate CAs, OCSP Responder Certificates, or periodic CRLs. Firewalls and boundary control devices are configured to allow access only by the addresses, ports, protocols and commands required for the trustworthy provision of PKI services by such systems.

ACCC and/or the Operational Authorities security policy is to block all ports and protocols and open only ports necessary to enable CA functions. All CA equipment is configured with a minimum number of services and all unused network ports and services are disabled. Any boundary control devices used to protect the network on which the PKI equipment is hosted will deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network. The ACCC PKI network configuration is available for review on-site by its auditors and consultants under an appropriate non-disclosure agreement.

6.8 TIME-STAMPING

The system time on the ACCC CA computers are updated using the Network Time Protocol (NTP) to synchronize system clocks at least once every eight hours (Windows default). All times are traceable to a real time value distributed by a UTC(k) laboratory or National Measurement Institute and are updated when a leap second occurs as notified by the appropriate body. ACCC maintains an internal NTP server that synchronizes with cellular telephone networks and maintains the accuracy of its clock within one second or less.

Certificates, CRLs, and other revocation database entries contain time and date information. Asserted times will 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).

Time derived from the time service is used to establish 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.

7. CERTIFICATE, CRL, AND OCSP PROFILES

The ACCC PKI uses the ITU X.509, version 3 standard to construct digital Certificates. The ACCC PKI adds certain certificate extensions to the basic certificate structure for the purposes intended by X.509v3 as per Amendment 1 to ISO/IEC 9594-8, 1995.

7.1 CERTIFICATE PROFILE

Certificates shall conform to [RFC 5280 & 6818]: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008 & Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, January 2013.

Refer to the ACCC CP for full Certificate Profile details.

7.2 CRL PROFILE

CRLs shall conform to [RFC 5280 & 6818]: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008 & Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, January 2013.

Refer to the ACCC CP for full CRL Profile details.

7.3 OCSP PROFILE

OCSP requests and responses shall be in accordance with RFC 2560, 5019 and 6960.

Refer to the ACCC CP for full OCSP Profile details.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The practices in this CPS are designed to meet or exceed the requirements of generally accepted industry standards, including the latest versions of the WebTrust Programs for Certification Authorities. For purposes of interoperation with the US Government, compliance can be determined by reference to any current auditor letter of compliance meeting FPKIPA Audit Requirements.

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

Refer to the ACCC CP Section 8.1.

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

Refer to the ACCC CP Section 8.2.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

Refer to the ACCC CP Section 8.3.

8.4 TOPICS COVERED BY ASSESSMENT

Refer to the ACCC CP Section 8.4.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

If an audit reports a material noncompliance with applicable law, this CPS, the CP, or any other contractual obligations related to ACCC's PKI services, then;

(1) the auditor will document the discrepancy,

(2) the auditor will promptly notify ACCC, and

(3) ACCC will develop a plan to cure the noncompliance. ACCC will submit the plan to the DCPA for approval and to any third party that ACCC is legally obligated to satisfy.

The DCPA may require additional action if necessary to rectify any significant issues created by the noncompliance, including requiring revocation of affected Certificates.

8.6 COMMUNICATION OF RESULTS

The results of each audit are reported to the DCPA and to any third-party entities which are entitled by law, regulation, or agreement to receive a copy of the audit results.

8.7 SELF-AUDITS

ACCC may perform regular internal audits against a randomly selected sample of at least three percent of its Certificates issued since the last internal audit. Self-audits on Certificates are performed in accordance with Guidelines adopted by the ACCC.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

Refer to ACCC CP Section 9.1.

9.2 CERTIFICATE ISSUANCE, MANAGEMENT AND RENEWAL FEES

Refer to ACCC CP Section 9.2.

9.3 CERTIFICATE ACCESS FEES AND OTHER SERVICES

Refer to ACCC CP Section 9.3.

9.4 REVOCATION OR STATUS INFORMATION ACCESS FEES

Refer to ACCC CP Section 9.4.

9.5 FINANCIAL RESPONSIBILITY

9.5.1 INSURANCE COVERAGE

Refer to ACCC CP Section 9.5.1.

9.6 CONFIDENTIALITY OF BUSINESS INFORMATION

Refer to ACCC CP Section 9.6.

9.7 PRIVACY OF PERSONAL INFORMATION

Refer to ACCC CP Section 9.7.

9.8 INTELLECTUAL PROPERTY RIGHTS

Refer to ACCC CP Section 9.8.

9.9 REPRESENTATION AND WARRANTIES

9.9.1 ACCC REPRESENTS THAT, TO ITS KNOWLEDGE:

Refer to ACCC CP Section 9.9.1.

9.9.2 SUBSCRIBER REPRESENTATION

Refer to ACCC CP Section 9.9.2.

9.9.3 RELYING PARTY REPRESENTATIONS

Refer to ACCC CP Section 9.9.3.

9.10 DISCLAIMER OF WARRANTY

Refer to ACCC CP Section 9.10.

9.11 LIMITATIONS OF LIABILITY

Refer to ACCC CP Section 9.11.

9.12 INDEMNITIES

9.12.1 INDEMNIFICATION BY RELYING PARTIES

Refer to ACCC CP Section 9.12.1.

9.12.2 INDEMNIFICATION BY SUBSCRIBERS

Refer to ACCC CP Section 9.12.2.

9.13 TERM AND TERMINATION

9.13.1 TERM

Refer to ACCC CP Section 9.13.1.

9.13.2 TERMINATION

Refer to ACCC CP Section 9.13.2.

9.13.3 EFFECT OF TERMINATION AND SURVIVAL

Refer to ACCC CP Section 9.13.3.

9.14 AMENDMENTS

9.14.1 PROCEDURE FOR AMENDMENT

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

If the ACCC PMA wishes to recommend amendments or corrections to this CPS 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 CPS 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 CPS 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 CPS from its date of publication:

9.14.3 CIRCUMSTANCES UNDER WHICH OID MUST BE CHANGED

Refer to the ACCC CP Section 9.14.3.

9.15 MISCELLANEOUS PROVISIONS

9.15.1 DISPUTE RESOLUTION PROVISIONS

Refer to the ACCC CP Section 9.15.1.

9.15.2 GOVERNING LAW

Refer to the ACCC CP Section 9.15.2.

9.15.3 Compliance with Applicable Law

Refer to the ACCC CP Section 9.15.3.

9.15.4 Assignment

Refer to the ACCC CP Section 9.15.4.

9.15.5 Severability

If any provision or portion of a provision of this CPS 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 CPS.

9.15.6 Waiver

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

9.15.7 Force Majeure

Refer to the ACCC CP Section 9.15.7.

10. CERTIFICATE, CRL AND OCSP FORMATS

Refer to the ACCC Certificate Policy document for details containing the formats for the various PKI objects such as Certificates, CRLs, and OCSP requests and responses.

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